



UNIVERSIDADE FEDERAL DO MARANHÃO – UFMA
CENTRO DE CIÊNCIAS SOCIAIS, SAÚDE E TECNOLOGIA – CCSST
CURSO DE DIREITO

RUAN MARTINS DA SILVA

CRIMES VIRTUAIS: UMA ABORDAGEM DA CONDUTA CRIMINOSA POR
MEIO DA INTERNET

Imperatriz – MA

2022

RUAN MARTINS DA SILVA

**CRIMES VIRTUAIS: UMA ABORDAGEM DA CONDUTA CRIMINOSA POR
MEIO DA INTERNET**

Trabalho de Conclusão de Curso
apresentado a Universidade Federal do
Maranhão – Campus Imperatriz como
requisito para obtenção do Grau de Bacharel
em Direito, sob orientação da Prof^a Dra.
Conceição Aparecida.

Imperatriz - MA

2022

RUAN MARTINS DA SILVA

Ficha gerada por meio do SIGAA/Biblioteca com dados fornecidos pelo(a) autor(a).
Diretoria Integrada de Bibliotecas/UFMA

MARTINS DA SILVA, RUAN.

CRIMES VIRTUAIS: UMA ABORDAGEM DA CONDUTA CRIMINOSA POR
MEIO DA INTERNET / RUAN MARTINS DA SILVA. - 2022.
50 f.

Orientador(a): CONCEIÇÃO APARECIDA BARBOSA.

Monografia (Graduação) - Curso de Direito, Universidade
Federal do Maranhão, IMPERATRIZ - MA, 2022.

1. AVANÇO TECNOLÓGICO. 2. CRIMES VIRTUAIS. 3.
GLOBALIZAÇÃO. 4. LEGISLAÇÃO. I. APARECIDA BARBOSA,
CONCEIÇÃO. II. Título.

RUAN MARTINS DA SILVA

Trabalho de Conclusão de Curso apresentado a Universidade Federal do Maranhão – Campus Imperatriz como requisito para obtenção do Grau de Bacharel em Direito, submetido à Banca Examinadora.

BANCA EXAMINADORA

Orientador (a):

Prof^a. Dr^a. Conceição Aparecida Barbosa
Universidade Federal do Maranhão – Campus Imperatriz

Membro:

Prof. Dr. Artur Antonio da Rocha
Universidade Federal do Maranhão – Campus Imperatriz

Membro:

Prof. Gabriel Araújo Leite
Universidade Federal do Maranhão – Campus Imperatriz

Julgado em: 09 de dezembro de 2022

Aos meus pais, amigos e familiares que
sempre me ajudaram e incentivaram
durante minha trajetória acadêmica.

AGRADECIMENTOS

Primeiramente a Deus, pelo dom da vida, sabedoria, por sempre me fazer persistir e me ajudar a chegar até aqui em meio a tantos obstáculos enfrentados;

A minha família, em especial meus pais, que me ajudaram e sempre me apoiaram para que o meu sonho de graduação pudesse ser alcançado, abdicando de seus sonhos pessoais para que o meu fosse atingido e sempre me ensinando a andar pelo caminho da ética, moral e da fé;

Aos meus familiares por todo incentivo e confiança depositada;

A minha professora e Orientado Dra. Conceição Aparecida, por todo auxílio durante construção do meu trabalho de conclusão de curso, e por toda a atenção prestada quando necessário;

Enfim, a todos que de forma direta ou indireta contribuíram para que essa graduação pudesse ser concluída.

“A única maneira de fazer um bom trabalho é amando o que você faz”. Se você ainda não encontrou, continue procurando. Não se desespere. “Assim como no amor, você saberá quando tiver encontrado”.

(Steve Jobs)

RESUMO

Apesar de sua grande utilidade, a internet tem se tornado um ambiente vulnerável à prática de várias condutas danosas, tornando-se necessário, a aplicação de legislações específicas para conter a prática de tais atos. Com a evolução da internet, surge uma problemática neste mundo virtual: novas modalidades de ataques à honra alheia. Outro grande problema está relacionado a falta de proteção aos usuários da internet, já que o direito possui uma certa morosidade em acompanhar evolução do mundo virtual, acerca da criação de novas leis ou atualizar as já existentes. O presente trabalho tem como alvo demonstrar os tipos de crimes praticados por meio da internet, bem como a legislação brasileira vigente, que com a correta aplicação das leis, rebatam os crimes virtuais. Metodologicamente, o presente trabalho é construído a partir de uma abordagem dedutiva e por meio de pesquisa bibliográfica, onde foram analisadas legislações. Dessa forma, é possível evidenciar que a prática desse tipo de crime aumente cada vez mais à medida que nos tornamos dependentes dos meios virtuais.

Palavras chave: Avanço tecnológico. Globalização. Crimes virtuais. Legislação.

ABSTRACT

Despite its great utility, the internet has become a vulnerable environment for the practice of various harmful conducts, making it necessary to apply specific legislation to contain the practice of such acts. With the evolution of the internet, a problem arises in this virtual world: new ways of attacking the honor of others. Another major problem is related to the lack of protection for internet users, since the law has a certain delay in following the evolution of the virtual world, regarding the creation of new laws or updating existing ones. The present work aims to demonstrate the types of crimes committed through the internet, as well as the current Brazilian legislation, which with the correct application of the laws, rebut virtual crimes. Methodologically, the present work is built from a deductive approach and through bibliographical research, where legislations were conducted. Thus, it is possible to show that the practice of this type of crime increases more and more as we become dependent on virtual means.

Keywords: Technological advancement. Globalization. Cyber crimes. Legislation.

LISTA DE ABREVIATURAS E SIGLAS

ARPANET - Advanced Research Projects Agency Network

CF – Constituição Federal

CP – Código Penal

ECA – Estatuto da Criança e do Adolescente

IBGE – Instituto Brasileiro de Geografia e Estatística

IP – Internet Protocol

MC - Ministério das Comunicações

MCT - Ministério da Ciência e Tecnologia

NCP - Network Control Protocol

ONU – Organização das Nações Unidas

UCLA – Universidade da Califórnia em Los Angeles

UCSB – Universidade da Califórnia em Santa Bárbara

UNCTAD - Conferência das Nações Unidas sobre Comércio e Desenvolvimento

SUMÁRIO

1. INTRODUÇÃO	11
2. REVISÃO DE LITERATURA.....	14
2.1 A INTERNET	14
2.1.2 Surgimento, evolução e transformações na sociedade a partir da internet.....	14
2.1.3 A Internet e seus conceitos.....	20
2.1.4 A relação entre a internet e o Direito	20
3. CRIMES VIRTUAIS	22
4. CLASSIFICAÇÃO DOS CRIMES VIRTUAIS.....	25
5. TIPIFICAÇÃO DOS CRIMES VIRTUAIS	26
5.1 Invasão de Privacidade	26
5.2 Aquisição e transferência ilegal de dados	31
5.3 Exposição e utilização indevida de informações	32
5.4 Crime contra a honra	33
5.5 Estelionato	35
5.6 Pornografia infantil	35
5.7 Estupro virtual	37
6. SUJEITOS DOS CRIMES VIRTUAIS	38
6.1 Sujeito ativo	38
6.2 Sujeito passivo	40
7. LEIS APLICÁVEIS NO ÂMBITO DOS CRIMES VIRTUAIS.....	40
8. CONSIDERAÇÕES FINAIS	45
REFERÊNCIAS.....	47

1. INTRODUÇÃO

Com as mudanças paradigmáticas ocorridas com a chegada do século XXI, a sociedade atingiu um nível de desenvolvimento tecnológico surpreendente, em virtude do processo de globalização. Com o passar do tempo, os meios tecnológicos foram se modernizando, tornando-se algo de prioridade no nosso dia a dia e nos deixando bastante dependentes dos meios de comunicação e tecnologia.

Apesar de todas essas facilidades provenientes do desenvolvimento da tecnologia, surge a problemática: a vulnerabilidade da sociedade contemporânea, a partir das modificações no comportamento humano provenientes do uso do computador, da internet e dos diversos meios tecnológicos de comunicação. Essa problemática está diretamente ligada a implementação de novos paradigmas culturais que são inseridos pelo meio virtual através das relações humanas, já que esse meio está povoado de pessoas com boas e más atitudes e intenções que desencadeiam os crimes virtuais.

Diante do surgimento de novas práticas criminosas, o Direito precisou adequar-se à nova realidade, a fim de tutelar os bens jurídicos e garantir a preservação dos direitos e de dignidade humana. Dessa forma, foi decretada a Lei nº 12.737/2012, denominada Lei Carolina Dieckmann, sancionada no dia 30 de novembro de 2012 que promoveu mudanças no Código Penal Brasileiro. Essa lei foi criada a partir do caso ocorrido com a famosa atriz brasileira e que teve grande repercussão. No caso em questão, a atriz teve o seu computador pessoal invadido e seus arquivos pessoais foram roubados e publicados por meio das redes sociais. A criação da Lei obteve vários elogios no meio jurídico e surgiu para garantir mais dignidade aos usuários da internet, preservando a privacidade e intimidade das pessoas.

Para o desenvolvimento do tema abordado foi utilizada a metodologia de cunho científico, tendo como base o método dedutivo, além da utilização de recursos bibliográficos que forneceram instrumentos analíticos para a construção do trabalho. Além desses, outros meios foram utilizados para mais informações e levantamentos acerca do tema discutido como jornais, periódicos e livros.

Não obstante, o presente trabalho tem o intuito de observar os conceitos, definições e tipos de crimes virtuais, analisando a composição histórica acerca do surgimento da internet e dos diversos meios de comunicação virtual.

A metodologia é definida como o procedimento utilizado para a análise e coleta de dados a partir da utilização de materiais que levem à obtenção de um resultado. O método utilizado na presente pesquisa foi a metodologia de cunho científico, tendo como base o método dedutivo, que a partir de teorias e leis existente pode-se chegar ao resultado.

Para o desenvolvimento do estudo, foi realizado o levantamento bibliográfico, a partir do uso de conceitos redigidos pelo Direito Brasileiro e demais legislação voltadas para a regulamentação da relação dos crimes virtuais e seus possíveis problemas para a segurança virtual da sociedade.

A evolução tecnológica provocou grandes mudanças que interferiram diretamente no comportamento humano. Por um lado, a criação da Internet e dos diversos meios de comunicação digital trouxeram inúmeros benefícios, por outro, apresentaram diversos riscos quanto a segurança digital e seus usuários tonando crimes como ataques cibernéticos contra a honra, difamação, estelionato e difamação cada vez mais comuns.

Segundo Cassanti (2014, p.22), um dos grandes problemas que tornam os crimes virtuais cada vez mais comuns é a falta de conhecimento dos usuários, pois não possuem entendimento necessário sobre os riscos que correm ao utilizar os meios de comunicação virtual.

O estudo do presente trabalho justifica-se pela necessidade de mostrar aos usuários os riscos existentes no meio virtual para quem o utiliza, fazendo com que assim eles possam identificar a quais riscos estão expostos e a partir disso se prevenir dos ataques. Também é relevante citar o posicionamento da legislação quanto

prática desses tipos de crimes como forma de punir o agressor quando praticar o delito e preservar os direitos das vítimas que sofrem com esse tipo de crime.

