



ANA LÍVIA CUNHA DE LIMA

**EFICÁCIA DAS LEIS 12.735 E 12.737 DE 2012 AO COMBATE DO CRIME
VIRTUAL**

**JI PARANÁ
2019**

ANA LÍVIA CUNHA DE LIMA

**EFICÁCIA DAS LEIS 12.735 E 12.737 DE 2012 AO COMBATE DO CRIME
VIRTUAL**

Artigo apresentado no Curso de Direito do Centro Universitário São Lucas 2019, como requisito para obtenção do título de Bacharel em Direito.

Orientador Professor. Hudson da Costa Pereira

JI PARANÁ

2019

Dados Internacionais de Catalogação na Publicação – CIP

L732e	Lima, Ana Livia Cunha de. Eficácia das leis 12.735 e 12.737 de 2012 ao combate do crime virtual / Ana Livia Cunha de Lima. – Ji-Paraná, 2019. 30p. Artigo Científico (Bacharelado). – Centro Universitário São Lucas, 2019. Orientação Prof. Hudson da Costa Pereira, Coordenação de Direito. 1. Direito 2. Direito Digital 3. Crime Virtual I. Título II. Pereira, Hudson da Costa. CDU: 34:004
-------	---

ANA LÍVIA CUNHA DE LIMA

**EFICÁCIA DAS LEIS 12.735 E 12.737 DE 2012 AO COMBATE DO CRIME
VIRTUAL**

Artigo apresentado à Banca Examinadora do
Centro Universitário São Lucas, como
requisito de aprovação para obtenção do
Título de Bacharel em Direito.
Orientador Prof. Hudson da Costa Pereira

Ji Paraná, 18 de novembro de 2019.

Avaliação/Nota: _____

BANCA EXAMINADORA

Professor Hudson da Costa Pereira

Centro Universitário São Lucas de Ji-Paraná:

Professora Kellyana Bezerra de Lima Veloso

Centro Universitário São Lucas de Ji-Paraná

Professor Oscar Francisco Alves Junior

Centro Universitário São Lucas de Ji-Paraná:

**JI PARANÁ
2019**

EFICÁCIA DAS LEIS 12.735 E 12.737 DE 2012 AO COMBATE DO CRIME VIRTUAL¹

Ana Livia Cunha de Lima²

RESUMO: O presente trabalho tem como objetivo apreciar as consequências diretas com a promulgação das Leis 12.735 e 12.737 de 2012 ao combate do crime virtual. Desse modo devemos compreender que a prática desse delito está influenciando diretamente a vida da sociedade moderna. Sendo assim, descrevermos uma abordagem técnica a nova legislação vigente e o estudo do seu contexto cultural, social e histórico. Constatando que a conduta de invadir dispositivo informático não era considerada crime e após a promulgação das Leis 12.735 e 12.737 de 2012 essas condutas passaram a ter uma tipificação específica. O presente estudo proporciona precipuamente, analisar o contexto dessas leis e das alterações no Código Penal Brasileiro.

Palavras-chave: Lei 12.735 e 12.737 de 2012. Crime virtual. Dispositivo informático. Código Penal Brasileiro.

EFFECTIVENESS OF LAWS 12.735 AND 12.737 OF 2012 ON CYBER CRIME FIGHTING

ABSTRACT: This paper aims to assess the direct consequences of the enactment of Laws 12.735 and 12.737 of 2012 to combat cyber crime. Thus we must understand that the practice of this crime is directly influencing the life of modern society. Thus, we describe a technical approach to the new legislation in force and the study of its cultural, social and historical context. Noting that the conduct of hacking a computer device was not considered a crime and after the promulgation of Laws 12.735 and 12.737 of 2012 these conducts began to have a specific typification. The present study provides precipitously, to analyze the context of these Laws and the alterations in the Brazilian Penal Code.

Keywords: Law 12,735 and 12,737 2012. Virtual Crime. Computer device. Brazilian Penal Code.

¹ Artigo apresentado no curso de graduação do curso de Direito do Centro Universitário São Lucas como requisito para conclusão do curso, sob orientação do professor Hudson da Costa Pereira. E-mail: hudson.pereira@saolucas.edu.br

² Graduanda do curso de Direito do Centro Universitário São Lucas, 2019 e-mail: analiviadelima@gmail.com

1 Introdução

Este trabalho de pesquisa através de um olhar sistêmico busca apreciar o desempenho das Leis 12.735³ e 12.737⁴ de 2012 diante da atuação do judiciário nacional perante as ações praticadas através do crime virtual.

Nos dizeres de Pierre Lévy “Um dos principais agentes de transformação das sociedades atuais é a técnica”. (LEVY,1998)⁵. Diante disto analisaremos que a evolução da comunicação está associada a prática de comunicar-se para alcançar a evolução.

A comunicação é o meio social que mais se destaca no âmbito evolutivo. Desde a criação da escrita e do alfabeto, o homem desenvolve maneiras de expandir cada vez mais a forma de comunicar-se.

Nos meios de comunicação que utilizamos: rádio, televisão, cartas, jornais e impressos. Iremos especificadamente neste trabalho, abordar o termo “digital”.

Com o avanço tecnológico da sociedade moderna, a comunicação e as trocas de informações vêm passando por inegáveis transformações.

Conforme o Centro de Pesquisas TIC Domicílios⁶ o crescente número de brasileiros que operam a internet através de qualquer outro aparelho além do celular cresceu de 67% para 70% da população o que equivale a 126,9 milhões de pessoas.

É de se notar que o expressivo uso dos aparelhos eletrônicos tornam-se crescente. Para entendermos melhor isso uma pesquisa realizada pela Revista Exame⁷ cita que o Brasil encontra-se no 4º lugar no *ranking* mundial de acesso a internet.

Desta forma podemos ter uma perspectiva clara e objetiva do quanto esse recurso vem aumentando e superando as expectativas de uma invenção que havia sido criada somente para obter a troca de comunicação auditiva. No entanto o uso de aparelhos eletrônicos veio crescendo e se atualizando para suprir outras necessidades do cotidiano.

³ Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências.

⁴ 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.

⁵ LÉVY, Pierre. As Tecnologias da Inteligência, pág.2. 1998

⁶ Revista G1. Disponível em: <<https://g1.globo.com/economia/tecnologia/noticia/2019/08/28/uso-da-internet-no-brasil-cresce-e-70percent-da-populacao-esta-conectada.ghtml>>

⁷ Disponível em: <https://exame.abril.com.br/tecnologia/brasil-e-o-4o-pais-em-numero-de-usuarios-de-internet/>,> acesso 21 de out de 2019.

No decorrer da evolução virtual o homem moderno adapta as suas necessidades e o que antigamente os únicos recursos de um aparelho eletrônico celular auditivos (envio de áudio) ou visuais (imagens ou escrita) torna-se progredido para o uso de grande relevância tais como transações bancárias, arquivo de dados e informações empresarias.

Em uma pesquisa realizada por Valente os números só aumentaram, no ano de 2012 a 2016, o uso de celular no Brasil subiu 3,5 vezes, passando de 14% em 2012 para 62% em 2016. No mundo, o aumento foi de 33,3% em 2012 para 70% em 2016. Ou seja, em apenas 04 (quatro) anos, a utilização de *smartphones* dobrou de tamanho em todo o planeta. Empresa Brasil de Comunicação, 18 de jan. de 2019⁸.

Segundo o diretor de Tecnologia da FEBRABAN⁹ (Federação Brasileira dos Bancos) Gustavo declara:

A opção pelo mobile ajudou a manter a tendência de alta no total de transações bancárias em todos os canais, que saltaram de 71,8 bilhões em 2017 para 78,9 bilhões, no ano passado. “A facilidade em poder resolver questões financeiras apenas utilizando o celular é um ponto-chave desse crescimento”, afirma. Ele acrescenta que o incremento de transações com movimentação financeira por mobile banking atesta que o cliente se sente cada vez mais seguro para movimentar seu dinheiro por esse canal¹⁰.

Em contrapartida atender as necessidades do cotidiano acaba-se por abrir um leque de possibilidades para a criação de novos crimes, tendo em vista que o legislativo não acompanha a crescente evolução informática dia a dia, consequentemente a prática desse crime virtual gera consequências jurídicas nas esferas penais e cíveis da legislação brasileira.

