UNIVERSIDADE FEDERAL DE CAMPINA GRANDE - UFCG
CENTRO DE CIÊNCIAS JURÍDICAS E SOCIAIS - CCJS
UNIDADE ACADÊMICA DE DIREITO

NATÁLIA LIMA RIBEIRO

# DESAFIOS ENFRENTADOS NA REPRESSÃO DOS CRIMES INFORMÁTICOS À LUZ DOS AVANÇOS TECNOLÓGICOS

SOUSA-PB
2017

NATÁLIA LIMA RIBEIRO

# DESAFIOS ENFRENTADOS NA REPRESSÃO DOS CRIMES INFORMÁTICOS À LUZ DOS AVANÇOS TECNOLÓGICOS

Trabalho de Conclusão de Curso apresentado ao Curso de Direito do Centro de Ciências Jurídicas e Sociais da Universidade Federal de Campina Grande-UFCG, como exigência parcial para obtenção do título de bacharel em Ciências Jurídicas e Sociais.

.

Orientador (a): Prof. Dr. Jardel de Freitas Soares.

SOUSA-PB

2017

NATÁLIA LIMA RIBEIRO

# DESAFIOS ENFRENTADOS NA REPRESSÃO DOS CRIMES INFORMÁTICOS À LUZ DOS AVANÇOS TECNOLÓGICOS

Trabalho de Conclusão de Curso apresentado ao Curso de Direito do Centro de Ciências Jurídicas e Sociais da Universidade Federal de Campina Grande- UFCG, como exigência parcial para obtenção do título de bacharel em Ciências Jurídicas e Sociais.
.
Orientador (a): Prof. Dr. Jardel de Freitas Soares.

Data de aprovação: 15/03/2017

Banca Examinadora:

_____
Prof.Dr. Jardel de Freitas Soares
Orientador

_____
Prof. Dr. André Gomes de Sousa Alves
Membro da banca examinadora

_____
Prof. Mes. Emília Paranhos Santos Marcelino
Membro da banca examinadora

*Dedico:*

*Aos meus pais, na certeza de que se orgulharão de mim, como sempre tem sido, até mesmo nas pequenas vitórias.*

## AGRADECIMENTOS

A Deus, criador e razão da minha existência. Aquele que é minha fonte de força, fé e esperança. Ao Senhor, toda honra e glória.

Aos meus pais, Idalia Lima e Monilton Marcio. A eles, que me motivam, que acreditam em mim e que me apoiam quando fraquejo. A vocês que sempre fizeram de tudo para que eu pudesse realizar meus sonhos, não medindo esforços emocionais e financeiros.

Aos meus irmãos, Yuri Lima e Monilton Júnior, pelo amor, cumplicidade e torcida de sempre.

Ao meu amor e namorado, Milton Neto, por todo apoio, carinho e momentos felizes proporcionados nessa caminhada. A você que sempre me deu força e acreditou em mim.

As minhas amigas, Jaqueline Pereira, Jéssica Lima, Maíra Brito, Maria Amélia, Monalisa Leitão, Valéria Lima e Vanessa Severino, que foram minha família longe de casa. A vocês com as quais compartilhei aprendizados, conquistas e derrotas. Serei eternamente grata a Deus por Ele ter escolhido exatamente vocês para por no meu caminho.

Ao meu orientador, professor Jardel de Freitas, por toda orientação e paciência dispensadas na construção desse trabalho.

*“O sucesso nasce do querer, da determinação e persistência em se chegar a um objetivo. Mesmo não atingindo o alvo, quem busca e vence obstáculos, no mínimo fará coisas admiráveis”.*
*José de Alencar*