Portanto, objetiva-se demonstrar os conceitos dos tipos de crimes virtuais mais praticados, bem como os perigos que os usuários da Internet estão expostos, levando em consideração a prática criminosa proveniente do ambiente virtual e as leis aplicáveis a esse tipo de delito.

Acerca da Revisão de Literatura, será difundida a temática da internet que surgiu com o propósito de estreitar os laços da comunicação por meio de uma rede, na qual mudou, de fato, o cotidiano das pessoas. Desse modo, tornando-as cada vez mais dependentes dessa rede, não obstante, caberá ressaltar o surgimento, evolução e transformações da sociedade a partir da internet.

No que diz a respeito aos Crimes Virtuais, é imprescindível salientar o quão importante é o mecanismo da comunicação virtual para concretizar determinadas condutas criminosas. Sendo assim, há diversas formas para praticar esse ato ilícito, como, por exemplo, a inserção de vírus nocivos a um determinado computador, com intuito de subtrair dados do usuário ou até mesmo chantagem com a obtenção desses dados específicos e pessoais.

A temática da Classificação dos Crimes Virtuais aborda os crimes já previstos no ordenamento jurídico e praticados apenas por meio da utilização de recursos tecnológicos, onde sua consumação se dá apenas no meio digital, denominados crimes próprios; e os crimes iniciados no meio virtual, mas que seus efeitos se realizam no meio real, ou seja, os recursos tecnológicos funcionam como intermediário para a prática da ação, denominados crimes impróprios. Crespo (2011, p. 63)

O tópico de Tipificação dos Crimes Virtuais concerne a citação de diversos tipos de crimes, a exemplo o crime de invasão de privacidade, no qual as facilidades de propagação de informações de forma rápida através da utilização dos recursos tecnológicos, fazem da internet um instrumento causador de uma problemática para o homem contemporâneo que demanda atitudes desafiadoras para o campo do Direito (CANOTILHO, 2012).

A conceituação dos Sujeitos dos Crimes Virtuais é crucial no presente trabalho, tendo em vista que os sujeitos que podem ser classificados como sujeitos ativos e passivos, sendo o O sujeito ativo de um crime é caracterizado por uma pessoa que pratica uma conduta ilícita e é culpado para responsabilização de seu ato danoso, podendo 38 realizar essa ação individualmente ou com a participação de outros

autores (CAPEZ, 2005). Já o O sujeito passivo de um crime é caracterizado por um indivíduo que sofre algum tipo de delito oriundo de alguma conduta criminosa, seja ele pessoa física ou jurídica (BITENCOUT, 2007).

Por fim, o tópico das Leis Aplicáveis no Âmbito dos Crimes Virtuais tem a finalidade de demonstrar que devido a facilidade de prática do delito, os crimes virtuais podem ser executados por qualquer pessoa, de qualquer lugar ou dispositivo informático. Portanto, o grande número de usuários de tecnologia faz com que aumente a possibilidade de disseminação de informações falsas, desafiando a legislação ao investigar casos e identificar os sujeitos responsáveis por tais práticas (SIQUEIRA, 2017).

2. REVISÃO DE LITERATURA

2.1 A INTERNET

A internet é uma rede de comunicação que surgiu com o intuito de interligar dispositivos por meio de uma rede, e que foi evoluindo com o tempo. Os tópicos a seguir irão abordar seus principais conceitos, o seu desenvolvimento e a relação entre a internet e o direito.

4.1.2 Surgimento, evolução e transformações na sociedade a partir da internet

O processo de globalização foi um fenômeno capaz de revolucionar o mundo estabelecendo a conexão entre países e pessoas, melhorando as relações comerciais e fazendo com as grandes empresas elevassem seus status e otimizassem os seus negócios (COSTA, 2014, p.01).

Podemos melhor definir o conceito de globalização sendo como:

O processo pelo qual é estabelecido uma conexão entre diversas sociedades e nações existentes no mundo, estabelecendo uma influência a todo o globo no âmbito social, econômico, político e cultural. É caracterizado principalmente pela intensificação do fluxo de capital, mercadorias, informações e pessoas, ocasionada pelo desenvolvimento da tecnologia nas diferentes formas de comunicação (LIMA, 2022. p. 13).

Em decorrência do desenvolvimento do processo de globalização no mundo, o meio tecnológico obteve um grande avanço, passando a estabelecer novas relação

entre pessoas, através da utilização de equipamentos eletrônicos que revolucionaram os meios de comunicação, fazendo com que novas relações profissionais e pessoais pudessem surgir (BONDYREVA, 2021, p. 73).

Com o forte emulsionamento da tecnologia e o desenvolvimento do processo de globalização, surgiu a tão conhecida rede mundial de computadores: a internet (CASTELLS, 2013, p. 87).

Para Inellas (2009), o funcionamento da internet é definido da seguinte maneira:

O funcionamento da Internet não é uma questão meramente privada: é uma forma extrema de globalização, com efeitos políticos e sociais que envolvem a ordem pública e a necessidade de regulamentações. Não se trata de auspicar intervenções que causem distorções mais sim intervenções de tipo institucional que tendam a resguardar a privacidade, o consumo, a moral, o tratamento igualitário e não discriminatório.

Segundo Trentin (2012), o desenvolvimento da tecnologia e da internet foram um dos principais fatores de mudança do cotidiano da vida das pessoas, pois com a sua expansão, novas mudanças foram aplicadas ao contexto social contemporâneo, o que contribui, de forma positiva, para o crescimento da globalização a partir do momento em que criou novas oportunidades de práticas comerciais, negócios, novos relacionamentos e novos métodos de comunicação, além de estimular a criação de um novo espaço público.

A Era Digital, de fato, influenciou diretamente na mudança do comportamento e dia-a-dia da sociedade contemporânea da seguinte forma:

A introdução de um novo conceito de espaço (ciberespaço) e a efetiva utilização de uma nova ferramenta, a Internet, modificou grandemente o cotidiano da vida das pessoas. Esta, por seu turno, tem se mostrado uma das principais armas da globalização, [...] corolário do neo-liberalismo – movimento econômico que afeta o mundo em várias facetas. [...] este quadro evidencia de que maneira as novas tecnologias afetam o cotidiano das gentes, e o direito, especial o penal, não pode ficar alheio a tão-gritantes transformações, até porque a criminalidade se amolda e

também utiliza todo o ferramental tecnológico para a prática de condutas já historicamente tipificadas e outras a se tipificar. (ROSSINI, 2004 p. 23)

Apesar dos métodos mais antigos ainda serem poucos utilizados como forma de comunicação, a Internet é a ferramenta mais utilizada nos dias atuais, pois hoje, não há uma pessoa sequer que não tenha utilizado ou se beneficiado da Internet. Em seu desenvolvimento, a Internet funciona como uma rede que depende de outras ferramentas interligadas, formando uma rede de comunicação onde corre a transferência ininterruptas de informações, seja por um computador interligado à um sistema via satélite, via rádio ou a uma linha telefônica (ORRICO, 2004).

Segundo Trentin (2012, p. 25), a Internet possui quatro características:

a) é uma rede aberta, visto que qualquer um pode ter acesso a ela; b) é interativa já que o usuário gera dados, navega e estabelece relações; c) é internacional, no sentido de que permite superar as barreiras nacionais; d) há uma multiplicidade de operadores.

Mesmo com o conceito de Internet ser definido como a “rede mundial de computadores”, necessariamente não significa que apenas o computador em si esteja relacionado ao conceito de Internet. Nesse sentido, diversos dispositivos como celulares, geladeiras, micro-ondas ou agendas eletrônicas podem ser considerados dispositivos computacionais, desde que estabeleçam conectividade à rede (GEMIN, 2010, p. 35).

A evolução tecnológica proporcionou uma maior disponibilidade de recursos de comunicação revolucionando a forma de como as pessoas se conectam e transmitem informações, onde antes só era possível por meio da presença física. Dessa forma, a Internet permitiu a transferência de informações de forma rápida, onde hoje já é possível o ensino educacional à distância, o comércio, dentre outras atividades (MARTINS, 2003, p. 57).

A Internet sem dúvidas pode ser considerada como uma das grandes invenções do século, pois nunca foi possível a transmissão de informações e a comunicação de forma tão rápida e eficaz. Segundo Rohrmann (2005), podemos

melhor entender o surgimento e como a Internet vem se desenvolvendo no decorrer do tempo.

No que tange a história da Internet, propriamente dita, temos a primeira fase na década de 1960. No início daquela década, começaram as pesquisas para a troca de mensagens em redes do tipo packet switched, ou seja, comunicações que se valiam de interligações lógicas, e não físicas, entre os usuários. No final da década, em 1969, uma rede de computadores de origem militar, a ARPANET, do Departamento de Defesa dos Estados Unidos, já fazia uso da tecnologia packet switched. Os computadores passaram a ser interligados à ARPANET ao longo dos anos seguintes a uma taxa acelerada. [...] Até o início da década de 1970, a rede ARPANET ainda utilizava como protocolo o Network Control Protocol – NCP – e contava com quatro pontos de presença localizados em Stanford, Los Angeles (UCLA), Santa Bárbara (UCSB) e Utah.

Por volta da década de 90, a utilização da Internet passou a ser mais disseminada a partir do momento em que a utilização dessa ferramenta revolucionou o meio tecnológico.

A década de 1990 começa com o fechamento da ARPANET. Foi também o marco do início da maior utilização da Internet pelas pessoas naturais e jurídicas.

O grande crescimento da Internet entre os usuários não-ligados à atividade de pesquisa deu-se em razão de dois fatores essenciais.

O primeiro foi a popularização da World Wide Web (WWW), graças ao surgimento de programas capazes de manipular interfaces gráficas.

O segundo fator foi o surgimento dos provedores de acesso, isso é, as empresas que possibilitam o acesso do público em geral à Internet. [...]

Os provedores têm seus computadores ligados à Internet e dispõem de canais de acesso para seus clientes por meio de dispositivos que permitem a ligação dos computadores, por exemplo, às linhas telefônicas. (ROHRMANN, 2005, p. 6-7)

A possibilidade de estabelecer novas formas de interação e fazer com que a sociedade entrasse na revolucionária Era Digital foi possível graças aos provedores de Internet. Para melhor entendermos como esses provedores funcionam, Gois (2001, p. 49) explica:

Assim, no sistema atual de rede temos, basicamente, milhões de computadores nos lares e empresas, ligados a computadores servidores maiores, em geral instalados em empresas que fornecem acesso, chamadas comumente de provedores de acesso à Internet.

Os provedores inscrevem as máquinas de menor porte como suas usuárias e tornam disponíveis serviços para essas máquinas, que passam a ter acesso à grande rede por meio dos seus computadores. Por sua vez, os servidores das empresas provedoras são ligados a grandes estruturas de comunicação chamadas de backbones que escoam pelo mundo afora o imenso tráfego de informações proveniente dos provedores de acesso mediante canais de satélite ou cabos submarinos.

Em seu surgimento, a Internet era algo restrito e disponível apenas a centros de pesquisa e universidades. Sua utilização foi então liberada e facilitado o acesso após a criação e divulgação da Portaria nº 295 de 20/07/1995 que possibilitou a comercialização do acesso a essa ferramenta (NUNES; OLIVEIRA, 2008, p.270).

