PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
ESCOLA DE DIREITO, NEGÓCIOS E COMUNICAÇÃO
NÚCLEO DE PRÁTICA JURÍDICA
COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO
TRABALHO DE CURSO II

CRIMES CIBERNÉTICOS E A LEGISLAÇÃO BRASILEIRA

ORIENTANDA : NATHALIA NOGUEIRA CARRIJO
ORIENTADORA: Prof.ª Ms. SILVIA MARIA GONÇALVES SANTOS DE LACERDA SANTANA CURVO

GOIÂNIA

2023

NATHALIA NOGUEIRA CARRIJO

CRIMES CIBERNÉTICOS E A LEGISLAÇÃO BRASILEIRA

Artigo Científico apresentado à disciplina Trabalho de Curso II, da Escola de Direito, Negócios e Comunicação, do Curso de Direito, da Pontifícia Universidade Católica de Goiás (PUC-GOIÁS).

Orientadora: ***Prof.ª Ms. Silvia Maria Gonçalves Santos de Lacerda Santana Curvo.***

GOIÂNIA

2023

NATHALIA NOGUEIRA CARRIJO

CRIMES CIBERNÉTICOS E A LEGISLAÇÃO BRASILEIRA

Data da Defesa 26 de Maio de 2023.

BANCA EXAMINADORA

Orientadora: Prof.ª Ms. Silvia Maria Gonçalves Santos de Lacerda Santana Curvo Nota:

Examinadora Convidada: Prof.ª Ms. Maria Augusta Fernandes Justiniano Nota:

SUMÁRIO

CRIMES CIBERNÉTICOS E A LEGISLAÇÃO BRASILEIRA

Nathalia Nogueira Carrijo[1]
Silvia Maria Gonçalves Santos de Lacerda Santana Curvo[2]

RESUMO

Este trabalho tem como temática os crimes cibernéticos, sobretudo com enfoque na legislação vigente a respeito, como por exemplo: a Lei 12.737/2012, entre outras importantes leis que entraram em vigor a partir do escândalo ocorrido com a atriz Carolina Dieckmann. Posteriormente, foi abordado algumas modalidades que os criminosos têm utilizado atualmente e colecionou-se algumas jurisprudências a respeito. Ao final, foi constatado que apesar de desfrutarmos de importantes leis sobre os crimes cibernéticos, ainda assim, possuímos muitas lacunas a serem supridas, sendo necessário um maior investimento em políticas públicas para a conscientização da sociedade brasileira sobre o tema e seu potencial combate.

Palavras-chave: Internet. Crimes cibernéticos. Modalidades de crimes.

INTRODUÇÃO

Não é novidade que a Internet tem conquistado gradativamente mais espaço e relevância em nosso cotidiano no Brasil e no mundo. No entanto, com seu vultoso crescimento e, principalmente, com as iniciativas governamentais para promover políticas públicas de inclusão digital junto à sociedade, pouco se sabe sobre os riscos e os meios de proteção disponíveis aos usuários conectados à rede mundial de computadores.

---

[1] Nathalia Nogueira Carrijo, Graduanda do Curso de Direito pela Pontifícia Universidade Católica de Goiás PUC-GO.

[2] Silvia Maria Gonçalves Santos de Lacerda Santana Curvo, Doutoranda pela Universidade de Salamanca- ES, mestre em Direito Agrário pela UFG- Universidade Federal de Goiás (2002), bacharel em Direito pela Pontifícia Universidade Católica de Goiás (1993), graduação em Pedagogia pela Pontifícia Universidade Católica de Goiás (1983). Especializações em : Direito Penal , Direito Civil, Direito Processual Civil, Direito Constitucional. Atualmente é professora assistente da Pontifícia Universidade Católica de Goiás PUC/GO

Portanto, este artigo científico busca analisar como foi o desenvolvimento da Internet, mas sobretudo, com foco nos crimes cibernéticos, legislação vigente a respeito e discorrer sobre algumas modalidades de crimes cometidos atualmente.

O presente trabalho foi elaborado em três seções. Na primeira seção buscou-se investigar a origem da internet e como foi a sua evolução até chegar ao Brasil. Mais adiante, explanou-se sobre a inclusão digital perante a sociedade brasileira, em seguida, elucida-se sobre o conceito de crimes cibernéticos.

Na seção dois, foram realizadas pesquisas acerca das legislações vigentes em nosso ordenamento jurídico, que visam proteger os usuários conectados à internet. Dentre elas: A Lei Carolina Dieckmann- Lei 12.737/2012; Lei do Marco Civil da Internet- 12.965/2014; Lei Geral de Proteção de Dados (LGPD)- Lei 13.709/2018, entre outros.

Por fim, na terceira seção, apresenta-se algumas modalidades de crimes cibernéticos praticados atualmente, considerando que se trata de um tema recente e que acarreta muitas dúvidas tanto para os usuários, quanto aos aplicadores do direito.

As fontes usadas para consulta foram: artigos científicos, legislação, jurisprudência e consulta a sites e reportagens.

I CONCEITO HISTÓRICO DA INTERNET

Por mais inusitado que pareça, o principal propulsor da Internet foi a Guerra Fria entre (1947-1991), no qual, os Estados Unidos (USA) e a União Soviética (URSS), estavam em um conflito ideológico e científico. De um lado os USA procurava expandir o capitalismo e de outro a URSS, tentava estabelecer o socialismo como sistema econômico.

Nesse período, os Estados Unidos buscou mecanismos para manter a comunicação e o armazenamento de suas informações, garantido o seu funcionamento, mesmo dentro de um período de ataques das tropas inimigas. A partir dessa necessidade, foi criada a Agência de Investigação de Projetos Avançados dos Estados Unidos (ARPANET), uma rede capaz de interligar, transmitir e armazenar informações do país.

Essa tecnologia, inicialmente, era utilizada somente pelos peritos militares.

Mais adiante, foi estendida para as universidades que começaram a usá-la para comunicação via e-mail, entre professores e estudantes. Com isso, as universidades viram essa tecnologia como meio de propagação do acesso ao conhecimento e de compartilhamento de informações. Mais tarde, procurava-se expandir a Net para além dos limites militares, porém era preciso estimular o interesse comercial da época.

Os autores Briggs e Burke (apud, 2006, p.301), relatam o seguinte:

> Qualquer computador podia se ligar à Net de qualquer lugar, e a informação era trocada imediatamente em 'fatias' dentro de 'pacotes'. A noção da quebra de mensagens em "pacotes de informação"[...] é uma ideia mais antiga, presente nas pesquisas de computação desde os anos finais da década de 1960. Era importante, para efetuar tais "trocas" de informações entre as máquinas que houvesse interfaces que possibilitasse o processo codificação/decodificação/recodificação entre os microcomputadores que utilizassem "faces" diferentes e linguagens distintas.

Percebe-se, que uma das dificuldades na expansão da internet era fazer com que todos os computadores conseguissem trocar informações, mesmo que possuíssem um sistema diferente do outro. Muitos foram os estudiosos que contribuíram para o aperfeiçoamento da Internet, mas foi Tim Berners Lee, cientista da computação, quem a fez expandir de fato. Ele foi o criador do que hoje conhecemos, como: a sigla "WWW" - World Wide Web, que é utilizada por todo o mundo.

A rede mundial de computadores, foi criada para possibilitar uma navegação mais conveniente aos usuários, pois em seus proêmios os computadores não conseguiam trocar informações entre si, por causa dos sistemas que não eram compatíveis. O "WWW", foi como a criação de uma língua padrão de comunicação entre os computadores, possibilitando aos usuários da rede um acesso universal ao ciberespaço.

Esse período da história, foi tido como uma nova etapa no desenvolvimento da sociedade e na evolução do homem, sendo definida como a era Infosocial. (apud Turner e Muñoz, 2002, p. 15). Segundo os autores, tratava-se de um período tão importante, que foi comparado ao período de evolução do ser humano.

Inicialmente, a Internet era uma ferramenta de alto custo e poucos tinham acesso a essa nova tecnologia. Conforme descreve Monteiro (2001, p. 6):

> Até o final do século XX, a divulgação pública de informações nunca esteve ao alcance do cidadão comum. Por exigir grandes recursos financeiros (necessários para o acesso à tecnologias de reprodução e difusão, como parques gráficos e emissoras de rádio ou televisão), essa possibilidade estava restrita a uma elite, que detinha o controle dos veículos de massa. Além disso, por serem provenientes de poucas fontes, essas informações podiam ser facilmente controladas.

De fato, a internet foi um divisor de águas, que passou de um investimento militar e que posteriormente, foi expandido para as universidades. Contudo, por tratar-se de uma tecnologia nova a internet era muito onerosa e, por isso, poucos tinham acesso. Mas com o passar dos anos, as universidades perceberam o quanto a rede era importante para a comunicação e divulgação das informações em massa, o que levou à necessidade de ampliá-la para todos.