Um impacto desse avanço é a proliferação dos crimes virtuais. A denominação “crime virtual” foi adotada no presente artigo, pois a partir dessa nomenclatura iremos transcorrer diversas modalidades operadas através dos meios informáticos.

No campo do crime virtual uma série de delitos podem ocorrer tais como o furto de informações confidenciais e o acesso não autorizado a uma conta em um computador com o intuito de cometer fraude, causar dano e sabotagem. A manipulação eletrônica de dados atualmente se encontra ao alcance de todos através de um simples terminal de computador. Os programas de computadores

⁸ Disponível em: <http://agenciabrasil.ebc.com.br/geral/noticia/2019-01/brasil-foi-5o-pais-em-ranking-de-uso-diario-de-celulares-no-mundo> Acesso em 17 de agosto de 2019.

⁹ Federação Brasileira de Bancos.

¹⁰ Disponível em <https://portal.febraban.org.br/noticia/3301/pt-br/> acesso 12 de nov 2019.

possuem uma interface de comunicação amigável com o usuário, possibilitando uma rápida interação homem-máquina.

Conforme o Recurso Ordinário em Habeas Corpus¹¹, interposto contra acórdão da Quinta Turma do Superior Tribunal de Justiça, relator Ministro Alexandre de Moraes.¹²

A denúncia imputa ao recorrente a suposta prática dos crimes de organização criminosa (art. 2º, §3º, da Lei n. 12.850/13) e furto qualificado (art. 155, §4º, II e IV, do Código Penal), por três vezes. Conforme a inicial acusatória, LUIZ HENRIQUE, vulgo RICK RIBEIRO, é identificado em conversas pelo SKYPE pelo nickname STRIKER e STK, atuando na função de HACKER. Utilizava seus conhecimentos em tecnologia da informação e uma rede de "CABEÇAS", "LAVADORES", "LIGADORES", "LARANJAS" e outros colaboradores, para desviar valores de contas bancárias de todo o Brasil.

Observamos que o hacker com habilidades técnicas que opera através de um dispositivo eletrônico causa um prejuízo ao bem patrimonial de terceiros.

Um terminal de um computador pode ser invadido em um banco na Inglaterra produzindo um resultado fraudulento em uma filial de um banco na França.

Não existem barreiras físicas no campo da informática!

Para que a Ciência do Direito possa vencer o desafio e regulamentar tais delitos é preciso identificar os diversos aspectos jurídicos do crime informático. Os aspectos gerais dos crimes informáticos englobam a identificação das particularidades de tais crimes e as dificuldades existentes em relação ao meio físico.

É preciso também identificar o bem jurídico que se pretende proteger: informação, privacidade, integridade do sistema de computador, caráter sigiloso das informações, bens materiais e valores.

O objetivo do estudo é apresentar o entendimento jurisprudencial e legislativo acerca da matéria abordada, verificando se a lei existente está no nível de evolução da criminalização virtual, e de que forma ela ajudará o Estado na construção de uma sociedade livre, justa e solidária segundo os comandos constitucionais de maneira eficaz, no que se espera dentro de um modelo de Estado Social e Democrático de Direito.

¹¹ Número Único: 0339812-89.2018.3.00.0000. Disponível em <http://portal.stf.jus.br/processos/detalhe.asp?incidente=5702830>

¹² Alexandre de Moraes . Nascido em São Paulo, 13 de dezembro de 1968. Jurista. Mmagistrado e ex-político brasileiro. atual ministro do Supremo Tribunal Federal (STF).

Para que possamos obter o resultado desejado no estudo, empregaremos o método histórico, dedutivo da ciência jurídica, cuja operação se fará por meio do procedimento técnico baseando-se na legislação e jurisprudência. Devemos relacionar primariamente uma análise explicativa sobre o a função da internet, sua história e no decorrer do estudo, fazer um autoexame da legislação atual, até chegarmos ao foco principal do trabalho, eficácia das leis ao combate do crime virtual.

1.1 O Ciberespaço

Perante aos avanços da tecnologia no século XXI os crimes praticadas no ambiente virtuais acabam equivalendo-se a aos crimes comuns, afinal hoje a informatização está em alta velocidade que acaba transformando a cultura da sociedade moderna, o que nos faz acompanhar os passos de um novo lançamento tecnológico. O ser humano em sua zona de conforto almeja a praticidade como uma característica muito importante de sobrevivência e através dos recursos tecnológico obtemos essa praticidade, sendo assim a tecnologia nos traz o mecanismo mais útil até agora para o homem primata: a *internet*¹³.

Através desse mecanismo hoje passamos a operar diversas funções. A praticidade é tamanha que antigamente movimentos que eram feitos de forma artesanal hoje com um simples toque se antecipa várias ações.

No ano de 1969 a Agência de Projetos de Pesquisa Avançada do Governo Americano iniciou um projeto onde a *ARPANET* mostrou que a rede de interações entre os computadores era eficaz, foi esse o marco inicial para a estratégia de incentivo a pesquisa¹⁴.

Através de um projeto militar os Estados Unidos da América, iniciou um sistema descentralizado e independente para que durante a Guerra Fria a comunicação de seus agentes: cientistas, engenheiros e militares não fossem acessados por *hackers* de outros países¹⁵. (Network Brasil, Terra, 2011).

O objetivo dos militares era que a internet pudesse interligar a comunicação, repassando aos demais generais as ordens de comando para os devidos

¹³ A Internet é um sistema global de redes de computadores interligadas que utilizam um conjunto próprio de protocolos com o propósito de servir progressivamente usuários no mundo inteiro

¹⁴ Gláucia da Silva Brito e Inonélia da Purificação. Livro Educação e as Novas Tecnologias, pág. 101. 2ª edição 2006.

¹⁵ Disponível em < <http://tecnologia.terra.com.br/internet10anos/interna/0,,OI541817-EI5026,00.html>>

bombardeios, e que esse conceito não fosse descoberto nem destruído, tendo assim militares específicos e capacitados com o sistema operacional para aquela época, o que gerou nos dias de hoje, como um grande avanço na tecnologia.

O nome oficial “internet” teve sua origem a partir da separação entre as operações após o final da Guerra Fria, surgindo aplicações operacionais de comunicação para as áreas civis além das militares.

De acordo com Frias aproximadamente por duas décadas o uso da internet foi restrito somente para pesquisas acadêmico-científica sendo liberado nos estados unidos no ano de 1987 para uso comercial (FOLHA DE SÃO PAULO, 2001).¹⁶

No território brasileiro no ano de 1990, o Ministério da Ciência e Tecnologia lança pela Rede Nacional de Pesquisas, a rede acadêmica. Com a finalidade de gerenciar estudos tecnológicos.

Após 02 (dois) anos, a internet é interligada a faculdades de renome nacional e centro de pesquisas, além de organizações e também a algumas não governamentais.

A internet criou um novo mecanismo de relacionamento (CORRÊA, 2000). Computadores e internet passam a se conectar gerando a facilidade de comunicação de uma e outra ou de vários outros computadores conectados na rede, esse mecanismo de informações e transferência de arquivo. O devido avanço tecnológico faz com que o seu uso ultrapasse os limites de comodidade e eficiência para seus usuários. O acesso frequente a rede de dados ou acesso a um terminal bancário através de um aparelho móvel que tenha capacidade técnica operacional, gera grande ações ou operações, um exemplo muito comum que fazemos através do celular é a compra virtual, onde se insere os dados pessoais e bancários, gerando um cadastro digital. Ou também, transferência bancárias, todos esses exemplos utilizam a ferramenta internet, causa impactos no âmbito do direito.

Conforme Henrique Gandelman a *internet* interligou grandes e pequenos computadores pelo mundo todo. (GANDELMAN, 1997). A *internet* tornou-se um grande marco revolucionário mundial passou a ter uma fascinante história de evolução e conquista no espaço econômico e social após sua grande “mutação”.

1.2 A influência da Internet no mundo real

¹⁶ Folha de São Paulo. Domingo, 12 de agosto de 201. Disponível em <
<https://www1.folha.uol.com.br/fsp/cotidian/ff1208200103.htm>>

Devemos entender que os delitos praticados pelo sistema informático são de natureza formal, pois se consumam no ato da conduta, independente do resultado.