Ainda no ano de 1995, foi emitida uma nota conjunta informando sobre a introdução da Internet no Brasil, a partir da edição feita pelo Ministério das Comunicações (MC) e o Ministério da Ciência e Tecnologia (MCT) informando os seguintes conceitos:

2. A Internet

2.1 A Internet é um conjunto de redes interligadas, de abrangência mundial. Através da Internet estão disponíveis serviços como correio eletrônico, transferência de arquivos, acesso remoto a computadores, acesso a bases de dados e diversos tipos de serviços de informação, cobrindo praticamente todas as áreas de interesse da Sociedade.

2.2 A Internet é organizada na forma de espinhas dorsais backbones, que são estruturas de rede capazes de manipular grandes volumes de informações, constituídas basicamente

por roteadores de tráfego interligados por circuitos de alta velocidade.

2.3 Interligadas às espinhas dorsais de âmbito nacional, haverá espinhas dorsais de abrangência regional, estadual ou metropolitana, que possibilitarão a interiorização da Internet no País.

2.4 Conectados às espinhas dorsais, estarão os provedores de acesso ou de informações, que são os efetivos prestadores de serviços aos usuários finais da Internet, que os acessam tipicamente através do serviço telefônico.

2.5 Poderão existir no País várias espinhas dorsais Internet independentes, de âmbito nacional ou não, sob a responsabilidade de diversas entidades, inclusive sob controle da iniciativa privada.

2.6 É facultada aos provedores de acesso ou de informações a escolha da espinha dorsal à qual se conectarão, assim como será de livre escolha do usuário final o provedor de acesso ou de informações através do qual ele terá acesso à Internet. (GEMIN, 2010)

Com os inúmeros benefícios provenientes da Internet sua utilização foi crescendo cada vez mais, a partir do momento em que tornou-se uma ferramenta de fácil acesso e indispensável para a realização das atividades diárias do ser humano (GEMIN, 2010).

Segundo Castells (2013), a Internet e as demais redes de comunicação constituem uma configuração lógica da sociedade moderna, caracterizando uma geração de pessoas conectadas pela troca de informações. Os meios de comunicação virtual como Facebook, Instagram e Twitter são instrumentos de forte influência já que são utilizados como métodos para divulgar produtos, diversificar mercados, atrair clientes além de influenciar no comportamento das pessoas que utilizam dos meios de comunicação virtual.

Apesar dos inúmeros benefícios oferecidos com a difusão da internet, a mudança comportamental que essa ferramenta provocou à sociedade trouxe alguns problemas a partir do momento em que pessoas utilizam desse meio para a prática de atos que trazem danos a bens jurídicos de terceiros, já que a cultura da utilização da internet influencia diretamente na forma como interagimos tanto na vida pessoal como profissional (FRANCISCO, 2017).

4.1.3 A Internet e seus conceitos

Quando nos referimos a Internet é relevante descrever os diversos termos empregados nesse meio. Como o conceito básico já foi abordado no tópico anterior, passamos a conceituar os demais termos envolvidos no conceito de Era Digital. Dessa forma, iniciamos pelos usuários dessa ferramenta, que são conhecidos como *internautas* e que navegam nessa rede através de um programa, conhecido como *browser*, que permite o usuário a navegar de uma página a outra (GOIS JÚNIOR, 2001).

Ainda nos referindo a Internet podemos citar os sites que são compreendidos como uma página que armazenam informações as quais são inseridas pelo usuário e que estão interligados entre si, podendo ser acessados por inserção de informações ou através de um link que leva o internauta ao site (GEMIN, 2010).

Segundo Gemin (2010), diversas outras ferramentas constituem essa rede das quais o usuário pode utilizar como por exemplo o e-mail e o download de arquivos. Apesar da vasta utilidade e das infinitas ferramentas disponibilizadas esse ambiente está repleto de pessoas de má fé que utilizam de métodos maldosos para prejudicar o usuário de alguma forma.

Diante dos problemas provenientes da prática maldosa aplicada a rede de comunicação, foram criados alguns mecanismos de defesa contra esses ataques como o *firewall*, que se trata de um sistema de segurança afim de proteger o acesso a rede do computador e o antivírus que se trata de um software visa impedir que algum vírus malicioso tenha acesso ao computador ou até mesmo tenta removê-lo. Os vírus são desenvolvidos por crackers que os elaboram com o objetivo de invadir a segurança dos sistemas, inserindo-se no computador e provocando danos ao mesmo (GÓIS, 2011, p. 182).

4.1.4 A relação entre a internet e o Direito

O Direito surgiu pela necessidade de conter as atividades exercidas pelas pessoas, estabelecendo a concretização da realização da justiça perante a sociedade. Com as constantes transformações e a aceleração do processo de globalização o Direito precisou acompanhar as constantes mudanças e se adequar as novas práticas da sociedade (GEMIN, 2010).

Na década de 90 foram publicados os primeiros artigos que tratavam da aplicação do Direito na rede mundial de computadores. Esse posicionamento jurídico

ocorreu principalmente a partir da popularização da Internet que tomou grande proporção espalhando-se por todo o mundo e sendo utilizada tanto no meio empresarial como nas atividades diárias da sociedade (GEMIN, 2010).

Com a inserção da rede mundial de computadores no cotidiano da vida das pessoas, o Direito começou a estabelecer uma relação com a Internet pela necessidade de regulamentação e implementação de medidas de controle que não possuía até então, visando garantir a segurança da sociedade contra os males e possíveis atos ilícitos praticados no meio virtual (ORRICO, 2006).

Sobre os crimes cometidos pelo meio virtual, o juiz federal Ivan Lira de Carvalho (Apud DAOUN, 2001, p. 203-204) apresentou o seguinte pensamento a respeito dos crimes virtuais:

Os diversos seguimentos da sociedade moderna, e dentre estes destacado o que engloba os profissionais do Direito, demonstram clara preocupação do homem moderno com os rumores da rede mundial de computadores (Internet), que apesar de ser, inegavelmente, um marco na divisão da história da humanidade, ao lado de tantos benefícios que propicia, tem também o seu lado nefasto: é instrumento de crime.

Lucca (2015) profere o seguinte pensamento em relação as abordagens do direito cibernético, conhecido como Juscibernética:

1. O mundo do Direito, na sua totalidade, é considerado como um subsistema em relação ao sistema social e são estudadas as interrelações entre os dois, conforme um modelo cibernético.
2. O mundo do Direito é estudado como um sistema normativo, dinâmico e auto-regulador. O Direito é concebido como um todo do qual são estudadas não as relações externas (nº 1), mas sim as relações internas, isto é, aquelas que ligam entre si as várias partes do sistema. Procura-se definir, aqui, uma estrutura cibernética do sistema jurídico.
3. Os modelos cibernéticos, em geral, deveriam ser idealizados tendo em vista a sua utilização em máquinas cibernéticas. Esta passagem para o computador pressupõe, porém, uma formalização da linguagem jurídica.

Na Juscibernética, neste terceiro tipo de pesquisa, estão contidos a lógica formal aplicada ao Direito, a análise da linguagem jurídica e, de maneira geral, os estudos de Teoria Geral do Direito. Aqui, a norma não é mais uma parte dentro de um todo (o Direito) da qual se estudam as relações com as outras partes do mesmo conjunto (como no nº 2), mas sim ela mesma torna-se um subsistema, do qual se estudam as diferentes partes e as suas relações recíprocas.

4. Estudamos, assim, os aspectos do Direito e das normas que podem tornar acessíveis aos computadores eletrônicos determinados fenômenos jurídicos. Contudo, a passagem para esta aplicação prática faz surgir numerosos problemas não encontrados nos níveis anteriores. Esses problemas pressupõem noções não só jurídicas, mas também técnicas. Por isso, o setor de tratamento das normas jurídicas como informações (isto é, da sua recuperação eletrônica) é o setor interdisciplinar que marca a fronteira entre a Juscibernética e a tecnologia dos computadores.

A partir dos atos ilícitos praticados por meio dos recursos tecnológicos, percebe-se a importância do posicionamento jurídico direcionado à rede mundial de computadores e a necessidade de implementação de normas que contenham os crimes praticados virtualmente e que crescem diariamente à medida que novas tecnologia vão surgindo (ROSSINI, 2004).

5. CRIMES VIRTUAIS

Com a popularização da internet e dos demais meios de comunicação virtual, o crime digital tornou-se uma prática bem comum. Este tipo de crime é considerado nocivo, já que não existe o contato físico com a vítima pois todo o ato é praticado por meio virtual por meio do uso da utilização de meios de tecnologia e informação (D'URSO, 2019).

Diversas são as denominações para o conceito de crimes eletrônicos que também são conhecidos como cibercrimes, crimes virtuais, entre outras diversas denominações que independentemente de como são conhecidos seu conceito é bem fácil de ser entendido. Rosa (2006), conceitua os crimes virtuais da seguinte forma:

A conduta atente contra o estado natural dos dados e recursos oferecidos por um sistema de processamento de dados, seja pela compilação, armazenamento ou transmissão de dados, na sua forma, compreendida pelos elementos que compõem um sistema de tratamento, transmissão ou armazenagem de dados, ou seja, ainda, na forma mais rudimentar; O “Crime de Informática” é todo aquele procedimento que atenta contra os dados, que faz na forma em que estejam armazenados, compilados, transmissíveis ou em transmissão; Assim, o “Crime de Informática” pressupõe dois elementos indissolúveis: contra os dados que estejam preparados às operações do computador e, também, através do computador, utilizando-se software e hardware, para perpetrá-los; A expressão crimes de informática, entendida como tal, é toda a ação típica, antijurídica e culpável; Nos crimes de informática, a ação típica se realiza contra ou pela utilização de processamento automático de dados ou a sua transmissão. Ou seja, a utilização de um sistema de informática para atentar contra um bem ou interesse juridicamente protegido, pertença ele à ordem econômica, à integridade corporal, à liberdade individual, à privacidade, à honra, ao patrimônio público ou privado, à Administração Pública.