1.1 A INTERNET NO BRASIL

O processo de descoberta e desenvolvimento da internet, iniciou-se desde 1947, mais precisamente nos Estados Unidos. No entanto, somente foi estendida para outros países na década de 80, período em que ocorreu a sua chegada ao Brasil.

Como mencionado no capítulo anterior, o acesso a internet pertencia, inicialmente, somente aos militares e às universidades. Dessa forma, o principal objetivo das universidades era a troca de informações entre si, e foi esse fato, que levou ao primeiro contato do país com a internet. Foi quando a Universidade LNCC (Laboratório Nacional de Computação Científica), localizada no Rio de Janeiro, se comunicou pela primeira vez com a Universidade de Maryland, nos Estados Unidos.

Conforme explica Monteiro (2001. p. 2):

> [...] o desenvolvimento e utilização do TCP/IP (Transmission Control Protocol/Internet Protocol) como protocolo para a troca de informações na ARPAnet possibilitou a conexão entre redes diferentes, aumentando bastante a abrangência da rede. Em 1990, a ARPAnet foi transformada em NSFnet (National Science Foundation 's Network), se ligando a outras redes existentes, inclusive fora dos Estados Unidos, passando a interconectar centros de pesquisa e universidades em todo o mundo. Estava formada a internet, utilizada principalmente como uma ferramenta de troca de informações entre o meio acadêmico.

Similarmente, muitas outras universidades começaram a se comunicar por meio de mensagens eletrônicas (e-mail) e de compartilhamento de arquivos pelo

mundo todo. No primeiro momento, e até nos dias de hoje, o principal motivo da circulação em massa da internet é promover o acesso à educação de forma democrática a todos.

Nessa fase, a internet era conectada por meio de cabos telefônicos, pagos mensalmente, no qual a única fornecedora do serviço era a EMBRATEL (Empresa Brasileira de Telecomunicações). Entretanto, existiam diversos projetos que visavam a ampliação desse serviço, como por exemplo: A Rede Sul de Teleprocessamento (RST), situada no Rio Grande do Sul e, até mesmo a PUC do Rio de Janeiro, foi uma das pioneiras nesse projeto, mas, infelizmente, não conseguiram avançar nessa finalidade.

O primeiro evento em território brasileiro com acesso à internet foi a Conferência das Nações Unidas, que tem como tema o Meio Ambiente e seu Desenvolvimento, conhecida como Rio- 92 ou ECO-92. Na qual a sua segunda edição ocorreu no Rio de Janeiro em 1982, como se tratava de uma nova tecnologia, não se tinha muitos computadores disponíveis para a reunião, no entanto a ONU fez algumas doações a fim de viabilizar a ocorrência do evento.

A internet não era tão acessível no início, mas com a ampliação do conhecimento sobre essa nova ferramenta, começou-se a promover a sua distribuição de forma gradativa. Mais adiante, o Instituto Brasileiro de Análises Sociais e Econômicas (IBASE), foi o fundador da Alternex, a primeira rede privada de internet, qual seja, o primeiro provedor do Brasil (KLEINA, 2018). Nessa fase, foi se desenvolvendo diversos domínios, a título de exemplo: “.BR”, que possibilitou acesso nacional, em seguida, foram criados os: .ORG; .GOV; .COM.BR e o .NET.BR.

Descobrindo-se o quão fundamental era a internet para o desenvolvimento do país e, considerando que a única empresa fornecedora do serviço era a EMBRATEL, viu-se, a necessidade de promover a sua ampliação. Foi nesse momento, que o Ministro das Comunicações, Sérgio Motta, publicou um decreto que retirava a exclusividade da empresa.

Segundo Monteiro, (2001, p. 2), explana o seguinte:

> Desde então, a internet no Brasil experimentou um crescimento espantoso, notadamente entre os anos de 1996 e 1997, quando o número de usuários aumentou quase 1000%, passando de 170 mil (janeiro/1996) para 1,3 milhão (dezembro/1997). Em janeiro de 2000, eram estimados 4,5 milhões de “internautas”iii . Atualmente, cerca de 10 milhões de brasileiros podem

> acessar a rede de suas residências. Se consideradas as pessoas que têm acesso apenas nos seus locais de trabalho, esse número sobe para 15 milhões.

Com o aumento do fornecimento realizado pelas empresas privadas, mais usuários puderam ter acesso à internet, o que antes era limitado somente à parte mais rica da sociedade, agora estava se tornando acessível. Esse fato foi um grande progresso para a época, pois sem dúvidas interligou o Brasil com o mundo todo, iniciando-se um processo de ampliação do acesso à informação de forma livre e democrática para todos.

1.2 INCLUSÃO DIGITAL

A inclusão digital no Brasil, vem representando uma grande transformação desde do século XX, onde surgiu o termo “sociedade da informação” que simboliza o acesso democratizado à informação, permitindo que todos tenham direito a inserção no meio digital.

Com o passar dos anos, muitos países se conscientizaram sobre a importância da inclusão digital, no Brasil não foi diferente. A promoção do acesso à internet, tornou-se sinônimo de desenvolvimento, com isso muitos países começaram a investir nessa tecnologia. O Brasil ocupa atualmente a 72ª posição entre 156 países do mundo todo.

Um importante estudo, realizado em 2010 pela Fundação Getúlio Vargas (FGV), mostra que:

> [3]O Índice Integrado de Telefonia, Internet e Celular (Itic) de Inclusão Digital mede o acesso das pessoas ao computador, à internet e à telefonia, segundo cálculos da Fundação Getulio Vargas (FGV) e da Fundação Telefônica/Vivo, com base em dados do Censo 2010 do Instituto Brasileiro de Geografia e Estatística (IBGE) e do Instituto Gallup. De acordo com o índice, 51,25% da população brasileira têm acesso ao computador, à internet, ao celular e ao telefone fixo. O país com maior índice de inclusão digital é a Suécia (95,8%), seguido pela Islândia e Cingapura, empatadas com 95,5%. Nas últimas colocações da lista, estão a Etiópia (8,25%), República Centro Africana (5,5%) e Burundi (5,75%), todos no continente africano.

---

[3] VIEIRA. Isabela. Brasil ocupa 72ª posição em ranking mundial de inclusão digital. EBC. Publicação em: 31/07/2012. Disponível em: <https://memoria.ebc.com.br/tecnologia/2012/07/brasil-ocupa-72a-posicao-em-ranking-mundial-de-inclusao-digital>. Acesso em: 04/04/2023

A presente pesquisa buscou analisar como foi o desenvolvimento do acesso à internet no Brasil e quais os meios utilizados pelos usuários, além disso, demonstrou como os países têm investido na inclusão digital, sendo a Suécia, o país com o maior percentual de acesso ao meio digital.

Segundo Marcelo Neri, o responsável pela pesquisa FGV, ressaltou que um dos principais motivos de alguns indivíduos não terem acesso à internet é a falta de estudos. Isso demonstra que a inclusão digital não se trata somente de ferramentas, como: computador, celular e acesso à internet. É necessário um maior investimento em conhecimento, principalmente, as partes mais carentes da sociedade, a fim de viabilizar a inclusão desses indivíduos à sociedade da informação.

Já em outra pesquisa realizado pelo Instituto Brasileiro de Geografia e Estatística (IBGE), realizada no ano de 2018/2019:

> O crescimento da conexão de domicílios à internet aconteceu de forma mais significativa na área rural. O percentual de domicílios conectados saltou de 49,2%, em 2018, para 55,6%, em 2019, o que corresponde a um aumento de 6,4 pontos percentuais. Nos domicílios urbanos, a utilização da internet subiu de 83,8%, em 2018, para 86,7%, em 2019. O aumento também ocorreu em todas as grandes regiões do país. No Nordeste, por exemplo, houve evolução de 5,2 pontos percentuais nos domicílios conectados à internet, saindo de 69,1%, em 2018, para 74,3%, em 2019. O levantamento do IBGE mostra também que 12,6 milhões de domicílios ainda não tinham internet. Os motivos apontados foram falta de interesse (32,9%), serviço de acesso caro (26,2%) e o fato de nenhum morador saber usar a internet (25,7%).

A presente pesquisa, vem demonstrando o quanto tem aumentado o índice de acesso a internet, inclusive no meio rural. Contudo, ainda é preciso muito investimento do governo federal para viabilizar o acesso à internet às pessoas mais carentes, ampliando não só o acesso à educação e diminuindo os custos da Internet, para viabilizar um maior acesso à população.