Com o crescente acesso a internet, os crimes virtuais vêm aumentando no Brasil, de acordo com DataSafer Brasil (2019)¹⁷, 1.410.648 (um milhão quatrocentos e dez mil, seiscentos e quarenta e oito) processos foram recebidos pela polícia federal, envolvendo exclusivamente crimes referente a pornografia infantil no ano de 2018.

Não existe um termo específico para a doutrina brasileira sobre qual é a nomenclatura que devemos utilizar no caso dos crimes praticados através do dispositivo eletrônico sendo assim, hoje nos referimos de diversas formas: “crime virtual”; “crime digital”; “cibercrime”; “crimes da internet”. Algumas são mais abordadas pelos operadores de direito do que as outras, porém não existe diferenciação entre o termo.

Segundo o jurista Vicente de Paula Rodrigues Maggio¹⁸ este faz uma classificação acerca do crime virtual. *In verbis*:

Trata-se de crime comum (aquele que pode ser praticado por qualquer pessoa), plurissubsistente (costuma se realizar por meio de vários atos), comissivo (decorre de uma atividade positiva do agente: “invadir”, “instalar”) e, excepcionalmente, comissivo por omissão (quando o resultado deveria ser impedido pelos garantes – art. 13, § 2º, do CP), de forma vinculada (somente pode ser cometido pelos meios de execução descritos no tipo penal) ou de forma livre (pode ser cometido por qualquer meio de execução), conforme o caso, formal (se consuma sem a produção do resultado naturalístico, embora ele possa ocorrer), instantâneo (a consumação não se prolonga no tempo), monossujeivo (pode ser praticado por um único agente), simples (atinge um único bem jurídico, a inviolabilidade da intimidade e da vida privada da vítima)¹⁹.

Fala-se muito no termo cibernético, mas sabemos realmente o significado de tal vocábulo? Antes de abordarmos esse significado, vamos compreender como funciona o sistema de processamento, transmissão e coleta de informações no meio digital.

¹⁷ Disponível em < <http://indicadores.safernet.org.br/> > acesso em: 23 de setembro de 2019.

¹⁸ Advogado militante formado pela UnG; mestre em direito pelo Mackenzie e doutor em direito penal pela PUC-SP. Professor de direito penal e processo penal em cursos de graduação e pós-graduação. Avaliador de cursos de direito pelo MEC (pertence ao Banco de Avaliadores do Sinaes (BASIS)).

¹⁹ Disponível em <https://vicentemaggio.jusbrasil.com.br/artigos/121942478/novo-crime-invasao-de-dispositivo-informatico-cp-art-154-a> acesso em 22 de out de 2019.

Nas palavras de CHIAVENATO, 2002²⁰: “a informática é a disciplina que lida com o tratamento racional e sistemático da informação por meios automáticos e eletrônicos”

Criado pelo cientista *Karl Steinbuch* a palavra informática é derivada do termo alemão “*informatika*”.

Assim: informática = informação + automática (trata-se, aliás, do mesmo jogo de palavras que gerou a palavra automação). Ou utilizando expressão decorrente da comunicação virtual.

A internet é o meio de comunicação mais eficaz sua criação tomou proporções globais. Esse recurso de comunicação facilita a troca de informações gerando elos através das redes.

As máquinas estão a cada passo conquistando mais a confiança do homem e os dispositivos eletrônicos passam a executar tarefas de extrema importância, a informática e a internet passam a ser bens imprescindíveis para a sociedade. Outro exemplo do uso da tecnologia no Brasil é a partir do ano de 1996, quando oficialmente iniciou o uso das urnas eletrônicas²¹. Os benefícios que a sociedade passou a ter como: celeridade, transparência e organização, evitando os enormes arquivos.

Porém, mesmo com grandes benefícios para a sociedade moderna, a mesma também sofre com o mau uso, pessoas se aproveitam dessa ferramenta para o crime. Crimes que a cada instante passam a ser aprimorados.

No ano de 1960, quando a internet começou a ser descoberta, surgem os indícios de manipulação e sabotagem através de tal ferramenta.

Em 1970 a figura do *hacker* passa a ser temido gerando os crimes de pirataria, invasão de *softwares* e pedofilia, através da rede de informações tornando em 1980 uma epidemia de crime virtual.

Com a popularização do computador o mundo começou a assistir no início da década de 90 a uma verdadeira revolução dos costumes as máquinas invadiam cada vez mais os lares das famílias de todo o planeta. Em paralelo e como decorrência deste fenômeno a internet experimentava um gigantesco avanço. Com a

²⁰ Idalberto Chiavenato. Mestre e Doutor em Administração de Empresas pela City University of Los Angeles, California (EUA). Livro Teoria Geral da Administração. 6ª edição.

²¹ Guia 501 Curiosidades Históricas Ed.02. Por On Line Editora, Curiosidades On Line Editora, História On Line Editora. Pág 78. Disponível em https://books.google.com.br/books?id=_ndGDgAAQBAJ&printsec=frontcover&hl=pt-BR#v=onepage&q&f=false

chegada do fim do milênio as pessoas de todas as classes e lugares estão cada dia mais próximas dessas tecnologias e cada vez mais acessam a grande rede virtual através de computadores instalados em suas casas e no trabalho. Termos como *Peer to peer*, *homebanking*, *e-mail*, *e-commerce*, *network* passam a ser ouvidos, lidos e empregados com mais frequência.

Segundo Wendt e Jorge, no Brasil o uso da internet teve início como meio de comunicação entre as universidades, dando início ao surgimento mundial.

[...] a primeira rede conectada à internet interligava as principais universidades brasileiras. Diferentemente da internet dos dias atuais, não existia interface gráfica, [...] Porém, no ano de 1995 passaram a disponibilizar o uso comercial da internet no país [...] Neste mesmo ano ocorreu a criação do Comitê Gestor da Internet no Brasil (CGI-BR), com a finalidade de “coordenar e integrar todas as iniciativas de serviços de internet no país, promovendo a qualidade técnica, a inovação e a disseminação dos serviços ofertados” (WENDT, 2012, p.09)

Um panorama de crescimento e desenvolvimento com um futuro tão promissor atrai investimentos de muitos milhões de dólares para o ramo, assim como atrai indivíduos com intenções desonestas, voltados para lesar clientes, usuários, provedores e investidores, fraudando, roubando e mentindo com fins escusos e prejudiciais para aqueles que se utilizam ou fazem parte deste mercado. Lojas virtuais, instituições bancárias, usuários domésticos, todos já foram vítimas de golpes e crimes por computador, ou conhecem inúmeros exemplos deles. Estes crimes atingem o cidadão e as organizações, diariamente, e ocorrem desde a simples compra de um equipamento, quando os consumidores são enganados na qualidade e no preço, até fraudes no valor de milhões de dólares ou ações de *hackers*, que invadem sistemas de alta segurança dos países mais avançados do mundo, como *cyberguerras* que vem sendo travadas silenciosamente, longe dos olhos da sociedade.

Atualmente, sofremos grandemente com esses ataques, recentemente uma declaração da empresa de segurança cibernética *Fortinet*²² declarou o seguinte:

O Brasil sofreu **15 bilhões** de tentativas de ataque cibernético em apenas 3 meses. O levantamento foi feito usando dados de clientes da companhia no país e, também, fornecidos por entidades de classe. Segundo a Fortinet, o Brasil continua sendo um alvo mundial importante para cibercriminosos, que escolhem sistemas ainda não corrigidos ou atualizados em empresas no país. O modo de operar é semelhante ao de ataques antigos, como os ocorridos em 2017 pelo ransomware WannaCry (que jogou boa parte do

²² A Fortinet é uma empresa multinacional da Califórnia, com sede em Sunnyvale, Santa Clara, que desenvolve e comercializa software, produtos e serviços de cibersegurança, como firewalls, antivírus, prevenção de intrusão e segurança de dispositivos de usuários, entre outros.

mundo em um caos enorme) e os que violaram o Banco do Chile e o mexicano Bancomext em 2018 (obra de hackers norte-coreanos).

