UNIVERSIDADE FEDERAL DO RIO GRANDE - FURG

Faculdade de Direito - FaDir

Curso de Direito

Trabalho de Conclusão de Curso

Crimes Cibernéticos: A problemática de uma rede compartilhada e uma análise da efetividade normativa com foco na Lei Carolina Dieckmann e o Marco Civil da Internet

Matheus Costa Arocha[1]

Prof. Orientador: Salah Hassan Khaled Júnior

Rio Grande, 2022.

[1] Graduando no curso de Direito da Universidade Federal do Rio Grande, inscrito sob a matrícula nº 128982. E-mail: matheus.c.arocha@gmail.com

RESUMO

O presente trabalho busca abordar, com fulcro na legislação vigente, com foco nas Leis 12.737 de 2012, também conhecida como Lei Carolina Dieckmann – norma referente à tipificação dos crimes virtuais –, e 12.965 de 2014, nomeada como Marco Civil da Internet – norma referente à regulamentação do uso da Internet no Brasil –, além da tipificação, a análise dos Crimes acometidos no âmbito cibernético em solo brasileiro, visando o exame e a ocorrência destes delitos no âmbito criminal, além de abordar a efetividade destas normas vigentes dentre o ordenamento jurídico de nosso país, que possuem como objetivo punir e impedir a ocorrência de tais práticas criminógenas dentre a nossa sociedade. É válido estabelecer que este trabalho ainda visa estudar a ampla evolução da rede compartilhada mundialmente, conhecida como a Internet, correlacionada à questão referente ao âmbito penal e constitucional, principalmente ao se versar perante a dignidade da pessoa humana, tendo em vista que a prática de delitos envolvendo estes critérios evoluiu juntamente com os aspectos circundantes da evolução da própria sociedade e da acessibilidade aos dados pessoais acometida aos dias atuais através da própria Internet.

Palavras-chave: Internet; Direito; Lei Carolina Dieckmann; Marco Civil da Internet; Direito Penal; Criminologia; Crimes Virtuais; Ineficácia.

ABSTRACT

The present work seeks to address, with a focus on the actual legislation, focusing on Laws 12,737 of 2012, also known as the Carolina Dieckmann Law - norm referring to the typification of virtual crimes -, and 12,965 of 2014, named as Marco Civil da Internet - referring norm to the regulation of the use of the Internet in Brazil -, in addition to the classification, the analysis of Crimes committed in the cybernetic scope on Brazilian soil, aiming at the examination and the occurrence of these crimes in the criminal scope, in addition to addressing the effectiveness of the rules in force within the legal system of our country, which aim to punish and prevent the occurrence of such criminogenic practices within our society. It is valid to establish that this work still aims to study the wide evolution of the shared network worldwide, known as the Internet, correlated to the issue regarding the criminal and constitutional scope, especially when dealing with the dignity of the human person, considering that the practice of offenses involving these criteria evolved along with the surrounding aspects of the evolution of society itself and the accessibility to personal data affected today through the Internet itself.

Keywords: Internet; Right; Carolina Dieckmann Law; Civil Rights Framework for the Internet; Criminal Law; Criminology; Virtual Crimes; Ineffectiveness.

AGRADECIMENTOS

Primeiramente agradeço a Deus por ter me mantido na trilha correta durante todo o percurso da faculdade e do projeto de pesquisa, com saúde e forças para concluir mais uma etapa tão importante da minha vida.

Aos meus pais, Geovane e Rosane, por todo apoio, amor, educação e esforço remetidos à meu desenvolvimento pessoal ao longo de toda a vida, sempre acreditando em meu potencial, e me incentivando a ser uma pessoa melhor. Todas as minhas conquistas sempre serão dedicadas a ambos. Amo vocês.

À minha namorada, Sheron, que nunca deixou de estar ao meu lado nos momentos turbulentos dos últimos meses de desenvolvimento deste projeto, me apoiando e demonstrando que não existe desafio ou barreira que não possa ser ultrapassada com empenho, esforço e paixão. Você é uma inspiração. Amo-te.

À minha vó, Ivone, e meus dindos, João Luiz e Zilá, por serem os alicerces da minha criação na infância, me estabelecendo um carinho incondicional, sempre estando ao meu lado e me acolhendo quando preciso. Sempre serei grato a vocês.

Aos meus amigos e colegas da faculdade que fizeram parte dessa história, acompanhando o início, o processo e a conclusão de mais uma jornada na graduação. Nunca esquecerei todos os momentos ao lado de vocês.

Ainda, à Universidade Federal do Rio Grande (FURG), e o seu corpo docente, que sempre demonstrou comprometimento com a qualidade e a excelência do ensino.

Por fim, agradeço a meu orientador, Salah Hassan Khaled Jr., por aceitar me orientar no desenvolvimento desse trabalho fundamental à conclusão desta etapa, pela confiança depositada em minha proposta de projeto, por me guiar, indicando a direção correta do desenrolar dessa pesquisa, e por todas as contribuições durante todo o processo.

Dedico este trabalho a meus avós, Oscar e Maria, que estão assistindo esse processo e zelando por mim ao lado de Deus. Um dia estaremos juntos novamente. Amo vocês e até logo.

LISTA DE IMAGENS E FIGURAS

SUMÁRIO

1. INTRODUÇÃO

Vivenciamos um momento histórico evidenciado por grandes avanços tecnológicos que cada vez moldam a rotina e o desenvolvimento de nossa sociedade, e que tem, em seu holofote principal, a grande disseminação de uma rede compartilhada, e acessível à grande parte da população mundial, conhecida como a Internet. Contudo, desta não advém somente avanços e benefícios, mas também, malefícios evidentes e que cada vez mais se põem em pauta dentre os brasileiros e o ordenamento jurídico: Os Crimes Virtuais, ou Crimes Cibernéticos. Cabe-se a ressalva de citar o âmbito Constitucional, uma vez que a pauta da dignidade da pessoa humana está intrinsicamente ligada à ampla diversidade dos crimes virtuais, citando que o momento histórico atual acometido pela Internet se dá por um convívio social e econômico muito mais amplo do que os séculos anteriores, tendo em vista que a disseminação dos dados pessoais e privados estaria atrelada diretamente como uma "facilitadora" do ato criminógeno, sendo circundada principalmente de fatores como o direito à vida privada, à intimidade e privacidade, direitos relacionados à base do princípio da dignidade humana.

A partir disso, com o desenrolar dos anos, e com a incidência dos crimes acometidos em âmbito virtual, foram sancionadas normas que efetivamente possuíam em seu cerne, a punição direta desta nova esfera delituosa, ao que, nos dias atuais, conta-se com a presença de Leis em holofote no âmbito criminal, se dando estas na forma da Lei 12.737 de 2012, conhecida também como Lei Carolina Dieckmann, que buscaria interpretar, destrinchar e abordar os aspectos que circundam os crimes na Internet deste ínterim, e a Lei 12.965 de 2014, nomeada como Marco Civil da Internet, que estabelece os princípios, garantias e deveres do uso desta rede compartilhada em nosso país, protegendo os direitos fundamentais da liberdade, privacidade e livre desenvolvimento de personalidade da pessoa natural.

Contudo, é evidente que, por mais que haja regulamentação, ainda há a ausência de punibilidade, uma vez que há a dificuldade da aplicação das normas supracitadas tendo em vista que o universo cibernético ainda se demonstra muito "obscuro", citando a própria *Deep Web* – Termo usado para denotar uma classe de conteúdo na Internet que, por várias razões técnicas, não é indexada pelos mecanismos de pesquisa [2] –, a partir de que a busca de informações e provas efetivas de autoria muitas vezes acabam se perdendo na infinidade e complexidade de dados, tornando complicada a plena punição dos infratores que recorrem à esta esfera de crime,

[2] DEEP WEB – Definição – GTA UFRJ. Disponível em: https://www.gta.ufrj.br/ensino/eel878/redes1-2018-1/trabalhos-v1/deepweb/definicao.html. Acesso em: 2 de setembro de 2022.

e a partir disso, remontando à problemática: seria a população brasileira devidamente e efetivamente protegida pelos mecanismos normativos que a deveriam amparar no que concerne à plena égide e relevância da dignidade humana correlata ao ambiente virtual?

A metodologia utilizada no presente trabalho se deu efetivamente a partir de análise bibliográfica acometida a sites, revistas, doutrinas, notícias e, primordialmente, a própria legislação vigente.

2. A EVOLUÇÃO E DESENVOLVIMENTO DA INTERNET

2.1 A criação e o advento da Internet

Primordialmente, é valido estabelecer que a origem da Internet, segundo Araya, remonta-se a 1958, quando o Departamento de Defesa dos Estados Unidos cria a Advanced Research Projects Agency (Arpa) para favorecer a pesquisa no ambiente universitário e alcançar a superioridade tecnológica militar ante a União Soviética, que por causa de seu programa espacial tinha se tornado uma ameaça à segurança nacional norte-americana.[3]

Contudo, o que inicialmente surgiu apenas como um mecanismo de desenvolvimento científico em meados de Guerra Fria, evoluiu em curto período de tempo, a partir de que, segundo Merkle e Richardson, as aplicações comerciais da Internet começaram a acontecer nos anos oitenta com os primeiros provedores de serviço da Internet (ISP – International Service Providers) possibilitando ao usuário comum a conexão com a Rede Mundial de Computadores, de dentro de sua casa.[4]

Desde então, a Internet evoluiu de forma drástica, ao ponto de que, 64 anos após ao seu surgimento, se tornou o principal meio de comunicação, acessibilidade, informação e de relações sociais dentre o mundo inteiro. Quando começou a ser difundida, a base desta rede compartilhada ainda se dava de forma muito restrita, tendo em vista que a comunicação direta apenas circundava a utilização de e-mails, porém, a partir de investimento e do próprio

---

[3] ARAYA, Elizabeth Roxana Mass, e VIDOTTI, Silvana Aparecida Borsetti Gregório. **Criação, proteção e uso legal de informação em ambientes da World Wide Web [online].** São Paulo: Editora UNESP; São Paulo: Cultura Acadêmica, 2010, pág.14.

[4] Merkle, E. R., & Richardson, R. (2000). **Digital dating and virtual relating: Conceptualizing computer mediated romantic relationships.** *Family Relations,* 2000, pág. 188.

desenvolvimento científico atrelado a mesma, se tornou possível a comunicação simultânea com qualquer indivíduo espalhado pelo globo.

2.2 As Redes Sociais

No cerne deste desenvolvimento, principalmente tendo em vista as relações entre indivíduos, se remonta a presença das redes sociais. Segundo Vermelho, o termo "rede social" tornou-se sinônimo de tecnologia da informação e comunicação; seu uso transcorreu áreas e destruiu fronteiras sendo apropriado, hoje, por muitos atores sociais. Uma das apropriações mais intensas deu-se no campo da comunicação - mas não exclusivamente - com o uso de termos como rede social digital, mídia social, mídia digital, entre outros, para expressar o fenômeno em questão.[5]

A partir do surgimento das redes sociais, se possibilitou cada vez mais a acessibilidade de contato perante os indivíduos dentre uma mesma sociedade, uma vez que a distância física foi relativizada, tendo em vista que se comunicar com pessoas próximas, ou distantes, agora estaria apenas à distância efetiva de alguns “cliques”.

Entretanto, ao acometer que o advento e a evolução da Internet no âmbito mundial trouxe múltiplos benefícios para a relação direta dentre a sociedade, também se deu acompanhada de determinados malefícios para a própria, principalmente ao remontar a algo fundamental de cada indivíduo: a privacidade.

2.3 A privacidade no âmbito virtual

Como cita Carvalho, invasão de privacidade, calúnia e difamação em escala nacional ou mesmo mundial não envolvem mais apenas celebridades. Com a internet, pessoas anônimas também podem ser vítimas, com sérios prejuízos a sua reputação. [6]

---

[5] VERMELHO, Sônia Cristina. Et al. **Refletindo sobre as redes sociais digitais**. Educ. Soc. 35 (126), Março, 2014. Disponível em: https://doi.org/10.1590/S0101-73302014000100011. Acesso em 2 de setembro de 2022.