Para que ocorra a inclusão digital, são necessárias três ferramentas, são elas: aparelhos eletrônicos (computadores, smartphones, TVs, entre outros), acesso à internet e conhecimentos básicos de informática. Vale ressaltar, que esses instrumentos mencionados são meios e, não, a finalidade da inclusão digital, pois o objetivo principal é trazer à sociedade uma ascendência no acesso ao ambiente virtual.

Apesar de possuir uma ampla proteção e democratização, a inclusão digital não alcançou de forma uniforme toda a sociedade brasileira, pois ainda hoje,

existem lugares no território brasileiro que carecem principalmente de recursos financeiros e educacionais.

A fim de viabilizar o acesso à internet no Brasil, no ano de 2020, foi colocado em votação pelo Senador Luiz Pastore do MDB/ES, a emenda à Constituição Federal nº 8/2020. A presente emenda tinha como proposta a inserção do acesso à internet, como um direito fundamental, a fim de complementar o art 5º da CF.

Segundo o Senador essa proposta se devia ao fato que:

> [4]"O acesso à internet é, hoje, elemento fundamental para o desenvolvimento pleno da cidadania e para o crescimento profissional de todas as pessoas. Sem dúvida, a eventual falta de acesso à internet limita as oportunidades de aprendizado e de crescimento, de educação e de emprego, comprometendo não apenas o futuro das pessoas individualmente, mas o próprio progresso nacional", defende Pastore.

Contudo, a proposta foi arquivada em 22/12/2022, pelo final de sua legislatura, em conformidade com o art. 332, do RISF.

Desse modo, partimos para outra vertente, ainda, dentro da inclusão digital: Afinal, a internet é mesmo um direito fundamental? São essenciais à vida, ou seja, são direitos imprescindíveis, obrigatórios e, neste caso, indispensáveis à "vida jurídica", dos sujeitos de direito?

Novelino (apud 2017, p. 261), conceitua direitos fundamentais, da seguinte forma:

> São Direitos universais porque, como dito, se vinculam a um núcleo mínimo de proteção à dignidade humana, de forma que representam os direitos que todos os componentes de uma sociedade (um Estado político, no caso) titularizam, mesmo que de forma potencial, independentemente de quaisquer condições físicas, sociais, morais, etc. Já a noção de que são históricos parte da ideia de que "surgem e se desenvolvem conforme o momento histórico", de forma que aquela noção de núcleo 4 mínimo de proteção à dignidade humana não somente varia de época para época (o que é fundamental no século XXI não poderia ser tão essencial, ou até mesmo inexistente, para a pessoa humana que viveu no século XIX – ou vice-versa), como é produto dos fatos e eventos sociais presentes naquela sociedade ou naquele grupo naquele momento histórico.

---

[4] NATHANY. Morgana. Proposta inclui na Constituição o direito de acesso à internet. Senado Notícias. Publicado em 13/03/2020. Disponível em: <https://www12.senado.leg.br/noticias/materias/2020/03/13/proposta-inclui-na-constituicao-o-direito-de-acesso-a-internet#:~:text=O%20acesso%20%C3%A0%20internet%20pode,quinta%2Dfeira%20(12)>. Acesso em: 08/04/2023

Via de regra, os direitos fundamentais devem estar expressos em lei. Dessa forma, o direito à internet somente seria um direito fundamental, caso a PEC 8/2020, fosse aprovada. Todavia, a lei não consegue acompanhar em tempo real (o caso concreto), não devendo ser considerado somente o rol taxativo previsto na CF em seu artigo 5º.

Colontonio (2020, p. 7), define que:

> [...] o direito natural não somente indica quais normas devem ser positivadas, mas demonstram quais são as normas fundamentais, de forma que, mesmo diante da omissão de um Estado em realizar os trâmites necessários para a textualização de dispositivos, os valores do direito natural são obrigatórios e já vinculam a todos.

Devemos partir do pressuposto que antes de existir o direito positivado, já existia o direito natural, que são aqueles direitos inerentes ao homem. Dele, derivam-se os direitos humanos e os direitos fundamentais.

Não é novidade, que apesar dos esforços do legislador, ainda sim, existem muitas lacunas na lei, o que abre espaço para várias interpretações sobre temas novos. Dessa forma, o questionamento sobre o acesso ao espaço virtual, ainda é um tema em aberto.

Se tratado como um direito fundamental atípico, de forma estrita, e se aplicado ao caso concreto, verificar-se-a inúmeros caso em que o não acesso à internet, implicaria na violação de direitos básicos, como por exemplo: Caso um aluno não pudesse assistir a uma aula virtual, por não possuir acesso à internet em sua residência, violaria o seu direito à educação. Por outro lado, observa-se uma grande informatização dos serviços jurídicos, Colontonio (2020, p. 11), aviste:

> O advento dos processos judiciais eletrônicos, cujos atos dependem do acesso à rede mundial de computadores, demonstram que o acesso à justiça, hodiernamente, exige uma conexão de banda larga. O direito à petição caminha cada vez mais para se tornar um direito eletrônico de petição, uma vez que a quase totalidade dos órgãos públicos caminham para a informatização dos seus sistemas de recepção de protocolos.

Trazendo dúvidas no sentido de: “ser ou não ser um direito fundamental”. Contudo, trata-se de uma ferramenta importante ao ser humano, mas não inerente a ele, conforme Colontonio (2020, p. 14), esclarece:

> O uso da internet, por exemplo, nesta toada, não é o direito à educação, mas sim um meio de realizar tal direito essencial. Entretanto, o acesso e o

> uso da internet não se tornaram tão essenciais e universais que poderiam (ou deveriam) se tornar um direito fundamental? A resposta é negativa, porque, insistimos, a internet é um instrumento, uma ferramenta, não um valor essencial da natureza e da existência humana. Como uma ferramenta tecnológica, certamente a internet será substituída, talvez em um futuro nem tão remoto, por outra tecnologia que sequer podemos conceber com nossos conhecimentos atuais. Como toda tecnologia, ficará obsoleta e será substituída.

Concluindo, que apesar de sua importância nos dias de hoje, trata-se de uma ferramenta para o ser humano, mas não indispensável. Todavia, não anula o fato de sua relevância para a atualidade, pois o meio digital vem conquistando bastante espaço, principalmente, após a Pandemia do COVID-19.

Durante a pandemia muitas empresas precisaram transferir seus profissionais para o trabalho em home-office (escritório em casa), a fim de manter a segurança e preservar a saúde de seus profissionais. Até mesmo escolas e faculdades tiveram que transferir as aulas para o meio virtual (como foi o caso, inclusive da nossa universidade).

Em resumo, desde a criação da internet, até alguns anos atrás, pretendia-se manter o seu acesso completamente livre, sendo considerada “terra de ninguém", um espaço sem regras e sem consequências.

Por outro lado, com o crescimento da sensação de anonimato, criminosos perceberam a oportunidade de cometer crimes dentro do ciberespaço, o que levou ao surgimento do que hoje conhecemos como: cibercrimes, crimes virtuais, crimes cibernéticos, entre outras nomenclaturas.

Pelo fato de inicialmente, não existirem regras ou legislação regulamentado o uso da internet, pouco se falava em proteção virtual, preservação de dados pessoais, entre outros. Dessa forma, com o crescimento expressivo de crimes nesse ambiente, foi necessário uma maior atenção do legislador para o presente assunto, apesar de ainda ser um tema recente, já é possível encontrar algumas leis regulamentando sobre o assunto.

1.3 CONCEITO DE CRIMES CIBERNÉTICOS

O autor Alexandre Júnior (2019, p. 3), conceitua cibercrime, como:

> O cibercrime nada mais é que todo ato em que o computador ou meios de tecnologia de informação serve para atingir um ato criminoso ou em que o

> computador ou meios de tecnologia de informação é objeto de um crime. O cibercrime está associado ao fenômeno da criminalidade informacional de condutas violadoras de direitos fundamentais, seja por meio da utilização da informática para a prática do crime ou como elemento de tipo legal de crime.

Dessa forma, o crime cibernético é uma modalidade de crime, como qualquer outro, contudo, o seu principal diferencial é o meio pelo qual é praticado. Esses crimes são cometidos através de computadores, smartphones, tablets, entre outras ferramentas vinculadas ou não a internet.

Como se sabe, os atos criminosos podem ocorrer a qualquer momento, como por exemplo: Crimes Contra a Honra- Injúria, difamação e calúnia, tipificados no (Art. 139, do CP), Estelionato (art. 171, do CP), Induzir ou instigar ao suicídio (art. 122, do CP). Todavia, os criminosos conseguiram encontrar meios de cometer esses crimes e muitos outros dentro do ambiente virtual, pois até alguns anos atrás, acreditava-se estar completamente escondidos por trás do anonimato e, consequentemente, impunes de seus atos.