Há alguns anos a preocupação com a internet vem aumentando, pois são muitas ações através desse mecanismo, infelizmente não temos como descaracterizar as ações que o indivíduo irá tomar podendo ser elas: lícitas ou ilícitas.

1.3 A evolução do direito positivo

O referido artigo tem a específica missão de nos esclarecer quais são os direitos que o Estado Democrático nos guarda.

Conforme o artigo 5º, inciso X da Constituição Federal de 1988: “São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurando o direito a indenização pelo dano material ou moral decorrente de sua violação.

No entendimento de Nery Junior e Rosa Maria de Andrade Nery, “Ofensas contra a honra, contra a liberdade ou a intimidade das pessoas, enseja em ação de indenização de dano moral”.²³

Desta forma, para que se obtenha uma efetiva conduta por parte do Estado Democrático de Direito o referido inciso, irá tratar de princípio regente, sendo a missão deste, proteger a dignidade da pessoa humana.

O Princípio da Dignidade da Pessoa²⁴ Humana defende que é um direito inerente e inalienável. Portanto, é dever do Estado zelar pelo direito à imagem e a intimidade do cidadão.

Trazendo essas defesas ao direito do cidadão brasileiro, embasado de conceitos, princípios e artigos. Como o judiciário brasileiro defenderá a dignidade da pessoa humana perante essa nova ótica criminal? Haja vista que devemos mencionar que mesmo sendo tão jovem, a nossa Carta Magna não acompanhou o processo de atualização aos crimes virtuais.

Salientamos que o Código Penal brasileiro foi criado no ano de 1940²⁵, tendo como o meio mais tecnológico da época o rádio, sendo assim podemos ter

²³ NERY JÚNIOR, Nelson; NERY, Rosa Maria de Andrade. 11. ed. São Paulo: Editora Revista dos Tribunais, 2010

²⁴ Artigo 1º, III da Constituição Federal de 1988. CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA DO BRASIL DE 1988 . Disponível em http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm

²⁵ DECRETO-LEI Nº 2.848, DE 7 DE DEZEMBRO DE 1940.

claramente uma percepção de que as leis não acompanharam o desenvolvimento tecnológico.

Conforme a Constituição Federal em seu artigo 5º inciso XXXIX: “não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal”. Por meio dessa previsão pode-se dizer que tudo o que não estiver expressamente proibido, é lícito em direito penal.

Este princípio tem seus primeiros passos na Declaração dos Direitos do Homem e do Cidadão de 1789²⁶, onde estabeleceu a transição entre Estado de Polícia e Estado de Direito. Passando assim a oferecer garantia jurídica a todos os filhos dessa nação.

Diante do Princípio da Legalidade²⁷ o Estado tem que ter um efetivo dever de punir sendo assim o legislativo deve observar a evolução social, para poder criar normas incriminadoras. O princípio defende que se o fato não pode ser considerado crime sem que exista uma lei o tipificando.

Sendo assim, abordaremos a partir de agora um novo olhar para os atos cometidos no universo virtual. Atos esses que conforme as leis a seguir se enquadram e tornam-se crimes.

1.4 A história das Leis 12.735 e 12.737 de 2012.

Para que possamos compreender mais sobre os crimes cibernéticos, tomaremos ciência de que essa abordagem jurídica aos crimes de informática, circulam no sistema legislativo a uma década. Portanto, iremos adentrar na história da Lei 12.735 e 12.737 de 2012.

1.4.1 Comentários da elaboração da Lei 12.735 de 2012 ²⁸

De iniciativa do Deputado Cassio Cunha Lima, em seu PL nº 1.713/96²⁹, que dispõe: sobre o acesso, a responsabilidade e os crimes cometidos nas redes integradas de computadores. Porém, esse projeto sofreu uma minuta do substitutivo

²⁶ A Declaração dos Direitos do Homem e do Cidadão é um documento culminante da Revolução Francesa, que define os direitos individuais e coletivos dos homens como universais. 26 de agosto de 1789. Assembleia Nacional Constituinte Francesa

²⁷ Artigo. 5º, inciso II, da Constituição Federal, “ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei”. ... Por isso o princípio da legalidade é verdadeiramente uma garantia dada pela Constituição Federal a todo e qualquer particular

²⁸ Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências

²⁹ Diário da Câmara dos Deputados. Terça-feira 11 de maio de 1999. Pág. 19976. Imagem disponível em <http://imagem.camara.gov.br/Imagem/d/pdf/DCD0019990511000820000.PDF#page=57>

ocorreu que por falta de tempo suficiente o substitutivo não foi devidamente apreciado. Razão pela qual o PL 1.713/96 foi arquivado.

O Deputado Luiz Piauhyllino desse modo fazendo uso do referido projeto de lei nº 1.713/96 que havia sido arquivado, abordou em sua justificativa para aprovação do projeto de lei nº 84, de 1999 explanado:

“Não podemos permitir que pela falta de lei, que regule os crimes de informática, pessoas inescrupulosas continuem usando computadores e suas redes para propósitos escusos e criminosos. Dai a necessidade de uma lei que, defina os crimes cometidos na rede de informática e suas respectivas penas³⁰.

O PL nº 84/1999 tramitou com suas listas de substitutivos apresentados no Senado Federal à Comissão de Ciência e Tecnologia, Comunicação e Informática; Segurança Pública e Combate ao Crime Organizado.

Despachado pelo Relator Deputado Eduardo Azeredo, no dia 24 de maio de 2011 o mesmo votou pela aprovação do Substitutivo do Senado Federal³¹.

Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), o Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), a Lei nº 7.716, de 5 de janeiro de 1989, a Lei nº 8.069, de 13 de julho de 1990, e a Lei nº 10.446, de 8 de maio de 2002, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, de rede de computadores, ou que sejam praticadas contra dispositivos de comunicação ou sistemas informatizados e similares, e dá outras providências.

Sendo Transformado no dia 30.11.2012, em Lei Ordinária 12.735 de 2012 ³², onde se caracteriza como crime informático ou virtual os ataques praticados por "*hackers*" e "*crackers*", em especial as alterações de "*home pages*" e a utilização indevida de senhas.

1.4.2 Comentários da elaboração da Lei 12.737 de 2012

A Lei 12.737 de 2012 conhecida hoje nacionalmente pela mídia como Lei Carolina Dieckmann.

Ocasionou da situação 36 (trinta e seis) fotos íntimas da atriz que foram publicadas na internet no dia 07 (sete) de maio de 2012.

³⁰ Diário da Câmara dos Deputados. Terça feira 11 de maio de 1999. Pág 19976. Imagem disponível em <http://imagem.camara.gov.br/Imagem/d/pdf/DCD0019990511000820000.PDF#page=57>

³¹ Consulta disponível em <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=15028>

³² DOU 03/12/12, Mesa Diretora da Câmara dos Deputados. Vetado parcialmente. Razões do veto: MSC 525/12-PE. DOU 03/12/12 PÁG 09 COL 03

Carolina Dieckmann procurou a polícia no dia 7 de maio, data do início das investigações comandadas pelo delegado Gilson Perdigão. Trinta e seis fotos pessoais da atriz foram publicadas na internet três dias antes, inclusive imagens ao lado do filho de quatro anos, o que, segundo o advogado dela, Antonio Carlos de Almeida Castro, o Kakay, “agrava de forma substancial o crime”. A atriz recebeu ameaças de extorsão desde o fim de março, mas disse que não havia registrado queixa antes para evitar mais exposição. Na delegacia, contou que estava tendo problemas nas suas contas em sites de relacionamentos desde o ano passado. Contou também que a empregada atendeu o telefonema de um homem que dizia ter fotos dela. Em seguida, o hacker teria enviado duas imagens por e-mail para o empresário de Carolina, por meio da conta vempopapai200101@hotmail.com. Para não as divulgar, pediu R\$ 10 mil (G1, São Paulo, 2012)³³

Transcorrendo uma repercussão nacional por não existir uma legislação específica para determinada situação. O plenário da Câmara dos Deputados aprovou o projeto de lei n. 2793/2011.