[6] CARVALHO, Patrícia Maurício. **Considerações sobre a privacidade na internet.** Interin, vol. 20, núm. 2, julio-diciembre, Universidade Tuiuti do Paraná Curitiba, Brasil, 2015. pág. 67.

Têm-se em vista que, os usuários da Internet e das redes sociais, não somente possuem acesso à uma comunicação simplificada, mas principalmente aos dados pessoais e individuais de qualquer outro indivíduo que utiliza o mesmo ambiente virtual deste, observando a partir disso que essa rede compartilhada possibilitou diretamente a criação de um novo campo de análise criminológica. Como estabelece Matheus de Araújo Alves, no Resumo de sua obra "*Crimes Digitais: análise da criminalidade digital sob a perspectiva do Direito Processual Penal e do Instituto da Prova*", os riscos e adversidades no chamado mundo real também se repetem no meio digital, uma vez que a internet é uma extensão da sociedade de risco atual. Com a possibilidade de acesso anônimo, o usuário é beneficiado com a sensação de privacidade, mas, por outro lado, tem-se a ideia de oportunidade para o cometimento dos crimes chamados digitais.[7]

Neste espectro, a privacidade individual, se põe como um dos fatores mais facilmente violáveis dentre o ambiente virtual, tendo em vista que, segundo Oliveira:

> "A amplitude cada vez maior dos canais informacionais e comunicacionais pela Internet fazem com que muitos setores da sociedade se estruturem e também levem os indivíduos a divulgarem ou compartilharem seus dados pessoais na rede, espontaneamente ou captados por empresas ou geradoras informáticas que se utilizam desses dados para fins pacíficos ou prejudiciais, para o Estado e para o usuário."[8]

Tal fato é remetido como um facilitador da captação direta de informações e dados pessoas dos indivíduos que frequentemente utilizam a Internet em seu cotidiano, podendo estes dados serem utilizados diretamente no âmbito criminógeno.

Tendo isto em vista, é relevante suscitar que a privacidade – intrínseca ao próprio fator da dignidade humana – na Internet ainda é constantemente violada a partir do momento de insegurança que esse âmbito estaria exposto, uma vez que ainda se há a crença de que o meio de convívio virtual seria diretamente ligado a uma impunidade estrutural, desde que o indivíduo haja no anonimato.

Tal fato é correlacionado diretamente à falta de segurança, tanto na proteção de sites e das redes de convívio via Internet, quanto efetivamente dos dados lançados pelas próprias

---

[7] ALVES, Matheus de Araújo. **Crimes Digitais:** análise da criminalidade digital sob a perspectiva do Direito Processual Penal e do Instituto da Prova. São Paulo: Editora Dialética, 2020. RESUMO.

[8] OLIVEIRA, Rafael Santos de. Et al. **O Direito à privacidade na internet: Desafios para a proteção da vida privada e o Direito ao Esquecimento**. Rev. Fac. Direito UFMG, Belo Horizonte, n. 70, 2017, pág. 573.

vítimas destes delitos, relatando um descuido no tratamento destas informações privadas por parte da população, citando, portanto que, conforme o Portal de E-Governo:

> "na maioria dos casos, os usuários têm uma parcela de culpa. Porém, não são estes que devem ser responsabilizados. A responsabilidade cabe aos mal-intencionados da rede. Porém, Cabe ao usuário, garantir sua própria segurança, seja usando softwares seguros ou ainda, sendo consciente ao passar suas informações por meio da internet, pois mesmo com uma boa política de controle dos hackers e demais usuários com más intenções, a rede não se tornará um lugar 100% seguro."[9]

Ademais, remete Barbosa que, cabe a todos os usuários, no desenrolar de suas atividades virtuais cotidianas, sejam quais forem, utilizar a internet e suas ferramentas conscientes de seus benefícios e facilidades, bem como de seus riscos, empregando sempre as formas de proteção da privacidade disponíveis.[10] Depreende-se a partir disso, portanto, uma relevância estabelecida perante o usuário desses ambientes e redes sociais, uma vez que o cuidado e atenção com os seus próprios dados individuais poderia providenciar uma maior segurança pessoal nestes ambientes cibernéticos.

3. DOS CRIMES CIBERNÉTICOS

3.1 O estudo do delito na Internet

A criminologia, segundo Menezes:

> "É um conjunto de conhecimentos que estudam o fenômeno e as causas da criminalidade, a personalidade do delinqüente e sua conduta delituosa e a maneira de ressocializá-lo. É a definição de Sutherland. Ciência que como todas as que abordam algum aspecto da criminalidade deve tratar do delito, do delinqüente e da pena. Segundo a Unesco, a criminologia se divide em geral (sociológica) e clínica."[11]

Com base nisto, busca-se o entendimento breve e a compreensão da base criminológica acometida aos delitos virtuais, uma vez que se depreende esta nova vertente do crime a partir

---

[9] FRANCO, Eduardo. **Notícia: Falta de segurança na internet causa prejuízos a usuários e provedores.** E-GOV, 2011. Disponível em: < https://egov.ufsc.br/portal/conteudo/not%C3%ADcia-falta-de-seguran%C3%A7a-na-internet-causa-preju%C3%ADzos-usu%C3%A1rios-e-provedores>. Acesso em 3 de setembro de 2022.

[10] BARBOSA, Adriana Silva et al. **Relações Humanas e Privacidade na Internet**: **implicações Bioéticas**. Barcelona: Revista Bioética y Derecho n. 30, 2014, pág. 121.

[11] MENEZES, Cristiano. **Noções de Criminologia.** Doraci. Disponível em: www.doraci.com.br/files/criminologia.pdf Acesso em: 10 de novembro de 2022.

do desenvolvimento tecnológico e social, buscando o melhor embasamento teórico na aplicação das Leis que virão a ser pauta posteriormente do presente estudo.

Em conformidade a isto, o professor e criminólogo indiano Karuppannan Jaishankar criou a Teoria de Transição de Espaços (*Space Transition Theory*), objetivando estudar e referir os fatores circundantes dos crimes virtuais, estabelecendo que "a realidade virtual e as comunicações mediadas por computador desafiam o discurso tradicional da criminologia, introduzindo novas formas de desvio, crime e controle social."[12] Portanto, observa-se claramente uma relação evolutiva conjunta desses dois fatores no mesmo âmbito: a Internet, e o crime, valendo-se da separação de duas esferas para exemplificar o molde do delito, sendo uma esfera física, referente aos crimes cometidos pessoalmente, tais como homicídios, roubos, etc., e uma esfera virtual, pautada pelos delitos que envolvam diretamente a tecnologia e a internet por si só.

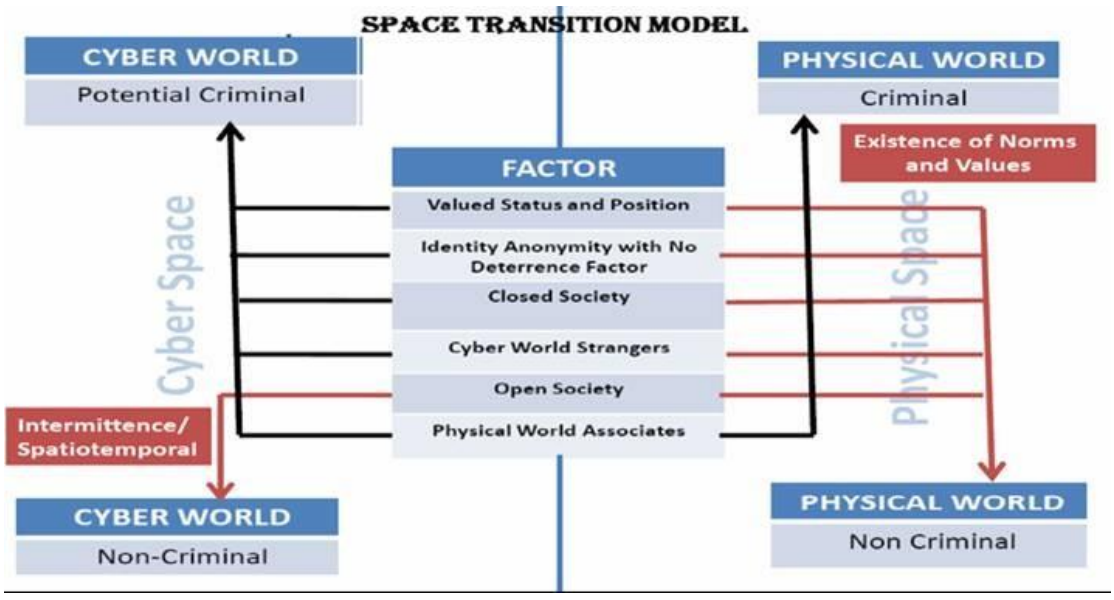
De acordo com os estudos realizados pelo professor Jaishankar, se estabelecem proposições relativas à sua Teoria de Transição de Espaços, ao passo que estas levariam em consideração os ambientes físicos e cibernéticos para a explicação dos fatores que pautariam o delito na Internet, sendo a análise destas, o foco central de seu trabalho. Cabem-se citar as suas hipóteses, ao passo que se estabelece que:

> "1 – As pessoas, com comportamento criminoso reprimido (no espaço físico) têm uma propensão a cometer crimes no ciberespaço, o que, de outra forma, não cometeriam no espaço físico, devido ao seu estatuto e posição.
>
> 2 – A flexibilidade da identidade, o anonimato dissociativo e a falta de fator de dissuasão no ciberespaço proporcionam aos infratores a opção de cometer crimes cibernéticos.
>
> 3 – É provável que o comportamento criminoso dos infratores no ciberespaço seja importado para o espaço físico que, no espaço físico, também pode ser exportado para o ciberespaço.
>
> 4 – Empreendimentos intermitentes de infratores no ciberespaço e a natureza espaço-temporal dinâmica do ciberespaço fornecem a chance de escapar.
>
> 5 – (a) É provável que estranhos se unam no ciberespaço para cometer crimes no espaço físico. (b) É provável que os associados do espaço físico se unam para cometer crimes no ciberespaço.
>
> 6 – As pessoas da sociedade fechada são mais propensas a cometer crimes no ciberespaço do que as pessoas da sociedade aberta.

[12] JAISHANKAR, Karuppannan. **Space Transition Theory of Cyber Crimes.** In Schmallager, F., & Pittaro, M. (Eds.), Crimes of the Internet (pp.283-301). Upper Saddle River, NJ: Prentice Hall, 2008. Disponível em: http://www.jaishankar.org/theory.html .

> 7 – O conflito de Normas e Valores do Espaço Físico com as Normas e Valores do ciberespaço pode levar a crimes cibernéticos."[13]

Com base nisto, pode-se depreender que o crime cibernético está atrelado, não somente à facilitação de um modus operandi delituoso, como à própria questão social, pautando, novamente, a evolução do crime em conjunto com a própria sociedade. Ressalvam-se os aspectos pertinentes à questão de identidade do indivíduo, esta que é pautada nos dois primeiros tópicos, e que estaria ligada principalmente à pauta do anonimato, tendo em vista que o individuo que possuísse uma inclinação ao cometimento de crimes e que zelasse pela sua imagem pública, tendo um comportamento criminoso reprimido, poderia recorrer à prática dos crimes cibernéticos, uma vez que a praticidade da ocultação do caráter individual seria evidente, e além disso, em conformidade com os tópicos 3 e 5, há diretamente uma ligação entre os espaços físicos e virtuais, uma vez que segundo a Teoria supracitada, há também a probabilidade da importação do caráter delituoso de um meio para o outro, sendo diretamente ligado ao fato do concurso de agentes na migração do cometimento de crimes, tanto da esfera física quanto da virtual. Neste sentido, cabe-se analisar o modelo proposto para interpretação desta teoria, tendo em vista que:



Fonte: Space Transition Theory, 2018. (Imagem 1)

[13] JAISHANKAR, Karuppannan. **Space Transition Theory of Cyber Crimes.** In Schmallager, F., & Pittaro, M. (Eds.), Crimes of the Internet (pp.283-301). Upper Saddle River, NJ: Prentice Hall, 2008. Disponível em: http://www.jaishankar.org/theory.html.