## RESUMO

O presente trabalho tem como tema os desafios enfrentados na repressão dos crimes informáticos à luz dos avanços tecnológicos. Nessa senda, verifica-se que os computadores e demais equipamentos eletrônicos, juntamente com a internet, evoluíram ao decorrer dos anos, se democratizando ao ponto da tecnologia ser o pilar da sociedade atual. Vale salientar que agregados aos benefícios proporcionados pela tecnologia, surgem também malefícios. Os criminosos enxergaram no suposto anonimato proporcionado pela internet, “terra fértil” para praticar delitos. Embora esses crimes sejam crescentes no Brasil, o Estado ainda não tomou as devidas providências para que a questão tenha o tratamento e importância merecida. Nesse sentido, foi adotada uma abordagem dedutiva, estudando os aspectos que tornam complexa a punição dos crimes informáticos e suas características. Foi realizado um estudo histórico-evolutivo da internet e do computador, assim como um estudo do surgimento desses crimes informáticos e todo o avanço até a atualidade. Esse trabalho objetiva analisar os aspectos jurídicos referentes a esses crimes, assim como os desafios enfrentados pelas autoridades brasileiras na persecução penal destes. Foram discutidas as principais legislações brasileiras que tratam dos crimes informáticos, abordando suas falhas técnicas, assim como, os desafios investigativos que vão desde precariedade em equipes investigativas especializadas, até as peculiaridades que esse meio digital possui e que dificultam a identificação do autor do delito. Conclui-se que a existência e crescimento constante dos crimes informáticos é um desafio para a sociedade e para os operadores do direito, e que é necessário o desenvolvimento de alternativas para solução desses empasses.



Palavras-chave: Crimes informáticos. Internet. Computador. Tecnologia. Repressão.

**ABSTRACT**

The present work has as its theme the challenges faced in the repression of internet crimes in the light of technological advances. In this way, it is verified that computers and other electronic equipment, along with the Internet, have evolved over the years, becoming democratizing to the point where technology is the pillar of the current society. It is worth noting that, in addition to the benefits provided by technology, there are also operational problems. Criminals have seen the alleged anonymity provided by the internet, "fertile ground" for committing crimes. Although these crimes are increasing in Brazil, the State has not yet taken the necessary measures to ensure that the issue is treated and deserved. In this sense, a deductive approach was adopted, studying the aspects that make the punishment of computer crimes and their characteristics complex. A historical and evolutionary study of the internet and the computer was carried out, as well as a study on the emergence of these computer crimes and all the progress made to date. The objective of this work is to analyze the legal aspects related to these crimes, as well as the challenges faced by the Brazilian authorities in the criminal process of these crimes. The main Brazilian laws dealing with computer crimes, addressing their technical flaws, as well as the research challenges ranging from the precariousness of specialized research teams to the peculiarities that this digital medium has and that make it difficult to identify the perpetrator, were discussed. It is concluded that the existence and constant growth of computer crimes is a challenge for society and for the operators of the law and that the development of alternatives for the solution of these crimes is necessary.

Keywords: Cybernetic crimes. Internet. Computer. Technology. Repression.

## LISTA DE SIGLAS E ABREVIATURAS

a.C - antes de Cristo

ABRANET - Associação Brasileira de Provedores de acesso, serviço e informação da rede de internet

ARPANET - Advanced Research Projects Agency Network

Art. - Artigo

Arts. - Artigos

BBS - Bulleting Board System

C. - Câmara

CC - Conflito de competência

CPP - Código de Processo Penal

CRFB/88 - Constituição da República Federativa do Brasil de 1988

DF - Distrito Federal

DJe - Diário de Justiça eletrônico

DRCI - Departamento de Recuperação

ENIAC - Electronic Numerical Integrator And Calculator

HC - Habeas Corpus

IBGE - Instituto Brasileiro de Geografia e Estatística

m - metros

Min. – Ministro

ns. - números

p. - página/páginas

PT - Partido dos Trabalhadores

SP - São Paulo

STF - Supremo Tribunal Federal

STJ - Superior Tribunal de Justiça

TJPR - Tribunal de Justiça do Paraná

TOR - The Onion Router

TRE - Tribunal Regional Eleitoral

UNIVAC - Universal Automatic Computer

**SUMÁRIO**

# 1 INTRODUÇÃO

A globalização proporcionou um cenário nacional e internacional de avanços tecnológicos, consequentemente, um desenvolvimento da sociedade de informação e a democratização do uso do computador e da internet. Essas inovações trouxeram novas discussões jurídicas sobre privacidade, ética, intimidade e liberdade.

Essa realidade trazida pelo fenômeno da globalização possibilita a vasta propagação de uma criminalidade nova, a virtual. Desta forma, diante do suposto anonimato que a internet proporciona, os criminosos encontraram um meio fértil para praticarem seus crimes, e usuários da rede desinformados e despreparados, tornam-se alvos perfeitos.

