APLICABILIDADE DA LEI Nº 12.737/12 SOBRE CRIMES CIBERNÉTICOS

João Manoel de Vasconcelos Bezerra
Urbano Vitalino Advogados Associados
E-mail: joaomanoelvb@gmail.com

Artigo Revisão

Recebido em: 22 de Agosto de 2021
Aceito em: 15 de Dezembro de 2021

RESUMO

O presente trabalho apresenta uma análise das conquistas do direito brasileiro e do direito internacional acerca de como funciona o mundo cibernético e os diversos dispositivos de informática para armazenamento e troca de informações, bem como trata das questões no tocante à elaboração de uma lei específica para combater à ocorrência dos chamados crimes cibernéticos. É apresentado também como é a realidade das infrações no campo da informática perante o direito internacional e como os países atuam em conjunto para combate e prevenção de tais delitos, relativizando a soberania destes. Por outro lado, são analisadas as inovações trazidas pela Lei nº 12.737/12 ao ordenamento jurídico brasileiro, bem como será esclarecido como o direito pátrio atua no combate à ocorrência de tais delitos, bem como a aplicabilidade do referido diploma legal especifico quanto à tipificação do delito, identificação do agente infrator, da vítima, do local de cometimento da infração, da proporção da pena aplicada, para que seja possível identificar as características necessárias da infração penal. Além disso, são analisadas as alterações trazidas pela Lei 14.155/2021, com alteração na aplicação da pena e agravantes, bem como, aplicação para outros crimes previstos no Código Penal, como furto e estelionato, agora cometidos através de dispositivo informático.

Palavras-chave: Ciberespaço. Dispositivos de informática. Crime cibernético.

APPLICABILITY OF LAW Nº. 12.737/12 ON CYBER CRIMES

ABSTRACT

The work presents an analysis of the achievements of Brazilian law and international law about how the cyber world and the various computing devices for storing and exchanging information, and addresses issues regarding the development of a specific law to combat the occurrence of so-called cyber crimes. It is also shown how the reality of violations in the computer field under international law and how countries work together to combat and prevent such crimes and thereby questioning the sovereignty of these. On the other hand, it analyzes the innovations introduced by Law No. 12.737/12 the Brazilian legal system, as well as will be clarified as the right parental acts in combating the occurrence of such crimes, as well as the applicability of the statute as to the definition of specific

offense, agent identification offender, the victim, the place of commission of the offense, the proportion of the sentence imposed to be able to identify the necessary characteristics of the criminal offense. In addition, the innovations brought by Law No. 14.155/21it analyzes, with changes in the application of the penalty and aggravating factors, as well as application for other crimes available in the Penal Code, such as theft and fraud, now committed through a computer device.

Keywords: Cyberspace. Computing devices. Cyber crime.

INTRODUÇÃO

Criada há quase quatro décadas, no fim da Guerra Fria, a internet tornou-se um dos veículos mais importantes de comunicação e tecnologia de todos os tempos, ganhando, através do processo de globalização e neoliberalismo estatais, um patamar excessivamente diferenciado frente à sociedade.

A massificação desse veículo de comunicação atingiu todas as camadas econômicas e políticas da sociedade fazendo com que a ciência do direito não acompanhasse tal desenvolvimento, permitindo que, através dessa popularização no compartilhamento e divulgação de imagens e dados pessoais ficasse cada vez mais comum e sem o devido acato e preservação legal.

O crime cometido na internet, ou até mesmo sem ela, com o auxílio de computador, é denominado crime cibernético. Os agentes criminosos beneficiando-se de suas aptidões e conhecimentos específicos realizam inúmeros artifícios para alcançarem seus objetivos. Infelizmente, a grande maioria das pessoas que utilizam de redes de computadores e outros veículos de comunicação, como celulares, endereços eletrônicos e redes sociais ainda são suficientemente despreparados para se defenderem da habilidade desses criminosos.

No âmbito jurídico, em virtude do fato de ser ainda uma temática bastante recente, a legislação para proibir essa prática delituosa ainda é escassa, posto que, os crimes cometidos em computadores, os chamados cibercrimes, podem desencadear, além dos crimes de invasão da própria rede de computadores, outros, como os crimes contra cartões de crédito, de pedofilia, sequestro, estelionato, entre outros.

Na grande maioria das vezes, as vítimas sequer têm conhecimento de que estão tendo suas redes de computadores, memória e internet invadidos, como foi o caso popularmente conhecido no final do ano de 2012 da atriz brasileira Carolina Dieckmann

que detinha em seu computador fotos íntimas com o seu marido e precisou reparar alguns danos na memória de seu dispositivo, tendo 36 de suas imagens íntimas divulgadas nas redes sociais.

Tal prática criminal vai de encontro aos direitos básicos do indivíduo, quais sejam: liberdade, à vida e ao patrimônio consideravelmente prejudicados.

Devido à repercussão do caso, em pouco mais de um mês a lei foi sancionada pela presidente Dilma Rousseff em 30 de novembro de 2012. A legislação, disciplina que a pena para esses delitos será de reclusão de seis meses a dois anos acrescidos de multa para quem obtiver segredos comerciais e industriais ou conteúdos privados por meio da violação de mecanismo de segurança de equipamentos.

A lei também disciplina acerca dos crimes praticados com uso de dados de cartões de débito e crédito, sem autorização do proprietário. Tal prática delituosa deverá ser equiparada à falsificação de documento particular e as penas podem variar entre um a cinco anos, acrescidos de multa.

Em paralelo à promulgação da Lei n°12.737/12, entrou em vigor a Lei 12.735/12 (Lei Azeredo), proposta pelo deputado do partido PSDB mineiro, Eduardo Azeredo, versando acerca da tipificação de condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares e outras providências.

O objetivo principal deste artigo é demonstrar a aplicabilidade da nova lei em vigor no tocante à prática e cometimento de delitos no âmbito da internet, computadores e dispositivos de hardware, a fim de verificar tipificação do criminoso, a vítima, o tipo de perícia realizado nesses crimes como também, a análise do processo de punibilidade do infrator.

Especificamente, deseja-se explorar alguns fatores relacionados com o exercício e a aplicabilidade do direito brasileiro pátrio diante do cometimento de infrações ligadas à seara informática. Ademais, ressalta-se a importância das decisões dos organismos internacionais e aplicação do direito interno brasileiro, principalmente nas decisões judiciais que versem sobre o tema em questão.

Por essas razões, primeiro serão apresentadas as noções básicas acerca do surgimento da internet, o conceito de informática e conhecimento dos diversos dispositivos informáticos, bem como seu modo de funcionamento. Em um segundo

momento, serão destacados o conceito do crime cibernético, bem como as noções de autoria, da vítima, do lugar onde é cometido o crime, como também da produção de provas para conclusões da autoria e especificidades no crime.

Será feita uma análise do crime cibernético no âmbito internacional e no direito brasileiro, tendo em vista, a aplicabilidade e eficácia da nova Lei nº 12.737/12 e suas providências, uma vez que, após a promulgação desta, a legislação brasileira passará a caminhar junto ao combate dos crimes cometidos nessa esfera que até então, não representava segurança nenhuma para seus usuários.

Por fim, analisaremos as inovações trazidas por meio da Lei 14.155/21, que alteram o art. 154-A do Código Penal. A norma recente prevê outras modalidades mais abrangentes para o cometimento do delito, bem como, a aplicação de penas mais rigorosas, se comparadas ao dispositivo anterior, a fim de tornar o dispositivo penal mais eficaz e com maior aplicabilidade na prática forense atual.

DESENVOLVIMENTO

HISTÓRIA DA INTERNET E O ACESSO À INFORMAÇÃO

Pretendeu-se, com a criação da internet no contexto da Guerra Fria, desenvolver uma rede descentralizada a qual tivesse uma capacidade de sobreviver a uma guerra nuclear com destruição parcial da rede e de, ainda assim, preservar a comunicação entre as redes de computadores remanescentes. Em caso de guerra nuclear, a internet ficaria funcionando (ALBUQUERQUE, 2006).