Neste sentido, cabe-se interpretar alguns fatores desse modelo, ao passo que:

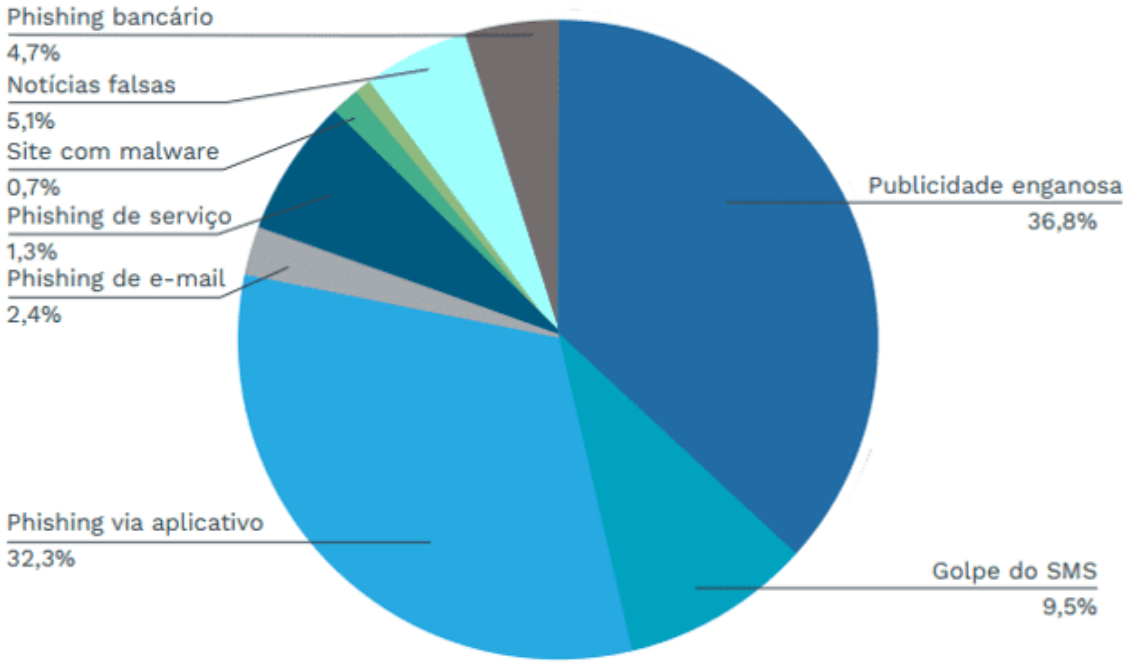
a) O Modelo de Transição de Espaços é dividido em duas partes: O espaço físico e o espaço virtual;
b) No centro dessa divisão são especificados os "Fatores", sendo estas as questões levadas em consideração na criação e desenvolvimento dessa teoria, para explicar a relação dos espaços virtuais e físicos e a transição criminal de uma esfera à outra. Estes fatores seriam: Status e Posição social valorizadas; Anonimato de Identidade sem valor de dissuasão; Sociedade Fechada; Desconhecidos no ambiente virtual; Sociedade Aberta; Associados do Mundo Físico.
c) Na questão do espaço físico, todos os fatores, com exceção dos Associados do Mundo Físico, são interligados a uma conduta não criminógena, tendo em vista a presença de normas e valores pautadas na sociedade, uma vez que, por exemplo, há a valorização de uma imagem individual, tendo em vista que no mundo físico, não se pode deixar de relevar fatores como o próprio anonimato e posição social na prática de crimes.
d) Na questão do espaço virtual, todavia, apenas com exceção da Sociedade Aberta, todos os fatores são visualizados como potencialmente criminógenos, uma vez que neste tópico, é evidente a facilidade e praticidade na ocultação do caráter individual, levando ao indivíduo que possua características criminógenas reprimidas a relativizar fatores como o seu status e posição social na prática de delitos cibernéticos, tendo em vista, principalmente, o fator referente ao anonimato.

3.2 Algumas tipificações dos Crimes Virtuais

Como base de elucidação e abordagem deste tópico, cabe-se analisar duas imagens estatísticas: A primeira publicada pelo DFNDR Lab, no ano de 2017 (Imagem 1), e abordada no artigo científico de Ricardo Leopoldo da Silva e Anderson Vieira[14], ao que versa perante a

[14] SILVA, Ricardo Leopoldo da. VIEIRA, Anderson. **Segurança cibernética: o cenário dos crimes virtuais no Brasil.** Revista Científica Multidisciplinar Núcleo do Conhecimento. Ano 06, Ed. 04, Vol. 07, pp. 134-149. Abril de 2021. Disponível em: https://www.nucleodoconhecimento.com.br/ciencia-da-computacao/crimes-virtuais Acesso em: 22 de setembro de 2022.

incidência dos crimes acometidos em âmbito virtual no solo brasileiro; e a segunda que se dá pelo levantamento realizado em 2018 pela associação SaferNet Brasil em parceria ao Ministério Público Federal, que contabilizou, no total, 133.732 (cento e trinta e três mil e setecentas e trinta e duas) queixas perante os delitos informáticos (Imagem 2) ao passo que:



Fonte: DFNDR Lab. (Imagem 2)

Fonte: SaferNet Brasil. (Imagem 3)

A partir da análise estatística de ambas figuras, cabe-se citar e estabelecer a espécie de alguns delitos informáticos, não somente os dispostos nestes dados, mas os que se mostram no âmbito da relevância ao desenvolvimento deste trabalho.

3.2.1 *Phishing*

É evidente que o *Phishing* se destaca no meio da estatística supracitada, sendo diretamente interligado ao raciocínio da problemática, uma vez que este se daria por uma

espécie de fraude, ao qual o criminoso possuiria como objetivo geral, a obtenção direta de dados pessoais e financeiros do afetado, tais como senhas de cartões de crédito e/ou débito, dados financeiros, entre outros, crime acometido diretamente no âmbito virtual.

O *Phishing* tem seu holofote em meio às outras espécies de crime virtuais no Brasil, devido a sua amplitude delituosa, ou seja, por poder sem abrangido de diferentes formas e métodos, ao passo que, conforme os dados supracitados, poderia se dar por aplicativos nos dispositivos móveis e computadores, através de e-mails, serviços e no âmbito bancário. Conforme o raciocínio de Morgenstern e Tissot[15]:

> "No início a palavra phishing era utilizada para definir a fraude que consistia no desvio de e-mail não solicitado pela vítima, que era estimulada a acessar sites fraudulentos. Os sites tinham a intenção de permitir o acesso às informações eletrônicas da pessoa que lhe acessava, como por exemplo, número da conta bancária, cartão de crédito, senhas, e-mails e outras informações pessoais ."

A partir disso, esse *Phishing* tem sua ocorrência pautada através de mensagens enviadas ao usuário em que se busca afetar, ao passo que o criminoso se passaria diretamente por uma instituição bancária, empresa conhecida, etc., objetivando atrair a atenção do remetente, induzindo o mesmo a inserir e compartilhar seus dados pessoais e financeiros ao criminoso. Devido à "facilidade" para cometer este crime, ele é ainda acometido como uma das espécies de delito na Internet mais conhecidas no meio da utilização desta ferramenta, principalmente no Brasil.

Cabe-se a ressalva que os Golpes de SMS, também remetidos à pesquisa supracitada, por mais que não estejam abordados na definição do *Phishing*, ainda assim, possuem objetivos similares, se não idênticos a esse tipo penal, uma vez que objetivam a obtenção dos dados pessoais e financeiros dos afetados.

---

[15] MORGENSTERN, Grasiele Giusti; TISSOT, Tânia Regina Gottardo. **Crimes Cibernéticos: Phishing – Privacidade Ameaçada.** Artigo Científico Realizado no Curso de Direito da FEMA. Santa Rosa, 2015.

3.2.2 Pornografia Infantil

Remetida pela Imagem 2 como o crime cibernético mais denunciado no país no ano de 2018, com mais de 60 mil casos registrados. Pauta-se pelo delito de adquirir, possuir ou armazenar qualquer tipo de material que possua qualquer forma ou registro de sexo ou pornografia envolvendo crianças e adolescentes. Sua tipificação se dá a partir de alteração no Estatuto da Criança e do Adolescente, com a inserção dos artigos 240 a 241-E, valendo-se a citação do artigo 241-B do mesmo dispositivo, ao passo que[16]:

> **Art. 241-B.** Adquirir, possuir ou armazenar, por qualquer meio, fotografia, vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:
>
> Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.
>
> § 1º A pena é diminuída de 1 (um) a 2/3 (dois terços) se de pequena quantidade o material a que se refere o caput deste artigo.
>
> § 2º Não há crime se a posse ou o armazenamento tem a finalidade de comunicar às autoridades competentes a ocorrência das condutas descritas nos arts. 240, 241, 241-A e 241-C desta Lei, quando a comunicação for feita por:
>
> I – agente público no exercício de suas funções;
>
> II – membro de entidade, legalmente constituída, que inclua, entre suas finalidades institucionais, o recebimento, o processamento e o encaminhamento de notícia dos crimes referidos neste parágrafo;
>
> III – representante legal e funcionários responsáveis de provedor de acesso ou serviço prestado por meio de rede de computadores, até o recebimento do material relativo à notícia feita à autoridade policial, ao Ministério Público ou ao Poder Judiciário.
>
> § 3º As pessoas referidas no § 2o deste artigo deverão manter sob sigilo o material ilícito referido.

Em suma, se daria como um grave delito disseminado na internet brasileira por muitos usuários mal intencionados. Cabe-se ainda suscitar que, em conformidade com os §§ 2º e 3º deste artigo, não se há acometido o delito se a posse destes registros objetivar a comunicação das autoridades competentes, quando esta for acometida pelos legitimados nos incisos I a III, pautando ainda que o material ilícito deve ser mantido sob sigilo.

---

[16] BRASIL. Lei no 8.069, de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 16 jul. 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L8069.htm#art266 . Acesso em: 28 de setembro de 2022.

3.2.3 Pirataria

Por mais que não esteja especificada devidamente nas duas imagens estatísticas, a pirataria ainda é um dos, se não o, delito informático mais conhecido e disseminado, não somente no Brasil, mas em âmbito mundial.

Tal delito se estabelece a partir da distribuição de propriedade intelectual, marcas e produtos, sem a devida autorização legal daqueles que são autores e proprietários de tal. Tal fato ainda tem sua problemática em correlação à questão dos direitos autorais, uma vez que, a partir da pirataria, o autor da propriedade que é pirateada não teria acesso ao pagamento desta espécie legal. Como estabelece Garcia[17]:

> "A pirataria de softwares já está regulamentada pela Lei 9.609 de 1998, que dispõe sobre a proteção da propriedade intelectual de programas e computadores. Sua tipificação consiste em distribuir ou vender programas de computador sem a autorização do proprietário e não pagando os seus direitos autorais."

No auxílio à repressão desta mazela, foi aprovada a Lei 10.965 de 2003, que alterou devidamente o artigo 184 e modificou o artigo 186, ambos do Código Penal, versando sobre a tipificação e pena de violação dos direitos de autoria, além do procedimento de ação pública correlata aos casos.

3.2.4 *Cyberbullying*

O *Cyberbullying*, assim como o *Phishing*, é uma expressão de origem inglesa, que manteve sua grafia na língua portuguesa, ao passo que, basicamente trata do mesmo ato acometido presencialmente na sociedade, o *Bullying*, porém, este se dando especificamente no âmbito virtual. Conforme a definição estabelecida pelo Fundo das Nações Unidas para a Infância (UNICEF), "podem ocorrer nas mídias sociais, plataformas de mensagens, plataformas de jogos e celulares. É o comportamento repetido, com intuito de assustar, enfurecer ou envergonhar aqueles que são vítimas."[18]

---

[17] GARCIA, Alline Tavares. **O Direito à Intimidade e a Frágil Privacidade da Era Digital: uma análise sobre os crimes cibernéticos e a eficácia da Lei Carolina Dieckmann.** São Luís, 2017. Disponível em: https://monografias.ufma.br/jspui/handle/123456789/1651 Acesso em: 15 de setembro de 2022. Pág. 36.