A escolha do tema se justifica mediante a grande importância de se debater esse cenário de criminalidade informática, uma vez que se vive em uma sociedade digital, dependente da internet para realizar muitas tarefas, e os delitos informáticos estão cada vez mais presente no dia-a-dia das pessoas, tirando toda tranquilidade dos usuários e deixando a sociedade assustada.

Com efeito, constata-se a crescente prática de crimes informáticos no Brasil, sem a eficaz punição do Estado, sendo, desse modo, de grande importância identificar os motivos que levam a essa impunidade e fazem com que os criminosos sintam-se cada vez mais à vontade para a prática desses delitos.

O ordenamento jurídico brasileiro e os agentes responsáveis pela persecução penal dos crimes informáticos não acompanham o mesmo ritmo de avanço da internet e as diversas formas de prática desses crimes.

Desta forma, nota-se que no cenário nacional, muitas vezes, esse tipo de crime fica impune em decorrência da dificuldade de encontrar o autor e puni-lo adequadamente. Isso decorre de uma omissão do Poder Legislativo na criação de legislações eficazes e na precariedade de agentes preparados para uma investigação eficiente dos crimes informáticos.

Haja vista que esses crimes evoluem conforme os avanços tecnológicos, faz-se necessária também uma rápida evolução do direito e das autoridades policiais responsáveis pela investigação desses crimes

Ante ao exposto, o objetivo geral desse trabalho é analisar os desafios legislativos e investigativos enfrentados na tentativa de esclarecer a autoria e materialidade dos crimes informáticos para que seja aplicada a reprimenda devida.

Os objetivos específicos são apresentar um breve estudo sobre o histórico e evolução da internet e dos crimes informáticos, analisar as leis existentes no ordenamento jurídico brasileiro que tratam do tema, abordar os obstáculos encontrados para identificar um criminoso virtual em investigação policial, assim como examinar a precariedade técnica dos órgãos responsáveis pela persecução penal.

A abordagem do tema é desenvolvida com base na seguinte questão norteadora: Como o ordenamento jurídico omisso e a carência de meios de investigações eficientes contribuem para impunidade dos delitos informáticos?

Quanto à metodologia, nesse trabalho foi adotada a abordagem dedutiva, uma vez que se estudaram quais os motivos que tornam tão complexa a punição dos crimes cibernéticos, assim como suas características e requisitos. O procedimento adotado foi o método histórico-evolutivo, aplicado no histórico evolutivo da internet, o surgimento dos crimes cibernéticos e todo o seu avanço até os dias atuais. A técnica de pesquisa adotada foi a da documentação indireta, uma vez que houve um estudo baseado na pesquisa bibliográfica e documental acerca dos crimes cibernéticos em todos os seus aspectos, visando demonstrar toda estrutura teórica, doutrinária e jurisprudência relacionada à temática.

Com relação à estrutura, o trabalho está dividido em três capítulos, dispostos de tal forma que o primeiro apresenta uma visão geral do surgimento das máquinas de computar e sua evolução até os computadores pequenos e modernos dos dias atuais, da evolução histórica da internet e sua importância na sociedade e de toda a questão histórica e conceitual dos crimes informáticos.

Já o segundo capítulo faz uma abordagem dos aspectos jurídicos dos crimes informáticos, trazendo uma análise das legislações brasileiras sobre o tema e estabelecendo um comparativo com algumas peculiaridades das legislações de outros países.

No último capítulo são analisados os aspectos procedimentais e legislativos que dificultam a punição dos agentes que praticam os crimes no mundo virtual. Nesse contexto, são feitas críticas à principal legislação específica existente sobre delitos informáticos, a Lei 12.737/2012, assim como uma análise dos aspectos

peculiares do sujeito ativo destes delitos, que dificultam a sua identificação, e a deficiência dos órgãos investigativos do Brasil.

Desse modo, o presente trabalho se propõe a demonstrar quais são os maiores problemas encontrados ao tentar combater os delitos informáticos, tendo em vista a enorme dificuldade encontrada pelas autoridades para punir adequadamente as condutas delituosas que muitas vezes acabam impunes sem que o seu autor seja identificado.

.