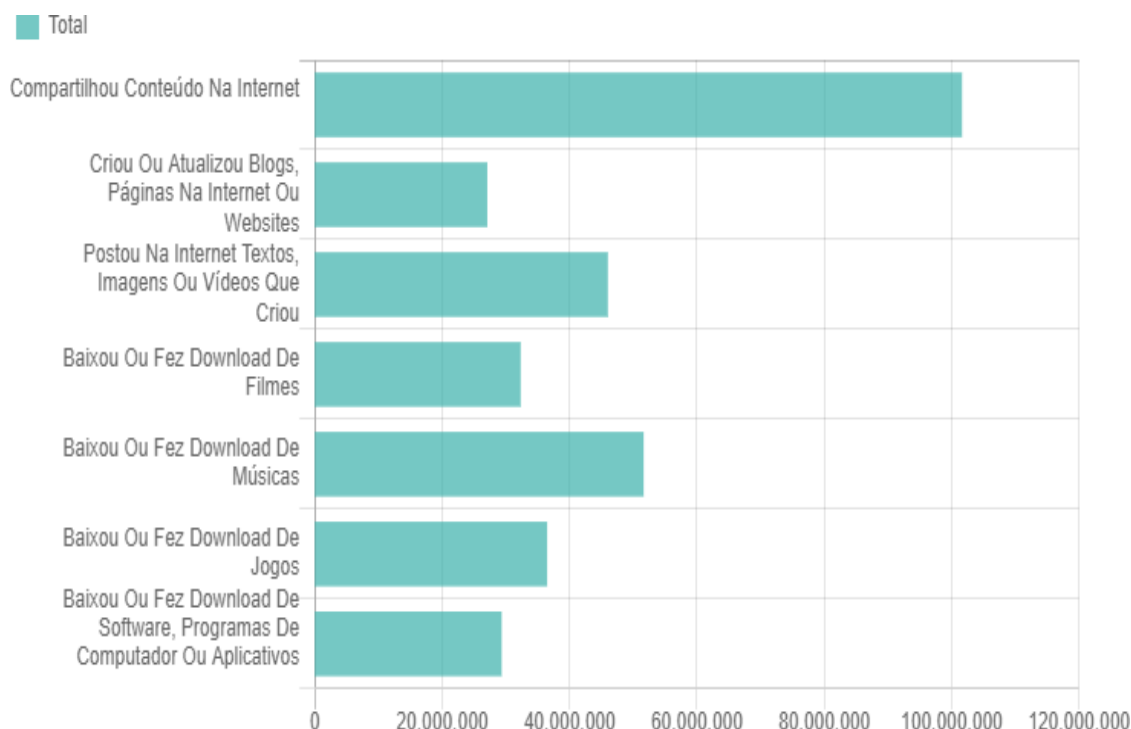
Segundo dados da Organização das Nações Unidas (ONU), ao todo, existem cerca de 5,3 bilhões usuários de internet no mundo, o que equivale a um terço da população mundial. Logo, pode-se concluir, que ano após ano as pessoas estão cada vez mais aderindo ao uso desse meio, já que facilita a forma como as pessoas se comunicam.

Em 2017, a Conferência das Nações Unidas sobre Comércio e Desenvolvimento (UNCTAD) divulgou uma pesquisa onde o Brasil apresenta-se em quarto lugar no ranking mundial de usuários da internet com 120 milhões de pessoas conectadas, ficando apenas atrás dos Estados Unidos, com 242 milhões de usuários.

Segundo o Instituto Brasileiro de Geografia e Estatística (IBGE) um dos grandes aparelhos responsáveis pelo aumento da utilização da internet foi o aparelho celular, sendo utilizado por cerca de 94,6% dos brasileiros (IDGNOW, 2018).

A figura a seguir mostra o número de usuários de internet, por atividades realizadas como downloads, criação e compartilhamento de conteúdo no Brasil em 2021, veja:

Figura 1 – Usuários de internet, por atividade realizada na internet – downloads, criação e compartilhamento de conteúdo digital



Fonte: CETIC.br (2022).

O gráfico da Figura 1 mostra que cerca de 100.000.000 de pessoas no Brasil realizam a atividade de compartilhamento de conteúdo na internet, sendo essa, uma das grandes atividades vilãs para a divulgação de conteúdos ilícitos e prática de crimes cibernéticos. Outra atividade realizada por meio dos recursos digitais que acarretam grandes problemas é o download de conteúdo da internet, que muitas vezes, contém vírus maliciosos que invadem o computador, fazendo acesso aos arquivos pessoais do usuário.

Segundo Gimenes (2013), a medida em que o número de usuários da internet cresceu, os crimes virtuais tornaram-se mais frequentes e difíceis de serem solucionados, vista a dificuldade de investigação no ambiente virtual.

No Brasil, o número de vítimas dos crimes virtuais segundo dados do relatório de 2017 da Norton Cyber Insights, trouxe um prejuízo calculado em aproximadamente 22 bilhões de reais, sendo que cerca de 62 milhões de brasileiros, em 2017, foram alvos desse tipo de delito (REPORT, 2018).

A prática desse ato ilícito pode ser feita de diversas formas, bem como, a inserção de vírus, possuindo diversas modalidades e com finalidades específicas. Quanto a sua classificação podem ser classificados como o Vírus Hijacker: que utiliza o navegador de internet da vítima e faz a mesma navegar por sites diferentes do que foi digitado; Vírus Sniffer: onde inspecionam todo o tráfego da rede, fazendo análise de dados; Vírus Backdoor: onde deixa o computador vulnerável a invasões; Hoax: consiste na divulgação de informações falsas por meio da internet e por fim, o vírus Keylogger: monitora todas as informações digitadas no computador (BARROS, 2018).

Quanto aos tipos de crimes virtuais podem ser classificados em três tipos: os puros, mistos e os crimes eletrônicos comuns. Os crimes puros são considerados aqueles que envolvem tanto a parte física do computador, quanto os seus dados internos; São classificados de crimes mistos, os que tem como prática, a intensão de prejudicar algum bem jurídico da vítima, como por exemplo, o acesso a dados bancários para transferência de valor, e por fim, os crimes eletrônicos comuns, que em sua prática, não necessitam da informática como meio para execução do ato ilícito, podendo realizar-se através dos meios digitais (VIANA, 2003).

6. CLASSIFICAÇÃO DOS CRIMES VIRTUAIS

Apesar de não existir legislações e estudos suficientes para conter os crimes virtuais, estes ganharam definições próprias podendo ser classificados como próprios e impróprios (ROSSINI, 2004).

A sua classificação se difere a partir do tipo da prática de crime: os crimes já previstos no ordenamento jurídico e praticados apenas por meio da utilização de recursos tecnológicos, onde sua consumação se dá apenas no meio digital, denominados crimes próprios; e os crimes iniciados no meio virtual, mas que seus efeitos se realizam no meio real, ou seja, os recursos tecnológicos funcionam como intermédio para a prática da ação, denominados crimes impróprios. Crespo (2011, p. 63) apresenta o seguinte pensamento sobre o tema:

Neste sentido, podemos dizer que todas as condutas praticadas contra bens jurídicos informáticos (sistemas, dados) são delitos de risco informático ou próprios, ao passo que aquelas outras condutas que se dirigem contra bens

jurídicos tradicionais (não relativos à tecnologia) são crimes digitais impróprios.

Ainda sobre a classificação desse delito, Rossini (2004) aponta que os crimes virtuais próprios tem como objetivo exclusivo a utilização dos sistemas informáticos, seja eles computador e periféricos, para a concretização do ato. Nesse contexto, a prática busca exclusivamente atingir o sistema informático da vítima, tendo como consequência a prática de atos como utilização indevida de informações, invasão de privacidade, dano informático, dentre outros.

Tratando-se dos crimes virtuais impróprios, este tem como objetivo a utilização dos recursos informáticos como intermédio para a execução do delito que se inicia no meio virtual e finaliza no meio real. Temos como exemplo o crime contra a honra, o estelionato, a pornografia infantil, o estupro virtual e em casos mais extremos o cometimento de homicídio por meio da Internet (ROSSINI, 2004).

7. TIPIFICAÇÃO DOS CRIMES VIRTUAIS

Conforme abordado no tópico anterior, os crimes virtuais podem ser classificados em próprios e impróprios. A partir dessa classificação, podemos citar os diversos tipos de crimes, assim como será apresentado nos tópicos seguintes.

7.1 INVASÃO DE PRIVACIDADE

A amplitude em que o número de informações pode ser guardado ou transmitido é de tamanha proporção que se exige a aplicação de soluções para os problemas gerados da relação entre informática e intimidade. As facilidades de propagação de informações de forma rápida através da utilização dos recursos tecnológicos, fazem da internet um instrumento causador de uma problemática para o homem contemporâneo que demanda atitudes desafiadoras para o campo do Direito (CANOTILHO, 2012).

Com a conexão entre computadores por toda a parte do mundo, os dados divulgados na internet são informações de difícil controle, já que as informações divulgadas circulam em uma velocidade muito grande, atingindo um grande número de pessoas em um curto espaço de tempo. Dessa forma, a preservação desses

direitos vem crescendo a medida em que a vida privada é ameaçada pelas novas modalidades de invasão virtual (AZUMA, 2012).

Segundo dados divulgados pelo FortiGuard Labs, laboratório de inteligência de ameaças da empresa, o Brasil no ano de 2021, sofreu mais de 88,5 bilhões de tentativas de ataques cibernéticos, apresentando um aumento de 950% em relação ao ano anterior (com 8,5 bilhões em 2020).

A imagem a seguir mostra, divulgada pelo FortiGuard Labs, o ranking dos países que sofreram ataques cibernéticos em 2021, veja:

Figura 2 – Ranking dos países que sofreram ataques cibernéticos em 2021

México	156,000,000,000
Brasil	88,500,000,000
Peru	11,500,000,000
Colômbia	11,200,000,000
Chile	9,400,000,000
Argentina	3,200,000,000
Panamá	3,200,000,000
Costa Rica	2,500,000,000
República Dominicana	2,200,000,000
Porto Rico	926,000,000
LATAM	289,000,000,000

Fonte: TIinside, 2022.

De acordo com a imagem acima, o Brasil ocupou o segundo lugar em número de ataques, ficando atrás apenas do México (com 156 bilhões) e a frente do Perú (com 11,5 bilhões). Toda a região chegou a registrar 289 bilhões de ataques, apresentando um aumento de 600% em relação ao ano de 2020 (com 41 bilhões).

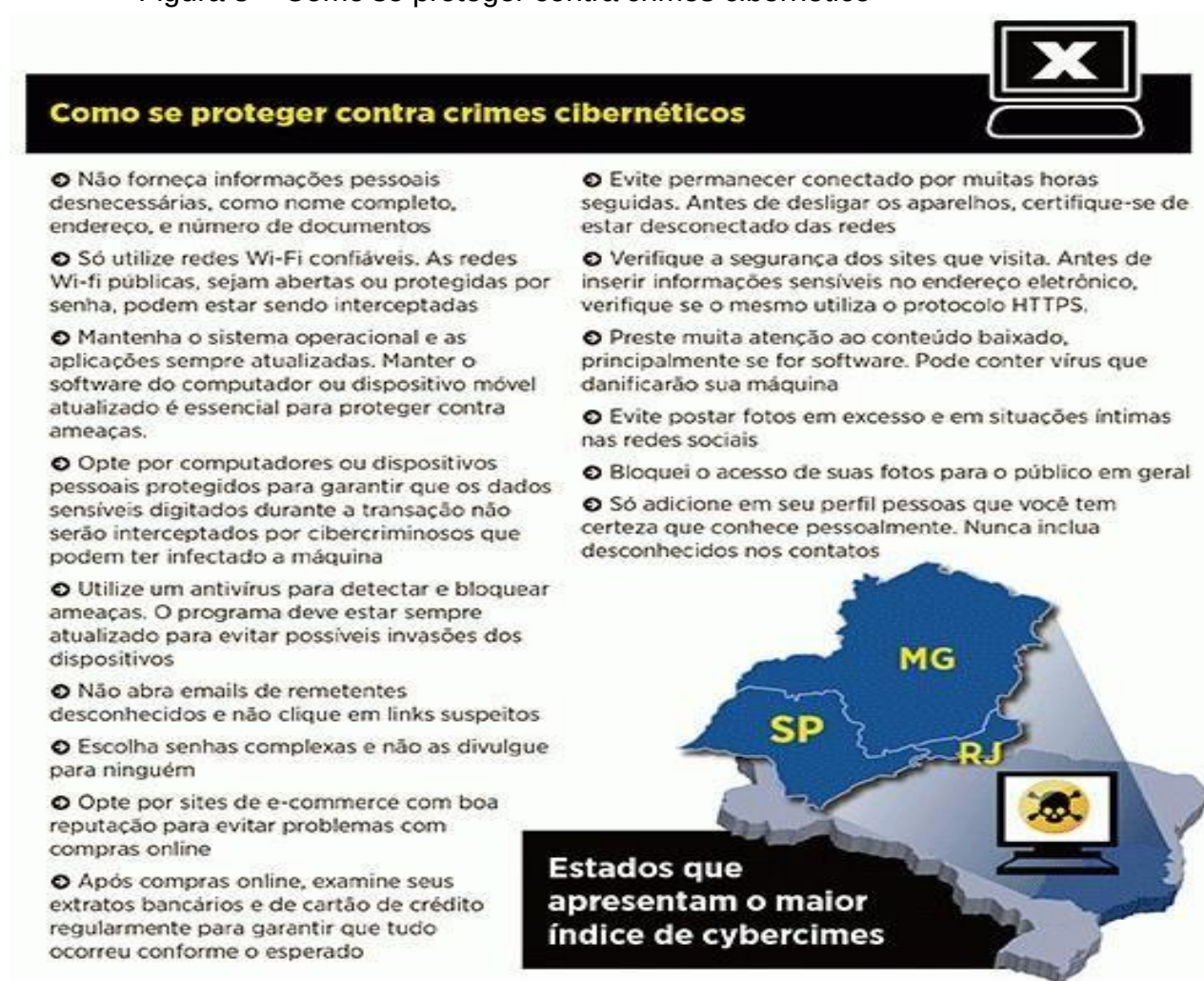
Com o agravamento de uma nova modalidade de crimes virtuais o direito precisa adequar-se a esses novos tipos de práticas ilícitas, fazendo a criação de disposições legais que possam ser aplicadas a tudo que envolva a Internet,