O cenário mundial era, de temor quanto à eclosão de uma nova guerra, dessa vez nuclear, onde as principais potências não almejavam perder seus dados históricos em virtude de qualquer ataque. Foram criados, portanto, uma série de ramificações como, por exemplo, os protocolos de comunicação, a World Wide Web e os e-mails que, são as caixas de correios eletrônicos. (MALAQUIAS, 2012).

Segundo Malaquias (2012, p.52): “em decorrência de seu alcance, gratuidade e velocidade de acesso a informações, a internet é o grande fenômeno tecnológico da humanidade, gerando problemas em virtude de sua utilização”.

Isto é, o processo de divulgação e de acesso à internet por diversas camadas sociais configurou um processo de massificação que, além de trazer inúmeros benefícios no tocante ao acesso à informação trouxe também, inúmeros prejuízos e inseguranças frente ao descompasso do crescimento e do acesso (MALAQUIAS, 2012).

É o que se evidencia de acordo com Albuquerque (2006, p. 01):

> A tecnologia da informação apresenta uma relação compensadora de custo-benefício para a prática de crimes, oferecendo novos recursos técnicos para se por bens jurídicos em risco. Essa relação de custo benefício, trazida por Chalcon de Albuquerque, é tida na situação de facilidade de acesso em virtude de poucas medidas repressoras (ALBUQUERQUE, 2006, p. 01).

É o que se evidencia de acordo com Albuquerque (2006, p.1) Ter acesso à internet não requer muitos conhecimentos o que fica bastante fácil para qualquer pessoa comum, através de links de pesquisa, pretende buscar sites acerca de qualquer matéria de seu interesse. Em questão de segundos, o acesso ao mundo está na palma da mão de qualquer usuário de forma gratuita ou até mesmo privada, em alguns casos. (ALBUQUERQUE, 2006).

Segundo Albuquerque (2006, p.19): “a internet constitui uma vasta plataforma onde qualquer indivíduo pode consultá-la e ter acesso aos inúmeros conteúdos que são divulgados. Não existe o que se chama de controle centralizado, mas sim uma universalidade em cadeia de informações”.

Existem hoje, mais de 79,9 milhões de internautas no Brasil e a tendência é esse número crescer ainda mais à medida que a demanda aumentar. Conforme se evidencia por tal dado, não é um número ainda bastante expressivo, pois diz respeito a apenas aproximadamente 40% da população brasileira se comparada a outros países. (MALAQUIAS, 2012).

Entende-se que essa área geográfica de abrangência da internet e computador é mundial, assegurando a maior reunião de redes de comunicação do planeta conectando-se a diversos computadores através da rapidez e gratuidade no acesso. (MALAQUIAS, 2006).

Tecnicamente, segundo Malaquias (2006, p.53): “através dos canais de comunicação, os sinais criptográficos trafegam com o auxílio de fibras óticas ou ondas eletromagnéticas, utilizando-se de vários satélites para que as pessoas, dessa forma,

possam estar interadas em vários locais ao mesmo tempo.”

Tudo que se massifica rapidamente pode fugir ao controle não só de seus criadores, como também das referidas autoridades. Surgem assim, não só criminosos que se aproveitam de tal situação, como também, principalmente tem-se a ocorrência dos chamados crimes cibernéticos ou cibercrimes (ALBUQUERQUE, 2006).

DAS MODALIDADES DE ARMAZENAMENTO E ACESSO À INFORMAÇÃO

A utilização dos recursos informáticos tem crescido desde o final do último século, assegurando o acesso e compartilhamento de dados por diversas pessoas. A internet, rede mundial de computadores, deve ser composta pela conexão ou interligação de um ou mais redes locais ao redor do mundo. A troca de informações dá-se, predominantemente, de forma globalizada, pouco importando se os usuários ou veículos de comunicação estão próximos ou devidamente dispersos no globo. (COLLI, 2010).

Um dos mais famosos meios de acesso à informação é a internet, porém, esta é apenas uma das ramificações campo tecnológico, onde, dentro desta, existem outras espécies e modalidades de acesso a informação, sendo estas espécies do gênero internet. São exemplificadas, principalmente, os protocolos de comunicação, a World Wide Web e os e-mails e o Armazenamento em Nuvem (COLLI, 2010).

Os chamados protocolos de comunicação permitem que qualquer sistema informático possa estar ligado à uma rede central de computadores, geralmente vinculada ao acesso a internet, gerando assim um intercâmbio de dados. Defini-los, portanto, seria como tentar exemplificar uma espécie de transferência de dados entre computadores secundários à uma rede central. Tais dados são, por sua vez, registrados e encaminhados para o destinatário, que é quem receberá a informação ou até mesmo, confundindo-se com quem a pesquisou. (ALBUQUERQUE, 2006).

A World Wide Web, que significa “teia de alcance mundial”, foi criada em 1990 pelo Conselho Europeu a Pesquisa Nuclear com objetivo precipuamente científico. Posteriormente, teve sua finalidade alterada a fim de permitir acesso à dados em tempo real, independentemente da capacidade ou tamanho do arquivo a ser acessado. Tornou-se uma das modalidades mais almejadas no tocante à busca de informação em virtude de sua facilidade de ser encontrada nas telas do computador. (ALBUQUERQUE, 2006).

Os e-mails correspondem a uma modalidade de troca de informações pessoais no ambiente da internet, tendo sido criados em 1971, a fim de permitir ao usuário a criação de uma espécie de correio postal eletrônico. A grande particularidade dessa espécie de troca de informações através do computador é que, nos e-mails, estão certificados com símbolos próprios e características do agente usuário, como por exemplo, o nome, sobrenome, etc. O risco, sem dúvida, existe e, se o usuário não tomar as devidas precauções podem cair em alguns golpes ou até mesmo, terem o conteúdo dos seus textos alterados. (ZANIOLO, 2012).

Por fim, a modalidade de armazenamento em nuvem diz respeito a modalidade de navegação que possibilita ao usuário uma maior quantidade de aplicações, independente do local físico onde esteja. Tal "nuvem" de informações corresponde a um ambiente intrínseco, representada pela internet e composta de um conjunto de dispositivos computadorizados, que permitem a entrega de serviços através de computador. (HURWITZ et al, 2010).

Em suma, atualmente não há mais distinção entre o local em que o serviço do armazenamento em nuvem é realizado. Seja no âmbito doméstico, comercial ou empresarial, a sua área de atuação refere-se às mais corriqueiras atividades já desempenhadas no ciberespaço (troca de imagens, e-mails, acesso à redes sociais, etc) só que de maneira mais rápida, onerosa e com um certo grau de segurança (PEDROSA, 2011).

O CIBERESPAÇO E OS SISTEMAS COMPUTACIONAL: HARDWARES E SOFTWARES

O ciberespaço pode ser entendido como a dualidade na existência de um terreno completamente distinto do real criado pelas redes de acesso a computador, onde diversas pessoas interagem das mais várias formas possíveis. É, justamente, por ainda haver esse quase que completo desconhecimento da matéria cibernética que se abrem lacunas onde a criminalidade pode vir a ocorrer (CANONGIA, 2009).

Não há limitações quanto a jurisdição e competência territorial do próprio ciberespaço e, além disso, cada sujeito é um emissor e receptor de dados diferenciado em

virtude da interatividade e da diversa gama de preceitos que cercam o ambiente informático. (FERREIRA, 2008.)

O espaço cibernético representa um novo campo social criado e modificado a cada dia, trazendo uma nova realidade para o ser homem que caminha por meio do século XXI, agrupando-se as conquistas sociais da chamada Era da Informação. O conceito do espaço geográfico não representa mais a realização de atos ou fatos jurídicos. A sociedade cibernética, por sua vez, traz uma mudança no conceito de fronteira física com o surgimento de uma nova concepção de jurisdição. (MALAQUIAS, 2012).