O Projeto de Lei nº 2.793/2011³⁴, de seus autores: Paulo Teixeira - PT/SP, Luiza Erundina - PSB/SP, Manuela D'Ávila - PCdoB/RS, apresentado no dia 29 (vinte e nove) de novembro de 2011, no Senado Federal, em que defendem em sua justificativa para aprovação:

Nossa proposta observa, ainda, os direitos e garantias do cidadão que utiliza a Internet, nos termos propostos pelo já mencionado PL 2.126/2010, em tramitação nesta Câmara dos Deputados. Em nosso entendimento, a aprovação deste Projeto deve ser precedida da aprovação do Marco Civil da Internet. Não se deve admitir que legislações penais infelizmente, um mal necessário em nossa sociedade precedam o estabelecimento de direitos e garantias. A face repressiva do Estado não deve sobressair sobre seu papel como fiador máximo dos direitos do cidadão. Em sua redação, buscamos evitar incorrer nos mesmos erros do PL 84/1999. O Projeto propõe, sim, a criação de tipos penais aplicáveis a condutas praticadas na Internet, mas apenas aquelas estritamente necessárias à repressão daquelas atividades socialmente reconhecidas como ilegítimas e graves. Vejamos algumas diferenças entre este Projeto e o PL 84/1999. Em primeiro lugar, destaca-se que o presente projeto trata apenas de tipificações penais. Diferentemente do PL 84/99, não se abordam as questões relativas a guarda e fornecimento de registros, ou demais obrigações imputáveis a provedores de serviços de internet - questões que encontram lugar mais adequado numa regulamentação civil sobre a matéria. Em segundo lugar, cabe notar que a presente proposta apresenta um número de tipos penal significativamente inferior àquele apresentado pelo PL 84/99. Norteamo-nos, nesta escolha, pela compreensão de que grande parte das condutas relativas praticadas por meios eletrônicos já se encontra passível de punição pelo ordenamento jurídico pátrio. Ainda, pautamo-nos pela visão de que não é a proliferação de tipos penais que levará à maior repressão de condutas.

A referida lei tipifica principalmente o “crime de invasão de dispositivo informático”. Sendo este encaminhado para análise do Senado, pois na data de 06

³³ Disponível em <http://g1.globo.com/pop-arte/noticia/2012/05/carolina-dieckmann-fala-pela-1-vez-sobre-roubo-de-fotos-intimas.html>

³⁴ Câmara dos Deputados. Disponível em <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=529011>

(seis) de novembro de 2012, foi proposto à apreciação do Plenário, através do Regime de Tramitação de Urgência. E no dia 04 de dezembro de 2012 o Plenário comunica a Presidenta da República:

A sanção do Projeto de Lei que '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' e restitui, para o arquivo do Congresso Nacional, dois autógrafos do texto ora convertido na Lei nº 12.737, de 30 de novembro de 2012".

Após tamanha repercussão as Leis nº 12.735/12 e 12.737/12 foram promulgadas, onde a primeira altera o Código Penal, Código Penal Militar e a Lei de Preconceitos, tipificando condutas mediante uso de sistemas eletrônicos e digitais contra sistemas informatizados;

LEI Nº 12.735 - Art. 1º Esta Lei altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei no 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei no 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências.(...)Art. 4º Os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado. Artigo 5º O inciso II do § 3o do art. 20 da Lei nº 7.716, de 5 de janeiro de 1989, passa a vigorar com a seguinte redação:(...)II - a cessação das respectivas transmissões radiofônicas, televisivas, eletrônicas ou da publicação por qualquer meio.

E a segunda lei nº 12.737, de 30 de novembro de 2012, que passou a dispor sobre a tipificação de delitos informáticos e alterou o Código Penal, sendo conhecida informalmente como “Lei Carolina Dieckmann”

Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:

Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.

§ 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.

§ 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.

§ 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:

Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.

§ 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidas.

§ 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.

Diante dessa alteração do Código Penal, o artigo 154 – A possui o objetivo de combater a prática do delito danoso que se trata especificadamente do ato de que o agente ativo “invade” o dispositivo eletrônico do agente passivo. A partir dessas informações adicionadas no código penal brasileiro, essas ações tornam-se mais claras e objetivas.

Continuando o seguimento do artigo 154-A do código penal o legislador tomou a apropriada atenção nesse artigo ao se posicionar perante a conexão ou não da rede, portanto computadores conectados ou não a rede web de computadores podem ser objeto de crime virtual.

O sujeito ativo para alcançar o seu propósito de obter, corromper ou destruir dados ou informações, precisa anteriormente violar, invadir, transgredir o dispositivo alheio para que este seja tipificado na conduta do referido artigo. Sendo que não necessariamente estes devam estar ligados à rede de internet.

Ao relembrar o caso da atriz global Carolina Dieckmann o sujeito ativo através do ato de chantagear para com a finalidade de obter recurso financeiro com as fotos íntimas da atriz, esse tipo é qualificado pelo parágrafo 1º, produzir, oferecer, distribuir, vender ou difundir dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput do artigo 154 –A.

Continuando a análise dos demais parágrafos 2ª ao 5ª do artigo 154-A do código penal, alterado pela Lei 12.737 de 2012, eles preveem as formas de qualificação obtida pelo resultado. Verificando-se a configuração de que a invasão do dispositivo informático relacionou-se para a obtenção de informações privadas que contenham conteúdos comerciais, sigilosos, industriais. A pena será de clausura de seis meses a dois anos, e multa.

Todavia, se dessas referidas operações ainda exista a divulgação, comércio ou transferência a terceiros dos dados obtido. A pena será aumentada de um a dois terços.

Diante da qualificação de invasão de dispositivos informáticos para obter informações restritas temos a pena de reclusão de seis meses a dois anos e multa, logo após descrevemos que a pena será aumentada de um a dois terços em que essa conduta delitiva tenha a finalidade de comercialização ou transmissão para terceiros dos dados obtidos. Aumentando de um terço ou até a metade se diante dessas ações acima explicadas, o agente passivo seja: o Presidente da República, governantes e prefeito municipal, Presidente do STF, o da Câmara dos Deputados e Senador, o da Assembleia Legislativa, o presidente da Câmara Legislativa do Distrito Federal e Municipal e contra pessoas que possuam “cargos máximos” da Administração Pública direta e indireta, seja qual for à posição.

1.5 Da Ação Penal

A natureza da ação penal praticada diante da invasão de dispositivo informático compreende-se que está configurado como crime virtual ou crime de informática afinal veste anteriormente a legislação brasileira não possui uma nomenclatura específica, sendo assim, qualquer termo que leve ao conceito da esfera informática, compreende-se como crime no âmbito virtual.

Para a definição da natureza dessa ação penal, o legislador aplica a “ação penal pública condicionada à representação”, visto que a vítima deve autorizar expressamente para a autoridade policial que desejar realizar a investigação em razão que o membro do *Parquet* inicia a persecução penal, conseqüentemente é de interesse particular da vítima uma investigação criminal.

Nos casos em que a vítima é a Administração Pública, direta ou indireta, a ação penal não será pública condicionada à representação, mas sim pública incondicionada.

Aos dizeres do Ministro Raul Araújo. ³⁵“A justiça está em constante atenção perante os direitos das pessoas. Aos agentes que pensam estar encobertos pelo anonimato, estes estão equivocados e deverão ser responsabilizados por suas práticas”.

³⁵ Disponível em: <http://www.stf.jus.br/portal/diarioJustica/verDiarioAtual.asp>. Acesso em 01 de nov de 2019.

Em atenção aos crimes cibernéticos, analisaremos um julgado recente pelo Ministro Reynaldo Soares da Fonseca (HABEAS CORPUS Nº 540.168 - DF (2019/0311522-4))³⁶. Dos fatos do HABEAS CORPUS, no dia 19 de setembro de 2019, o paciente foi preso temporariamente, no curso da Operação *Spoofing*, pelo suposto envolvimento na formação de organizações criminosas destinadas a prática de crimes cibernéticos contra autoridade pública a Deputada Federal Joice Hasselmann, através do aplicativo *Telegram*. Como podemos observar o agente ativo através dos dispositivos eletrônicos invadiu as contas de terceiros para acessar as informações e posteriormente vende-las ao jornalista Glenn Greenwald.