Acerca do tema, Simas (apud, 2014, p. 14), discorre:

> A evolução operada nas novas tecnologias, projectou-se sobre o fenómeno criminal, pois se atendermos às suas duas vertentes, por um lado, a tecnologia poder, ela mesma, objecto de prática de crimes e por outro lado, suscita e potencia novas formas criminais ou novas formas de praticas antigos crimes.

A evolução da internet proporcionou inúmeros benefícios ao nosso cotidiano, mas também ampliou o campo de atuação dos criminosos. Simas (apud, 2014, p. 12), traz considerações a respeito:

> Cibercrime está associado ao “fenómeno da criminalidade informática estão, sem dúvida, condutas violadoras de direitos fundamentais, seja através da utilização da informática para a prática de um crime, ou como um elemento do tipo legal de crime”.

Com o passar dos anos viu-se a necessidade da criação de mecanismos de segurança e principalmente, meios de estabelecer limites dentro do ambiente tecnológico. Procurou-se mecanismos de proteção de dados, arquivos pessoais, e até mesmo a inviolabilidade da integridade física das pessoas.

No Brasil, a legislação ainda é escassa sobre o tema mas, já possuímos

algumas leis, como: A Lei Carolina Dieckmann- 12.737/2012, o Marco Civil da Internet- Lei 12.965/2014, a LGPD, entre outros. Todas as leis acima mencionadas, foram criadas com o intuito de proteger e possibilitar a polícia um maior controle e propensão na busca do(s) autor(es) do(s) crime(s).

II LEGISLAÇÃO BRASILEIRA

2.1 CÓDIGO PENAL E A LEI CAROLINA DIECKMANN

Em proêmio, cabe salientar que, o Código Penal Brasileiro- Lei 2.848/1940, possui um grande aparato no sentido de abranger o maior número de crimes possíveis visando uma maior segurança jurídica às vítimas de possíveis crimes. Contudo, com as constantes mudanças e evoluções da sociedade, muitos fatos ocorridos no mundo concreto não encontravam amparo satisfatório na lei, sendo necessária a criação de leis para proteger as vítimas.

Vale destacar, que muitos crimes previstos no código penal, como por exemplo: O crime de estelionato, falsificação ideológica, crimes contra à honra e muitos outros, ocorrem também no meio virtual.

Todavia, por tratar-se de um instituto novo e com a ocorrência de casos mais específicos na internet, o legislador buscou melhor amparar essas vítimas, portanto, a edição da Lei 12.737/2012 e, muitas outras que seguiremos abaixo.

A presente Lei 12.737, foi promulgada na data de 30/11/2012, pela então presidente Dilma Rousseff, tipificando criminalmente os delitos informáticos e trazendo alterações ao Código Penal. Inicialmente, o ambiente virtual não possuía regras e nem legislação vigente específica para esses casos, sendo essa a primeira lei no país a tipificar diretamente sobre os crimes virtuais.

A lei 12.737/12, ficou conhecida como a lei mais rápida a tramitar no Congresso Nacional, pois da sua edição até sua publicação teve duração de somente 1 ano. Isso se deve, ao escândalo experimentado à época pela atriz Carolina Dieckmann, que teve seu computador invadido e, posteriormente, teve suas 36 fotos íntimas divulgadas na rede mundial de computadores, em razão de não ter se submetido às chantagens dos criminosos.

Tamanha repercussão social teve o presente caso, já que, naquela época

não havia tipificação no nosso ordenamento jurídico para o presente crime. Logo, foi introduzido ao Código Penal dois novos artigos o 154-A e o 154-B, que diz:

> **Invasão de dispositivo informático**
>
> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
> [...]
>
> **Ação penal**
>
> Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos.

Ademais, foram introduzidos outros crimes ao Código Penal, são eles: Interrupção ou perturbação de serviços telegráfico, telefônico, informático, telemático ou informação de utilidade pública (Art. 266); Falsificação de documento particular e falsificação de cartão (Art. 298), veja-se:

> **Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública**
> [...] § 1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.
> § 2º Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública.
> **Falsificação de documento particular**
> **[...]**
> **Falsificação de cartão**
> Parágrafo único. Para fins do disposto no caput , equipara-se a documento particular o cartão de crédito ou débito.

Trazendo proteção a bens dos quais o Código Penal não amparava em seus proêmios, principalmente pelo fato que a época de sua promulgação não havia temas tão modernos.

Vale ressaltar, que no caso da atriz Carolina Dieckmann o que foi criminalizado à época, foi o fato dos criminosos terem "invadido" o computador da vítima e, não, a divulgação das fotos íntimas. A divulgação de fotos íntimas só veio a ser descrito como crime com a lei 13.718/18, da qual trata sobre os crimes de importunação sexual, divulgação de cena de estupro, entre outros.

A Lei Carolina Dieckmann, também dividiu os crimes informáticos como: próprios ou impróprios. Sendo o primeiro, aqueles crimes que somente podem ser cometidos através do computador, celular, dentre outros. Já os impróprios, são aqueles que já existem dentro do Código Penal, mas podem ser cometidos dentro do ambiente virtual.

O bem tutelado na presente lei é a liberdade, pois visa proteger a intimidade do indivíduo e o segredo informático da vítima. Contudo, a lei é bastante restrita, pois só ampara aquelas vítimas que possuem senha em seu dispositivo (e essa, venha a ser violada), e é restrita ao titular do dispositivo informático, não protegendo os dados de terceiros que possam estar no dispositivo.

2.2 MARCO CIVIL DA INTERNET - Lei 12.965/2014

Conforme explanado sobre o surgimento da internet, preliminarmente, tratava-se de uma ambiente completamente livre, sem dono, sem regulamentação e nem mesmo orientações de segurança aos seus usuários. Juntamente com o crescimento da internet no Brasil, cresceu também o número de crimes dentro do ambiente virtual.

A partir do caso da Atriz Carolina Dieckmann e com a promulgação da Lei 12.737/2012, da qual foi apelidada de “Lei Carolina Dieckmann” (atualmente, com 10 anos desde entrada em vigor), o legislador passou a dar especial atenção a esse tema, estabelecendo direitos e deveres em seu uso.

Em 23/04/2014, foi criada a Lei 12.965/2014, conhecida como o Marco Civil da Internet, que conta com 5 capítulos e 32 artigos, regularizando e estabelecendo: “art. 1º *“[...] princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria.”*

A Lei 12.965/2014, foi criada para a proteção de dados privados dentro do ambiente virtual, principalmente, no que tange ao modo como esses dados serão utilizados pelas empresas e, além disso, busca-se evitar a comercialização de dados a terceiros.

Os 3 princípios básicos do Marco Civil, são: fiscalização (existem órgãos responsáveis pela fiscalização dentro do ambiente digital, como por exemplo a Agência Nacional de Telecomunicações e a Secretária Nacional do Consumidor;

privacidade (exige das empresas e provedores de conexão a inviolabilidade de dados dos usuários); e por último a neutralidade (que proíbe que os provedores de conexão alterem a velocidade da conexão banda larga, entre as páginas da internet).

Esta lei exige que as empresas existentes dentro do meio digital, esclareçam em seus termos de uso e contratos virtuais, de que forma os dados do usuário serão utilizados, como serão tratados, coletados, entre outros. Não podendo as empresas usá-los de forma diversa da permitida pelo usuário, sendo chamado de "Licitação de Proposito".

Em síntese, o Marco Civil foi inspirado no art. 5º da CF, tendo em vista que muitos princípios nela estabelecidos são semelhantes aos princípios fundamentais, regulando a forma como os direitos são protegidos no ambiente virtual, pois à época não havia nenhuma regulamentação sobre o tema, mas já naquele período procurava-se proteger os usuários dentro do meio digital.

2.3 LEI 13.709/2018

A Lei Geral de Proteção de Dados (LGPD) era um projeto de lei que tramitava desde da criação do Marco Civil, a intenção inicialmente era publicar as duas leis em conjunto, mas na época não foi possível. O Marco Civil e a LGPD são complemento uma da outra, pois o Marco Civil como explanado acima visa proteger os dados dos usuários, a privacidade e neutralidade da rede, enquanto a LGPD visa proteger a privacidade e liberdade de expressão dos usuários.

A LGPD foi sancionada em 14 de agosto de 2018- Lei 13.709/2018, e disciplina sobre o seguinte:

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

A presente lei trouxe diversas definições de conceitos antes obscuros na aplicação prática, como por exemplo: apresentou a definição do que se entende por dados pessoais; dados sensíveis; dado anonimizado; banco de dados; entre muitos outros descritos em seu art. 5 em diante. Além disso, estabelece em seu texto como os dados devem ser tratados, armazenados e como deve ocorrer sua exclusão.

A LGPD dedicou um capítulo especial às crianças e adolescentes, visando o princípio do melhor interesse, garantido que os dados destes sejam tratados pelas empresas e, somente, repassado a terceiros com o autorização dos pais ou responsável, conforme prevê o art. 14 e seus parágrafos, da presente lei.