# 2 CONSIDERAÇÕES GERAIS SOBRE O COMPUTADOR, A INTERNET E OS CRIMES INFORMÁTICOS

A evolução da tecnologia é constante, fazendo surgir dispositivos cada vez mais modernos e funcionais. Os computadores, que antes eram máquinas enormes, ocupando várias salas, se tornaram pequenas máquinas, altamente evoluídas, capazes de realizar atividades antes inimagináveis.

Com o desenvolvimento tecnológico surgiram outros dispositivos digitais como *tablets* e *smartphones*. Todos esses aparelhos eletrônicos quando conectados a rede mundial de internet possibilitam a realização de diversas atividades.

A sociedade utiliza os aparelhos digitais conectados à internet para se comunicar com pessoas que estão a quilômetros de distâncias, para fazer transações bancárias, buscar informações, se distrair, entre outras coisas fruto dessa tecnologia.

Se vive em uma era digital, onde a internet se democratizou e grande parcela da população passa o dia conectado a esta. A internet deixou de ser uma distração e passou a ser indispensável no dia-a-dia das pessoas.

A internet alcança um público incontável ao redor do mundo inteiro e é um canal de publicidade, interação social, negócios e entretenimento. Porém, as pessoas utilizam esses meios para diversas práticas, há os que utilizam para propagar coisas boas, porém, também há os que utilizam de uma forma errada. Em meio a toda essa era digital surgem os crimes informáticos, que aumentam em proporção alarmante.

É justamente devido a essa falta de consciência digital de muitas pessoas que a sociedade sente a necessidade de que o Estado se posicione, modernizando o direito frente a essa nova realidade em que as pessoas vivem, para que a internet seja um lugar de navegação segura para os seus usuários e os crimes sejam repreendidos.

## 2.1 EVOLUÇÃO HISTÓRICA DO COMPUTADOR

O computador é meio essencial para a prática de muitos crimes informáticos nos dias atuais. Trata-se de um aparelho eletrônico que processa dados. O termo vem do latim *computare*, que significa calcular. Cada vez mais o computador se moderniza, tornando-se essencial na vida diária das pessoas, sendo utilizado para desenvolvimento das mais diversas atividades.

O primeiro instrumento de computar foi o ábaco, uma máquina chinesa, desenvolvida por volta de 3.500 a.C. Era uma espécie de máquina de calcular que resolvia operações algébricas. A partir daí as máquinas de computar evoluíam constantemente.

O Mark I foi o primeiro computador eletromecânico, construído em 1944 por uma equipe liderada por Howard Aiken da Universidade de Harvard em Cambridge U.S.A. O Mark I tinha 17 metros de comprimento, 2,5 metros de altura e um peso por volta de 5 toneladas.

O primeiro computador eletrônico foi o ENIAC (*Electronic Numerical Integrator And Calculator*), construído entre 1943 e 1945 pelos pesquisadores norte-americanos Jonh Eckert e Jonh Mauchly da Eletronic Control Company. O ENIAC possuía 30 toneladas e ocupava uma área de aproximadamente 180m². Foi desenvolvido durante a II Guerra Mundial, tinha como finalidade cálculos balísticos e tornou-se operacional após a guerra.

A evolução do computador teve grande força devido à grande necessidade de aperfeiçoamento durante a Segunda Guerra Mundial.

"[...] O que fica, entretanto, é que a evolução dessa tecnologia deveu-se ao advento da Segunda Guerra Mundial, que gerou, além de grande desgraça, enorme avanço tecnológico nas mais variadas áreas, inclusive na computação." (ROSSINI, 2004, p. 24).

O UNIVAC (*Universal Automatic Computer*), projetado pelos mesmos inventores do ENIAC, foi o primeiro computador comercial, fabricado e comercializado nos Estados Unidos, em 1951. Ao todo se vendeu 46 unidades do UNIVAC modelo I.

O IBGE (Instituto Brasileiro de Geografia e Estatística) adquiriu em 1961 um UNIVAC, sendo um dos primeiros computadores do Brasil. Pesava aproximadamente 13 (treze) toneladas e ocupava um espaço de 13m².

Os computadores, que antes pesavam toneladas, foram evoluindo ao longo das últimas décadas, até se chegar as máquinas modernas, potentes e portáteis dos dias atuais. A evolução histórica dos computadores compreendem 5 gerações.