Comentando os atos da operação *Spoofing* podemos primeiro observar que ato de invadir “dispositivo eletrônico” está elencado no artigo 1º da Lei 12.735 de 2012 tipificando como conduta realizada mediante o uso de sistema eletrônico, digital ou similar. A segunda análise é o sujeito passivo do crime virtual a Deputada Federal Joice Hasselmann, protegido de acordo com o §5º do artigo 154 - A do Código Penal, a pena aumenta-se de um terço à metade.

Com esses acontecimentos jurídicos podemos apreciar que as Leis 12.735 e 12.737 de 2012 e suas respectivas alterações no código penal geram passos igualitário pela justiça do cidadão, através dela identificamos as ações perpetradas pelos criminosos e as tipificamos como crime virtual.

Temos então a constatação de um passo evolutivo da justiça brasileira, com as Leis 12.735 e 12.737 de 2012 nessa “era cibernética”. A internet não é um mundo sem lei.

É de grande importância a classificação dos crimes informáticos, uma vez que o legislador possa elaborar penas ou normas eficazes para cada caso proposto, por isso é imprescindível estudos dos delitos de informática (COSTA 2011)

Viana e Felipe Machado conceituam que a simples utilização do agente por um dispositivo eletrônico; o computador para a execução de um delito, não configura crime informático, caso o direito afetado não seja a informação automatizada (Crimes informáticos, 2013, pág. 30). Já por outro lado, temos diversos autores que por analogia, denominaram que a serventia do computador para meio de instrumento para a prática do delito é considerada como crime virtual.

³⁶ HC 540168(2019/0311522-4 - 21/10/2019) Disponível em <https://ww2.stj.jus.br/processo/pesquisa/?tipoPesquisa=tipoPesquisaNumeroUnico&termo=03115223020193000000&totalRegistrosPorPagina=40&aplicacao=processos>. Acesso em 01 de nov de 2019.

Conforme aborda Stair (1998) quando se pratica o crime ao se utilizar o computador pode se observar uma dupla natureza, visto que o computador pode ser utilizado como ferramenta ou objeto para cometer o crime virtual. A partir desta concepção Vianna interpreta as diversas classificações do crime que podem ser cometidos através do dispositivo informático. Ora quando o bem jurídico é violado, estamos diante de uma caracterização do delito.

Dessa forma a doutrina estabeleceu classificações para que o crime possa ser analisado.

Crimes Informáticos Impróprios são os delitos em que o computador foi inserido como instrumento para a execução do crime. Mesmo diante dessa ação, a prática delituosa não ofendeu o bem jurídico ou violaram dados e informações.

Tal modalidade nos traz o esclarecimento que o meio usado para obter o resultado foi através do computador, importante compreender que a ausência do computador não atrapalha o resultado do criminoso, sendo que outros meios poderiam ser igualmente eleitos para a prática. Devendo ser punido com o tipo penal já existente.

Exemplos para esses crimes: pedofilia, estelionato e calúnia.

A afirmação acima abordada possui fundamentos que conforme demonstrado na jurisprudência brasileira segue:

PROCESSUAL PENAL. QUEIXA-CRIME. DESEMBARGADOR. TRIBUNAL DE JUSTIÇA FORO POR PRERROGATIVA DE FUNÇÃO. COMPETÊNCIA. STJ. ART. 105, I, A, DA CF/88. **CRIMES CONTRA A HONRA**. INJÚRIA. CAUSA DE AUMENTO. MEIO QUE FACILITE A DIVULGAÇÃO. ARTS. 140 E 141, III, DO CP. INTERNET. COMPETÊNCIA TERRITORIAL. LOCAL DA INSERÇÃO DA **OFENSA EM REDE SOCIAL**. OFENSAS AUTÔNOMAS. DIVERSOS AUTORES. DIREITO DE QUEIXA. RENÚNCIA TÁCITA. INOCORRÊNCIA. DECADÊNCIA. TERMO INICIAL. CONHECIMENTO DA AUTORIA. PROVA EM CONTRÁRIO. ÔNUS DO OFENSOR. ELEMENTO ESPECIAL DO INJUSTO. ESPECIAL FIM DE AGIR. ATIPICIDADE MANIFESTA. NÃO COMPROVAÇÃO. ABSOLVIÇÃO SUMÁRIA. ART. 397, III, DO CPP. IMPOSSIBILIDADE. (STJ –Ação Penal nº 895 - DF, 2018/0065246-0, RELATORA: Ministra NANCY ANDRIGHI, JULGADO: 15/05/2019, data de publicação: 07.06.2019) (APn nº 895 / DF (2018/0065246-0) autuado em 22/03/2018).³⁷

Em contrapartida no Crime Informático Próprio o criminoso faz o uso do dispositivo informático da vítima, ao invadir esse sistema tecnológico ele obtém o resultado de duas ações, sendo o primeiro “invadir” e segundo a “execução”. Aqui estamos diante da violação do bem jurídico protegido.

³⁷ Superior Tribunal da Justiça, Ação Penal nº 895 / DF (2018/0065246-0).

Esse tipo de crime é exclusivamente executado e consumado por meio da informática. (CAZELATTO e SEGATTE, 2014) (CARVALHO *et al.*, 2008). Segundo Majolo (2006) são os crimes que a tecnologia serve como meio e fim para a prática criminosa almejada pelo agente. O objetivo dessa classe de crime geralmente é de danificar ou atingir elementos pertencentes a outros sistemas informáticos, como *software* e *hardware*.

As instituições financeiras e seus usuários são vítimas comuns para essa classificação de crime, através do sistema de computadores os criminosos passam a ter acesso às informações sem nenhum impedimento. Essa segunda classificação é bem diferente da primeira (imprópria), pois é de se observar que uma não viola o bem jurídico protegido ao contrário da outra (própria), que viola o bem jurídico protegido que é a inviolabilidade dos dados ou informações.

Nesse rol de crimes tem-se a violação de *e-mail*, vandalismo na *web*, difusão de vírus, entre outros.

Na visão de Túlio Vianna, os crimes informáticos mistos já passam a ser um crime de complexidade maior, pois além do detalhe: proteção da inviolabilidade dos dados, a legislação também atribui a tutela do bem jurídico de natureza diversa.

Ainda na visão de Vianna esses delitos ganharam o status de singular, pois de invasão de dispositivo informático, e conceituado com a importância do bem jurídico protegido. (VIANNA, p. 35, 2013)

Por último temos o crime informático mediato ou indireto, o agente ativo conclui duas operações através de um dispositivo informático, conforme o artigo 1º da Lei 12.735 de 2012.

Portanto, usaremos com exemplo: o agente ativo através de um aparelho informático violado transfere indevidamente um valor para sua conta. Ele cometerá dois crimes: 1º invasão de dispositivo eletrônico (artigo 154 –A, do Código Penal) e o furto (artigo 155 do Código Penal).

Devemos observar que para ser considerado como o crime-fim, essa modalidade de crime informático mediato ou indireto será punido pelo crime mais grave.

Segundo Fernando Capez³⁸: “é quando um fato menos amplo é consumido por um fato mais amplo”.

38 Disponível em:

www.stf.jus.br/portal/diarioJustica/verDecisao/codigoMateria=2. Acesso em 02 de novembro 2019.

Súmula 17 do STJ: Quando o falso se exaure no estelionato, sem mais potencialidade lesiva, é por este absorvido.

Sendo assim, no crime informático mediato ou indireto, a ação delituosa mais grave absorve a menos grave. Devemos falar de consunção quando o crime meio se revelar de menor ou igual gravidade em relação ao crime fim.

1.6 Jurisdição do crime virtual e a transnacionalidade

Para falarmos de jurisdição previamente iremos abordar o Princípio da Territorialidade.

De acordo com Damásio de Jesus: ³⁹ “a lei penal é elaborada para vigorar dentro dos limites que o Estado exerce a sua soberania; como cada Estado possui sua própria soberania, surge o problema da delimitação espacial do âmbito de eficácia da legislação penal”. (Jesus pág. 120, 2016 apud Roda pág. 19, 2019)

Como regra do direito penal o princípio da territorialidade definiu que a cada órgão do Poder Judiciário é competente para processar e julgar princípio do Juiz Natural. (Artigo 5^a, III da Constituição Federal de 1988⁴⁰).