É possível verificar na lei, que foi dado autonomia aos usuários para requerer informações das empresas de como os dados estão sendo armazenados, qual é a necessidade de armazenamento daqueles dados, além de serem livres para requerer que a empresa apague os seus dados armazenados, podendo desistirem do consentimento antes dado.

Mais adiante, estabeleceu o órgão responsável pela orientação e fiscalização desses dados, qual seja, Autoridade Nacional de Proteção de Dados Pessoais (ANPD). Por último, estabeleceu direitos e deveres às empresas estrangeiras para se adequarem à presente norma quando possuírem filial, agência, sucursal, dentre outros, estabelecidos no Brasil.

2.4 COVID-19 E A LEI 14.155/2021

No início do ano de 2020, passou-se por um momento nunca antes vivido, a Pandemia do COVID-19.

> [5]Em 30 de janeiro de 2020, a OMS declarou que o surto do novo coronavírus constitui uma Emergência de Saúde Pública de Importância Internacional (ESPII) – o mais alto nível de alerta da Organização, conforme previsto no Regulamento Sanitário Internacional. Essa decisão buscou aprimorar a coordenação, a cooperação e a solidariedade global para interromper a propagação do vírus.

Durante esse período, foi necessário adotarmos medidas de isolamento a fim de evitar uma maior propagação do vírus. A partir de então, muitas empresas precisaram transferir os seus funcionários para o modo home-office, visando manter a segurança e saúde de seus profissionais e, além disso, buscava-se manter o mercado financeiro ativo e evitar prejuízos ainda maiores.

A partir da necessidade de manter o funcionamento de inúmeros serviços, adotou-se como nunca antes o uso da Internet, tanto para o trabalho, quanto para a continuidade da vida escolar dos alunos, realização de compras, transferências,

---

[5] **Histórico da pandemia de COVID-19.** OPAS. Disponível em: <%20de%20mar%C3%A7o%20de,e%20n%C3%A3o%20%C3%A0%20sua%20gravidade.> Acesso em: 02/05/2023.

entre outros. Todavia, mesmo em um momento tão delicado os criminosos não deixaram de agir, passaram a estar presentes também no ciberespaço. Nessa fase do isolamento social, houve um aumento assustador no número de golpes dentro do ambiente virtual. Bottini (apud, 2020), registra que:

> Em relação aos crimes virtuais, com o isolamento, as pessoas buscam realizar a maioria de suas atividades online, seja compras, trabalho, envio de dinheiro, a insegurança e a falta de compreensão desses mecanismos de aquisição e transferência virtual de mercadorias tornam as pessoas passíveis a diversos golpes, como páginas falsas de bancos e lojas na Internet, muitas das quais veiculam anúncios promocionais imperdíveis.

Vale ressaltar, que já existia nesse momento regulamento sobre o uso da Internet e, inclusive, com cunho punitivo. Entretanto, foi observado que as penas eram tão baixas que não inibiam os bandidos da prática criminosa. Um dos principais crimes cometidos durante esse período foi o Phishing, trata-se de uma modalidade de roubo de dados. Segundo uma pesquisa da da Federação Brasileira de Bancos (FEBRABAN), o número de casos de Phishing chegou a um aumento de 80%, durante o período da Pandemia.

As principais vítimas de golpes no ambiente virtual, principalmente, durante o período pandêmico foram as crianças e idosos. Isso porque são a parte da sociedade com maior vulnerabilidade, em razão da desinformação e da falta de conhecimentos básicos para uma navegação segura. É o que demonstra Barbosa (2022):

> [6]Em meio ao isolamento social, houve a adequação de estudantes e professores em salas virtuais, tornando necessário o acesso de crianças e adolescentes à internet para a manutenção de conteúdos e redução de prejuízos de conhecimentos. [...] os idosos tiveram que seguir rigorosamente as recomendações da Organização Mundial de Saúde, por serem a parte mais afetada e mais vulnerável ao vírus da Covid-19. Em meio a tais mudanças eles passaram a utilizar mais as redes como forma de comunicação e atualização de notícias, para que pudessem se manter antenados em noticiários e se comunicando com familiares e amigos. [...] A busca pela segurança e não contágio do vírus, trouxe consigo o uso massivo de meios de comunicação virtuais, desencadeando uma série de outros

[6] BARBOSA, BRUNA GABRIELLY TEIXEIRA. **Criminalidade cibernética em tempos de pandemia no Brasil e o papel da responsabilidade civil no cenário atual.** Conteudo Juridico, Brasilia-DF: 28 nov 2022, 04:05. Disponível em: <https://www.conteudojuridico.com.br/consulta/artigos/60254/criminalidade-ciberntica-em-tempos-de-pandemia-no-brasil-e-o-papel-da-responsabilidade-civil-no-cenrio-atual> Acesso em 03/05/2023

> perigos . Os cibercriminosos viram o cenário pandêmico como uma forma de acompanhar pessoas e desempenharem ações dotadas de má fé, visando benefício próprio.

Com isso, no ano de 2021, foi criada a Lei 14.155/2021, que promoveu a alteração do Código Penal Brasileiro e do Código de Processo Penal:

> Para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato.

Anexo tabela 1, trazendo alterações nos Art. 154-A, Art. 155, Art. 171, do CP e Art. 70, do CPP, quanto ao regime punitivo e o tempo de prisão. As penas anteriores demonstraram serem pouco efetivas no que tange a inibição dos criminosos quanto às práticas delituosas.

III PROGRAMAS MALICIOSOS

O avanço da internet, trouxe inúmeros benefícios ao nosso cotidiano, dentre eles: possibilitou a comunicação e interligou o mundo inteiro, proporcionando lazer e entretenimento, criou fontes de trabalho (como no caso dos influencer digitais), além de auxiliar na modalidade home-office, facilitou o uso bancário (com a criação do PIX, que quer dizer pagamento instantâneo), entre muitos outros serviços e possibilidades. No entanto, no que tange a criminalidade ou melhor aos crimes cibernéticos, estes, também evoluíram.

Os criminosos viram essa nova ferramenta como um meio extensor de lesar as vítimas e o que antes era possível somente de forma física, agora, também estava presente no mundo virtual. Por acreditarem que a internet é “terra de ninguém”, os hackers agem livremente atingindo um grande número de vítimas simultaneamente.

O termo hacker significa:

> [7][...] alguém com uma avançada instrução em programação - bem como outros assuntos da informática - para explorar sistemas computacionais,

---

[7] O QUE É "HACKING"?. PEOPLE. 2022. Disponível em: <https://www.people.com.br/noticias/informatica/o-que-e-hacking#:~:text=Podemos%20colocar%20que%20a%20palavra,funcionamento%20e%20realizar%20qualquer%20atividade.>. Acesso em: 05/04/2023.

> descobrir seu funcionamento e realizar qualquer atividade.” seja para o bem ou para o mal.

O termo hacker nasceu quase que junto com a internet, trata-se de indivíduos com um grande conhecimento na área da computação e, com isso, podem usar suas habilidades tanto para o bem quanto para o mal.

Com isso, passamos as principais ferramentas que os criminosos têm utilizado no últimos anos, uma das mais utilizadas é o vírus, veja-se:

> [8]Um vírus de computador é um tipo de malware que se liga a outros programas, se autorreplica e se espalha de um computador para outro. Quando um vírus infecta um computador, ele faz cópias de si mesmo e anexa a outros arquivos ou documentos. Ele depois modifica esses arquivos e continua a se espalhar. Os vírus infectam os computadores discretamente e, muitas vezes, são projetados para destruir arquivos pessoais ou obter o controle de dispositivos. Ao fazer cópias de si mesmos, os vírus de computador se espalham por dispositivos e redes, como vírus biológicos, que passam de pessoa em pessoa. Assim como as versões biológicas, alguns vírus de computador são simplesmente irritantes, enquanto outros podem causar grandes danos.

Esclarecido sobre o que são vírus, passamos agora aos diferentes tipos existentes. Vale ressaltar, que são inúmeros, mas iremos explanar sobre os principais:

1) Cavalo de tróia ou trojan: tem esse nome por ser semelhante ao da mitologia grega. Trata-se de um malware que vem disfarçado de algo inofensivo, ocorre quando os usuários baixam algum arquivo não oficial, como por exemplo: softwares, games, músicas, etc. Dessa forma, o usuário baixa um “sistema” acreditando que é uma coisa, quando na verdade tem um segundo sistema por trás que faz o roubo de dados, informações confidenciais, entre outros.