[18] UNICEF. **Cyberbullying: O que é e como pará-lo.** Disponível em: https://www.unicef.org/brazil/cyberbullying-o-que-eh-e-como-para-

Essa espécie de delito, em sua grande maioria das vezes se demonstra a partir do anonimato, em que o ataque circunda um indivíduo em específico. Esse ato criminoso tem sua gravidade pautada principalmente pelo âmbito psicológico da vítima, remetendo que, em muitos casos já evidenciados ao redor do mundo, o *Cyberbullying*, assim como o próprio *Bullying*, foram causas de suicídio e automutilações envolvendo diversas crianças e adolescentes.

4. O MARCO CIVIL DA INTERNET

4.1 O advento da Lei 12.965 de 2014

Como devidamente suscitado no tópico introdutório, a velocidade da disseminação da Internet, não somente no ambiente brasileiro, mas mundial, remontou a um uso massivo e indiscriminado de ferramenta entre a sociedade, ficando evidente a plena afetação do cotidiano de todos os seus usuários, seja pelo lado positivo ou negativo, tendo em vista que também facilitou muitas práticas criminógenas pelos indivíduos mal intencionados, sendo evidente que para muitas pessoas, tal rede compartilhada seria uma espécie de "território sem lei".

A partir disso, no ano de 2014, foi aprovada a Lei 12.965, renomada também como O Marco Civil da Internet. Tal norma, basicamente surgiu objetivando disciplinar determinadas lacunas que estariam em óbice na legislação vigente, estabelecendo princípios, garantias, deveres e direitos a todos os usuários que utilizam esta ferramenta, sendo considerada a partir disso, uma espécie de "Constituição da Internet".

Vale-se citar que tal norma já tramitava na Câmera dos Deputados para sua devida aprovação desde o ano de 2011, sendo que o Projeto desta Lei foi devidamente criado em 2009, pela Secretaria de Assuntos Legislativos do Ministério da Justiça (SAL/MJ) e a Escola de Direito da Fundação Getúlio Vargas do Rio de Janeiro (FGV-RJ), em consonância com diversos usuários e indivíduos que utilizavam da Internet em seu dia a dia, remetendo grande comoção e debate público para a melhor aferição e otimização desta norma, principalmente nas redes sociais.

Como estabelece Anjos (2014):

---

lo#:~:text=Cyberbullying%20%C3%A9%20o%20bullying%20realizado,envergonhar%20aqueles%20que%20s%C3%A3o%20v%C3%ADtimas.> Acesso em: 3 de outubro de 2022.

> "(...) a internet passa a ser considerada um meio de exercício da cidadania, onde os seus usuários terão a garantia de que a sua vida privada, o fluxo de comunicações e o sigilo das suas comunicações gozam de proteção legal. Além disso, prevê, também, a Constituição da Internet – como também é conhecido o Marco Civil – que é direito do internauta à manutenção da qualidade e da não suspensão do seu sinal de conexão, salvo, neste último, em casos de débitos com o provedor de conexão." [19]

Além disso, vale-se citar que, anteriormente à devida promulgação desta norma no âmbito legislativo, e tendo em vista todo o desenrolar e desenvolvimento drástico da Internet, foi criada uma nova vertente do Direito, que até então, seria desnecessária, tendo em vista que essa ferramenta surgiu e se ampliou a partir das últimas décadas, remetendo essa nova vertente como o Direito Digital. Para conceituar este mecanismo, é justo suscitar o que estabelecem Filho e Carnio, uma vez que:

> "O direito digital é uma disciplina jurídica, com características como a transversalidade e a imprescindível aproximação a campos científicos não jurídicos, que o torna uma espécie de equivalente atual do que outrora, ainda há pouco, foi o direito ambiental. Do que se trata, afinal, é da incidência de normas, jurídicas e outras, no chamado ciberespaço, tanto que em inglês é comumente designado *Cyberlaw*."[20]

A partir disto, e com a devida promulgação do Marco Civil da Internet, buscou-se regulamentar e normatizar as disposições já conhecidas pelo próprio Direito Digital, que já interpretava os quesitos remetentes a utilização desta ferramenta, uma vez que, anteriormente a aprovação desta lei, não se trataria destas disposições além de uma disciplina jurídica por si só, demonstrando a necessidade de imposição e peso que traz uma norma legal, como foi o devido caso concreto.

---

[19] ANJOS, Thales. **Os principais aspectos do Marco Civil da Internet – Lei 12.965**, oabmt.org.br, julho de 2014. Disponível em: https://www.oabmt.org.br/artigo/213/os . Acesso em: 25/05/2022.

[20] CARNIO, Henrique Garbellini; FILHO, Willis Santiago Guerra**. Metodologia Jurídica Político-Constitucional e o Marco Civil da Internet: Contribuição ao Direito Digital.** *In:* MASSO, Fabiano D.; ABRUSIO, Juliana; FILHO, Marco A. Marco Civil da Internet: Lei 12.965/2014. São Paulo: Revista dos Tribunais, 2014. Cap. I, p. 13.

4.2 Algumas prerrogativas do Marco Civil da Internet

Ao se versar diretamente sobre as devidas prerrogativas estabelecidas com o advento desta norma no âmbito legislativo brasileiro, é imperioso suscitar os aspectos remontados pela mesma.

Primordialmente, remete-se a relevância que foi dada no tratamento da censura ao tema, uma vez que uma das pautas e polêmicas envolvendo a criação e aplicação desta norma, em prática, estabeleceria aspectos similares ao que haveria sido superado na Ditadura Militar, tendo em vista que houve a supressão de todos mecanismos midiáticos e do Direito da liberdade de expressão ao período, ao que o paralelo disto traria grande censura e "privatização" do uso desta ferramenta em solo brasileiro. Para sanar devidamente estas preocupações, é necessário citar o que estabelecem o caput do artigo 2, e os artigos 3, I, 19 e 21 desta norma, ao passo que:

> "**Art. 2º** A disciplina do uso da internet no Brasil tem como fundamento o respeito à liberdade de expressão, bem como:
>
> [...]"
>
> "**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;"
>
> [...]
>
> "**Art. 19.** Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário."
>
> "**Art. 21.** O provedor de aplicações de internet que disponibilize conteúdo gerado por terceiros será responsabilizado subsidiariamente pela violação da intimidade decorrente da divulgação, sem autorização de seus participantes, de imagens, de vídeos ou de outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado quando, após o recebimento de notificação pelo participante ou seu representante legal, deixar de promover, de forma diligente, no âmbito e nos limites técnicos do seu serviço, a indisponibilização desse conteúdo." [21]

Em suma, ao passo que os três primeiros artigos citados reforçam e pautam consistentemente a plena valorização da liberdade de expressão, o artigo 19 e 21 suscitam a

[21] 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, 2014. Art. 7º.

responsabilização de provedor de aplicações de internet que viole diretamente esses quesitos, primando pelo princípio da proporcionalidade, sendo evidente a preocupação no tratamento dessas questões pelo legislador.

Incumbe-se comentar ainda a atenção aferida, também, a questão da responsabilidade civil a esses provedores, tendo em vista a configuração do delito diretamente atrelada a uma ofensa aos direitos personalíssimos e individuais de quaisquer indivíduos que utilizam desta ferramenta, citando aspectos como a imagem, a moral, a intimidade, vida privada e honra daqueles que fossem afetados por essa prática delituosa, restando isto em evidência pelo que suscitam os artigos 19 e 21 desta Lei. Contudo, vale ressaltar que, em conformidade com o artigo 18 desta norma, o provedor não pode ser responsabilizado civilmente pelos danos decorridos de conteúdo gerado pelos usuários que utilizam de acesso a seus dados. Como estabelece Filho, "dessa maneira, a responsabilidade primária é do usuário da internet e o provedor de conteúdo somente responde conjuntamente com o causador do dano quando descumprir ordem judicial para que tornasse indisponível o conteúdo ofensivo."[22]

Em outro teor, é válido tecer o artigo 7º desta lei, tendo em vista a relevância do mesmo, uma vez que trataria diretamente perante os direitos garantidos a todos os usuários da Internet, uma vez que:

> "**Art. 7º** O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
>
> I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
>
> II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;
>
> III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;
>
> IV - não suspensão da conexão à internet, salvo por débito diretamente decorrente de sua utilização;
>
> V - manutenção da qualidade contratada da conexão à internet;
>
> VI - informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros

[22] FILHO, Eduardo Tomasevicius. **Marco Civil da Internet: Uma lei sem conteúdo normativo.** Disponível em: < https://www.scielo.br/j/ea/a/n87YsBGnphdHHBSMpCK7zSN/?lang=pt> Acesso em: 20 de setembro de 2022.

> de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade;
>
> VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;
>
> VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:
>
> a) justifiquem sua coleta;
>
> b) não sejam vedadas pela legislação; e
>
> c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;
>
> IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;
>
> X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei e na que dispõe sobre a proteção de dados pessoais;
>
> XI - publicidade e clareza de eventuais políticas de uso dos provedores de conexão à internet e de aplicações de internet;
>
> XII - acessibilidade, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, nos termos da lei; e
>
> XIII - aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na internet."[23]

Na correlação direta ao que foi devidamente tratado até então, a priori, destacam-se os incisos I, II e III, respectivamente, a proteção e inviolabilidade da intimidade e da vida privada; a inviolabilidade e sigilo do fluxo de suas comunicações ao se utilizar da Internet; e a inviolabilidade e sigilo das comunicações privadas e individuais acometidas a este âmbito. Vale-se da valorização destes incisos, uma vez que tratam e remetem primordialmente o que é pautado por este trabalho, em específico, a suma relevância interligada desses aspectos à privacidade, que é pautada também pelo artigo 3º, II e III da mesma Lei, ao passo que:

> "**Art. 3º** A disciplina do uso da internet no Brasil tem os seguintes princípios:

[23] 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, 2014. Art. 7º.

[...]

II - proteção da privacidade;

III - proteção dos dados pessoais, na forma da lei;

[...]”

Contudo, há de se pressupor cautela no tratamento do caso concreto, uma vez que a liberdade de expressão e o direito à privacidade podem ser vistos de forma antagônica, necessitando a ampla primazia do princípio da proporcionalidade para análise e aferição de uma justa aplicação normativa. Como estabelece Queiroz, a liberdade de expressão deve ser entendida de forma relativa e não absoluta, aplicando-se o princípio da proporcionalidade a fim de resguardar tanto a aplicação daquele princípio, quanto o da proteção à privacidade.[24]

5. A LEI CAROLINA DIECKMANN

5.1 O caso da atriz Carolina Dieckmann

Antes de adentrar a devida proposição e promulgação da Lei que recebeu o nome da atriz, se há de estabelecer e contextualizar o ocorrido, que serviu como base na criação da mesma.

Em maio de 2011, hackers conseguiram invadir o computador pessoal da atriz Carolina Dieckmann[25], adquirindo acesso direto a um total de 36 fotos de cunho íntimo da mesma, além de outras imagens referentes ao seu filho, que na época possuía quatro anos de idade. Em decorrência disto, o criminoso utilizou-se de chantagem para com a vítima, cobrando da atriz um montante de R$ 10.000,00 (dez mil) reais para que todas as suas fotos não fossem divulgadas ao público. A atriz recusou. A partir disso, todas as imagens privadas da atriz, que foram obtidas com esse ato delituoso, foram devidamente liberadas e divulgadas no ambiente da internet, sendo replicadas e disseminadas por muitos internautas que obtiveram acesso às mesmas.

---

[24] QUEIROZ, Tayrine. **Marco Civil da Internet: um estudo da sua criação sob a influência dos Direitos Humanos e fundamentais, a neutralidade da rede e o interesse público versus privado.** Jusbrasil.com.br, 2015. Disponível em: < https://tayrine.jusbrasil.com.br/artigos/303303808/marco-civil-da-internet-um-estudo-da-sua-criacao-sob-a-influencia-dos-direitos-humanos-e-fundamentais-a-neutralidade-da-rede-e-o-interesse-publico-versus-privado> Acesso em: 20 de setembro de 2022.