Dentre tais ambientes que podem ser alvo da ação de crimes, destacam-se os sistemas computacionais correspondem a um conjunto de dispositivos eletrônicos (os hardwares) que têm como característica intrínseca a capacidade de realizar o processamento de variadas informações de acordo com um programa determinado (o software) para atender as diversas necessidades de seus usuários. (GUIMARÃES, 2011).

A esse conjunto de dispositivos eletrônicos que os sistemas computacionais abrangem têm-se presentes figuras bastante complexas por envolverem conceitos não muito analisados pela computação. Estão envolvidos nesse complexo rol as questões de portabilidade, limite de consumo sem perda de seu desempenho, necessidade de segurança e a possibilidade de funcionamento quando anexados a uma rede maior. (WOLF, 2001).

Os dispositivos de hardware de um computador correspondem a todos os elementos e componentes eletrônicos ou mecânicos, internos ou externos do computador, podendo ser periféricos e não periféricos. (GUIMARÃES, 2011). Os hardwares são formados por alguns elementos básicos denominados de unidades funcionais que correspondem a uma Unidade Central de Processamento, a Unidade de Memória Principal e as Unidades de Entrada e Saída. (VELLOSO, 2011).

Já os dispositivos de software dizem respeito a uma contraposição aos hardwares e representam a parte lógica do sistema computacional. Por meio deles, é possível que haja o processamento dos programas e dos dados através de um circuito eletrônico de hardware. Sendo colocado sobre o hardware, o software será responsável por toda a interação dos usuários da máquina. (GUIMARÃES, 2011).

Todos os componentes desses sistemas devem funcionar em perfeita harmonia, porém, podem os sistemas do computador funcionar de uma maneira própria e distinta.

Quaisquer violações a tais dispositivos geram consequências que ultrapassam o ambiente tecnológico, em flagrante ofensa a ordem jurisdicional pátria em vigor. (GUIMARÃES, 2011).

DOS ASPECTOS TÉCNICOS E JURÍDICOS NO CRIME CIBERNÉTICO

É muito difícil tentar elaborar uma definição acerca dos crimes cibernéticos, ante à existência das dúvidas no tocante ao seu objeto e tipificação. Tal dificuldade de conceituação e interpretação decorre da ideia de que essa modalidade criminal é sempre uma atividade que incidirá em várias práticas criminais comuns já existentes. Em razão de a informática ter se tornado elemento essencial na vida de qualquer pessoa na modernidade é que esses crimes constituem uma espécie de veículo motor para que, condutas já conhecidas no campo material venham a se configurar no campo virtual através de elementos tecnológicos. (ALBUQUERQUE, 2006).

O crime cibernético, conforme já mencionado, envolvem confusão e divergências conceituais no tocante à sua classificação. Além das principais indagações acerca do seu objeto e da sua tipicidade, mister faz-se aludir também a ideia de como qualificar o criminoso, a vítima e os limites territoriais quando da prática dos mesmos. Apesar de não configurarem, na maioria dos casos, crimes relativamente inéditos para a sociedade, a novidade proposta pelos cibercrimes consiste no fato de que estes possuem características próprias através da diferenciação que se faz entre os sujeitos e ampla liberalidade do lugar da infração. (COLLI, 2010).

Algumas das atividades ilícitas desempenhadas através da informática são, por exemplo, a evasão fiscal, estelionato, sequestro, falsificação de balanços, fraudes em bolsas de valores, em investimentos, violação da intimidade pessoal e sexual, segredos dos mais variados, os quais não estão protegidos pelo usuário na grande maioria dos casos. Os dados armazenados ou transmitidos por computador exigem proteção diferenciada ante à criminalização. (ALBUQUERQUE, 2006).

Os crimes cibernéticos podem ser divididos em próprios e impróprios. O crime cibernético próprio ou comum corresponde ao crime em que é necessária a existência de um espaço virtual para o cometimento do delito. (MALAQUIAS, 2012). Aqui, o ambiente virtual deve ser utilizado como meio para a prática de condutas que já são conhecidas

como condutas criminais contra bens jurídicos já tutelados pelo direito material penal. (ALBUQUERQUE, 2006).

Em contrapartida, os crimes cibernéticos impróprios ou específicos são aqueles em que o computador ou o espaço cibernético passa a ser o instrumento essencial para a configuração do delito. Nessas hipóteses, não há definição geral do bem jurídico tutelado, passando, o direito material penal vigente a instituir suas diretrizes nas leis especiais de crimes como, por exemplo, estelionato, calúnia, a injúria, furto, divulgação de imagens ou fotografias contendo cenas de sexo ou violência e todas as outras demais hipóteses elencadas na parte especial da legislação criminal. (MALAQUIAS, 2012).

O legislador penal precisa adaptar os tipos penais já conhecidos bem como tentar readaptá-los as novas espécies de crimes criando uma espécie de paralelismo, como por exemplo, o estelionato e o estelionato cibernético. (ALBUQUERQUE, 2006).

Para que haja a configuração do crime faz-se necessário que este seja cometido por alguém e que, em decorrência da prática delituosa, outra pessoa sofra determinadas consequências negativas em sua esfera jurídica. Há, portanto, uma relação entre dois polos (ativo e passivo) onde, a partir desta, será possível analisar a forma de punibilidade do agente infrator. Além disso, a conduta criminosa, que poderá ser comissiva ou omissiva, dependerá de uma vontade ou anseio do ser humano (BITENCOURT, 2013).

Na relação jurídica criminal também há a possibilidade de existência do concurso de pessoas, o qual diz respeito, por sua vez, a um auxílio realizado por inúmeras pessoas para que a conduta delituosa venha a ser configurada. Entende-se como concurso de pessoas a coautoria, participação, concurso de delinquentes ou até mesmo, cumplicidade. (NUCCI, 2013).

Os criminosos cibernéticos, na grande generalidade do termo, representam sujeitos dotados de criatividade e são obcecados pela tecnologia buscando, quase sempre, autoafirmação que é desencadeada através de um prejuízo alheio (CORRÊA, 2010). Em princípio, conhecem a vulnerabilidade do sujeito passivo em lidar com os sistemas, os quais, quase sempre, são criados pelos próprios criminosos a mando de empresas que invadem operações de segurança. (LIMA, 2011).

O mundo do ciberespaço é quase que exclusivamente dotado de uma liberdade ilimitada superior ao campo real. Em virtude dessa ampla liberalidade de ações e até mesmo da falta de preparo de algumas atividades judiciais no manuseio do computador

que fica bastante fácil para uma pessoa, dotada de conhecimentos informáticos, de se aproveitar dessa situação de fragilidade para o cometimento e prática de delitos (MALAQUIAS, 2012).

Não deve o Poder Judiciário fazer uma espécie de estigma no tocante ao sujeito ativo, deve-se, em contrapartida, munir-se de elementos essenciais e concretos para a configuração criminal e consequente aplicação da punibilidade não pautada em meros indícios, porém em situações e fatos concretos (MALAQUIAS, 2012).

Dentre os sujeitos ativos no crime cibernético, é possível destacar os Hackers, Crackers e os Carders. Vejamos:

Os hackers são, em regra, invasores disfarçados de um sistema eletrônico. A natureza das informações obtida é relativa, variando de dados pessoais invadidos (o sujeito passivo tem sua seara de intimidade invadida) ou também bens digitais que são roubados (esfera patrimonial invadida). (CORRÊA, 2010). Já os crackers atuam com objetivo de adulterar programas, dados pessoais e informáticos e, principalmente furtar informações e valores monetários em atos de destruição deliberada. (LIMA, 2011). Podem ser definidos também como os reais criminosos da rede, os quais, valendo-se da particularidade de atuarem no desvio e roubo de valores em dinheiro, sendo também responsáveis por atos de vandalismo quando deixam mensagens de conteúdo ofensivo ou racista. (CRESPO, 2011).