Em concordância com o princípio da territorialidade devemos observar o local onde o crime foi praticado. Importante observar que o acesso à rede mundial de computadores não tem limites, podendo uma pessoa de outro país acessar determinado documento ou arquivo no Brasil, ou o agente ativo disponibilizar arquivos para o exterior.

Diante da relação globalização e forma eletrônica de se comunicar, a transnacionalidade vem a ser um fenômeno onde as relações humanas passam a ser um transpasse estatal, ou seja, aqui que vem a transpor as barreiras ou limites territoriais geográficos impostos por Estados a fim de delimitar seu espaço de atuação.

Conforme Jessup (1956, p.2), apud Mange (pág. 125, 2016) nos traz o entendimento a respeito do termo:

³⁹ Damásio Evangelista de Jesus, também conhecido como Professor Damásio, é um jurista brasileiro, considerado um dos mais respeitados especialistas em direito penal da atualidade. Foi membro do Ministério Público do Estado de São Paulo e atualmente é advogado criminalista

⁴⁰ CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA DO BRASIL DE 1988

“direito transnacional” inclui todo direito que regula ações e eventos que transcendem as fronteiras nacionais. Tanto o direito internacional público quanto o privado estão incluídos, bem como outras normas que não se enquadram perfeitamente em uma categoria padrão.

Destarte podemos conceituar que a transnacionalidade é o rompimento de fronteiras entre países, Essa evolução nos permite não ver mais os Estados aglomerados e interagindo entre eles, mas sim se aglomerando e formando uma única pessoa, uma única comunidade internacional.

Analisaremos no processo abaixo, no HC nº 544638/MG/STJ (2019/0336220-5)⁴¹ de recente decisão do Ministro Sebastião Reis Júnior, configurando nos autos que o conteúdo pornográfico foi disponibilizado a terceiros e expandido o acesso a outros países.

HABEAS CORPUS. WRIT IMPETRADO CONTRA DECISÃO QUE INDEFERE PEDIDO LIMINAR. APLICAÇÃO DA SÚMULA 691/STF. CRIMES DOS ARTS. 241-A E 241-B DO ECA. DISPONIBILIZAR E ARMAZENAR CONTEÚDO PORNOGRÁFICO ENVOLVENDO CRIANÇA OU ADOLESCENTE. EXCEÇÃO DE INCOMPETÊNCIA. JUÍZO FEDERAL AFIRMA A EXISTÊNCIA DE ELEMENTOS DE PROVA DA TRANSNACIONALIDADE. AUSÊNCIA DE ILEGALIDADE OU TERATOLOGIA. Writ indeferido liminarmente. 08 de novembro de 2019

A defesa alega que não houve a disponibilização de conteúdo pornográfico infantil na rede mundial de computadores. Defendendo o compartilhamento dos arquivos na modalidade privado e que não restou comprovada a transnacionalidade do crime. Defendendo também o afastamento da súmula 691 do STF.

Súmula 691 do STF: Não compete ao Supremo Tribunal Federal conhecer de *habeas corpus* impetrado contra decisão do relator que, em *habeas corpus* requerido a tribunal superior, indefere a liminar.

No relatório do HC, o Ministro Sebastião Reis Júnior, aplica a súmula 691 do STF, pois como não ocorreu caso de flagrante ilegalidade, não cabe *habeas corpus* contra o indeferimento do pedido liminar em outro writ. Destacou também a existência de evidência de ação delituosa transfronteiriça.

Embasando-se do RE 612.030 da Ministra Laurita Vaz, citou no Habeas Corpus em comento, o Ministro Sebastião Reis Júnior destaca que basta à mera potencialidade de envolvimento ou de acesso de pessoas que estejam em outros países o material de pornografia infantil por meio da rede mundial de computadores.

⁴¹<https://ww2.stj.jus.br/processo/pesquisa/?tipoPesquisa=tipoPesquisaNumeroRegistro&termo=201903362205&aplicacao=processos> acesso 09 de nov de 2019.

O Supremo Tribunal Federal, no julgamento do RE 628.624/SP, em sede de repercussão geral, firmou a tese de que "compete à Justiça Federal processar e julgar os crimes consistentes em disponibilizar ou adquirir material pornográfico envolvendo criança ou adolescente (arts. 241, 241-A e 241-B da Lei n. 8.069/1990) **quando praticados por meio da rede mundial de computadores**" 2. A decisão agravada não merece reparos, pois em consonância com a jurisprudência do Supremo Tribunal Federal "no sentido de que o crime de disseminação de material que contenha pornografia infantil, art. 241-A, do Estatuto da Criança e do Adolescente, somente compete à Justiça Federal quando verificado acesso além **das fronteiras nacionais**" (STF, RE 612.030 AgR/SC, 1.^a Turma, Rel. Min. DIAS TOFFOLI, DJe 26/05/2011). [...] 4. Agravo regimental desprovido. (AgRg no CC n. 132.367/SC, Ministra Laurita Vaz, Terceira Seção, DJe 2/9/2014 - grifo nosso)

Perante transnacionalidade do crime, o Ministro relator fundou-se nos artigos 76 inciso III e 78 inciso II alínea "c" ⁴²ambos do Código de Processo Penal.

Art. 76. A competência será determinada pela conexão: **III** - quando a prova de uma infração ou de qualquer de suas circunstâncias elementares influir na prova de outra infração. **Art. 78.** Na determinação da competência por conexão ou continência, serão observadas as seguintes regras: c) firmar-se-á a competência pela prevenção, nos outros casos.

Ficando estabelecida a conexão instrumental em que a prova de uma infração influi direta e necessariamente na prova de outra. Evidenciando a conexão instrumental, e competência pela prevenção.

Diante da conclusão do relator Ministro Sebastião Reis Júnior, em face do habeas corpus impetrado pelo paciente Bruno das Neves Oliveira, foi indeferido liminarmente.

Sendo de competência da Justiça Federal o julgamento para a transnacionalidade do crime. Segue decisão;

Diante desse contexto, e ao contrário do alegado na impetração, para a configuração do crime imputado ao paciente, basta a mera potencialidade de envolvimento ou de acesso de pessoas que estejam em outros países a material de pornografia infantil por meio da rede mundial de computadores. Tal o contexto, diante dos elementos de prova, ainda que indiciários, de que o acusado teria efetivamente compartilhado com pessoa residente no exterior diversos arquivos de pornografia infantil, resta caracterizada a **transnacionalidade** exigida para a fixação da competência da Justiça Federal, motivo pelo qual não há falar em flagrante ilegalidade a justificar o afastamento da referida súmula.

Por conseguinte passamos a compreender que a redação das Leis 12.735 e 12.737 de 2012 e suas respectivas alterações artigo 154 –A e 154- B do código penal traz melhorias para a atuação no judiciário diante da transnacionalidade.

⁴² (Redação dada pela Lei nº 263, de 23.2.1948)

2. Material e Métodos

Trata-se de um estudo histórico de pesquisa com revisão bibliográfica que visa apreciar problemática a partir de referências publicadas das Leis nº 12.735 e 12.737 de 2012, e sua análise histórica em pesquisas documentais no acervo digital da Câmara Legislativa Federal. De caráter descritivo, pois correlacionam fatos ocorridos no Superior Tribunal Federal, através de julgados e decisões monocráticas recentes. Situaremos a ocorrência do crime virtual e a atuação do Poder Judiciário.

De especificidade exploratória com descrições precisas e as relações existentes da eficácia das leis nº 12.735 e 12.737 de 2012 diante dos crimes cibernéticos. De argumentação dedutiva parte assim de uma premissa maior que busca tornar as verdades particulares em verdades universais.

3. Resultados e Discussão

Observa-se que este trabalho abordou a margem histórica do surgimento da internet e a sua praticidade ao homem moderno. Porém, em contrapartida a essa evolução cibernéticas, criminoso desenvolveram habilidades técnicas no espaço informático, e para a caracterização delituosa do indivíduo, não possuíamos uma legislação específica, tínhamos lacunas na lei, perante a tipificação de conduta do agente ativo.