[25] Atriz muito conhecida no âmbito nacional, principalmente pelos seus trabalhos discorridos ao longo dos anos, tanto em novelas, programas ou séries televisionadas pela rede Globo, emissora televisiva brasileira.

O acesso obtido ao computador da vítima, aparentemente se deu por um e-mail que foi enviado múltiplas vezes para Carolina, este que possuía um “malware” ou vírus, que possibilitava aos hackers acesso direto à todas as informações contidas naquele dispositivo.

Após o ocorrido, a atriz procurou as autoridades, dando início a uma investigação criminal perante o fato. Nestas investigações, a Polícia Civil do Rio de Janeiro, em consonância com a Delegacia de Repressão aos Crimes de Informática, chegaram aos suspeitos da autoria do fato concreto, constatando que, não somente estariam em posse de trinta e seis fotos, mas de mais de sessenta imagens obtidas através da prática deste crime.

No período, de forma evidente, tendo em vista a posterior promulgação da Lei Carolina Dieckmann, não havia dispositivo legal que efetivamente regulasse e punisse a prática do crime acometido pela invasão de dispositivo informático, o que se deu diretamente como um obstáculo jurídico análogo ao caso concreto vivenciado pela atriz. A partir disso, foi-se aberto um registro de ocorrência de extorsão qualificada pelo concurso de agentes, difamação e furto, aos indivíduos que efetivamente acometeram e efetivaram a prática delituosa, todavia, os mesmos não foram denunciados pelo crime de invasão, tendo em vista que este conceito não estaria devidamente normatizado.

5.2 A criação da Lei Carolina Dieckmann

Após a grande repercussão nacional tomada pelo caso envolvendo a atriz, se demonstrou necessária uma abordagem jurídica por parte do sistema legislativo brasileiro na aferição de normas que efetivamente cobrissem as lacunas no Código Penal Brasileiro, no que se refere aos crimes no ambiente virtual. Tem-se em vista que mesmo antes da promulgação da Lei 12.737 de 2012, já era considerada crime a invasão de dispositivo alheio e subtração de dados pessoais no âmbito cibernético, contudo, não havia uma norma específica para essa espécie de delito, respondendo o criminoso por adequação a outras normas vigentes ao período, estas também dispostas no Código Penal.

A partir disso, a apresentação do seu projeto de lei foi instaurada devidamente no dia 29 de novembro de 2011, sendo esta devidamente sancionada no dia 2 de dezembro de 2012, pela então presidente Dilma Rousseff. A norma foi então batizada com o nome da atriz Carolina Dieckmann, esta que participou diretamente no apoio e pressão midiática para sua aprovação,

sendo fundamental na agilidade de sua promulgação, e tendo em vista que o caso que alavancou definitivamente esta norma, decorreu do prejuízo e dos atos causados contra a mesma, conforme o caso suscitado anteriormente, valendo-se citar que, conforme Lira, "a pressão da opinião pública, nesse caso, de fato influenciou a célere reação do Congresso Nacional."[26] Vale-se da ressalva que esta norma também é conhecida como Lei dos Crimes Cibernéticos.

Em virtude disto, a Lei 12.737 de 2012 efetivamente buscou impactar o âmbito do Direito Penal na esfera virtual, tutelando diretamente o bem jurídico do direito ao sigilo pessoal e profissional – em paralelo à privacidade –, e a liberdade individual, tendo sua necessidade prevista em conformidade com o avanço tecnológico acometido principalmente no século XXI, decorrente da disseminação e acessibilidade em massa da internet, tipificando crimes relatados neste âmbito.

Tal segurança jurídica pautada e buscada por essa norma no âmbito cibernético se deu a partir do acréscimo dos artigos 154-A e 154-B ao Código Penal Brasileiro, além da alteração direta das normas previstas nos artigos 266 e 298 do mesmo dispositivo, valendo-se citar essas alterações, efetivamente na letra da Lei, a partir de que[27]:

> **Art. 154** - Revelar alguém, sem justa causa, segredo, de que tem ciência em razão de função, ministério, ofício ou profissão, e cuja revelação possa produzir dano a outrem:
> Pena - detenção, de três meses a um ano, ou multa de um conto a dez contos de réis.
>
> **Parágrafo único** - Somente se procede mediante representação.
>
> Invasão de dispositivo informático
>
> **Art. 154**-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita:
> Pena – reclusão, de 1 (um) a 4 (quatro) anos, 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 1/3 (um terço) a 2/3 (dois terços) se da invasão resulta prejuízo econômico.

[26] LIRA, Leide de Almeida. **Lei Carolina Dieckmann: (in)eficácia na proteção dos direitos fundamentais à intimidade e à vida privada em face da pena cominada aos delitos informáticos.** Conteúdo Jurídico. Brasília, Distrito Federal, 1 de julho de 2014. Disponível em: https://conteudojuridico.com.br/consulta/Artigos/40026/lei-carolina-dieckmann-in-eficacia-na-protecao-dos-direitos-fundamentais-a-intimidade-e-a-vida-privada-em-face-da-pena-cominada-aos-delitos-informaticos Acesso em: 23 de outubro de 2022.

[27] BRASIL. Decreto-Lei nº 2.848 de 7 de dezembro de 1940. Código Penal Brasileiro.

§ 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.
Pena – reclusão, de 2 (dois) a 5 (cinco) anos, e multa.

§ 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.

Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representacao, salvo se o crime e cometido contra a administracao pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municipios ou contra empresas concessionarias de servicos publicos."

"**Art. 266** - Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento:
Pena - detenção, de um a três anos, e multa.

§ 1 o Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.

§ 2 o Aplicam-se as penas em dobro se o crime e cometido por ocasiao de calamidade pública. "

"**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."

Compreende-se, a partir da interpretação do que foi devidamente alterado e adicionado ao Código Penal Brasileiro, que os artigos 154-A e 154-B tratariam diretamente perante o crime de Invasão de dispositivo informático; o artigo 266 a partir da Interrupção ou Perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública; e o artigo 298 pela Falsificação de documento particular.

5.2.1 Invasão de Dispositivo Informático

Tal delito é acometido diretamente pelas definições dos artigos 154-A e 154-B do Código Penal, primordialmente do primeiro citado, se estabelecendo a partir de que "invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita."[28] Ainda como é estabelecido pelo teor geral destes artigos, se trataria diretamente como um crime de menor potencial ofensivo, sendo prevista pena de três meses a um ano e multa, pautando ainda que sua ação penal se daria como pública, condicionada à representação, em conformidade com o artigo 154-B.

Pauta-se desta definição, portanto, como meio de proteção de liberdade individual, em que, nas palavras de Scarmanhã[29]:

> "Ao proteger a liberdade individual, na sua forma de inviolabilidade da intimidade e da vida privada, buscou-se preservar o direito de cada um ter seu universo pessoal protegido contra invasões e devastações. Por outro lado, ao tutelar a liberdade individual, nos aspectos do direito à intimidade e à privacidade, não se procurou proteger a rede mundial de computadores."

Ademais, no mesmo sentido, Bitencourt estabelece que o crime em tela tutela o direito à liberdade individual, dentro do contexto da "privacidade individual, pessoal ou profissional do ofendido", cuja "divulgação possa acarretar dano a outrem".[30]

O objeto desta aplicação, portanto, em conformidade com o que suscita novamente Scarmanhã seriam[31]:

> "[...] os dispositivos informáticos, interligados ou não à rede mundial de computadores, tais como desktop, notebook, netbook, smartphone, ipod, tablet, Iphone, ou seja, dispositivos que contenham capacidade de armazenar o fluxo das comunicações informáticas, seja de uso pessoal, corporativo, comercial ou industrial.

---

[28] BRASIL. Decreto-Lei nº 2.848 de 7 de dezembro de 1940. Código Penal Brasileiro. Art. 154-A.

[29] SCARMANHÃ, Bruna de Oliveira da Silva Guesso, et al. **Invasão de Dispositivo Informático: Aporte com a Legislação Espanhola.** Revista EM TEMPO, V.13, Marília, 2014, P. 240.

[30] BITENCOURT, Cézar Roberto. Invasão de dispositivo informático. Disponível em: < http://atualidadesdodireito.com.br/cezarbitencourt/2012/12/17/invasao-de-dispositivo-informatico/>. Acesso em: 22 ago 2013.

[31] SCARMANHÃ, Bruna de Oliveira da Silva Guesso, et al. **Invasão de Dispositivo Informático: Aporte com a Legislação Espanhola.** Revista EM TEMPO, V.13, Marília, 2014, P. 241.

> Exige-se, da mesma maneira, que seja alheio, portanto, pertencente a outrem e não ao próprio invasor."

Depreende-se portanto, que tutela-se e busca proteger diretamente a questão da inviolabilidade dos dados informáticos, interligada ao direito à privacidade, tão pautado e remetido no desenrolar deste trabalho, uma vez que esta correlacionado ao centro do delito acometido nos crimes virtuais. Tal invasão de dispositivo informático, como a citação anterior remete, deve se dar de forma alheia ao conhecimento do proprietário do dispositivo invadido, ao passo que, logicamente, o mesmo não deva possuir conhecimento perante as ações delituosas acometidas em sua propriedade, sendo que a definição de "invasão" se pauta diretamente na ausência de autorização por parte daquele indivíduo que possui efetivamente o bem.

Ademais, por se tratar de um crime comum, como é devidamente tipificado, o crime de invasão de dispositivo informático pode ter qualquer indivíduo como criminoso, na definição de seu sujeito ativo, sendo ainda pautável a participação de terceiros no desenrolar do delito, ao passo que há a possibilidade de aferição de concurso de agentes, valendo-se citar, inclusive, que foi o que ocorreu no caso concreto da atriz Carolina Dieckmann.

Por fim, a competência para julgar o referido delito é estabelecida em conformidade com o artigo 109, IV, da Constituição Federal Brasileira de 1988, tendo em vista que não há um dispositivo específico que faria referência a este quesito no ordenamento jurídico, valendo-se, portanto, de que estes crimes deveriam ser julgados diretamente no âmbito da Justiça Federal, uma vez que, [32]seria de competência dos juízes federais o julgamento de infrações penais praticadas em detrimento de bens, serviços ou interesses da União [...].

5.2.2 Interrupção ou Perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública

Em conformidade com o que estabelece o artigo 266 do Código Penal, como faz referência ao próprio tópico, trata-se da normatização da punição de conduta que vise interromper ou perturbar serviços telegráficos, telefônicos, informáticos ou de informações de utilidade pública, tendo em vista que o artigo ainda estabelece penas variáveis de um a três anos

[32] BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil.** Brasília, DF: Senado Federal: Centro Gráfico, 1988.

de reclusão e multa, penas estas que podem ser aplicadas em dobro em caso concreto que envolva calamidade pública, pautando, a partir deste raciocínio, que o bem juridicamente tutelado se daria especificamente pela incolumidade pública, sendo que o sujeito ativo, tal qual o crime de Invasão a Dispositivo Eletrônico, poderia se dar por qualquer indivíduo, enquanto o sujeito passivo se daria no âmbito da coletividade.

O objeto material desta norma circundaria os serviços telemáticos, ou seja, serviços que estejam interligados por tecnologias de informação, possibilitando a grande difusão de dados em grande escala, tendo como exemplos, ferramentas como o próprio WhatsApp, Skype, entre outros. Ainda, como estabelece Garcia, "trata-se de crime comum, doloso, comissivo, de perigo, instantâneo, monossubjetivo, plurissubsistente e não transeunte."[33]

5.2.3 Falsificação de documento particular

Espécie de delito devidamente tipificada no artigo 298 do Código Penal, a partir de que, configura-se crime, a falsificação, no todo ou em parte, de documento particular, ou a devida alteração de documento verdadeiro aferido a essa espécie, tendo em vista ainda, que equipara-se a documento particular, cartões de crédito ou débito, sendo estes os objetos materiais dessa espécie de crime, delito este remetido por reclusão de um a cinco anos, e multa. Para ocorrer a configuração deste tipo penal, se há a necessidade de inserção de dados falsos impregnados em tarja magnética do documento referido ao caso concreto, permitindo ao criminoso, assim, a possibilidade de acessar quaisquer dados bancários e financeiros da vítima.