2) Spywares: Conhecido como vírus espião, diferente dos outros, ele não visa o roubo de dados, mas seu principal intuito é inspecionar o que os usuários estão realizando a fim de coletar informações úteis ao possuidor do vírus ou até mesmo benefícios financeiros. Contudo, existem muitas empresas que coletam esses dados para mapear e terem acesso às preferências dos clientes e, posteriormente, comercializar esses dados a outras empresas.

---

[8] LATTO. Nica. O que é e como funciona um vírus de computador?. Academy. 12/2020. Disponível em: <https://www.avast.com/pt-br/c-computer-virus> Acesso em: 05/04/2023.

3) Phishing: Atualmente é um dos mais usados pelos criminosos, devido a facilidade em sua aplicação. Ele possui diversas modalidades, entre elas: O envio de falsos e-mails/ mensagens (um golpe clássico é o suposto envio de mensagens de bancos, ou pedido de atualização de dados), bastando a vítima clicar no link para ter seu dispositivo infectado; Phishing do Dropbox, ataque a arquivos do Google Docs ou Google Drive: Em todos os casos, os criminosos visam o roubo de arquivos e imagens pessoais; Outro ataque dentro dessa modalidade é a do Peixe Grande: Nesse ataque, os hackers buscam os dados de empresas e funcionários de maior cargo dentro desse ambiente. O vírus espalha mensagens aos funcionários solicitando arquivos confidenciais da empresa e, infelizmente, acabam conseguindo, pois as vítimas acreditam estar cumprindo ordens de seus superiores.

4) Keylogger: é um vírus que armazena tudo aquilo que é digitado no computador/ou aparelho da vítima, após a coleta das informações o programa envia os dados ao autor da violação via e-mail. Outro detalhe, é que se trata de um vírus difícil de ser detectado já que todo esse processo é feito de forma silenciosa.

É importante frisar, que essas são só algumas das modalidades praticadas pelos hackers.

Apesar disso, para propiciar uma ambiente mais seguro durante a navegação, recomenda-se sempre o uso de antivírus, programas oficiais, atenção ao receber link e e-mails suspeitos, sempre tomar cuidado com fake news e acima de tudo sempre se atualizar sobre os novos golpes e como se proteger deles.

3.1 ALGUMAS MODALIDADES DE CRIMES CIBERNÉTICOS

Pornografia infantil: O crime de pornografia infantil está previsto no art. 241-A, do Estatuto da Criança e Adolescente (ECA):

> Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa.

Importante destacar, o crime de pornografia infantil não se confude com o de pedofilia infantil, pois no primeiro basta que o agente pratique uma das condutas acima mencionado (sem necessariamente, ter relação com a criança ou adolescente), já no segundo, conforme a OMS, o pedofilo é um agente possuidor de

transtorno de preferência sexual (nesse caso o adulto tem atração sexual por crianças ou adolescentes).

Lavagem de dinheiro: Segundo o art. 1º, da Lei 9.613/1998, descreve o seguinte: *"Art. 1º Ocultar ou dissimular a natureza, origem, localização, disposição, movimentação ou propriedade de bens, direitos ou valores provenientes, direta ou indiretamente, de infração penal."*

No ano de 2022, a mencionada lei sofreu alterações pela Lei 14.478/2022 que trouxe regulamentação sobre a forma de prestação de serviço de ativos virtuais.

> [9]É sabido que o objetivo principal da Lei n. 9.613/98 (Lavagem de Dinheiro) é dar contribuição ao combate ao crime organizado em nível transnacional. A "lavagem de dinheiro" (tradução literal de "money laundering" – expressão utilizada no começo do século passado pela polícia norte-americana, em razão de a máfia possuir lavanderias como empresas de fachada para justificar seus ganhos ilícitos) é um dos mecanismos mais eficientes, por suas múltiplas formas, de financiar a criminalidade organizada, possibilitando às organizações criminosas e aos criminosos em geral apresentarem justificativas aparentemente lícitas para seus ganhos ilícitos. A tipificação da "lavagem de dinheiro" constitui, assim, um instrumento visando ao combate da macrocriminalidade.

O principal objetivo dos criminosos nessa modalidade é fazer com que o dinheiro obtido de maneira ilícita, se torne lícito a fim de evitar ser descoberto.

Cyberbullying: O cyberbullying é o mesmo que conhecemos como bullying só que praticado no meio virtual (utiliza-se principalmente, redes sociais, aplicativos de mensagens, como o Whatsapp, entre outros). No início, quando surgiu essa modalidade de crime não existia legislação específica. Contudo, entendeu-se que encaixava-se na modalidade de crimes contra a honra.

Sexting: significa "sexo" mais "texto", ou seja, trata-se do envio de mensagens sexuais, podendo ser imagens ou vídeos. Tornou-se uma prática muito comum dentro da rede social entre alguns casais ou sites de relacionamento. Mas, percebeu-se que quando acontecia o rompimento da relação o indivíduo que tinha acesso ao conteúdo sexual o lançava na rede mundial de computadores, como uma forma de vingança, por isso, foi criada a lei 13.718/18, art. 218-C:

---

[9] ANDREUCCI. Ricardo Antonio. O crime de lavagem de dinheiro por meio da utilização de ativo virtual. Empório do direito.com.br. 02/02/2023. Disponível em: <https://emporiododireito.com.br/leitura/o-crime-de-lavagem-de-dinheiro-por-meio-da-utilizacao-de-ativo-virtual#:~:text=O%20CRIME%20DE%20LAVAGEM%20DE%20DINHEIRO%20POR%20MEIO%20DA%20UTILIZA%C3%87%C3%83O%20DE%20ATIVO%20VIRTUAL,-Ricardo%20Antonio%20Andreucci&text=A%20nova%20Lei%20n.,algumas%20mudan%C3%A7as%20na%20Lei%20n.>. Acesso em: 06/04/2023.

> [...]de cena de sexo o[...] Oferecer, trocar, disponibilizar, transmitir, vender ou expor à venda, distribuir, publicar ou divulgar, por qualquer meio - inclusive por meio de comunicação de massa ou sistema de informática ou telemática -, fotografia, vídeo ou outro registro audiovisual que contenha cena de estupro ou de estupro de vulnerável ou que faça apologia ou induza a sua prática, ou, sem o consentimento da vítima, cena de sexo, nudez ou pornografia: Pena - reclusão, de 1 (um) a 5 (cinco) anos, se o fato não constitui crime mais grave.

A presente lei, buscou proteger as vítimas que após o termino das relações amorosas, tinham fotos, video, conversar, entre outros conteúdos pessoais divulgados na internet, esse crime é popularmente chamado de “Pornografia de Vingança”.

3.2 JURISPRUDÊNCIAS

Veja-se abaixo um julgado realizado pelo Desembargador Leandro Crispim, da 2ª Camara Criminal, do Tribunal de Justiça do Estado de Goiás (TJGO), a respeito de pornografia infantil:

> HABEAS CORPUS. ARMAZENAMENTO E TRANSMISSÃO DE IMAGENS E VÍDEOS CONTENDO PORNOGRAFIA INFANTIL. EXCESSO DE PRAZO PARA A FORMAÇÃO DA CULPA. INOCORRÊNCIA. Não há configuração de constrangimento ilegal por excesso de prazo quando não vulnerado o prazo de 148 dias, previsto para o encerramento da instrução criminal, consoante estabelecido Ofício Circular n. 042/2011/ASSJ, atendendo recomendação da Corregedoria Nacional de Justiça (Ofício Circular n. 008/DMF). 2- MANUTENÇÃO DA SEGREGAÇÃO PREVENTIVA. GARANTIA DA ORDEM PÚBLICA. Resta prudente a manutenção da prisão preventiva, derivada de uma operação realizada pela Delegacia Estadual de combate a crimes cibernéticos, especialmente para salvaguardar a ordem pública, diante de elementos que demonstram o armazenamento e a transmissão de imagens/vídeos, em computadores de local de trabalho, contendo pornografia envolvendo crianças e adolescentes, via internet, seja para evitar a repetição das práticas em questão, seja para desestabilizar eventual esquema de pedofilia em que o suposto agente estava envolvido. ORDEM DENEGADA.
> **(TJGO, Habeas Corpus 5578507-74.2018.8.09.0000, Rel. LEANDRO CRISPIM, 2ª Câmara Criminal, julgado em 23/01/2019, DJe de 23/01/2019)**

Verifica-se no presente caso que o réu foi detido em flagrante acessando conteúdo pornografico envolvendo menores. Em análise ao processo (0134396-25.2018.8.09.0011), foi verificado que foi expedido pela 8ª Vara Criminal um mandado de busca e apreensão, o denunciado já vinha sendo investigado pela Delegacia Estadual de Crimes Cibernéticos, com isso, foi realizado buscas em seu

dispositivo eletrônico, computadores, vídeos armazenados, entre outros, que levaram até o suspeito.