Por fim, os carders são considerados os estelionatários virtuais, apropriando-se de dados bancários, por meio de invasões eletrônicas. Diante de tal fato, distribuem os dados obtidos em redes próprias de outros criminosos, com vistas a garantir a manutenção de suas práticas. Geralmente a atuação destes agentes é em conjunto com a dos crackers. Em tal modalidade de crime, os crackers são os simples invasores e os carders são os responsáveis por fazerem as compras no lugar dos sujeitos passivos. (CRESPO, 2011).

Além do sujeito ativo na prática do crime, também faz-se necessário destacar a presença da vítima do crime, podendo tipificado como sujeito passivo no crime cibernético em virtude do fato de usar o equipamento informático como uma ferramenta meramente acessória, não cuidando de cercar-se das precauções necessárias. Em muitos casos, em razão da ausência de conhecimento técnico, são vítimas de golpes e infrações penais, sem sequer imaginar que tais crimes foram praticados. (MALAQUIAS, 2012).

Em muitos casos, o aumento de acessos em proporções astronômicas é diagnosticado pelo uso de pessoas completamente despreparadas e inexperientes as quais, por estarem diante de um mundo completamente novo cometem deslizes que facilitam a prática de delitos pelos criminosos cibernéticos.

Outro ponto que merece destaque é acerca do lugar do crime cibernético, podendo este ambiente ser fundamental para a coleta de provas e métodos de investigação do crime cibernético. Para o crime cibernético, não existem fronteiras. Pode ocorrer que seja iniciado em um determinado país; que o criminoso esteja operando a situação em outro; que a vítima esteja em um terceiro e que, por fim, o seu desfecho possa ocorrer em um local completamente inesperado. (ALBUQUERQUE, 2006).

O ciberespaço, proporciona um maior grau de liberalidade no momento do uso e gozo dos benefícios da internet. Em razão da ausência de limites espaciais objetivamente declarados, o que fica evidente é a existência de uma rede transnacional de sujeitos (ativo e passivo) além dos outros elementos que caracterizam e configuram o delito cibernético. (COLLI, 2010).

Tais ocorrências fazem surgir as ideias de Direito Penal Internacional e Direito Internacional Penal, onde, apesar da hierarquia presentes nas formas desses dois institutos jurídicos, o que vigora é o sentimento de comunidade internacional entre as nações. Ao primeiro instituto incide a análise de crimes previstos nos ordenamentos internos dos países, porém que assumem reconhecimento também no exterior. O segundo instituto, por sua vez, preconiza a cooperação e auxílio entre os Estados na esfera das comunidades internacionais. (COLLI, 2010).

Diversos países podem se considerar aptos para julgarem determinados delitos informáticos, enxergando alguns pontos extraterritoriais nesse tipo de ação delituosa. Tais modalidades de infração podem estar relacionadas à destruição ou comprometimento de dados e arquivos governamentais ou de outras entidades privadas as quais atentem contra segurança de sistemas e o desenvolver de atividades consideradas como essenciais. Esse princípio de mútua ajuda e de interesses múltiplos pode aumentar a jurisdição extraterritorial para que dados sejam protegidos (ALBUQUERQUE, 2006).

Os conceitos de jurisdição e competência podem, algumas vezes, gerarem confusão a respeito de sua aplicabilidade prática. A jurisdição nada mais é do que o poder atribuído, em caráter constitucional, para que o Estado possa aplicar as leis e resolver

conflitos. O estado é o detentor central do poder de julgar através, é claro, de um juiz competente. Em contrapartida, a competência é a própria delimitação da jurisdição, isto é, o campo físico no qual a jurisdição irá atuar. (NUCCI, 2013).

Para o direito penal e processual penal brasileiro entende-se que o local da infração é, em regra, o local do foro competente para que o crime seja julgado. Trata-se do princípio do ratione loci (em razão do lugar), pois além de terem sido configurados todos os elementos para o delito, este consumou-se propriamente no local. Caso haja, por sua vez, tentativa de crime aplicar-se-á a competência territorial do último local da infração. De modo subsidiário, quando não é possível verificar o local de consumação do delito, aplica-se a situação do foro supletivo ou foro subsidiário onde o que vai vigorar é o local do domicílio ou residência do acusado, posto que, o domicílio configura uma residência em caráter definitivo e permanente, presumindo-se ser nesse lugar que o indivíduo pratica a maioria de suas atividades cotidianas. (NUCCI, 2013).

No Brasil, concluiu-se que o foro competente é o do local da infração e a lei processual só se aplica dentro do território nacional. A esse princípio dá-se o nome de Lex fori, porém, a lei processual penal também admite que crimes sejam cometidos fora da esfera nacional, devendo ser aplicadas as leis do país em que os atos forem praticados além dos atos de cumprimento de rogatória, homologação de sentença estrangeira e extradição, em alguns casos (CAPEZ, 2012).

Os crimes cibernéticos não são delimitados através de fronteiras e territórios físicos, podendo alguns ou todos os seus atos desdobrarem-se em diversas partes do mundo. (ALBUQUERQUE, 2006). A essa modalidade de crimes dá-se o nome de crimes plurilocais em virtude de sua ação ou omissão se configurarem em um local e o seu desfecho ocorrem em outro completamente diferente. Nessa modalidade de crimes, prefere-se que o local competente seja o local de consumação, na maioria dos países. (NUCCI, 2013).

Para que um delito seja julgado por um país considerado internacionalmente competente deve, portanto, ser determinado pelo direito interno de cada país, como também pela incidência de tratados internacionais. Em regra, não existem parâmetros que determinem a ocorrência de um crime em um país ou seu desenrolar em outro. Em determinados países, o lugar da infração, pode ser o local onde o resultado deveria ter

ocorrido, mas não chegou a acontecer ou até mesmo se desenrolou e teve seu resultado. o. (ALBUQUERQUE, 2006).

CRIMES CIBERNÉTICOS NO BRASIL

No sentido tecnológico da evolução social, verificou-se sem dúvida que a década de 1990 foi promissora para propagação e amplitude da internet e do uso de sistemas informáticos, não só na seara internacional, como também no cenário brasileiro. É nesse contexto de ampla extensão e facilidades na navegação que o Brasil, atualmente, é um dos países do mundo que apresentam grandes números de ataques cibernéticos. (ZANIOLO, 2012).

O Brasil é um país que detém mais de 79,9 milhões de usuários ou internautas. Em alguns casos, se houvesse uma comparação com outros países do mundo, tal número representa-se bastante significativo. Entretanto, em parâmetros nacionais, tal soma representa apenas 37,16% de toda a população brasileira. A tendência, por conseguinte, é de crescimento ainda por muitos anos em razão do incentivo governamental e político, bem como internacional, de atividades de lazer, diversão, compras públicas e operações financeiras. (ALBUQUERQUE, 2006).

Por reiteradas vezes, o Brasil foi líder em listas de países com maior incidência de atividades ilegais na seara computacional do mundo e, recentemente, atingiu o patamar alarmante que lhe concedeu o título de campeão mundial em pornografia infantil. Além do mais, apesar do crescente incentivo e aumento do uso da internet para todos os cidadãos indistintamente é considerável notar que o crescimento de tais acessos têm gerado uma fase difícil quanto à prática de crimes virtuais. (MALAQUIAS, 2012).

O sistema jurídico brasileiro, diferentemente dos outros países latino americanos, não está vinculado a tratados internacionais de combate à criminalidade informática. A legislação brasileira preconiza a ideia de que as normas jurídicas internas podem vir a posicionar-se em um mesmo patamar ou nível hierárquico que as demais convenções ou tratados internacionais. (MALAQUIAS, 2012).