Contudo, cabe remeter que apenas a falsificação destes documentos por si só, já se estabeleceria como crime. Como remete Albarello[34]:

> "[...] neste crime, é admitida sua forma tentada. No entanto, a consumação do crime se dá pela simples adulteração do documento, não sendo necessário seu uso, ou seja, basta que o sujeito ativo praticante do delito adultere ou falsifique o documento particular, já podemos falar em consumação do delito por ele praticado, mesmo que o sujeito nada pratique com tal documento."

---

[33] GARCIA, Alline Tavares. **O Direito à Intimidade e a Frágil Privacidade da Era Digital: uma análise sobre os crimes cibernéticos e a eficácia da Lei Carolina Dieckmann.** São Luís, 2017. Disponível em: https://monografias.ufma.br/jspui/handle/123456789/1651 Acesso em: 15 de setembro de 2022. Pág. 48.

[34] ALBARELLO, Caio. **Falsidade de Documento Particular: Elementos.** Jusbrasil, 2017. Disponível em: https://caioalbarello.jusbrasil.com.br/artigos/449046625/falsidade-de-documento-particular-elementos Acesso em: 20 de setembro de 2022.

Com a devida utilização deste documento com o fim de obter vantagem e verba de forma ilícita, na forma da lei, configurar-se-á, ainda, crime de furto qualificado pela fraude, ocorrendo a absorção do delito da falsificação.

6. DA ANÁLISE PERANTE A EFETIVIDADE NORMATIVA NA PUNIÇÃO DOS CASOS ENVOLVENDO CRIMES NA INTERNET NO ESPECTRO DO MARCO CIVIL DA INTERNET E DA LEI CAROLINA DIECKMANN

6.1 Uma crítica ao Marco Civil da Internet

Ao devidamente propor e aprovar o Marco Civil da Internet, buscou-se diretamente a plena regulação e definição de diretrizes que afastassem as práticas criminógenas do ambiente virtual. Como pontos positivos desde o advento desta norma, observa-se fatores tais como: a supracitada vedação da censura remetida ao meio, tendo em vista que haveria diretamente o receio de um controle estatal nas relações e publicações estabelecidas a partir dessa ferramenta, como ocorre em alguns lugares ao redor do mundo; a disciplina e cautela atrelada à aplicação de *cookies* na rede conforme o artigo 7º, VIII, tendo em vista que esta ainda é uma problemática muito debatida, uma vez que tratam-se de arquivos que são instalados nos dispositivos que possuem acesso a esse meio, através de sites que o usuário devidamente visita, funcionando com o intuito de "monitorar" as atividades do mesmo e, por exemplo, agir diretamente na recomendação de bens e produtos, com base no conteúdo consumido pelo indivíduo; e a como remete novamente Eduardo Tomasevicius Filho, "a regulamentação dos procedimentos judiciais específicos para obtenção dos registros de navegação para fins de instrução processual civil e penal." [35]

Contudo, observa-se também que a Lei 12.965 de 2014 não é isenta de críticas desde sua implementação. Primordialmente, é necessário suscitar a redundância de alguns aspectos que a circundam e de suas próprias normativas aferidas, principalmente na repetição de fatores e princípios que já são devidamente consagrados na própria Constituição Federal de 1988. Como estabelece o artigo 5º, XII deste dispositivo:

> "**Art. 5º** Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do

[35] FILHO, Eduardo Tomasevicius. **Marco Civil da Internet: Uma lei sem conteúdo normativo.** Disponível em: < https://www.scielo.br/j/ea/a/n87YsBGnphdHHBSMpCK7zSN/?lang=pt> Acesso em: 20 de setembro de 2022.

> direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
>
> [...]
>
> **XII** - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal.
>
> **[**...]"[36]

Ou seja, já se havia definido no âmbito legislativo efetivamente uma norma que pautasse pela inviolabilidade do fluxo de dados pessoais aferidos aos usuários que utilizassem os meios pré-definidos, sendo que a internet se conforma diretamente com a questão dos dados e comunicações telefônicas que são pautadas pela própria Constituição, contudo, o Marco Civil da Internet, na forma de seu artigo 7º, apenas reiterou o que já restava dito, não obstando a soma do peso normativo a este fato.

Neste mesmo interim, o é pautado pelo artigo 5º, IX, também da Constituição Federal, que:

> **"Art. 5º** 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:
>
> [...]
>
> **IX** - é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença.
>
> [...]"[37]

A partir deste artigo, interpreta-se a questão do direito da liberdade de expressão, sendo esta independente de quaisquer censuras ou licenças. Todavia, o Marco Civil da Internet, em seus artigos 3º, I, e em seu artigo 8º, praticamente repetem e suscitam o que já estaria devidamente normatizado na lei constitucional, tal seja o fato de que, para o pleno exercício do direito à internet, seria requisito para tal a plena e devida garantia do direito de privacidade e liberdade de expressão.

---

[36] BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil.** Brasília, DF: Senado Federal: Centro Gráfico, 1988.

[37] Idem.

Vale-se ressalvar que ainda são cabíveis outros exemplos de redundância e reafirmação de normas preestabelecidas por parte da Lei 12.965 de 2014, contudo, não se demonstram necessárias em sua plena abordagem, tendo em vista a interferência na objetividade da crítica.

Portanto, é evidente que em determinados quesitos, principalmente na digitação e concepção desta Lei, não se deu atenção o suficiente ao que já estaria disposto normativamente no ambiente jurídico, remetendo a aspectos que, por si só, não somam de forma alguma ao objetivo primário da proposição desta norma, qual seja de devidamente inovar e regulamentar as lacunas evidentes na legislação aos casos concretos envolvendo a rede compartilhada, além de, também, se tratarem em algumas definições apenas como normas vazias. Como estabelece, novamente, o doutrinador Filho[38]:

> "O texto do Marco Civil da Internet trouxe normas vazias de conteúdo. Por exemplo, o art.2º, IV, segundo o qual prevê como fundamento da disciplina do uso da internet a "abertura e a colaboração". Há que perguntar de que abertura se trata e que colaboração se pretende. O art.5º do Marco Civil da Internet, que apresenta definições para fins de interpretação, deixou de definir "provedor de conexão à Internet", "provedor de aplicações de Internet", "provedor responsável pela guarda dos registros" e "responsável pela transmissão, comutação e roteamento". Não se trata de definições de menor importância, já que são estes os principais destinatários dos deveres reflexos previstos na declaração dos direitos dos usuários da internet."

Ainda, a partir do desenrolar do raciocínio do doutrinador, em caso mais grave, cita-se que, não somente se pauta de crítica de concepção normativa ao Marco Civil da Internet, mas também no teor que a norma objetivou diretamente a defender, no caso, o direito e a prevalência dos direitos dos usuários afetados pela prática de crimes no ambiente virtual, uma vez que decorreu-se de um regresso a este quesito, no sentido da responsabilização subsidiária dos provedores. De forma anterior à promulgação desta Lei, cita-se o artigo 942 do Código Civil:

> "**Art. 942.** Os bens do responsável pela ofensa ou violação do direito de outrem ficam sujeitos à reparação do dano causado; e, se a ofensa tiver mais de um autor, todos responderão solidariamente pela reparação."[39]

---

[38] FILHO, Eduardo Tomasevicius. **Marco Civil da Internet: Uma lei sem conteúdo normativo.** Disponível em: < https://www.scielo.br/j/ea/a/n87YsBGnphdHHBSMpCK7zSN/?lang=pt> Acesso em: 20 de setembro de 2022.

[39] BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o **Código Civil**. Brasília, 2002.

Ou seja, relata-se que, antes do Marco Civil da Internet, aquele usuário que fosse lesado de alguma forma no ambiente virtual, poderia acionar, não apenas o indivíduo que devidamente causou o dano, mas também o provedor dos dados correlacionados, em forma de uma solidariedade *ex delito*, o que aferia, também, a esses provedores, um maior cuidado no tratamento da segurança da disseminação dos dados envolvidos em seu próprio ambiente. Contudo, com o advento da Lei 12.965 de 2014, tal responsabilização passou a ser subsidiária, ou seja, não há mais o dever de diligência estabelecido a esses provedores, o que, consequentemente, gera maior instabilidade e insegurança na manutenção dos dados estabelecidos nesses ambientes, gerando, também, maior incidência de crimes virtuais.

6.2 Uma crítica à Lei Carolina Dieckmann

Assim como o Marco Civil da Internet, o advento da Lei Carolina Dieckmann, também conhecida como Lei dos Crimes Cibernéticos, trouxe ao ordenamento jurídico e a sociedade, não somente aspectos positivos, mas também, negativos. Destaca-se que a importância da promulgação desta Lei, ao período, se deu de forma essencial, e até tardia, uma vez que em 2012 os mecanismos criminais envolvendo o âmbito cibernético já eram evidentes. Necessitou-se, portanto, um fato motivador, para esta pauta ser devidamente tratada e analisada com a devida agilidade, decorrente, portanto, dos prejuízos acometidos pela atriz Carolina Dieckmann.

Apesar de ser considerada limitada, a Lei se demonstrou de forma relevante ao combate dos crimes cibernéticos, ao passo que, segundo Almeida[40]:

> "Em uma análise, mesmo que superficial, do atual panorama sociológico global, demonstra a grande mudança de paradigmas sociais, e dessa maneira induz a conclusão de uma necessidade de se aprimorar a legislação penal informática, a fim de se evitar à impunidade dos chamados delitos informáticos próprios, ou seja, aqueles que só podem ser praticados por meio da internet."

A intenção da norma, neste raciocínio, é válida, uma vez que se apresenta a partir da tipificação dos Crimes Cibernéticos no âmbito legal brasileiro, tendo em vista que o âmbito

[40] ALMEIDA, Jéssica de Jesus et. al. **Crimes Cibernéticos**. Curso de Direito Universidade Tiradentes UNIT, janeiro de 2015. Disponível em: https://periodicos.set.edu.br/index.php/cadernohumanas/article/viewFile/2013/1217 . Acesso em: 25/05/2022. Pág. 218.

virtual não possuía, até então, uma norma vigente para a punição de crimes específicos, tais como o próprio delito da Invasão de Dispositivo Eletrônico, acometido ao caso da atriz que deu o nome à esta Lei.

Portanto, é evidente que a apreciação da Lei nº 12.737 de 2012 trouxe maior rigor penal e segurança jurídica ao ser relatada a estes casos, além de possibilitar aos magistrados, uma melhor fundamentação em sua sentença penal, uma vez que há dispositivo vigente que abarque normas até então "inexistentes", não necessitando de analogias a casos concretos para tal.

Contudo, como devidamente supracitado, esta Lei também possui defeitos. Por mais que cubra algumas espécies de tipos penais, tais como a Invasão de Dispositivo Eletrônico, a Interrupção ou Perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública e a Falsificação de Documento Particular, ainda assim, não faz jus à sua definição de "Lei de Crimes Cibernéticos". Neste raciocínio, também Almeida estabelece que[41]:

> "Essa legislação elencou as condutas consideradas penalmente típicas, não reconhecendo, contudo, a existência de diversas condutas delitivas praticadas no mundo virtual. Destarte, o legislador ao não considerar dadas condutas como sendo, propriamente, crimes cibernéticos, estas passaram, todavia, a serem conhecidas doutrinariamente como "crimes virtuais impróprios"".

Ou seja, crimes tais como os supracitados no tópico 2, como por exemplo, o *Phishing*, a Pirataria e a Pornografia Infantil, dentre outros, não estariam devidamente qualificados nesta norma, ao passo que, como estabelece a doutrinadora, passam a ser considerados "crimes virtuais impróprios". A diferença dos crimes virtuais próprios para os impróprios, não se dá apenas na sua abrangência pela norma, mas pela sua definição por si só, ao passo que os crimes virtuais próprios tratariam de delitos que ocorressem apenas no âmbito virtual, e que tivesse efeitos decorrentes e estabelecidos através da própria ferramenta, por exemplo, a própria Invasão de Dispositivo Eletrônico. Já os crimes impróprios, nas palavras de Lima[42]:

---

[41] ALMEIDA, Jéssica de Jesus et. al. **Crimes Cibernéticos**. Curso de Direito Universidade Tiradentes UNIT, janeiro de 2015. Disponível em: https://periodicos.set.edu.br/index.php/cadernohumanas/article/viewFile/2013/1217 . Acesso em: 25/05/2022. Pág. 215.