Foi impetrado um Mandado de Segurança, contudo teve o seu pedido denegado. Uma decisão acertada pelo Des. Leandro Crispim, tendo em vista que restou evidenciado que a soltura do preso feriria a ordem pública, pois o mesmo poderia voltar às práticas criminosas (em sua casa foi encontrado CPU, celulares, pen-drives, os quais foram apreendidos, possuindo o armazenamento de conteúdo pornografico infantil).

A seguir, temos uma jurisprudência a respeito de fraude/phishing:

> DE NEXO CAUSAL. CULPA EXCLUSIVA DO CONSUMIDOR E DE TERCEIRO. EXCLUDENTE DE RESPONSABILIDADE. SENTENÇA MANTIDA. RECURSO CONHECIDO E DESPROVIDO. I. A responsabilidade civil objetiva prevista no Código de Defesa do Consumidor será excluída quando restar comprovada que, tendo prestado o serviço, o defeito inexiste, ou a culpa exclusiva do consumidor ou de terceiro, consoante dicção do artigo 14, parágrafo 3º, incisos I e II, do referido Diploma Legal. II. No caso demandado, aduz a parte autora, ora recorrente, que adquiriu, junto ao site da empresa ré, três Smart TV 50º Samsung, pelo valor de R$ 529,01 cada. Explica que, embora tenha efetuado o pagamento do boleto emitido, os produtos não foram entregues, motivo pelo qual intenta a presente demanda. III. Do conjunto probatório acostado aos autos, conclui-se que a parte autora foi vítima de golpe virtual efetuado por terceiros, intitulado phishing, que enviou boleto falso, simulando uma confirmação de compra, utilizando-se de endereço eletrônico fraudulento. IV. Assim, não demonstrado que a compra tenha sido efetivamente feita através do site da requerida, que teria recebido o pagamento e não entregado o produto, resta rompido o nexo de causalidade entre a suposta conduta lesiva e o dano sofrido, não merecendo reparos a sentença de improcedência. V. RECURSO CONHECIDO E DESPROVIDO. VI. Honorários de advogado no montante de dez por cento do valor da causa, com exigibilidade suspensa, na forma do artigo 98, inciso 3º do Código de Processo Civil.
> **(TJGO, PROCESSO CÍVEL E DO TRABALHO -> Recursos -> Recurso Inominado Cível 5303546-35.2020.8.09.0079, Rel. Jose Carlos Duarte, 3ª Turma Recursal dos Juizados Especiais, julgado em 14/03/2022, DJe de 14/03/2022)**

No presente caso, o autor da ação realizou a compra por meio de um website de 3 TV 's pelo valor de R$1.587,06, após o pagamento do boleto e decorrido o prazo de entrega, não recebeu o produto. Irresignado, ingressou com a ação a fim de requerer os seus direitos.

A empresa ré, não encontrou em seu banco de dados registro da compra, ora mencionado pelo autor, alegou ainda que os dados eram sigilosos em razão da lei nº 12.965/2014- Marco Civil da Internet e pela LGPD- Lei nº 13.709/2018, e só poderiam ser acessados por meio de decisão judicial.

Contudo, restou demonstrado que a autora foi vítima de fraude, não podendo ser a empresa requerida responsabilizada por ato de terceiro. Dessa forma, houve a excludente de responsabilidade da empresa sendo observando o CDC, tendo em vista, que a empresa não possui responsabilidade objetiva quando a culpa decorrer exclusivamente de terceiro.

CONCLUSÃO

A origem do presente tema, se deu com o advento da Internet. Inicialmente tratava-se de uma ferramenta militar e universitária. Posteriormente, tornou-se sinônimo de inclusão social e desenvolvimento na vida em sociedade e, ainda, possuir reflexos no quesito educação em um país. Contudo, apesar dos inúmeros benefícios que a internet nos trouxe, verificou-se alguns malefícios, isso porque, existem muitos criminosos agindo em oculto dentro da rede.

Por tratar-se de um tema recente, os crimes cibernéticos têm sido um importante tema de estudo, devido a necessidade de esclarecimento sobre o tema. Tendo em vista, que há alguns anos atrás, não existia legislação vigente sobre o tema, nem mesmo diretrizes a serem seguidas pelos usuários ou empresas disponíveis na Internet.

Dessa forma, na primeira seção buscou-se explicar sobre a origem da internet, como chegou ao Brasil e de que maneira foi disponibilizada a sociedade. Verificou-se que os índices de acesso à Internet têm crescido cada dia mais, mas ainda não alcançou toda a sociedade de forma uniforme, principalmente, as classes mais pobres que por não possuírem conhecimento ou recursos financeiros, continuam sem acesso a esse mecanismo.

Na segunda seção, pontuou-se sobre as legislações existentes no nosso ordenamento jurídico. Tendo com início a Lei 12.737/2012 (Lei Carolina Dieckmann), a primeira lei a tratar sobre crimes virtuais, abrindo espaço para o surgimento de várias leis seguintes. Tamanha relevância trouxe a presente lei, pois começou-se um processo de construção de pensamento, no sentido de delimitar direitos e deveres dentro do ambiente virtual, além estabelecer punições aos criminosos que antes acreditavam estarem completamente encobertos pelo anonimato.

Por fim, na terceira e última seção, houve a explanação sobre alguns mecanismos utilizados pelos criminosos a fim de alcançarem as vítimas. Entre os meios utilizados, a maior parte deles são os malwares (vírus), que são instalados

nos dispositivos dos usuários a agem silenciosamente, roubando dados pessoais, senhas, fotos e vídeos, com o principal intuito de se beneficiarem financeiramente.

Com isso, foi verificado que pouco ainda é falado sobre o tema, causando dúvidas até mesmo nos aplicadores do direito e, principalmente, nas vítimas que muitas vezes não sabem como se proteger no meio digital. O presente trabalho possui informações básicas à sociedade, mas muito importantes para que tenham ciência dos perigos existentes no meio digital e demonstra alguns meios que os criminosos têm utilizado.

O conhecimento é poder, e com isso, os usuários do meio digital devem estar cada vez mais atentos para realizarem uma navegação segura, cabendo ainda ao governo o investimento em políticas públicas para conscientizar a sociedade brasileira a fim de evitarem serem vítimas do presente crime, além disso, existem muitas lacunas na lei o que por diversas vezes inviabiliza o combate aos crimes cibernéticos.

REFERÊNCIAS

BRASIL. **Lei 12.965/2014. Estabelece princípios, garantias e deveres para o uso da Internet no Brasil.** Planalto. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 27/04/2023.

BRASIL. **Lei 14.155/2021.** Planalto. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm>. Acesso em: 29/04/2023

BRASIL. **Lei n. 12.737/2012. Dispõe sobre a tipificação criminal de delitos informáticos; Decreto-Lei nº 2.848, de 7 de dezembro de 1940- Código Penal; e dá outras providências.** Planalto. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 22/04/2023

TJGO, HABEAS CORPUS: 5578507-74.2018.8.09.0000, Relator Leandro Crispim. PROJUDI. 2019. Disponível em:<https://projudi.tjgo.jus.br/LogOn>. Acesso em: 17/05/2023.

TJGO, RECURSO INOMINADO: 5303546-35.2020.8.09.0079, Relator José Carlos Duarte. PROJUDI. 2022. Disponível em:<https://projudi.tjgo.jus.br/LogOn>. Acesso em: 17/05/2023

ABREU, Karen Cristina Kraemer. **História e usos da Internet.** BOCC–Biblioteca Online de Ciências da Comunicação, p. 1-9, 2009. Disponível em:<http://bocc.ufp.pt/pag/abreu-karen-historia-e-usos-da-internet.pdf>. Acesso em: 18/03/2023.

ALEXANDRE JÚNIOR, J. C. (2019). **Cibercrime: Um Estudo Acerca do Conceito de Crimes Informáticos.** Revista Eletrônica Da Faculdade De Direito De Franca, 14(1), 341–351. Disponível em: <http://revista.direitofranca.br/index.php/refdf/article/view/602>. Acesso em 23/03/2023

ANDREUCCI. Ricardo Antonio. **O crime de lavagem de dinheiro por meio da utilização de ativo virtual**. Empório do direito.com.br. 02/02/2023. Disponível em: <https://emporiododireito.com.br/leitura/o-crime-de-lavagem-de-dinheiro-por-meio-da-utilizacao-de-ativo-virtual#:~:text=O%20CRIME%20DE%20LAVAGEM%20DE%20DINHEIRO%20POR%20MEIO%20DA%20UTILIZA%C3%87%C3%83O%20DE%20ATIVO%20VIRTUAL,-Ricardo%20Antonio%20Andreucci&text=A%20nova%20Lei%20n.,algumas%20mudan%C3%A7as%20na%20Lei%20n.>. Acesso em: 06/04/2023.