Destaque-se que a legislação brasileira se mostra por diversas vezes obsoleta e ausente no tocante à prática e disciplina de medidas judiciais e legislativas cabíveis. Durante um longo período, apenas o Código Civil e Penal, de maneira singela combatia

a criminalidade informática no tocante a reparação indenizatória cível e de aplicabilidade material de crimes convencionais, desconsiderando o uso ou auxílio do computador ou de sistemas informáticos. (ALBUQUERQUE, 2006).

Entretanto, ainda nessa concepção, já é pacífica a ideia de que para os crimes cometidos na seara informática não se deve aplicar as medidas judiciais convencionais. O Brasil, aos poucos, diante dessa situação, teve que se adequar e elaborar legislações específicas diante de fatos sociais ou jurídicos ocorridos no espaço cibernético e que têm obrigado, sobremaneira, os legisladores a abdicarem de imputações deficientes e ineficazes. (MALAQUIAS, 2012).

Considerável notar que a recente legislação que recebeu o título de "Lei Carolina Dieckmann" em homenagem a atriz vítima de invasão indevida de imagens contidas em sistema informático de natureza privada e cujo episódio desencadeou a celeridade de projetos que já tramitavam com o fito de regulamentar essas práticas invasivas perpetradas em meios informáticos para modernização do Código Penal Brasileiro. (CABETTE, 2012).

Os sistemas informáticos não são mais sistemas restritos quanto a seu acesso e a troca de dados pode ocorrer entre diversos lugares por meio de diversos computadores. Diante dessa troca cada vez mais frequente, a intimidade do usuário está cada vez mais passível de sofrer algum tipo de violação. A maior causa de ameaça a intimidade é a própria ausência de conhecimento de quem a utiliza e pela falta de transparência por parte dos agentes que compõe o meio cibernético. (ALBUQUERQUE, 2006).

O mundo cibernético está regrado de muitos princípios e comentários acerca da proteção à intimidade do usuário. De toda sorte, tais princípios mostram-se conflitantes e dificultam a proteção desse direito subjetivo do cidadão brasileiro. Entretanto, além da nova previsão legal, existe no direito brasileiro uma previsão, ainda que singela, de proteção a intimidade. Está previsto no artigo 5º, inciso X, da Constituição Federal de 1988, o qual prevê que serão invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, estando resguardados os direitos para pleitear ações de ressarcimento de danos morais ou patrimoniais decorrentes de sua violação. (ALBUQUERQUE, 2006).

Além de violações subjetivas à intimidade, a utilização inadequada de alguns sujeitos do espaço cibernético também pode acarretar prejuízos consideráveis na ordem econômica. Com técnicas apropriadas, hackers invadem sistemas e computadores e

cometem crimes das mais variadas espécies e que estão previstos no Código Penal Brasileiro como crimes comuns, e são eles: furto de uso de sistemas informáticos, estelionato e até mesmo, o crime de peculato. (ZANIOLO, 2012).

Por fim, outra vítima da atividade do agente infrator é o próprio sistema informático que, em quase todos os casos são alvos principais de invasão. O crime contra sistemas informáticos ou dados armazenados consuma-se no momento da subtração de suporte de dados ou se estes forem transferidos para outro tipo de aparelho ou suporte. O método de acesso ao determinado sistema, as vezes pouco importa. Entretanto, se o controlador do sistema conceder autorização para que os dados venham a ser copiados ou redistribuídos, não haverá prática de delito diante do prévio consentimento. (OLIVEIRA, 2012).

Nesse sentido, o interesse jurídico protegido é a integridade dos dados e serviços armazenados que podem ser de uso pessoal, público ou que diga respeito ao próprio sistema informático. Contudo, é necessário outro requisito para que seja configurada a conduta delitiva, que diz respeito ao fato de o sistema de computador estar previamente protegido por alguma medida preventiva cometida por parte do proprietário. As mais comuns delas diz respeito a instalação de algum programa de proteção contra ataques e invasões de vírus ou a existência de uma senha previamente instalada no dispositivo. (CABETTE, 2012).

A Lei 12.737, de 30 de novembro de 2012, trouxe para o ordenamento jurídico-penal brasileiro o novo crime de “Invasão de dispositivo informático”, a qual incide na situação de invasão de dispositivo informático alheio conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com 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. (JATOBÁ, 2012).

O bem jurídico tutelado em análise especial é a privacidade das pessoas, no sentido de assegurar-lhes a liberdade individual, eis que a conduta está prevista no rol de artigos entre os artigos 146 à 154 do Código Penal Brasileiro. A proteção mencionada, por sua vez, apenas está ligada aos interesses pessoais das pessoas físicas, excluindo-se aqui as jurídicas, bem como tutelas coletivas de redes mundiais de computadores (OLIVEIRA, 2012).

Por fim, o agente que praticou a conduta deve agir somente contra o dispositivo informático de outrem desde que estejam previamente protegidos com programas de segurança ou antivírus, por exemplo. Ainda que a invasão caracterize violação indevida de mecanismos de segurança e contra informações de redes sociais não são suficientes para caracterização do crime, tornando o fato atípico. (CABETTE, 2012).

Cometerá a infração cibernética prevista na Lei 12.737/12, isto é, será considerado como sendo agente ativo da conduta criminosa qualquer indivíduo, que tenha o fim especial de obter, adulterar ou destruir dados ou informações e instalar dados que acarretem prejuízo à vítima. Entretanto, interessante notar que não existe necessidade alguma de condição especial do agente, muito menos que este tenha alguma qualidade diferenciadora. (CUNHA, 2013).

Pelo que dispõe o referido artigo, não poderá figurar como sujeito ativo deste crime o titular legal ou dono do dispositivo informático posto que, a legislação penal vigente preconiza a ideia de que o crime seja cometido contra objeto material de outrem. O acesso realizado pelo titular a informações protegidas por terceiros configura, pois, fato atípico. (MIRABETE, 2013).

Ademais, conforme disposto no parágrafo primeiro do artigo 154-A do Código Penal, deverá também ser considerado com sujeito ativo, qualquer pessoa que venha a produzir, oferecer, distribuir, vender ou difundir dispositivo ou programa computacional almejando permitir a prática delituosa de invasão de dispositivo informático. (CUNHA, 2013). Excepcionalmente, o crime pode ser cometido por funcionário público, desde que este o realize no exercício regular de suas funções, entretanto, não há majoração de pena na lei para essa situação. (CABETTE, 2012).

Em contrapartida, figurará como sujeito passivo do crime cibernético qualquer pessoa, física ou jurídica, desde que, seja proprietária do dispositivo informático que fora invadido pelo criminoso. É necessário, para configuração do delito, que o dispositivo esteja com outrem a qualquer título, seja quanto à propriedade, bem como a simples posse. (CUNHA, 2013).

Também poderá figurar no polo passivo da conduta criminosa de invasão do dispositivo informático qualquer autoridade que se enquadre nos casos de: Presidente da República, governadores e prefeitos; Presidente do Supremo Tribunal Federal; Presidente da Câmara dos Deputados; Presidente do Senado Federal e de Assembleias Legislativas

estaduais, do Distrito Federal ou municípios; Dirigente máximo da administração pública direta e indireta em qualquer âmbito da federação. Nesses casos, a pena para o agente infrator deverá ser aumentada de um terço à metade e a ação penal deverá ser pública incondicionada. (MIRABETE, 2013).

Será punido o agente que invade dispositivo informático alheio, em decorrência da violação ilegal de mecanismo de segurança ou que exista instalação de vulnerabilidades. O objeto jurídico protegido é a inviolabilidade da intimidade e a vida privada das pessoas, porém, o objeto material do delito diz respeito ao dispositivo informático e há uma única ação típica descrita no caput do artigo que consiste na invasão do dispositivo informático de outrem ou a redes de computadores, por meio de violação de dispositivo de segurança pré-instalado. (NUCCI, 2013).