principalmente aquilo que se relacione com a informação além da aplicação de normas legislativas específicas (LUCCA, 2015).

No atual cenário virtual, a privacidade tornou-se algo bastante frágil necessitando a tomada de algumas precauções para afim de evitar a ser vítima desse tipo de delito. Algumas precauções são de grande valia contra esse crime como por exemplo: o cuidado ao inserir dados pessoais em sites não confiáveis, a utilização de um bom antivírus, não navegar em sites duvidosos e evitar a publicação de fotos que exponham imagens de sua casa, familiares e local de trabalho (LUCCA, 2015).

A figura a seguir, publicada pelo Jornal do Comércio – JC Online¹, apresenta quais as precauções devem ser tomadas para se proteger contra os crimes cibernéticos.

Figura 3 – Como se proteger contra crimes cibernético



Fonte: JC Online (2014).

¹Disponível em: < <https://jc.ne10.uol.com.br/canal/cidades/geral/noticia/2014/08/06/saiba-como-evitar-os-crimes-virtuais-138960.php> >. Acesso em: 02 set. 2022.

No artigo 5º, da Constituição Federal, está previsto a proteção ao indivíduo quanto à privacidade e intimidade, assegurando o direito a indenização caso ocorra dano material ou moral decorrente da sua violação (ANDRADE, 2015).

Conforme lei nº 12.737 de 2012, conhecida como Lei Carolina Dieckmann, do artigo 154-A do CP, diz respeito a invasão de privacidade:

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.
(BRASIL, 1940)

A lei denominada Lei Carolina Dieckmann, sancionada em novembro de 2012, dispõe da especificação criminal dos delitos informáticos. Ela foi criada a partir do ocorrido com a famosa atriz brasileira Carolina Dieckmann, que foi vítima de invasão de privacidade em seu computador, tendo como consequência a exposição de arquivos pessoais, dentre eles fotos íntimas que foram espalhadas na internet.

O objeto jurídico do crime especificado no artigo 154 - A é a privacidade individual profissional armazenada em dispositivo informático, sendo aplicável a punição pelo ato de invasão a dispositivos informáticos alheios sem autorização (GOULART, 2021).

A lei, em sua execução, prevê a garantia da preservação da intimidade, privacidade e sigilo dos dados armazenados em dispositivos informáticos, sendo penalizado o indivíduo ao exercer o ato de invadir sem autorização expressa do titular do dispositivo (CAPEZ, 2016).

Mesmo com a inserção da Lei nº 12.737/2012 no ordenamento jurídico ainda é constante os ataques cada vez mais complexos em diversos lugares dificultando a devida identificação para a punição dos praticantes desse ato ilícito.

7.2 Aquisição e transferência ilegal de dados

O acesso ilegal a dados de um indivíduo pode ser realizado de diversas formas, desde a quebra de barreira de segurança do computador provocada por alguma falha ou até mesmo por programas que rastreiam as informações contidas em um computador (CRESPO, 2011).

Dentre as diversas ferramentas utilizadas nos dias atuais para a aquisição de dados pessoais de um indivíduo, o programa spywares é um dos mais utilizados. Essa ferramenta tem como objetivo principal a identificação estratégica dos hábitos de um indivíduo e o direcionar a uma propaganda. É uma ferramenta bastante utilizada para promover a comercialização de produtos e serviços, mas que com o decorrer do tempo passou a ser utilizada para a prática de atos criminosos.

Essa ferramenta pode ser encontrada de diversas formas como por exemplo os cookies, considerado uma ferramenta de spyware já que são utilizados programas para envio de informações coletadas por meio da internet e enviadas para as empresas contribuindo para as estratégias de propagandas. Apesar de contribuir positivamente para as empresas, esses programas podem carregar dispositivos maliciosos e que dificilmente são percebidos, podendo adentrar em redes privadas e coletar dados como número de cartão de crédito, senhas e dados pessoais (BITTENCOURT, 2007).

A previsão da conduta de obtenção de dados é disciplinada pelo parágrafo 3º do art. 154-A do Código Penal Brasileiro:

§ 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido: Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave. (BRASIL, 1940, s.p.)

A transferência de dados de um dispositivo para o outro é possível a partir da obtenção dos dados e pode ser feita de forma rápida migrando dados para um outro dispositivo. Para a conduta de obtenção ou transferência de dados, conforme descrito no parágrafo 4º do artigo 154-A do Código Penal Brasileiro, o qual disciplina que “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.

7.3 Exposição e utilização indevida de informações

Com o advento da globalização e as constantes transformações no mundo tecnológico, veio à tona um tema bastante comentado: a exposição e utilização de informações de forma indevida (PINTO, 2017).

A divulgação de informações em redes sociais, blogs, páginas abertas ou qualquer outro meio de comunicação sem a prévia autorização do titular é considerado um ato ilícito, á que afronta aos princípios do direito sendo cabível a aplicação das penalidades vigentes. A prática deste ato está prevista no art. 154 do Código Penal Brasileiro:

Art. 154 - Revelar alguém, sem justa causa, segredo, de que tem ciência em razão de função, ministério, ofício ou profissão, e cuja revelação possa produzir dano a outrem:
Pena - detenção, de três meses a um ano, ou multa.

O então ato também está descrito no artigo 154-A do Código Penal Brasileiro, por meio do parágrafo 4º onde aumenta a pena de um a dois terços do previsto no parágrafo 3º do mesmo artigo, que penaliza sobre a obtenção e o acesso dos dados, caso houver a difusão, comercialização ou a repasse de informações a terceiros.

A divulgação de informações pessoais pode atingir a segurança pessoal a partir da exposição dos dados podendo ocorrer fraudes, pois os estelionatários utilizam das informações pessoais das vítimas para a realização de cadastros em sites, realização de compras, abertura de empresas e até financiamentos para a aquisição de imóveis ou veículos (CORAZZA, 2015).

Tal conduta interfere diretamente na violação do direito a privacidade, a qual está inerida no artigo 5º da Constituição Federal, que dita a seguinte penalização: “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação”.

Dentre as diversas formas para o acesso e divulgação de informações de forma indevida, podemos citar o spam, já que é uma das formas mais utilizadas. Esse

método consiste no recebimento de e-mails ou de mensagens indesejadas, sem que o usuário tenha solicitado. Dessa forma, o infrator envia e-mails para diversos endereços ao mesmo tempo através de um dispositivo tecnológico vinculado a internet (PINTO, 2017).

A prática desse delito não se limita apenas a invasão de informações de pessoas, mas também pode ser praticado no meio empresarial a partir do momento em que é forçado o acesso a informações importantes de uma empresa seja para a divulgação maldosa de algo ou para a utilização de informações que provoquem algum tipo de dano (CRESPO, 2011).

7.4 Crime contra a honra

Dentre os crimes virtuais mais praticados no Brasil, os crimes contra a honra são uns dos mais denunciados dentre os tantos crimes cibernéticos. Eles são praticados a partir do momento em que ferem a qualidade física, moral ou intelectual da pessoa atingida. Tratando-se dos tópicos dos crimes contra a honra, o Código Penal Brasileiro nos artigos 138, 139 e 140 especificam os três tipos de crimes distintos: calúnia, difamação e injúria.

Art. 138 - Caluniar alguém, imputando-lhe falsamente fato definido como crime:

Pena - detenção, de seis meses a dois anos, e multa.

§ 1º - Na mesma pena incorre quem, sabendo falsa a imputação, a propala ou divulga.

§ 2º - É punível a calúnia contra os mortos.

§ 3º - Admite-se a prova da verdade, salvo:

I - Se, constituindo o fato imputado crime de ação privada, o ofendido não foi condenado por sentença irrecorrível;

II - Se o fato é imputado a qualquer das pessoas indicadas no nº I do art. 141;

III - se do crime imputado, embora de ação pública, o ofendido foi absolvido por sentença irrecorrível.

Art. 139 - Difamar alguém, imputando-lhe fato ofensivo à sua reputação:

Pena - detenção, de três meses a um ano, e multa. Parágrafo único

- A exceção da verdade somente se admite se o ofendido é

funcionário público e a ofensa é relativa ao exercício de suas funções.

Art. 140 - Injuriar alguém, ofendendo-lhe a dignidade ou o decoro:

Pena - detenção, de um a seis meses, ou multa.

§ 1º - O juiz pode deixar de aplicar a pena:

I - Quando o ofendido, de forma reprovável, provocou diretamente a injúria;

II - No caso de extorsão imediata, que consista em outra injúria.

§ 2º - Se a injúria consiste em violência ou vias de fato, que, por sua natureza ou pelo meio empregado, se considerem aviltantes:

Pena - detenção, de três meses a um ano, e multa, além da pena correspondente à violência.

§ 3º Se a injúria consiste na utilização de elementos referentes a raça, cor, etnia, religião, origem ou a condição de pessoa idosa ou portadora de deficiência Pena - reclusão de um a três anos e multa.

Segundo Cunha (2017), a calúnia e a difamação ocorrem com o ato de imputar alguém a um fato concreto e ofensivo, sendo ele falso. No caso da injúria, ocorre a imputação genérica, uma má qualidade ou defeito que menospreze a vítima. Para considerar-se calúnia ou difamação é necessário que a frase desonrosa chegue ao conhecimento de terceiros, o que não se faz necessário para o caso da injúria.