[42] LIMA, Leonardo Barcellos. **Crimes Virtuais: Próprios e Impróprios.** SLAPLAW, 2021. Disponível em: https://slap.law/os-crimes-virtuais-proprios-e-improprios/?utm_source=rss&utm_medium=rss&utm_campaign=os-crimes-virtuais-proprios-e-improprios Acesso em: 2 de outubro de 2022.

> "São aqueles que utilizam a internet como um meio, e os seus efeitos repercutem na vida real. O computador é um mero intermediário destas ações. Os principais crimes impróprios são a falsificação de documentos, crimes contra a honra, ameaças, e o recentemente sancionado, crime de perseguição ou stalking."

A partir disso, vale-se depreender que esta norma não abrange diretamente todas as tipificações de tipos penais, mas somente aquelas incluindo crimes virtuais próprios. Contudo, mesmo na tipificação apenas destas normas próprias, a Lei Carolina Dieckmann peca no quesito interpretativo. Como estabelece Lira:

> "Em linhas gerais foram identificadas mais lacunas que avanços, pois os textos ambíguos e lacunosos trouxeram divergências entre juristas e doutrinadores, como por exemplo sobre o termo "invasão": se o dispositivo estiver completamente desprotegido, não há que se falar em punição pelo crime de invasão, uma vez que não está presente a violação indevida do mecanismo de segurança."

Ou seja, a exigência da Lei pautada pela "violação indevida de mecanismo de segurança" se demonstra mais como um prejuízo do que como um avanço, ao passo que, se o dispositivo estiver ligado, sem qualquer tipo de senha que impeça o criminoso de o acessar, não haverá a configuração de delito abarcado ao caso, sendo esta, uma das interpretações inócuas desta norma. Ainda, como estabelece Oliveira[43]:

> "Somente haverá crime em caso de invasão de dispositivo (computador, periféricos, etc). Se o autor limitar-se a invadir um perfil de rede social, um e-mail, banco de dados ou um álbum de fotografias, sem passar pelo computador da vítima, não incidirá no crime em análise. Cuida-se de um erro crasso do legislador."

É imprescindível acometer que a falha na concepção interpretativa desta norma, se estabelece como um óbice de extrema relevância ao que se refere à plena punição daqueles que são acusados por cometerem crimes no âmbito virtual. Ademais, é imprescindível acometer uma das, se não a principal falha da Lei Carolina Dieckmann, diretamente atrelada à resposta

[43] OLIVEIRA, William César Pinto de. **Lei Carolina Dieckmann**. Revista Jus Navigandi, ISSN 1518-4862, Teresina, ano 18, n. 3506, fevereiro de 2013. Disponível em: https://jus.com.br/artigos/23655/lei-carolina-dieckmann. Acesso em: 25/05/2022.

que se busca efetivamente conhecer através do estudo deste trabalho: As suas penas. Nas palavras de Lira[44]:

> "O maior questionamento se deu em virtude das penas atribuídas aos delitos informáticos para a proteção da intimidade, pois foram consideradas insignificantes - uma verdadeira ciranda despenalizante - pois: a pena máxima cominada em 1 (um) ano, arrasta o crime para o rito sumaríssimo dos Juizados Especiais, onde se estimulará a conciliação, a composição civil dos danos e a transação penal, além disso, se o réu for primário, penas inferiores a quatro anos podem ser convertidas, por exemplo, à prestação de serviços à comunidade."

Ou seja, se depreende que, para o indivíduo que comete efetivamente crimes no ambiente virtual, a possibilidade do mesmo ser preso, é ínfima, se não inexistente. As penas acometidas pela Lei Carolina Dieckmann, por se tratarem de penas "leves", prescrevem de forma ligeira, o que, consequentemente, inviabiliza uma punição decente aos casos concreto, uma vez que necessita de uma rápida apuração.

Pode-se entender que, ao depender do caso concreto, o delito pode "compensar", principalmente pelo fato de que as penas são ínfimas em comparação com a vantagem que possa ser aferida pelo delito cometido. Como estabelece Garcia[45], "esse é, inclusive, um dos maiores entraves para o sucesso da lei, visto que o Brasil ainda carece de profissionais treinados para lidar com esses delitos, apesar de já possuir alguns centros de excelência em perícia digital." É de suma relevância suscitar que, para a norma garantir minimamente sua função de defesa social abarcada aos crimes virtuais, é necessário que as suas penas possuam força dissuasória, ou seja, que possam afastar o criminoso de cometer o delito, o que, evidentemente, não é o caso concreto. Ainda nas palavras de Oliveira[46]:

---

[44] LIRA, Leide de Almeida. **Lei Carolina Dieckmann: (in)eficácia na proteção dos direitos fundamentais à intimidade e à vida privada em face da pena cominada aos delitos informáticos.** Conteúdo Jurídico. Brasília, Distrito Federal, 1 de julho de 2014. Disponível em: https://conteudojuridico.com.br/consulta/Artigos/40026/lei-carolina-dieckmann-in-eficacia-na-protecao-dos-direitos-fundamentais-a-intimidade-e-a-vida-privada-em-face-da-pena-cominada-aos-delitos-informaticos Acesso em: 23 de outubro de 2022. Pág. 111.

[45] GARCIA, Alline Tavares. **O Direito à Intimidade e a Frágil Privacidade da Era Digital: uma análise sobre os crimes cibernéticos e a eficácia da Lei Carolina Dieckmann.** São Luís, 2017. Disponível em: https://monografias.ufma.br/jspui/handle/123456789/1651 Acesso em: 15 de setembro de 2022. Pág. 53.

[46] OLIVEIRA, William César Pinto de. **Lei Carolina Dieckmann**. Revista Jus Navigandi, ISSN 1518-4862, Teresina, ano 18, n. 3506, fevereiro de 2013. Disponível em: https://jus.com.br/artigos/23655/lei-carolina-dieckmann. Acesso em: 25/05/2022.

> “Por mais estardalhaço que a imprensa faça, não será cabível a decretação de prisão temporária ou de prisão preventiva. Aliás, sequer a prisão em flagrante será viável, já que o autor dos fatos, assumindo o compromisso de comparecer em juízo, acabará sendo liberado. A prática demonstrará que a nova lei foi mal elaborada.”

Percebe-se portanto, uma má elaboração do legislador ao escrever esta Lei, uma vez que a norma apresenta-se como uma facilitadora aos crimes cibernéticos ao qual a própria objetivaria combater, principalmente no quesito da impunidade.

7. CONSIDERAÇÕES FINAIS

Primordialmente, cabe-se acometer que o foco deste trabalho circundou, além da observância das normas penais vigentes em relação ao âmbito cibernético, especialmente a Lei Carolina Dieckmann, e o Marco Civil da Internet, os dois principais dispositivos abarcados a especificação, tipificação e punição dos delitos que se estabeleceriam na Internet, e sua efetividade e peso normativo no desempenho efetivo de suas funções de reprimir tais crimes, analisando seus pontos positivos e negativos acometidos com as suas promulgações, também a estudar e buscar entender, brevemente, o delito cometido no âmbito virtual, com fulcro principalmente na Teoria de Transição de Espaços do professor e criminólogo indiano Karuppannan Jaishankar.

Neste sentido, é fundamental estabelecer que o crime, assim como a sociedade, continua a evoluir progressivamente, primordialmente, com foco no presente trabalho, a partir da presença da Internet. Como citado no estudo, é válido suscitar que há uma diversidade de fatores facilitadores que estão diretamente atrelados à prática criminógena, principalmente ao se referir aos crimes virtuais. Como supracitado, o estudo do professor Jaishankar pauta que há diretamente uma ligação dos fatores que interligam o crime no espaço físico e no espaço virtual, estabelecendo uma espécie de “transição” do crime entre ambas espécies, ao passo que, por exemplo, indivíduos com tendências criminógenas, e que possuiriam uma valorização de seus fatores individuais, estariam mais propensos ao cometimento de crimes no espaço virtual, uma vez que nesta esfera há a presença direta de um valor fundamental relativo à praticidade do crime, que seria o anonimato, o que não excluiria a importação do caráter delituoso ao meio físico, e vice-versa. É evidente que no espaço físico, há uma delimitação do caráter delituoso tendo em vista as normas e valores pautados na sociedade, o que não se decorre da mesma forma no ambiente virtual, tendo em vista que os fatores estabelecidos para a valoração e praticidade do crime se determinam como potencialmente criminógenos.

No quesito do Direito, é imprescindível citar a primazia e participação dos direitos da privacidade, intimidade, honra, imagem e vida privada correlacionados ao tema em específico, uma vez que estes se impõem na discussão central e primordial acometida desde o desenrolar dos crimes acometidos nesta ferramenta, sendo garantias invioláveis à todos os brasileiros, em conformidade principalmente ao que remete a própria Constituição Federal de 1988.

Incumbiu-se de estudar algumas espécies relevantes de crimes cibernéticos, e a evolução histórica do delito neste âmbito, tendo em vista que se estabeleceu nas últimas seis décadas com a criação e disseminação da Internet em âmbito global. Estudou-se, a partir disso, a plena fragilidade atribuída a esta ferramenta, tendo em vista que essa disseminação e evolução tecnológica acarretou em um desenvolvimento acelerado e difundido rapidamente entre a sociedade, ao passo que, ao mesmo tempo que possui seus benefícios, tal qual o exemplo da acessibilidade à informação, veio acompanhada também de malefícios evidenciados pelo tema do trabalho, ou seja, os crimes cometidos virtualmente.

Até 2012, por mais que já estivessem dispostos como Projetos de Lei, não havia uma regulamentação específica que abarcasse a tipificação dos delitos virtuais, demonstrando uma imensa lacuna para a aplicação normativa dos casos concretos. Contudo, nesse mesmo ano, surgiu a Lei Carolina Dieckmann, que foi promulgada rapidamente, após a plena aferição midiática envolvendo o caso da atriz que possui o mesmo nome dessa norma, que teve seu dispositivo hackeado por infratores que obtiveram acesso direto a imagens de cunho pessoal e privado da atriz, além de fotos de seu filho, ao que, em sequência, buscaram a obtenção de lucro indevido, chantageando a atriz ao pagamento de dez mil reais para a não publicação destas fotos na Internet. Como a atriz não acatou o pedido dos criminosos, as imagens foram postadas, e disseminadas rapidamente entre a sociedade brasileira, tendo em vista que a mesma seria conhecida e renomada entre o povo, através de seus trabalhos estabelecidos na rede Globo, principal veículo de entretenimento e comunicação do país. Tal lei surgiu objetivando suprir as lacunas normativas aferidas a esses crimes, principalmente a invasão de dispositivo eletrônico.

Já no ano de 2014, foi promulgada a Lei Lei 12.965, renomada também como O Marco Civil da Internet. Tal norma, basicamente surgiu objetivando disciplinar determinadas lacunas que estariam em óbice na legislação vigente, estabelecendo princípios, garantias, deveres e direitos a todos os usuários que utilizam esta ferramenta, sendo considerada a partir disso, uma espécie de “Constituição da Internet”. A partir disto, e com a devida promulgação do Marco Civil da Internet, buscou-se regulamentar e normatizar as disposições já conhecidas pelo próprio Direito Digital, que já interpretava os quesitos remetentes a utilização desta ferramenta,

uma vez que, anteriormente a aprovação desta Lei, não se trataria destas disposições além de uma disciplina jurídica por si só, demonstrando a necessidade de imposição e peso que traz uma norma legal, como foi o devido caso concreto.