Entende-se por dispositivo qualquer aparelho, mecanismo ou meio eletrônico que esteja munido de uma função eletrônica específica que estão aptos a armazenar informações na seara computacional. Pelo dispositivo informático, no tipo em questão, deve-se levar em consideração sistemas ou aparelhos que viabilizem o armazenamento de informações pela via eletrônica, como por exemplo, computadores de qualquer espécie, telefones móveis e smartphones, desktops, notebooks, ipads, tablets etc. (MIRABETE, 2013).

A invasão do dispositivo, isto é, seu tipo objetivo, consiste em entrar ou ingressar em software de outrem com a finalidade de ter acesso ao conteúdo que foi informatizado, seja ele de qualquer natureza, bem como o sistema operacional, programas ou aplicativos, dados, documentos, senhas etc. Entretanto, a lei silencia no que diz respeito ao fato de o dispositivo estar ou não conectado à rede mundial de computadores. (MIRABETE, 2013).

A lei exige que para configuração do crime, que o dispositivo esteja munido de aparatos, físicos ou não, desde que instalados com a finalidade precípua de evitar o acesso não autorizado, como por exemplo, senhas, códigos etc. Estará afastada a tutela, pois, nos casos de dispositivos desprotegidos ou desabilitados, temporária ou permanentemente. (NUCCI, 2013).

O elemento subjetivo do tipo penal em comento consiste na vontade de realizar a ação na forma descrita no artigo, com a consciência do agente que age de modo indevido. No que concerne a invasão do dispositivo, o elemento subjetivo é a a obtenção, alteração

e destruição dos dados e informações. Tipifica a lei, portanto, as finalidades que habitualmente configuram as atividades dos hackers. (CUNHA, 2013).

Preocupou-se o legislador em repreender as práticas ilícitas difundidas no âmbito da internet e em outras redes de comunicações eletrônicas ou informáticas. Em regra, o combate deve se dar em face dos chamados piratas da internet, os quais são capazes de promover a introdução de vírus ou pacotes de ameaças no dispositivo. Dentre estes, o mais notório pode ser exemplificado como cavalo de troia, o qual libera uma porta de comunicação com outros agentes infratores e que viabiliza invasões futuras. (MIRABETE, 2013).

Quanto à invasão que objetive conseguir vantagem ilícita, preocupou-se o legislador em determinar que o agente não obtenha para si um ganho patrimonial imediato. Por vantagem ilícita é compreensível que a obtenção de qualquer vantagem que exista em desacordo com as normas legais. Da redação final do artigo, está afastada a tipificação da conduta na hipótese de existência de propósitos distintos cometidos pelo agente que não os elencados acima, como por exemplo, o de simples vistoria ou espionagem. (NUCCI, 2013).

Estará consumado o tipo penal de invasão de dispositivo informático quando o agente infrator violar mecanismo de segurança e invadir o software do mesmo dispositivo, colocando-se em condições de acesso indevido ou qualquer outra hipótese que possibilite o manuseio do seu conteúdo. Por outro lado, para que esteja consumada a conduta do agente, é desnecessário que o agente tenha atingido qualquer das finalidades previstas no tipo. (MIRABETE, 2013).

Contudo, será admitida a tentativa quando o agente, embora tenha iniciado a execução do ato criminoso por meio da invasão do dispositivo informático, não obtém sucesso ante ao fato de não ter conseguido violar o mecanismo de segurança ou caso esteja presente qualquer outra situação estranha que lhe interrompa ou atrapalhe. (MIRABETE, 2013).

Como circunstância majorante, entende a doutrina que a pena será aumentada de 1/6 a 1/3 se houver prejuízo econômico para a vítima em decorrência da invasão, pelo que dispõe o §2º do art154-A do Código Penal. Ainda nessa circunstância, o §4º preconiza o aumento da pena de um a dois terços ante a ocorrência de divulgação, comercialização ou transmissão do conteúdo e dados a outrem, a qualquer título. (NUCCI, 2013).

Como circunstâncias qualificadoras, há a hipótese de punição do agente criminoso com a pena de reclusão de seis meses a dois anos, acrescidos de multa. Tal qualificadora é disposta no §3º do referido artigo é decorre da invasão que resulta da obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais e informações sigilosas. Ainda incorre nessa qualificadora se da invasão resultar o controle remoto não autorizado do dispositivo cibernético, atuando o agente como um hóspede indesejado nos domínios cibernéticos de sua vítima. (CUNHA, 2013).

Por fim, para que seja possível a apuração do crime de invasão de dispositivo informático é fundamental que, a ação penal seja pública condicionada à representação do ofendido ou de seu representante legal. Porém, proceder-se à mediante ação penal pública incondicionada quando o crime for praticado contra órgãos da administração pública, entidades da administração indireta ou empresas concessionárias de serviços públicos. Além disso, caso o crime seja praticado em face de bens, serviços ou interesse da União ou de seus entes, a competência para ação será da Justiça Federal. (CUNHA, 2013).

Após um hiato de nove anos, foi realizada uma alteração na Lei 12.737/12 que disciplina o art. 154-A do CP no tocante aos crimes de invasão de dispositivo informático. Em 27 de maio de 2021, a Lei 14.155/2021 passou também a tornar crimes a invasão do dispositivo informático, furto e estelionato cometidos pela via eletrônica ou pela internet.

O caput do art. 154-A do CP passou a considerar crime a invasão de dispositivo informático de uso alheio, esteja ele conectado ou não à rede de computadores. A finalidade trazida neste tipo penal é a obtenção, adulteração ou destruição de dados ou informações sem autorização, seja ela expressa ou tácita, da vítima.

Outro ponto que merece destaque é alteração no tocante à invasão para instalação de vulnerabilidades no dispositivo, com vistas a obtenção de vantagem ilícita. Por meio desta atualização do dispositivo, a pena para o crime foi majorada para reclusão, de 1 (um) a 4 (quatro) anos, e multa.

As agravantes para o crime disposto no art. 154-A também foram atualizadas, em caso de resultar vantagem econômica para o sujeito ativo, majorando-se para 1/3 (um terço) a 2/3 (dois terços), passando a pena a ser de reclusão, de 2 (dois) a 5 (cinco) anos, e multa.

Além do crime previsto no art. 154-A, a Lei de nº 14.155/2021, também alterou crimes já existentes no Código Penal, quais sejam: o crime de furto (art. 155 do CP) e o crime de estelionato (art.171 do CP).

No art. 155 do CPC (furto) passou a constar em seu §4-B que a pena será de reclusão de 4 (quatro) a 8 (oito) anos, e multa, se o furto de informações mediante fraude for cometido por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento análogo.

Nesta modalidade, através de violação de dispositivo de informática, também houve mudanças com a inclusão de agravantes da pena, aumentando-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. Além de tal ponto, a pena será aumentada de 1/3 (um terço) ao dobro, se o crime é praticado contra idoso ou vulnerável.

O novo dispositivo regulamenta e defende novas competências para o crime de estelionato (art. 171), cometido nesta modalidade por meio de invasão de dispositivo, configurando a denominada fraude eletrônica. A obtenção da vantagem mediante fraude também é elemento caracterizador para o crime de estelionato eletrônico. O art. 171, §2º-A prevê que a pena será de reclusão de 4 (quatro) a 8 (oito) anos, e multa, se a fraude for cometida com a utilização de informações obtidas mediante indução a erro da vítima, seja pelo uso de redes sociais, contatos telefônicos ou por qualquer outro meio fraudulento análogo.

Em caso de o crime de fraude eletrônica ser praticado mediante utilização de servidor mantido fora do território nacional, a pena será majorada de 1/3 (um terço) a 2/3 (dois terços), considerando a relevância do resultado gravoso.