Com o advento das Leis 12.735 e 12.737 de 2012, que possuem iniciativa legislativa na Câmara dos Deputados desde o ano de 1999, através do PL 84/99 que se originou na Lei 12.735/12, e o PL nº 2.793/2011 que se originou em Lei 12.737/2012, ambas foram sancionadas no dia 30 de novembro de 2012, devido a comoção social do país perante ao crime praticado contra uma atriz global, a população pressionou o Poder Legislativo quanto a promulgação de Leis específicas, haja vista que anterior as Leis 12.735 e 12.737/2012 não existam sanções penais para quem cometesse crime de espécie cibernética.

Desde a promulgação das Leis nº 12.735 e 12.737/2012, e sua entrada em vigor, elas passaram a ter caráter informativo e preventivo. Sendo assim o agente passivo como forma preventiva obtém mais segurança perante suas ações com o material informático, e sofrendo ato lesivo ao seu bem jurídico, o mesmo provém de recursos jurídicos. Conforme alguns julgados percorridos no presente trabalho, o

poder judiciário detém de fundamentos para uma eficaz atuação aos crimes no âmbito virtual.

Sendo assim o surgimento das leis representa uma significativa mudança no nosso ordenamento jurídico.

4. Considerações Finais

Neste trabalho houve o intuito de tratar acerca da eficácia das Leis nº 12.735 e 12.737 /2012 ao combate dos crimes cibernéticos, trazendo uma reflexão acerca do tema desde o seu surgimento até o ponto atual.

Ademais, fazendo-se um retrospecto de forma sucinta, é possível verificar características dos crimes cibernéticos que são indispensáveis para o bom entendimento do tema. Dessa forma, sabe-se que o primeiro passo do presente estudo consistiu em tecer breves comentários acerca da história/evolução do assunto em comento.

Vários aspectos relacionados à internet foram expostos de forma clara e objetiva, entre eles a origem histórica, definições da rede mundial de computadores, aspectos da internet e criminalidade na rede. Foi explicado, também, a classificação dos crimes virtuais e seus sujeitos, quais sejam, os crimes virtuais próprios e impróprios, sujeito ativo e passivo.

No que tange à ação penal prevista no artigo 154-B, que trata do impulso inicial acusatório a ser realizado quando da prática de um dos tipos penais, nos caso dos crimes do artigo 154-A, a ação penal será pública condicionada à representação da vítima. Dito de outro modo, levando em conta a natureza do ilícito praticado e o interesse geral da sociedade, o legislador outorgou para a vítima o oferecimento da condição de procedibilidade, observando-se a legitimidade e o decurso do prazo decadencial.

Todavia, a ação penal se converterá em pública incondicionada quando a infração penal for praticada 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 (art. 154-B da Lei nº 12.737/12).

Observa-se também, muito embora não tendo uma definição específica para os delitos cometidos no ambiente virtual, podemos tratar todo o rol de nomenclaturas

que envolvam os tipos delitivos do mundo digital, a saber: crime virtual, crime informático, crime virtuais, crime cibernético e etc.

As Leis 12.735 e 12.737 de 2012 tratam de crimes que passam a ser cada vez mais constantes na hodierna sociedade, tipificando condutas que não eram previstas de forma específica como infrações penais e hoje passam a ser.

Referencias Bibliografia

BRASIL, Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal. **Diário oficial da União**. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm. Acesso em 22 de agosto de 2019

BRASIL, Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, **Diário oficial da União**. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del1001.htm. Acesso em 25 de agosto de 2019

BRASIL, Lei nº 7.716, de 5 de janeiro de 1989, **Diário oficial da União**. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l7716.htm. Acesso em 25 de agosto de 2019

BRASIL, Constituição Federal de 1988. **Diário Oficial da União**. Disponível em http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em 26 de agosto de 2019

BRASIL, Mesa Diretora da Câmara dos Deputados. **Diário Oficial da união**. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=15028>. Acesso em 28 de agosto de 2019.

BRASIL, **Federação Brasileira de Bancos**. Disponível em <https://portal.febraban.org.br/noticia/3301/pt-br/> acesso 12 de nov 2019.

BRASIL, **Supremo Tribunal Federal**. Disponível em <http://www.stf.jus.br/portal/diarioJustica/verDiarioAtual.asp> Acesso em 01 de nov de 2019

BRASIL, **Supremo Tribunal Justiça**. Disponível em <http://www.stj.jus.br/sites/portalp/Inicio>. Acesso em 03 de setembro de 2019.

BRITO, Glaucia da Silva e Inonélia da Purificação. **Livro Educação e as Novas Tecnologias**, 2ª edição 2006. Disponível em <
<http://tecnologia.terra.com.br/internet10anos/interna/0,,OI541817-EI5026,00.html>>
Acesso em 29 de agosto de 2019

CHIAVENATO, Idalberto. **Teoria Geral da Administração**. 6ª edição. Disponível em <https://alexavidal.files.wordpress.com/2015/07/chiaavenato-introduc3a7c3a3o-c3a0-teoria-geral-da-administrac3a7c3a3o.pdf> acesso em 22 de out de 2019.

LÉVY, Pierre. **As Tecnologias da Inteligência**. Disponível em: <http://www.mozo.pt/tesp/livros/LEVY-Pierre-1998-Tecnologias-da-Inteligencia.pdf>. Acesso em 02 de novembro 2019.

JESUS, Damásio Evangelista de. **Direito Penal: Parte geral**. 21º Ed. rev. e atual. São Paulo: Saraiva 2016. Disponível em: <https://www.lexml.gov.br/urn/urn:lex:br:redede.virtual.bibliotecas:livro:2012;000944924>. Acesso em 03 de novembro 2019.

JORNAL. **Folha de São Paulo**. Domingo, 12 de agosto de 2001. Disponível em < <https://www1.folha.uol.com.br/fsp/cotidian/ff1208200103.htm> > Acesso em 05 de setembro de 2019

NERY JÚNIOR, Nelson; NERY, Rosa Maria de Andrade. 11. ed. São Paulo: Editora **Revista dos Tribunais**, 2010

MAJOLO, Ederlei Norberto. **Informática e Crime**. 2008. 59 f. Monografia (Bacharel em Direito) – Universidade Federal do Paraná. Curitiba, 2008. Disponível em: <http://www.faccrei.edu.br/wp-content/uploads/2018/07/15-CRIMES-INFORM%C3%81TICOS-DOS-DELITOS-E-DOS-INFRATORES.pdf> Acesso em 11 de setembro de 2019.

MANGE, Flavia Foz. **As Características do Direito Transnacional como Metodologia: Análise sob o enfoque dos Aspectos Processuais da Arbitragem**. In: Revista de Direito Internacional. Brasília, v. 13, n. 3, p. 125-144. Disponível: <https://www.publicacoesacademicas.uniceub.br/rdi/article/download/4157/pdf>. Acesso em 04 de novembro 2019.

REVISTA. **Guia 501 Curiosidades Históricas Ed.02**. Por On Line Editora, Curiosidades On Line Editora, História On Line Editora. Disponível em https://books.google.com.br/books?id=_ndGDgAAQBAJ&printsec=frontcover&hl=pt-BR#v=onepage&q&f=false. Acesso em 29 de agosto de 2019.

RODA, Arménio da. **A dimensão global do tráfico humano: o tráfico de pessoas aos olhos de Moçambique**. Bahia – Atarukas, 2019. Disponível em: https://books.google.com.br/books?id=SaKaDwAAQBAJ&printsec=frontcover&hl=pt-BR&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false Acesso em 03 de novembro 2019.

STAIR, Ralph M. **Princípios de Sistemas de Informação**. / Ralph M. Stair, George W. Reynolds: tradução Harue Avritscher: revisão técnica Flávio Soares Correia da Silva. 2º Ed. São Paulo: Cengage Learning, 1998. Disponível em:

<http://petry.pro.br/engsw/fundamentossi/materiais/LIVRO%20-%20Principios%20SI.pdf>. Acesso em 04 de novembro de 2019.

VIANNA, Túlio. **Crimes Informáticos. Conforme a lei 12.737/2012**. Túlio Vianna, Felipe Machado. - Belo Horizonte: Imprensa: 2013.

WENDT, Emerson. **Crimes cibernéticos: ameaças e procedimentos de investigação**. Emerson Wendt, Higor Vinicus Nogueira Jorge – Rio de Janeiro: Brasport, 2012. Disponível em <https://books.google.com.br/books>. Acesso em 19 de agosto de 2019.