Segundo o Código Penal Brasileiro, no artigo 3º, a chamada exceção da verdade, caracteriza-se pela prova da verdade da imputação, gerando atipicidade na conduta:

Exceção da verdade

§ 3º - Admite-se a prova da verdade, salvo:

I - se, constituindo o fato imputado crime de ação privada, o ofendido não foi condenado por sentença irrecorrível; II - se o fato é imputado a qualquer das pessoas indicadas no nº I do art. 141;

III - se do crime imputado, embora de ação pública, o ofendido foi absolvido por sentença irrecorrível.

As diversas formas de utilização de computadores e dos meios tecnológicos mostraram que os órgãos não estavam preparados para punir e julgar os usuários que utilizavam desse meio para a prática de crimes que atingem a honra e a dignidade das vítimas (SILVA, 1990).

Infelizmente no Brasil não é possível encontrar leis que ajam contra vários tipos de crimes, algumas tratam de assuntos específicos, ajudando a diminuir tais práticas e reduzindo o seu crescimento (SILVA, 1990).

7.5 Estelionato

O crime de estelionato na internet atingiu um amplo campo devido a possibilidade de prática do crime sem a necessidade de mostrar o rosto de quem pratica o delito. Dessa forma, criminosos utilizam do anonimato para atacar as vítimas, tendo como preferência aquelas que mantêm o costume de consultar o seu saldo bancário por meio do computador. Sendo assim, o criminoso encontra uma forma de clonar a página da internet de acesso ao banco da vítima e fazer com que ela tente fazer o acesso sem mesmo saber que os dados que estão sendo inseridos serão utilizados indevidamente por uma terceira pessoa (INELLAS, 2009).

Em 2011, na operação que ficou conhecida como “tentáculos”, ocorrida na cidade de São Paulo, a polícia prendeu 16 pessoas que faziam o uso de maquinetas de cartão de crédito e débito adulterados, onde os criminosos obtinham as senhas dos usuários do cartão, logo quando os clientes digitavam a senha nas máquinas adulteradas. Dessa forma, as senhas eram clonadas sem que os usuários soubessem e eram visualizadas por meio de um lap top, conectado à rede por meio da tecnologia wireless. Após obter os dados, os criminosos utilizavam as informações bancária coletadas para a efetuação de saques e compras (COUTINHO, 2014).

Na prática, para que seja considerado um crime de estelionato é necessário que a vítima seja induzida ao erro a partir da obtenção da prática ilícita, oferecendo vantagem para si ou para outrem (DELMANTO, 2016).

7.6 Pornografia infantil

A pornografia infantil é uma forma de violência sexual contra crianças e adolescentes caracterizada pela utilização de imagens de natureza erótica. Esse tipo de crime está inserido no Estatuto da Criança e do Adolescente (ECA) e no Código Penal (CP) (LANDINI, 2000).

Quanto a definição de criança e adolescente, o artigo 2º do Estatuto da Criança e do Adolescente ressalva que o indivíduo com até 12 anos de idade incompletos pode ser considerado criança e o adolescente está compreendido entre 12 a 18 anos de idade.

Apesar da semelhança, o crime de pornografia infantil se difere do crime de pedofilia, pois de acordo com a Organização Mundial de Saúde (OMS) a pedofilia consiste em um transtorno psicológico onde o indivíduo desperta interesse sexual por crianças ou adolescentes, sendo em alguns casos, o pedófilo considerado um doente e não um criminoso.

Porém, quando o doente ultrapassa a sua patologia e se enquadra dentro das diretrizes jurídicas, pode assim ser considerado um criminoso. Necessariamente, no crime de pornografia infantil, não há a necessidade de que ocorra a relação sexual em si para que seja considerado de fato um crime, tais condutas como a divulgação de fotos, vídeos ou conteúdos pornográficos podem ser considerados atos ilícitos (INELLAS, 2004).

Sobre a divulgação de conteúdos pornográficos envolvendo crianças, Crespo (2011), expõe a seguinte opinião:

Ocorre que a lei brasileira pune diversas formas situações envolvendo a exposição da sexualidade infantil em fotos, imagens, filmagens e interpretações teatrais, como, por exemplo, a produção, reprodução, filmagem e o registro de cenas de sexo explícito envolvendo situações de pornografia com crianças e adolescentes.

O Brasil é um dos poucos países que possuem leis específicas para coibir os crimes de pornografia infantil por meio de recursos virtuais. O Estatuto da Criança e do Adolescente, lei 8069/1991 apresenta em seus artigos os diversos tipos de condutas criminosas cometidas contra a criança e o adolescente, bem como a punição para a prática de cada delito:

O artigo 240 da lei 8069/1990 prevê punição de 4 a anos de reclusão para aquele tiver a conduta de produzir, reproduzir, dirigir, fotografar, filmar ou registrar, independente do meio utilizado, cena de sexo explícito ou pornográfica que envolva criança ou adolescente.

A mesma pena do caput do artigo 240 da lei 8069/90, aplica-se nos casos previstos no parágrafo primeiro do mesmo artigo para aquele que agenciar, recrutar, coagir ou intermediar a participação da criança ou do adolescente em cenas de sexo explícito ou pornográficas ou contracenando nestas cenas.

A pena aumenta em um terço do previsto no caput do artigo 240 da lei 8069/1990, previsão do parágrafo segundo do mesmo artigo em seus incisos, para os casos em que sejam cometidos por funcionário público; pelos que possuam relações domésticas, de coabitação ou ainda de hospitalidade; por parentes de sangue até 3º grau, ou ainda por adoção, tutor, curador, preceptor, empregador da vítima ou de quem tenha autoridade sobre esta.

O artigo 241 da lei 8069/90 dispõe sobre a comercialização ou exposição de vídeo, foto e outros registros que contenha cena de sexo explícito ou pornográfica que contenham criança ou adolescente, com previsão de pena de reclusão de quatro a oito anos.

A utilização dos meios virtuais por parte de crianças e adolescentes sem a supervisão de pais ou responsáveis, facilita a prática da pornografia infantil uma vez que torna esse ambiente mais suscetível a criação de perfis falsos e contas fakes afim de atrair as vítimas. É de grande importância que os pais acompanhem as fotos tiradas ou vídeos gravados diariamente por seus filhos e os sites que os mesmos tem acesso no seu dia a dia (PAIXÃO, 2019).

7.7 Estupro virtual

O crime de estupro não é considerado apenas pelo contato físico em si, ele vai além disso, podendo ser considerado também quando praticado pelo meio virtual. Nesse mesmo entendimento, o estupro sem contato físico pode ocorrer, por exemplo, quando há a exigência por meio da internet, que uma mulher frente a webcam mostre suas partes íntimas, sob ameaça de divulgação de arquivos pessoais (fotos ou vídeos íntimos da vítima). Santos (2017), explica que:

No caso em que o autor, ameaçando divulgar vídeo íntimo da vítima, a constrange, via internet, a se automasturbar ou a introduzir objetos na vagina ou no ânus, tem-se estupro, pois a

vítima, mediante grave ameaça, foi constrangida a praticar ato libidinoso diverso da conjunção carnal.

Em agosto de 2017, no estado do Piauí, ocorreu a condenação do primeiro caso considerado “estupro virtual”. No caso em questão, o agressor de 34 anos e técnico de informática ameaçou publicar fotos íntima, da ex namorada, caso a vítima não mandasse fotos dela se masturbando. Como a vítima resolveu não colaborar com o pedido do agressor, o mesmo criou um perfil com o nome da vítima, publicando fotos íntimas e da família da vítima. A polícia conseguiu efetuar a prisão do criminoso a partir do IP (endereço virtual), que fez com que o agressor fosse descoberto que além de publicar as fotos da ex namorada a polícia encontrou diversas outras fotos íntimas de outras mulheres (FERREIRA, 2017).

Sendo assim, o estupro virtual caracteriza-se a partir do momento em que se utiliza a internet como meio para a prática de conduta prevista no art. 213 do Código Penal (BRASIL, 1940).

O estupro virtual é um problema que vem ocorrendo cada vez mais na era tecnológica, sendo que essa prática de crime não requer uma nova distinção legal, mas sim um posicionamento por parte dos executores do direito, pois trata-se de um ato ilícito, que conforme previsto no art. 213 do CP, tem como principal meio de conduta os recursos tecnológicos devido a facilidade e velocidade para a propagação de informações (SILVA, 2021).

8. SUJEITOS DOS CRIMES VIRTUAIS

Dentro os crimes virtuais, estão inseridos os sujeitos que podem ser classificados como sujeitos ativos e passivos, fazendo parte dessa classificação tanto o lado que comete o ato danoso, quanto o que tem seu direito atingido pela conduta ilícita.

8.1 Sujeito ativo

O sujeito ativo de um crime é caracterizado por uma pessoa que pratica uma conduta ilícita e é culpado para responsabilização de seu ato danoso, podendo

realizar essa ação individualmente ou com a participação de outros autores (CAPEZ, 2005).

As práticas dos crimes virtuais por meio dos sujeitos ativos se diferem dos demais crimes pelo fato de utilizarem dispositivos tecnológicos e a Internet para a prática do ato além da utilização do conhecimento técnico sobre os sistemas e os dispositivos tecnológicos (ORRIGO; FILGUEIRA, 2016, p.5).

Dentre as inúmeras práticas executadas no mundo virtual, podemos citar os Hackers ou também conhecidos “piratas” do computador por possuírem grande conhecimento técnico sobre os dispositivos tecnológicos e pela sua facilidade em desenvolver sistemas que visam a obtenção de dados e informações para benefício próprio. Seu objetivo fundamental é de invadir um sistema criando novos programas e utilizando seus conhecimentos para dar continuidade a sequência em programas. Ainda assim os hackers não são considerados criminosos, desde que não utilizem das informações obtidas para a execução de práticas ilícitas (ORRIGO; FILGUEIRA, 2016, p. 5).

Diferentemente dos hackers, os crackers são considerados como pessoas com conhecimento elevado sobre os dispositivos informáticos e que utilizam de suas técnicas e conhecimentos para a prática de atos ilícitos, causando prejuízo alheio e invadindo a segurança de terceiros (MEDEIROS, 2015).

Carneiro (2012) define a diferença entre hackers e crackers da seguinte forma:

Os hackers e os crackers geralmente são muito parecidos em relação ao vasto conhecimento aprofundado em informática e a principal distinção é a finalidade que suas práticas resultam, sendo que os hackers realizam atividades positivas, não criminosas, enquanto a motivação dos crackers é criminosa em sua essência agindo normalmente premeditadamente com objetivo criminoso de obter vantagens ilícitas.

Dessa forma, fica claro que o hacker é o indivíduo que utiliza de suas técnicas e conhecimentos para a realização de ações não danosas. Contrariamente, o cracker utiliza de seu conhecimento técnico para a execução de atitudes danosas e condutas criminosas que prejudicam terceiros. Logo, pode-se dizer que o hacker é aquele que

utiliza seu conhecimento técnico avançado em informática para realização de ações positivas (MEDEIROS, 2015).

8.2 Sujeito passivo

O sujeito passivo de um crime é caracterizado por um indivíduo que sofre algum tipo de delito oriundo de alguma conduta criminosa, seja ele pessoa física ou jurídica (BITENCOUT, 2007).

Diferentemente do sujeito ativo o sujeito passivo é um personagem que se tem uma maior facilidade de descrever, já pode ser qualquer indivíduo que tenha um bem jurídico tutelado lesado ou ameaçado de lesão por práticas realizadas através de computador ou qualquer outro dispositivo tecnológico (ORRIGO, 2016).