Apontava-se que a lei anterior disciplinava penas mais brandas, frente à gravidade do ilícito cometido. O novo dispositivo legal (Lei 14.155/2021) traz mais segurança para a aplicabilidade da Lei “Carolina Dieckmann”, haja vista ter sido considerada ineficaz por alguns aplicadores do direito. Um dos pontos que destacaram a ineficácia da norma, refere-se às restrições trazidas pelo dispositivo, sem que pudessem ser ampliadas para outros crimes previstos no Código Penal.

Importante destacar que durante um longo período, o judiciário brasileiro mostrou inexistência de legislações especiais que pudessem definir as atitudes e condutas dos

sujeitos ativos dos crimes cibernéticos. Tal ausência legal, não só no Brasil, mas também em alguns pontos do cenário mundial, apenas contribuía para reforçar ainda mais a prática dessas atividades delitivas dos criminosos e consagrava a sua impunidade. (MALAQUIAS, 2012).

O delito cibernético é uma realidade indiscutível à atualidade forense. Tais crimes, muitas vezes, configurarem-se como atípicos, isto é, sem previsão legal anterior que os definissem como crimes cibernéticos. Ocorre que, o resultado do cibercrime pode ser mostrar completamente difuso e ramificado. (COLLI, 2010).

A ausência de previsibilidade dos cibercrimes na legislação brasileira fez com que tais condutas que, são de caráter especial por necessitarem do ambiente informático para se materializarem, fossem tipificadas como crimes comuns. Em alguns casos, havia a necessidade de os órgãos julgadores basearem-se no Princípio da Reserva Legal (Princípio da Legalidade) para absolverem os criminosos, ante a falta ou ausência de previsão, pois tal princípio apenas considera como típico ou punível as condutas que sejam previamente consideradas como crime. (ZANIOLO, 2012).

Apesar das lacunas legislativas terem perdurado por décadas no direito brasileiro, é possível destacar a existência de projetos de lei que tramitaram no Congresso Nacional. Um dos projetos mais importantes foi o do deputado Eduardo Azeredo do PSDB de Minas Gerais, versando sobre tipificar condutas realizadas mediante uso de sistema eletrônico.

A Lei 12.735/12 versa sobre tipificação de condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que tenham sido praticadas contra sistemas informatizados e similares. Além disso, serão estruturados, pelos órgãos da polícia judiciária, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado. (CABETTE, 2012).

Nesse sentido, a doutrina penal brasileira manifestou-se em relação ao previsto em tal dispositivo e defende que para que esteja configurado o crime do art.266 do Código Penal não basta apenas que haja prejuízo de um único aparelho telefônico, pois o mesmo artigo tutela o interesse coletivo na manutenção do serviço. É necessário que a conduta atinja um serviço considerável de uma região e que prejudique um número indeterminável de sujeitos. Concluiu-se, ao mesmo a princípio que, o criminoso que incide em tal conduta deve atentar contra certa circunscrição em um mesmo bairro ou até mesmo no país inteiro.

Levando em consideração a invasão combatida pela Lei 12.737/12, esta apenas deve ser defendida se a mesma ocorrer em um dispositivo informático seja ele computador ou periférico. Isto é, a conduta descrita pela Lei "Carolina Dieckmann" é apenas aquela realizada em um dispositivo eletrônico. Diante de tal situação, caso existam invasões de perfis de redes sociais, e-mails ou bancos de imagens que não tenham ligação com o objeto físico e material do computador da vítima, não ocorrerá a prática do crime em questão. (JATOBÁ, 2012).

Correntes doutrinárias apontam que a Lei 12.737/12 é, sobremaneira genérica e que apenas fora formulada no intuito de proteger ou de acalmar algo que era discutido pela mídia acerca da invasão de dispositivos eletrônicos da atriz e não propriamente do seu direito violado. Apesar de toda a repercussão nacional difundida pelo caso, algumas dúvidas surgiram. Uma questão importante para o doutrinador Wiliam César Pinto de Oliveira é acerca de que se o uso de um computador feito por pessoa diversa do seu proprietário configuraria a conduta de invasão como elemento caracterizador. (OLIVEIRA, 2012).

Além da generalidade do objeto material da referida lei, outro aspecto que se destaca em críticas doutrinárias é no tocante à cominação da pena. Esta pode ser considerada como expressivamente baixa em relação ao dano causado pela conduta e serão muitos os casos que poderá ocorrer os fenômenos jurídicos da prescrição e da transação penal.

Além do mais, entende a recente corrente doutrinária penalista brasileira de que nos casos descritos pela nova legislação não serão cabíveis os casos de prisão temporária ou preventiva, sequer os casos de prisões em flagrante ante a situação de que o autor do delito que comparece em juízo assume o compromisso acaba sendo liberado em razão desse comparecimento, mostrando-se inócua, apesar de inovadora a presente lei (OLIVEIRA, 2012).

CONSIDERAÇÕES FINAIS

As transformações ocorridas nos últimos anos têm afetado e muito o modo de vida e o comportamento do indivíduo. O advento da globalização, permitiu ao homem moderno, ter acesso à diversos setores da informação e conhecimento outrora incapazes

de serem percebidos. Uma das grandes transformações ocorridas no século XX, sem dúvida, foi o desenvolvimento da tecnologia da informação.

Diante da crescente utilização de mecanismos informáticos, como por exemplo, computadores, dispositivos de software e hardware, tecnologia wireless, entre outros, a mais significativa é, sem dúvidas, a internet. Tal descoberta científica oriunda do período da Guerra Fria, na década de 1970, permite ao usuário que este tenha acesso ou possa transmitir uma quantidade significativa de dados e informações em um pequeno lapso de tempo a qualquer região do mundo.

Entretanto, apesar das facilidades de conexão e acesso trazidas pela internet ao homem moderno, a mesma também trouxe facilidades quanto à ocorrência de delitos e infrações penais. Dentre essas infrações, é possível identificar a ocorrência dos chamados crimes cibernéticos. Diante disso, pode-se concluir que o ambiente informático pode servir não apenas para a consumação de delitos criminais, como também para a consecução ou elaboração de tais delitos.

Referidas facilidades e advertências decorrentes do acesso do computador e internet configuram, pois, o que alguns autores consideram de paradigma de acesso à informação. Posto que, apesar das diversas vantagens decorrentes deste uso, pode conter uma quantidade razoável de ameaças virtuais existentes e que, possam colocar em risco o progresso das relações pessoais, comerciais e internacionais decorrentes do uso da tecnologia da informação advento do século XXI.

Tal paradigma, contudo, apresenta alguns pontos sensíveis e com certa carência diante da atuação do Estado no sentido de fixar parâmetros legais, definir competências, instituir taxas e tributos, efetuar registros de domínios, bem como garantir os direitos ao consumidor virtual e outros inúmeros temas que apenas se consolidarão por meio da existência de uma legislação especial ou de uma reforma do Código Penal brasileiro atual.

Durante muito tempo, o direito brasileiro atravessou uma fase delicada no tocante à incidência de delitos cibernéticos em decorrência da amplitude e popularização do acesso aos dispositivos informáticos e da crescente necessidade de acesso às informações para relações sociais. Contudo, o direito brasileiro já dispõe de dispositivos legais específicos para combate ante a ocorrência dos cibercrimes.

Promulgada no final do ano de 2012, a Lei nº12.737/12 intitulada de “Lei Carolina Dieckmann” diante do fato de terem sido divulgadas fotos íntimas do computador da atriz

que estava em uma assistência técnica. Apesar de todo o alvoroço da época diante do fato, o Brasil agora pode contar com um mecanismo de combate aos delitos.

Tal dispositivo, no entender de alguns autores não assegura uma proteção muito eficaz, em razão algumas peculiaridades apresentadas diante da conduta do criminoso e tímida previsão da pena. O referido diploma, que acrescenta ao Código Penal brasileiro o art154-A que trata da invasão de dispositivo informático, apresenta algumas considerações que se mostram, de certa forma, antagônicas.