Contudo, por mais que ambas normas são tratadas como um avanço normativo e possuíssem em seu cerne a plena regulamentação dos crimes virtuais, pautando pela defesa dos direitos citados anteriormente, principalmente o direito à privacidade, ambas se demonstraram inócuas e ineficientes em suas atribuições. O Marco Civil da Internet, como comentado anteriormente, também conhecido como a Constituição da Internet, se demonstrou uma norma vazia, tendo em vista que, em muitos de seus artigos, demonstrou uma repetição e reiteração contínua do que já era abarcado legalmente, tal como a questão referente à censura e a inviolabilidade de dados pessoais, como estabeleceu a própria Constituição Federal de 1988. Não somente é redundante em muitos aspectos, mas falha no principal objetivo de sua concepção: a defesa dos indivíduos afetados por esses delitos. Isso se mostra evidente a partir da responsabilização subsidiária estabelecida aos provedores de sites na internet, não havendo o dever de diligência estabelecido a estas figuras, ao passo que gera maior instabilidade e insegurança na manutenção dos dados virtuais, e incidência desses crimes.

Já a Lei Carolina Dieckmann, tanto quanto o Marco Civil da Internet, não consegue cumprir devidamente com suas diligências e objetivos primordiais em sua concepção, se tratando de uma lei ambígua, e com muita margem interpretativa, além de não abranger especificamente a tipificação de todos os tipos penais envolvidos no ambiente virtual, e, principalmente, não possuir a capacidade punitiva que se dispõe efetivamente. A ambiguidade se demonstra principalmente pelo termo da “invasão” de dispositivo eletrônico, ao passo que o computador, celular, etc., que for devidamente invadido, não poderia estar operando sem nenhuma forma de proteção, tal como a presença de senhas ou antivírus, ao passo que, se a “invasão” se qualificar desta forma, não haverá a configuração de delito ao caso concreto, tendo em vista a necessidade da existência de violação indevida de mecanismo de segurança, remontando grande controvérsia envolvendo a sua própria concepção normativa.

Ainda, cita-se o pleno óbice relatado às punições pautadas por esta norma, uma vez que a pena máxima estabelecida ao mesmos seria cominada em um ano, arrastando o crime para o rito sumaríssimo dos Juizados Especiais, onde se estimularia, por si só, a conciliação, a composição civil dos danos e a transação penal, além disso, se o réu for primário, penas inferiores a quatro anos podem ser convertidas, por exemplo, à prestação de serviços à comunidade e pagamento de cestas básicas. Demonstra-se portanto, que as penas referidas e

estabelecidas pela Lei Carolina Dieckmann, seriam no mínimo insuficientes, além de que, por se tratarem de leis frágeis e leves, prescrevem de forma muito rápida na aferição dos casos concretos, necessitando ligeira aferição e análise para serem devidamente punidas por um magistrado, o que muitas vezes não acontece, devido a necessidade de investigação correlata a essa espécie de delito, que nem sempre é capaz de ser realizada no devido prazo curto.

Em suma, é evidente que, tanto o Marco Civil da Internet, quanto a Lei Carolina Dieckmann, necessitam de reformas em suas aferições, uma vez que não cumprem devidamente o que pautam e buscam defender: os interesses dos indivíduos afetados por terceiros que recorrem a esta espécie de crime. Ambas leis se demonstram ineficientes, ambíguas, de vastas interpretações, e mais facilitam e incentivam a presença dos crimes cibernéticos no solo brasileiro do que efetivamente os punem e os regulam. Para não desvalorizar e diminuir as garantias fundamentais pautadas principalmente na Constituição Federal, cita-se a necessidade de uma nova abordagem e configuração a estes dispositivos, para então, acometer a uma plena defesa dos direitos individuais da sociedade brasileira, principalmente os direitos a intimidade e privacidade.

REFERÊNCIAS BIBLIOGRÁFICAS

ALBARELLO, Caio. **Falsidade de Documento Particular: Elementos.** Jusbrasil, 2017. Disponível em: https://caioalbarello.jusbrasil.com.br/artigos/449046625/falsidade-de-documento-particular-elementos Acesso em: 20 de setembro de 2022.

ALMEIDA, Jéssica de Jesus et. al. **Crimes Cibernéticos**. Curso de Direito Universidade Tiradentes UNIT, janeiro de 2015. Disponível em: https://periodicos.set.edu.br/index.php/cadernohumanas/article/viewFile/2013/1217 . Acesso em: 25/05/2022.

ALVES, Matheus de Araújo. **Crimes Digitais:** análise da criminalidade digital sob a perspectiva do Direito Processual Penal e do Instituto da Prova. São Paulo: Editora Dialética, 2020.

ANJOS, Thales. **Os principais aspectos do Marco Civil da Internet – Lei 12.965**, oabmt.org.br, julho de 2014. Disponível em: https://www.oabmt.org.br/artigo/213/os . Acesso em: 25/05/2022.

ARAYA, Elizabeth Roxana Mass, e VIDOTTI, Silvana Aparecida Borsetti Gregório. **Criação, proteção e uso legal de informação em ambientes da World Wide Web [online].** São Paulo: Editora UNESP; São Paulo: Cultura Acadêmica, p. 144, 2010.

BARBOSA, Adriana Silva et al. **Relações Humanas e Privacidade na Internet**: **implicações Bioéticas**. Barcelona: Revista Bioética y Derecho n. 30, p. 109- 124, 2014.

BITENCOURT, Cézar Roberto. **Invasão de dispositivo informático.** Disponível em: < http://atualidadesdodi-reito.com.br/cezarbitencourt/2012/12/17/invasao-de-dispositivo-informatico/>. Acesso em: 22 de setembro de 2022.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil.** Brasília, DF: Senado Federal: Centro Gráfico, 1988.

BRASIL. Lei no 8.069, de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 16 jul. 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L8069.htm#art266 . Acesso em: 28 de setembro de 2022.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o **Código Civil**. Brasília, 2002.

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, 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, 2014.

BRASIL. Decreto-Lei nº 2.848 de 7 de dezembro de 1940. Código Penal Brasileiro.

CARNIO, Henrique Garbellini; FILHO, Willis Santiago Guerra**. Metodologia Jurídica Político-Constitucional e o Marco Civil da Internet: Contribuição ao Direito Digital.** *In:* MASSO, Fabiano D.; ABRUSIO, Juliana; FILHO, Marco A. Marco Civil da Internet: Lei 12.965/2014. São Paulo: Revista dos Tribunais, 2014. Cap. I, p. 13-26.

CARVALHO, Patrícia Maurício. **Considerações sobre a privacidade na internet.** Interin, vol. 20, núm. 2, julio-diciembre, Universidade Tuiuti do Paraná, Curitiba, pág. 66-82, 2015.

DEEP WEB – Definição – GTA UFRJ. Disponível em: https://www.gta.ufrj.br/ensino/eel878/redes1-2018-1/trabalhos-v1/deepweb/definicao.html. Acesso em: 2 de setembro de 2022.

FILHO, Eduardo Tomasevicius. **Marco Civil da Internet: Uma lei sem conteúdo normativo.** Disponível em: < https://www.scielo.br/j/ea/a/n87YsBGnphdHHBSMpCK7zSN/?lang=pt> Acesso em: 20 de setembro de 2022.

FRANCO, Eduardo. **Notícia: Falta de segurança na internet causa prejuízos a usuários e provedores.** E-GOV, 2011. Disponível em: < https://egov.ufsc.br/portal/conteudo/not%C3%ADcia-falta-de-seguran%C3%A7a-na-internet-causa-preju%C3%ADzos-usu%C3%A1rios-e-provedores>. Acesso em 3 de setembro de 2022.

GARCIA, Alline Tavares. **O Direito à Intimidade e a Frágil Privacidade da Era Digital: uma análise sobre os crimes cibernéticos e a eficácia da Lei Carolina Dieckmann.** São Luís, 2017. Disponível em: https://monografias.ufma.br/jspui/handle/123456789/1651 Acesso em: 15 de setembro de 2022.

JAISHANKAR, Karuppannan. **Space Transition Theory of Cyber Crimes.** In Schmallager, F., & Pittaro, M. (Eds.), Crimes of the Internet (pp.283-301). Upper Saddle River, NJ: Prentice Hall, 2008. Disponível em: http://www.jaishankar.org/theory.html . Acesso em: 25/05/2022.

LIMA, Leonardo Barcellos. **Crimes Virtuais: Próprios e Impróprios.** SLAPLAW, 2021. Disponível em: https://slap.law/os-crimes-virtuais-proprios-e-improprios/?utm_source=rss&utm_medium=rss&utm_campaign=os-crimes-virtuais-proprios-e-improprios Acesso em: 2 de outubro de 2022.

LIRA, Leide de Almeida. **Lei Carolina Dieckmann: (in)eficácia na proteção dos direitos fundamentais à intimidade e à vida privada em face da pena cominada aos delitos informáticos.** Conteúdo Jurídico. Brasília, Distrito Federal, 1 de julho de 2014. Disponível em: https://conteudojuridico.com.br/consulta/Artigos/40026/lei-carolina-dieckmann-in-eficacia-na-protecao-dos-direitos-fundamentais-a-intimidade-e-a-vida-privada-em-face-da-pena-cominada-aos-delitos-informaticos Acesso em: 23 de outubro de 2022.

MENEZES, Cristiano. **Noções de Criminologia.** Doraci. Disponível em: www.doraci.com.br/files/criminologia.pdf Acesso em: 10 de novembro de 2022.

MERKLE, E. R., & RICHARDSON, R. (2000). **Digital dating and virtual relating: Conceptualizing computer mediated romantic relationships.** *Family Relations, 49*, 187-192, 2000.

MORGENSTERN, Grasiele Giusti; TISSOT, Tânia Regina Gottardo. **Crimes Cibernéticos: Phishing – Privacidade Ameaçada.** Artigo Científico Realizado no Curso de Direito da FEMA. Santa Rosa, 2015.

OLIVEIRA, Rafael Santos de., et al. **O Direito à privacidade na internet: Desafios para a proteção da vida privada e o Direito ao Esquecimento**. Rev. Fac. Direito UFMG, Belo Horizonte, n. 70, pp. 561 - 594, 2017.

OLIVEIRA, William César Pinto de. **Lei Carolina Dieckmann**. Revista Jus Navigandi, ISSN 1518-4862, Teresina, ano 18, n. 3506, fevereiro de 2013. Disponível em: https://jus.com.br/artigos/23655/lei-carolina-dieckmann. Acesso em: 25/05/2022.

SCARMANHÃ, Bruna de Oliveira da Silva Guesso, et al. **Invasão de Dispositivo Informático: Aporte com a Legislação Espanhola.** Revista EM TEMPO, V.13, Marília, 2014, P. 231-251.

SILVA, Ricardo Leopoldo da. VIEIRA, Anderson. **Segurança cibernética: o cenário dos crimes virtuais no Brasil.** Revista Científica Multidisciplinar Núcleo do Conhecimento. Ano 06, Ed. 04, Vol. 07, pp. 134-149. Abril de 2021. Disponível em: https://www.nucleodoconhecimento.com.br/ciencia-da-computacao/crimes-virtuais Acesso em: 22 de setembro de 2022.

UNICEF. **Cyberbullying: O que é e como pará-lo.** Disponível em: < https://www.unicef.org/brazil/cyberbullying-o-que-eh-e-como-para-lo#:~:text=Cyberbullying%20%C3%A9%20o%20bullying%20realizado,envergonhar%20aqueles%20que%20s%C3%A3o%20v%C3%ADtimas.> Acesso em: 3 de outubro de 2022.

VERMELHO, Sônia Cristina. Et al. **Refletindo sobre as redes sociais digitais**. Educ. Soc. 35 (126), Março, 2014. Disponível em: https://doi.org/10.1590/S0101-73302014000100011. Acesso em 2 de setembro de 2022.

QUEIROZ, Tayrine. **Marco Civil da Internet: um estudo da sua criação sob a influência dos Direitos Humanos e fundamentais, a neutralidade da rede e o interesse público versus privado.** Jusbrasil.com.br, 2015. Disponível em: < https://tayrine.jusbrasil.com.br/artigos/303303808/marco-civil-da-internet-um-estudo-da-sua-criacao-sob-a-influencia-dos-direitos-humanos-e-fundamentais-a-neutralidade-da-rede-e-o-interesse-publico-versus-privado> Acesso em: 20 de setembro de 2022.