De uma forma geral o sujeito passivo nos crimes virtuais será sempre uma pessoa física ou uma pessoa jurídica qualquer, ou ainda uma entidade de natureza pública ou privada, que seja titular de um bem jurídico tutelado, ou seja, pode ser qualquer indivíduo, ainda que pessoa jurídica, que possa ter por exemplo: seus bens desviados, seu patrimônio deteriorado ou informações violadas (CARNEIRO, 2012).

9. LEIS APLICÁVEIS NO ÂMBITO DOS CRIMES VIRTUAIS

Em decorrência do surgimento de ataques informáticos no Brasil, os operadores do Direito utilizavam de normas já existentes para suprir as lacunas da lei, apesar da necessidade de uma legislação específica para reprimir os delitos. O que a legislação não imaginava, era que os crimes informáticos fossem evoluir tão rapidamente, fazendo com que as leis implementadas épocas atrás pudessem ser promulgadas conforme expõe Masson (2014, p. 276):

É inegável que leis promulgadas décadas atrás, nas quais sequer se pensava na existência de computadores, levavam a malabarismos adaptativos dos operadores do Direito para enfrentar novos comportamentos, muitas vezes resultando na impunidade dos criminosos. Era preciso adaptar a legislação penal aos novos tempos.

Devido a facilidade de prática do delito, os crimes virtuais podem ser executados por qualquer pessoa, de qualquer lugar ou dispositivo informático. Para crimes praticados no Brasil, o Código Penal afirma que:

Art. 70. A competência será, de regra, determinada pelo lugar em que se consumar a infração, ou, no caso de tentativa, pelo lugar em que for praticado o último ato de execução.

§ 1º Se, iniciada a execução no território nacional, a infração se consumar fora dele, a competência será determinada pelo lugar em que tiver sido praticado, no Brasil, o último ato de execução.

§ 2º Quando o último ato de execução for praticado fora do território nacional, será competente o juiz do lugar em que o crime, embora parcialmente, tenha produzido ou devia produzir seu resultado.

§ 3º Quando incerto o limite territorial entre duas ou mais jurisdições, ou quando incerta a jurisdição por ter sido a infração consumada ou tentada nas divisas de duas ou mais jurisdições, a competência firmar-se-á pela prevenção.

Em casos de crimes praticados fora do país, mas iniciados no Brasil, a competência de julgamento será por parte da Justiça Federal, fazendo-se se necessário a investigação de onde o crime ocorreu. Caso não seja descoberto, a competência será do juiz que iniciou a investigação do caso.

O grande número de usuários de tecnologia faz com que aumente a possibilidade de disseminação de informações falsas, desafiando a legislação ao investigar casos e identificar os sujeitos responsáveis por tais práticas (SIQUEIRA, 2017).

No que se refere ao meio para localização do criminoso e penalização pelos delitos, Siqueira destaca:

Seria possível a identificação do criminoso obtendo o seu endereço de IP, login e senha do aparelho utilizado para a prática do crime, porém, os criminosos utilizam endereços falsos, dificultando o trabalho investigativo dos policiais. (SIQUEIRA, 2017, pág.122)

Além da falta de legislações específicas outro grande problema é a dificuldade de rastreamento das informações, já que estas são transmitidas de forma rápida e dificulta a identificação da prática ilegal. Para isso, se faz necessário a aplicação de

treinamento e utilização de meios técnicos que possam identificar a localização do crime e o criminoso. Teixeira (2013), faz o seguinte apontamento sobre as leis brasileiras:

O primeiro decreto condenatório por crime eletrônico no Brasil foi proferido pela juíza da 3ª Vara da Justiça Federal de Campo Grande (MS), Janete Lima Miguel. Isso apenas vem confirmar que nossa legislação vigente pode ser aplicada aos crimes cibernéticos. Porém, para alguns autores deveria ser formulada uma lei prevendo todas as ações danosas na Internet, mesmo que o bem jurídico tutelado seja o mesmo já tutelado pela lei previamente existente. Para isso é preciso avaliar os bens. Devemos nos preocupar em achar um meio termo entre liberdade de informação e proteção de dados pessoais, para que os bens jurídicos tutelados por leis aplicadas no mundo físico tenham valia também para o mundo virtual, e vice-versa. Ainda assim, não podemos nos enganar e desejar que o Direito Penal tutele todos os bens relevantes para a sociedade, sob pena de levarmos o sistema à falência.

A tecnologia virtual recebeu legislações inovadoras quanto a proteção da propriedade intelectual de programa de computador ao inserir, no Brasil, a Lei 9.609 de 19 de fevereiro de 1998, que substituiu a Lei 7.646 de 18 de Dezembro de 1987. A lei 9.609/1998 define o programa de computador como:

Art. 1º Programa de computador é a expressão de um conjunto organizado de instruções em linguagem natural ou codificada, contida em suporte físico de qualquer natureza, de emprego necessário em máquinas automáticas de tratamento da informação, dispositivos, instrumentos ou equipamentos periféricos, baseados em técnica digital ou análoga, para fazê-los funcionar de modo e para fins determinados.

A legislação dispõe ainda da proteção ao direito de registro, direito de autoria de programas virtuais, garantia a usuários de programas, comercialização e contratos de licença de uso.

A Lei 9.609/1998, no Art. 12 dispõe das seguintes penas em caso de violação dos direitos de autor de programa de computador:

Art. 12. Violar direitos de autor de programa de computador:
Pena - Detenção de seis meses a dois anos ou multa.

§ 1º Se a violação consistir na reprodução, por qualquer meio, de programa de computador, no todo ou em parte, para fins de comércio, sem autorização expressa do autor ou de quem o represente:

Pena - Reclusão de um a quatro anos e multa.

§ 2º Na mesma pena do parágrafo anterior incorre quem vende, expõe à venda, introduz no País, adquire, oculta ou tem em depósito, para fins de comércio, original ou cópia de programa de computador, produzido com violação de direito autoral.

Segundo Barbosa (2014), com a necessidade de melhoria da legislação vigente aos crimes virtuais, em novembro de 2012, o Congresso Nacional aprovou a Lei 12.737, que dispõe dos tipos de crimes virtuais e delitos informáticos. Com isso, o Código Penal sofreu uma alteração com a introdução da Lei 12.737/2012, acrescentando o tipo denominado “invasão de dispositivo informático”, art. 5 - A do Código Penal Brasileiro, contendo a seguinte descrição da conduta:

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;

§ 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”. (BRASIL, 2012)

Após o ocorrido com a famosa atriz brasileira que teve suas fotos íntimas vazadas na internet e ter ganhado grande repercussão nacional, o poder legislativo sofreu uma grande pressão da sociedade para que houvesse a penalização rígida sobre as pessoas que praticam esse tipo de crime. Com tamanha repercussão e com os danos causados à vítima, foi criada a Lei 12.737/12, denominada Lei Carolina Dieckmann. O ocorrido fez com que aumentasse a visibilidade e preocupação a respeito do tema (SIQUEIRA, 2017).

A lei 12.737/12 ficou popularmente conhecida como lei Carolina Dieckmann em virtude do episódio com a atriz, que em maio de 2012, teve seu computador invadido por criminosos que divulgaram 36 fotos íntimas da mesma, causando um grande transtorno e constrangimento à vítima. (SIQUEIRA, 2017, p.126)

Apesar da aprovação da lei e da sua significativa representação, não foi suficiente para a coibição de tais atos, necessitando da aprovação de novas normas como a Lei 12.965/2014, denominada Marco Civil da Internet (TOMASEVICIUS FILHO, 2016).

O Marco Civil surgiu com o propósito de garantir os direitos e deveres para os usuários de Internet no Brasil. Siqueira (2017), descreve os objetivos da seguinte forma:

A lei do Marco Civil foi criada para suprir as lacunas no sistema jurídico em relação aos crimes virtuais, num primeiro momento tratando dos fundamentos, conceitos para sua interpretação e objetivos que o norteiam, além de enumerar os direitos dos usuários, tratar de assunto polêmicos como por exemplo a solicitação de histórico de registros, a atuação do poder público perante os crimes virtuais e por último garante o exercício do direito do cidadão de usufruir da internet de modo individual e coletivo estando devidamente protegido. (SIQUEIRA, 2017, p. 126)

No art. 3º, a Lei 12.965/2014 descreve seus princípios básicos do uso da Internet no Brasil:

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

- I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;
- II - proteção da privacidade;
- III - proteção dos dados pessoais, na forma da lei;
- IV - preservação e garantia da neutralidade de rede;
- V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;
- VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei;
- VII - preservação da natureza participativa da rede;
- VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei.

Apesar dos esforços dos profissionais do Direito para a criação e normatização de legislações específicas para as relações estabelecidas por meio da

internet, as normas desenvolvidas não conseguem atingir todo o campo de atuação dos criminosos, necessitando ainda da implementação de outras legislações, como por exemplo, a regulamentação utilizada para as compras realizadas por meio da internet (SIQUEIRA, 2017).

Dentre as diversas leis criadas como o Marco Civil da Internet e Lei Carolina Dieckmann, por exemplo, houve também a criação da normativa no Estatuto da Criança e do Adolescente inserida no Art. 241-A que trata sobre a divulgação, transmissão e publicação de conteúdo pornográfico (fotografia ou vídeo) envolvendo crianças ou adolescentes.

No mundo, existem diversas leis e tratados a favor dos crimes eletrônicos e algumas antigas normas ainda são utilizadas atualmente, mas devido a constante evolução do mundo tecnológico e do surgimento de novas práticas criminosas, novas regulamentações são implementadas (TEIXEIRA, 2007).

10. CONSIDERAÇÕES FINAIS

Com a popularização da Internet e dos demais meios de comunicação, a sociedade contemporânea encontra-se cada vez mais dependentes desses meios, tornando quase que impossível a realização das atividades do dia a dia sem a utilização dos recursos tecnológicos.

O avanço da tecnologia provocou o uso exacerbado dos meios virtuais, ocasionando o surgimento dos crimes cibernéticos exigindo a partir disso uma intervenção do Estado como forma de impedir as práticas criminosas que interferem nos direitos dos cidadãos. Apesar de existirem leis votadas para os crimes virtuais, a legislação brasileira não se mostra totalmente eficaz para que todos os usuários da Internet tenham a segurança necessária. Dessa forma, os agentes do Direito deveriam acompanhar as evoluções tecnológicas e as transformações do mundo virtual, desenvolvendo diretrizes capazes de garantir os direitos essenciais para o ser humano.

Mesmo com o trabalho do Estado e dos demais órgãos responsáveis pela garantia do Direito do cidadão, ninguém está isento de sofrer esse tipo de crime. Um exemplo que podemos citar, foi o ocorrido com a famosa atriz brasileira Carolina

Dieckmann, que teve seu e-mail infectado e suas fotos íntimas foram divulgadas na internet. Logo após o ocorrido, foi sancionada a Lei 12.737 no ano de 2012, conhecida como Lei Carolina Deickmann.

No intuito de impedir o crescimento acelerado dos crimes virtuais, muitas legislações foram criadas, mas uma das grandes dificuldades, que acaba contribuindo pra o aumento da impunidade, está relacionado a falta de normas específicas que regulem os atos ilícitos praticados via internet.