O que de fato pode ser concluído, no entender desses autores é que, a pena aplicada pelos crimes cometidos e abrangidos por tal dispositivo é extremamente insignificante, de no máximo um ano acrescidos de multa o que poderá configurar a conversão dessa pena restritiva de liberdade em penas alternativas ou restritivas de direitos apenas.

Ademais, a conduta do agente é muito específica, o que faz com que o dispositivo legal se mostre bastante restrito diante das inúmeras possibilidades de infrações que podem ser cometidas no ambiente cibernético. Tal restrição também se estende ao fato de que o dispositivo invadido deve estar previamente protegido por um mecanismo de segurança próprio do computador ou posteriormente instalado, como por exemplo um antivírus.

As especificidades decorrentes de tais diplomas apenas refutam a ideia de que a luta e combate aos crimes cibernéticos não deve ser dada por satisfeita e encerrada. Tal combate não deve só versar acerca do crime propriamente dito, como também, do aperfeiçoamento dos diplomas legais já existentes para que nenhum indivíduo possa vir a sair prejudicado e ter seus direitos devidamente resguardados.

A Lei 14.155/2021 traz ao ordenamento jurídico um marco significativo, qual seja o aumento das penas anteriormente previstas na lei 12.737/12, bem como amplia a ilicitude penal para outros delitos, tais como furto e estelionato, agora cometidos por meio da modalidade informática e que representam, sobremaneira, mais segurança para as vítimas dos crimes cibernéticos, que podem contar com um dispositivo legal mais inibidor.

Apesar disto, conclui-se que a situação não está completamente satisfeita. O Brasil é um dos países líderes no cometimento de crimes no âmbito da internet e de rede de computadores. As controvérsias estão longe de se tornarem pacíficas e o Brasil não pode, ao menos nesse momento, sentir-se país blindado e fortalecido para contra este tipo de

delito. Com a promulgação destes dispositivos legais, é sinal de que não só a população, assim como a legislação brasileira caminha a frente, junto ao combate dos crimes cometidos na esfera cibernética, sem qualquer amparo legal mais eficaz.

REFERÊNCIAS

ALBUQUERQUE, Roberto Chalcon de. **A Criminalidade Informática**. 1ª edição. São Paulo: Editora Juarez de Oliveira, 2006.

BITENCOURT, Cezar Roberto. **Tratado de Direito Penal**. Parte Geral 1. 19ª edição revista, atualizada e ampliada. São Paulo: Editora Saraiva, 2013.

BITENCOURT, Cézar Roberto. **Invasão de dispositivo informático**. Disponível em: <http://atualidadesdodireito.com.br/cezarbitencourt/2012/12/17/invasao-de-dispositivo-informatico/>. Acesso em: 27/05/2021.

BRASIL. **Lei nº 12.735, de 30 de novembro de 2012**. 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. Brasília, 30 de novembro de 2012; 191o da Independência e 124o da República.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal; e dá outras providências. Brasília, 30 de novembro de 2012; 191o da Independência e 124o da República.

CABETTE, Eduardo Luiz Santos. **Primeiras impressões sobre a Lei nº 12.737/12 e o crime de invasão de dispositivo informático**. 2012. Disponível em http://jus.com.br/artigos/23522/primeiras-impressoes-sobre-a-lei-no-12-737-12-e-o-crime-de-invasao-de-dispositivo-informatico. Acesso em 08/09/2013.

CANONGIA. Claudia. **Segurança cibernética: o desafio da nova Sociedade da Informação.** Brasil. 2009. Disponível em: http://www.cgee.org.br/parcerias/p29.php. Acesso em 17 de março de 2013 às 20:25.

CAPEZ, Fernando. **Curso de Direito Penal** – Parte Geral. 15ª edição. São Paulo. Editora Saraiva. 2012.

Convenção Sobre o Cibercrime. 2004. Disponível em: <://ccji.pgr.mpf.gov.br/documentos/docs_documentos/convenção_cibercrime.pdf>. Acessado em 23 de maio de 2013 às 19:47.

COLLI, Maciel. **Cibercrimes** – Limites e Perspectivas. A Investigação Policial de Crimes Cibernéticos. 1ª edição. Curitiba. Juruá Editora, 2010.

CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet**. 5ª edição revista e atualizada. São Paulo: Editora Saraiva, 2010.

CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. 1ª edição. São Paulo: Editora Saraiva, 2011.

CRESPO, Xavier de Freitas. **Diretivas Internacionais e Direito Estrangeiro** - Crimes Digitais. São Paulo. Saraiva, 2011.

CUNHA. Rogério Sanches Cunha. **Manual de Direito Penal Parte Especial**. Volume Único. 5ª Edição. Salvador-BA. Editora Jurispodium. 2013.

FERREIRA. Érica Lourenço de Lima. **Internet – Macrocriminalidade e Jurisdição Internacional**. 1ª Edição. Curitiba: Juruá Editora. 2008.

FRANÇA. Genival Veloso de. **Medicina Legal**. 9ª edição. Editora Guanabara Koogan. São Paulo/SP. 2011.

GUIMARÃES. Marco. **Informática para concursos**. IDAJ. Recife/PE. 2011.

HURWITZ, Judith; BLOOR, Robin; KAUFMAN, Marcia; HALPER, Fern. **Cloud Computing for Dummies**; 1 edição. Indiana. EUA. 2010.

JATOBÁ, João Felipe Brandão. **A falha da Lei nº 12.737/12**: abrangência dos serviços telemáticos. 2012. Disponível em: http://jus.com.br/artigos/23172/a-falha-da-lei-no-12-737-12-abrangencia-dos-servicos-telematicos. Acessado em 09/09/2013 às 17:25.

LIMA, Paulo Marco Ferreira. **Crimes de Computador e Segurança Computacional**. 2ª edição. São Paulo: Editora Atlas S.A. 2011.

MALAQUIAS. Roberto Antônio Darós Malaquias. **Crime Cibernético e Prova** – A Investigação Criminal em Busca da Verdade. 1ª Edição. Curitiba. Juruá Editora. 2012.

MIRABETE. Julio Fabbrini. FABBRINI. Renato N. **Código Penal Interpretado**. 8ª Edição. São Paulo/SP. Editora Atlas. 2013.

NUCCI, Guilherme de Souza. **Código Penal Comentado**. 13ª Edição revista, atualizada e ampliada. São Paulo. Editora Revista dos Tribunais. 2013.

OLIVEIRA, William César Pinto. **Lei Carolina Dieckmann**. 2012. Disponível em: http://jus.com.br/artigos/23655/lei-carolina-dieckmann. Acesso em 09/09/2012 às 18:45.

PEDROSA. Paulo H.C; NOGUEIRA, Tiago. **Computação em Nuvem**. Brasil, 2011. http://www.ic.unicamp.br/~ducatte/mo401/1s2011/T2/Artigos/G04-095352-120531-t2.pdf. Acesso em 16 de Março de 2013.

VELLOSO, Fernando de Castro. **Informática Conceitos Básicos**. 8ª edição revisada e atualizada. Elsevier Editora. São Paulo 2011.

WOLF, W. **Computers as Components**: Principles of Embedded Computing SystemDesign.Disponívelem:http://www.aedb.br/seget/artigos08/566_566_Artigo_Seget_14-08-2008.pdf. McGraw-Hill, 2001.

ZANIOLO, Pedro Augusto. **Crimes Modernos** – O Impacto da Tecnologia no Direito. 2ª Edição. Curitiba: Juruá Editora. 2012.

COMO CITAR

BEZERRA, J. M. V. APLICABILIDADE DA LEI Nº 12.737/12 SOBRE CRIMES CIBERNÉTICOS. **Revista Interdisciplinar Encontro das Ciências – RIEC**, v.5, n.2, 2022.