BAR.Hugo. **Conheça os tipos de malware que podem roubar dados de sua empresa.** 07/10/2019. Disponível em: <https://tripla.com.br/conheca-os-tipos-de-malware/>. Data de Acesso: 05/04/2023.

BARBOSA, BRUNA GABRIELLY TEIXEIRA. **Criminalidade cibernética em tempos de pandemia no Brasil e o papel da responsabilidade civil no cenário atual.** Conteudo Juridico, Brasilia-DF: 28 nov 2022, 04:05. Disponível em:

<https://www.conteudojuridico.com.br/consulta/artigos/60254/criminalidade-ciberntica-em-tempos-de-pandemia-no-brasil-e-o-papel-da-responsabilidade-civil-no-cenrio-atual> Acesso em 03/05/2023.

Histórico da pandemia de COVID-19. OPAS. Disponível em: <%20de%20mar%C3%A7o%20de,e%20n%C3%A3o%20%C3%A0%20sua%20gravidade.> Acesso em: 02/05/2023.

COLONTONIO, Carlos Ogawa. **O ACESSO À INTERNET É UM DIREITO FUNDAMENTAL?.** Revista do Curso de Direito do Centro Universitário Brazcubas, v. 4, n. 1, p. 1-17, 2020. Disponível em: <https://revistas.brazcubas.br/index.php/revdubc/article/view/906>. Acesso em 08/04/2023

FRANÇA, Marlene Helena. **A responsabilidade civil e criminal na internet: o papel do judiciário brasileiro.** REVISTA QUAESTIO IURIS, v. 13, n. 01, p. 480-507, 2020. Disponível em: <https://www.e-publicacoes.uerj.br/index.php/quaestioiuris/article/view/41943> Acesso em: 23/03/2023

KLEINA. Nilton. **Como tudo começou: a história da internet no Brasil.** TecMundo. Data de Publicação: 01/05/2018. Disponível em: <https://www.tecmundo.com.br/mercado/129792-tudo-comecou-historia-internet-brasil-video.htm>. Acesso em: 23/03/2023

LATTO. Nica. **O que é e como funciona um vírus de computador?**. Academy. 12/2020. Disponível em: <https://www.avast.com/pt-br/c-computer-virus> Acesso em: 05/04/2023.

Legislação atual já pune cyberbullying e cyberstalking, diz advogada à CPI. Câmara dos Deputados. 03/03/2016.Disponível em: <https://www.camara.leg.br/noticias/482215-legislacao-atual-ja-pune-cyberbullying-e-cyberstalking-diz-advogada-a-cpi/> Acesso em: 06/04/2023.

MATTOS, Fernando Augusto Mansor de; CHAGAS, Gleison José do Nascimento. **Desafios para a inclusão digital no Brasil**. **Perspectivas em Ciência da Informação**, v. 13, p. 67-94, 2008. Disponível em: <https://doi.org/10.1590/S1413-99362008000100006>. Acesso em: 04/04/2023.

MONTEIRO, Luís. **A internet como meio de comunicação: possibilidades e limitações.** In: Congresso Brasileiro de Comunicação. 2001. Disponível em: <https://d1wqtxts1xzle7.cloudfront.net/57799090/Internet_como_meio_comunicacao-libre.pdf?1542574638=&response-content-disposition=inline%3B+filename%3DA_INTERNET_COMO_MEIO_DE_COMUNICACAO_POSS.pdf&Expires=1684162233&Signature=QVI5A-kE~SGZJvV0bIIWV2bPTcK45-KAXjcSbf7tBPbK3qAydx8riO4AfBZ7RZvlzB68uR4KLh6YRu17zb6egzogmowY5GM9tzo~dqR0i4dsjhadtVMok1lA6rJOFWu3MOJ8lEKVJJ5idYN3wu6fOgl-qOTaoNlMTcx3gpUi4I7rGaAYioBetRhGNT2HBV5STvoU7zeR0Ru31BZQZbxHIUed1k5lxf9J3JeFXv2RZJ6vhp~rcI0kEB5vwI0vpao4TCrFjnBk5Xtbu6yUVz5vNesQU7~qgltR7jLREL89YbM1lpzzeEguwYVF5Hrhkz1bT4PTHMlBoEsKA1Wo29kYWQ__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA> Acesso em 26/03/2023.

NATHANY. Morgana. **Proposta inclui na Constituição o direito de acesso à**

internet. Senado Notícias. Publicado em 13/03/2020. Disponível em: <https://www12.senado.leg.br/noticias/materias/2020/03/13/proposta-inclui-na-constituicao-o-direito-de-acesso-a-internet#:~:text=O%20acesso%20%C3%A0%20internet%20pode,quinta%2Dfeira%20(12)>. Acesso em: 08/04/2023

O QUE É "HACKING"?. PEOPLE. 2022. Disponível em: <https://www.people.com.br/noticias/informatica/o-que-e-hacking#:~:text=Podemos%20colocar%20que%20a%20palavra,funcionamento%20e%20realizar%20qualquer%20atividade.>. Acesso em: 05/04/2023.

Pornografia de vingança. TJDFT. 2020. Disponível em:<https://www.tjdft.jus.br/institucional/imprensa/campanhas-e-produtos/direito-facil/edicao-semanal/pornografia-de-vinganca>. Acesso em: 06/04/2023.

Rodrigues Rezende, L. V. y Rodrigues de Lima, M. (Marzo de 2016). **Governança na internet: um estudo sobre o Marco Civil brasileiro.** *Palabra Clave,* 19(1), 133-155. DOI: 10.5294/pacla.2016.19.1.6. Disponível em : <http://www.scielo.org.co/scielo.php?pid=S0122-82852016000100006&script=sci_arttext&tlng=pt> Acesso em 30/04/2023

RODRIGUES REZENDE, Laura Vilela; RODRIGUES DE LIMA, Meyrielle. **Governança na internet: um estudo sobre o Marco Civil brasileiro.** Palabra Clave, v. 19, n. 1, p. 133-155, 2016. Disponível em: <http://www.scielo.org.co/scielo.php?pid=S0122-82852016000100006&script=sci_arttext&tlng=pt>. Acesso em: Acesso em 30/04/2023

SARAIVA. Elton Geraldo Rocha. **Relação entre a cultura da internet e os crimes digitais**. Meu Artigo. 2022. Disponível em: <https://meuartigo.brasilescola.uol.com.br/atualidades/relacao-entre-a-cultura-da-internet-e-os-crimes-digitais.htm> Acesso em: 05/04/2023.

STIVANI. Mirella. **Os dez tipos de phishing mais comuns.** Techtudo. 03/06/2018. Disponível em: <https://www.techtudo.com.br/listas/2018/06/os-dez-tipos-de-phishing-mais-comuns.ghtml>. Acesso em: 05/04/2023.

VIEIRA. Isabela. **Brasil ocupa 72ª posição em ranking mundial de inclusão digital.** EBC. Publicação em: 31/07/2012. Disponível em: <https://memoria.ebc.com.br/tecnologia/2012/07/brasil-ocupa-72a-posicao-em-ranking-mundial-de-inclusao-digital>. Acesso em: 04/04/2023

Tabela 1

Antes da Alteração	Depois da Alteração
Art. 154-A- Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa. § 2º Aumenta-se a pena de um sexto a um terço se da invasão resultar prejuízo econômico. § 3º Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.	Art. 154-A- Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa. § 2º Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços) se da invasão resultar prejuízo econômico. §3º reclusão, de 2 (dois) a 5 (cinco) anos, e multa.
No capítulo VI- DO ESTELIONATO E OUTRAS FRAUDES Art. 155- Não havia o §4-C e nem os incisos I e II	Art. 155- acrescentou: § 4º-B. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, [...] § 4º-C. [...]considerada a relevância do resultado gravoso: I – aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional; II – aumenta-se de 1/3 (um terço) ao dobro, se o crime é praticado contra idoso ou vulnerável.
Art. 171- Não havia a Fraude eletrônica e nem o Estelionato contra idoso ou vulnerável	Art. 171- Fraude eletrônica §2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa [...] § 2º-B. A pena prevista no § 2º-A deste artigo, considerada a relevância do resultado gravoso, aumenta-se de 1/3 (um terço) a 2/3 (dois terços) [...] Estelionato contra idoso ou vulnerável § 4º A pena aumenta-se de 1/3 (um terço) ao dobro[...]
Art. 70, do Código de Processo Penal, não havia o § 4º	Art. 70- acrescentou o § 4º [...] quando praticados mediante depósito, mediante emissão de cheques sem suficiente provisão de fundos em poder do sacado ou com o pagamento frustrado ou mediante transferência de valores, a competência será definida pelo local do domicílio da vítima, e, em caso de pluralidade de vítimas, a competência firmar-se-á pela prevenção.”