A ausência de uma classificação adequada para os delitos praticados pelo meio virtual, ocasiona uma insegurança tanto social quanto jurídica. Levando em consideração que o ambiente virtual está em constante transformação é necessária muita cautela na aplicação de um ordenamento sobre o problema, devendo ser analisado de forma adequada. Dessa forma, torna-se necessário uma maior atenção quanto segurança da informação, além da realização de um treinamento especializado para os agentes da lei para que haja uma legislação atualizada e efetiva, de modo que ofereça segurança à sociedade punindo aqueles que utilizam de meios escusos para atacar inocentes.

Por fim, conclui-se que ainda não há legislação necessária para conter a criminalidade no meio virtual, mesmo levando em consideração todos os esforços apresentados pelo Direito Digital. Vale ressaltar que a lei 12.737/2012 já se apresentou como uma grande evolução legislativa a medida que mostrou posicionamento jurídico, visando garantir a proteção e segurança de dados e informações dos usuários, mas que apesar de sua grande utilidade, ainda precisa ser melhorada.

REFERÊNCIAS

AGÊNCIA BRASIL. **Relatório aponta Brasil como quarto país em número de usuários de internet.** Disponível em: <http://agenciabrasil.ebc.com.br/geral/noticia/2017-10/relatorio-apontabrasil-como-quarto-pais-em-numero-de-usuarios-de-internet/>. Acesso em 30 out. 2022.

ANDRADE, Geraldo. **Direito à privacidade: intimidade, vida privada e imagem.** 2015. Disponível em: <<https://quentasol.jusbrasil.com.br/artigos/214374415/direito-a-privacidade-intimidade-vida-privada-e-imagem#:~:text=A%20Constitui%C3%A7%C3%A3o%20Federal%20no%20art,moral%20decorrente%20de%20sua%20viola%C3%A7%C3%A3o>>. Acesso em: 12 nov. 2022.

AZUMA, Eduardo Akira. **A intimidade e a vida privada frente às novas tecnologias da informação.** Artigo disponível em: <<http://jus2.uol.com.br/doutrina/texto.asp?id=6168>>. Acesso em: 23. ago. 2022.

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

BARROS, Alberto Felipe Friderichs. **Crimes na Internet.** Instituto Federal Santa Catarina. 2018. Disponível em: <https://albertofelipeblog.files.wordpress.com/2016/07/crimes-na-internet.pdf>. Acesso em: 13 out. 2022.

BONDYREVA, S. K.; NIKITIN, A. V.; SAVRUTSKAYA, E. P.; USTINKIN, S. V. **O campo problemático das práticas de comunicação no contexto da globalização. Revista EntreLinguas,** Araraquara, v. 7, n. esp.2, p. e021029, 2021. DOI: 10.29051/el.v7iesp.2.15155. Disponível em: <<https://periodicos.fclar.unesp.br/entrelinguas/article/view/15155>>. Acesso em: 4 out. 2022.

BRASIL. **Código Penal.** Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848.htm> Acesso em 5 nov. 2022.

BRASIL. **Projeto de Lei nº 154/2019.** Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940, Código Penal, para estabelecer uma agravante genérica para os crimes cibernéticos.

CANOTILHO, J. J. Gomes. **Direito Constitucional e Teoria da Constituição.** Imprensa: Coimbra, Almedina, 2012..

CAPEZ, Fernando. **Curso de Direito Penal** v. 2 – Parte Especial, arts. 121 a 212, 16ª edição. São Paulo: Saraiva, 2016.

CASSANTI, Moisés de Oliveira. **Crimes virtuais, vítimas reais.** Rio de Janeiro: Brasport, 2014.

CETIC.BR. **TIC Domicílios.** Disponível em:<https://data.cetic.br/cetic/explore/Selecione%20uma%20unidade%20de%20an%C3%A1lise?pesquisa_id=1&unidade=Usu%C3%A1rios>. Acesso em: 10 out. 2022.

COSTA, C. L. N. do A.; SILVA, C. S.; JUNIOR, A. G. S.; NETO, J. de M. V.; SANTOS, D. M. S. **O processo de globalização no Brasil da década de 1950 até 2012**. Caderno de Graduação - Ciências Humanas e Sociais - UNIT - SERGIPE, [S. l.], v. 2, n. 1, p. 55–60, 2014. Disponível em: <<https://periodicos.set.edu.br/cadernohumanas/article/view/982>>. Acesso em: 12 out. 2022.

COUTINHO, Mateus. **Polícia Federal prende 16 em operação contra fraude com cartões bancários em São Paulo e Minas**. São Paulo: Estadão. 2014. Disponível em: <<https://politica.estadao.com.br/blogs/fausto-macedo/policia-federal-prende-16-em-operacao-contrafraude-com-cartoes-bancarios-em-sao-paulo-e-minas/>>. Acesso em: 23 out. 2022.

CUNHA, Rogério Sanches. 2017. **Adequação Típica**- Sextorsão. Disponível em: <<https://www.youtube.com/watch?v=RPxHYKQC0bs>> Acesso em 5 out. 2022.

D'URSO, Filizzola Luiz. **Em Tempos de Ciber Crimes**. 2019. Disponível em: <<https://www.migalhas.com.br/dePeso/16,MI310551,31047Em+tempos+de+ciber+crimes>>. Acesso em 11 ago. 2022.

DELMANTO, Celso et. al. **Código penal comentado**. 9. ed. Rio de Janeiro: Renovar, 2016.

fer

FERREIRA, Sabryna. **O que é estupro virtual?** 2017. Disponível em: <<https://posocco.jusbrasil.com.br/noticias/497174996/o-que-e-estupro-virtual>>. Acesso em: 13 out. 2022.

FRANCISCO, H. **Globalização, cultura e território: o Brasil no novo milênio**. Espaço & Economia. 2017.

GIMENES, Emanuel Alberto Sperandio Garcia. 2013. **Crimes Virtuais**. Disponível em: <http://www.revistadoutrina.trf4.jus.br/index.htm?http://www.revistadoutrina.trf4.jus.br/artigos/edicao055/Emanuel_Gimenes.html>. Acesso em: 3 out. 2022.

GOULART, Guilherme Damasio. **Punição de crimes cibernéticos em 2021: efeitos das alterações na “Lei Carolina Dieckmann”**. Instituto de Referência em Internet e Sociedade. 2021.

JC ONLINE. **Como se proteger de crimes cibernéticos**. 2014. Disponível em: <<https://jc.ne10.uol.com.br/canal/cidades/geral/noticia/2014/08/06/saiba-como-evitar-os-crimes-virtuais-138960.php>>. Acesso em: 02 set. 2022.

LEI Nº 12.737, de 30 de novembro de 2012. **Dispõe sobre a tipificação dos crimes cometidos eletronicamente**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 24 de agosto de 2022.

LIMA, Diego. **O que é globalização?** São Paulo: Neux Internet Encyclopedia, 2022. Disponível em: <<https://neux.com.br/o-que-e-globalizacao/>> Acesso em: 21 ago. 2022.

LUCCA, Newton De; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira De. **Direito & Internet III: Marco Civil da Internet Lei no. 12.965/2014**. São Paulo: Quartier Latin, 2015. p. 79–100

MASSON, Cleber. **Código Penal Comentado**. 2. ed. rev., atual. e ampl. - Rio de Janeiro: Forense; São Paulo: MÉTODO, 2016.

ONU - Organização da Nações Unidas. **Crescimento da Internet desacelera e 2,7 bilhões ficam fora da rede**. 2022. Disponível em: <<https://news.un.org/pt/story/2022/09/1801381#:~:text=Ao%20todo%2C%20existem%205%2C3,da%20pandemia%20de%20Covid%2D19>>. Acesso em 11 ago. 2022.

REPORT, Security. **Brasil é o 2º País que mais Perdeu Dinheiro com Cibercrimes em 2017**. Disponível em: <<http://www.securityreport.com.br/destaques/brasil-e-o-2opais-que-mais-perdeu-dinheiro-com-cibercrimes-em-2017/#.XdNzCldKjIU>>. Acesso em 12 nov. 2022.

SANTOS, André. **Estupro Virtual**. 2017. Disponível em <<http://www.direitopenalemcontexto.com.br/estupro-virtual/>> Acesso em 5 nov. 2022.

SILVA, Camila Requião Fentanes da. **Análise das Leis nº 12.735/2012 e 12.737/2012 e a (des)necessidade de uma legislação específica sobre crimes cibernéticos**.

SILVA, Erasmo Jamir Soares. **Estupro virtual**: um crime emergido no âmago da era tecnológica. 2021. Disponível em: <https://jus.com.br/artigos/95664/estupro-virtual-um-crime-emergindo-no-amago-da-era-tecnologica/2>. Acesso em: 23 out. 2022.

SILVA, José Afonso da. **Curso de Direito Constitucional Positivo**. 6ª ed., São Paulo: Revista dos Tribunais, 1990.

SIQUEIRA, Marcela Scheuer et al. **Crimes virtuais e a legislação brasileira**. (Re)Pensando o Direito – Rev. do Curso de Graduação em Direito da Faculdade CNEC Santo Ângelo. v. 7, n. 13 (2017).

SIQUEIRA, Marcela Scheuer et al. **Crimes virtuais e a legislação brasileira**. (Re)Pensando o Direito – Rev. do Curso de Graduação em Direito da Faculdade CNEC Santo Ângelo. v. 7, n. 13 (2017).

TEIXEIRA, Ronaldo de Quadros. **Os Crimes Cibernéticos no Cenário Nacional**. Escola superior aberta do Brasil – ESAB, 2013 (Curso de pós-graduação lato sensu em engenharia de sistemas).

TEIXEIRA, Tarcísio. **Direito Eletrônico**. 4º Ed. São Paulo: Joarez de Oliveira, 2007.

TLINSIDE. **O Brasil sofreu mais de 88,5 bilhões de tentativas de ataques cibernéticos em 2021**. 2022. Disponível em: <<https://tiinside.com.br/08/02/2022/brasil-sofreu-mais-de-885-bilhoes-de-tentativas-de-ataques-ciberneticos-em-2021/>>. Acesso em: 03 set. 2022.

TOMASEVICIUS FILHO, Eduardo. Marco civil da internet: uma lei sem conteúdo normativo?. Disponível em: <https://jus.com.br/artigos/45471/marco-civil-da-internetuma-lei-sem-conteudo-normativo>. Acesso em: 12. set. 2022.

IDGNOW. **Brasil tem 116 milhões de usuários Internet e comunicação é principal uso**. Disponível em: <<http://idgnow.com.br/internet/2018/02/21/brasil-tem-116-milhoes-de-usuarios-internet-e-comunicacao-e-o-principal-uso/>> Acesso em 23 out. 2022.

TRENTIN, Taise Rabelo Dutra; TRENTIN, Sandro Seixas. **Internet**: Publicações Ofensivas em Redes Sociais e o Direito à Indenização por Danos Morais. Revista Direitos Emergentes da Sociedade Global, Santa Maria, n. 1, p. 79-93, jan.jun/2012.

VIANA, Marco Túlio; apud, CARNEIRO, Adeneele Garcia. 2003. **Fundamentos de direito penal informático**. Do acesso não autorizado a sistemas computacionais. Rio de Janeiro, Editora Forense.