A primeira geração do computador compreende o período de 1940 a 1952. Essa geração foi marcada pela utilização de circuitos e válvulas eletrônicas. Eram máquinas enormes, bem pesadas e consumiam uma enorme quantidade de energia. Os dados eram armazenados em cartões perfurados e, posteriormente, passaram a ser armazenados em fitas magnéticas.

O ENIAC é um representante da primeira geração. Os computadores calculavam com uma velocidade de milésimos de segundo e eram programados em linguagem de máquina. Nessa época, os computadores ainda não possuíam fim comercial.

A segunda geração ocorreu de 1952 a 1964 e foi quando ocorreram às substituições das válvulas por transistores, artefatos eletrônicos que funcionavam como interruptores, definindo se uma corrente ia passar de um ponto ao outro.

O tamanho, assim como o consumo de energia, diminuiu bastante, fazendo com que os computadores começassem a ter uso comercial. O IBM 7094 foi o computador mais popular da segunda geração, tendo milhares de unidades vendidas.

A terceira geração ocorreu entre 1964 a 1971, onde surgiu o microchip, circuitos integrados e feitos de silício. Os cálculos eram feitos em nanossegundos, com uma linguagem de programação de alto nível. Os computadores ganharam formas bem mais compactas, o custo diminuiu, assim como o consumo de energia.

Na quarta geração, entre 1971 e 1981, surgiram os microcomputadores. É conhecida como a geração dos computadores pessoais. Com menos de 20kg, os computadores possuíam microprocessadores que trouxeram uma enorme quantidade de novas opções para os usuários. Surgiram os processadores de textos, planilhas e banco de dados.

A quinta geração compreende o período de 1981 até os dias atuais. Nessa geração são utilizados processadores com milhões de transistores, e segue a tendência da miniaturização das máquinas.

Em relação a essas gerações Rossini (2004, p. 25) dispõe:

> 1ª geração (de 1940 a 1952) – computadores à base de válvulas à vácuo – alimentação por cartões perfurados – uso exclusivamente militar (nessa época surgiu a teoria da "informática jurídica" desenvolvida por Lee Loevinger). 2ª geração (de 1952 a 1964) – substituição das válvulas por transistores – maior velocidade – uso administrativo e gerencial. 3ª geração (de 1964 a 1971) – substituição dos transistores pelos circuitos integrados (surgidos em 1964) – miniaturização dos grandes computadores – evolução dos softwares e criação dos chips de memória – ampliação do uso comercial. 4ª Geração (de 1971 a 1981) – substituição dos circuitos pelos microprocessadores – criação dos floppy disks, ou disquetes, para o armazenamento de dados – nascimento da telemática. 5ª geração (de 1981 até hoje) – enorme avanço da computação – criação da inteligência artificial, da linguagem natural e da altíssima velocidade do processamento de dados – principal novidade: disseminação da internet.

Atualmente, na quinta geração, o computador se popularizou devido ao seu custo mais acessível, tornando-se elemento essencial na vida das pessoas. O computador é utilizado para diversos afazeres do dia-a-dia, como para trabalhar, assistir a um filme, e fazer uma transação bancária. Hoje em dia existem até cursos para que as pessoas aprendam a lidar com os computadores e seus *softwares*.

## 2.2 CONTEXTO HISTÓRICO DA INTERNET

A internet é uma rede mundial interligando milhares de computadores que tem em comum um conjunto de protocolos e serviços, de forma que os usuários conectados possam usufruir de serviços de informação e comunicação de alcance mundial.

Surgiu em plena Guerra Fria, quando, em 1969, foi desenvolvido a *Advanced Research Projects Agency Network* (ARPANET), um projeto do Departamento de Defesa norte-americano, tornando-se a primeira comunicação digital via comutação de pacotes.

Foi criada com o intuito de ser uma das formas das forças armadas dos Estados Unidos manter as comunicações em caso de ataques inimigos que destruíssem os meios convencionais de telecomunicações.

Conforme Paesani (2013, p. 25), tinha o objetivo de evitar que fosse interrompida a corrente de comando dos Estados Unidos por um possível ataque nuclear:

> O projeto Arpanet da agência de projetos avançados (Arpa) do Departamento de Defesa norte-americano confiou, em 1969, à Rand Corporation a elaboração de um sistema de telecomunicações que garantisse que um ataque nuclear russo não interrompesse a corrente de comando dos Estados Unidos. A solução aventada foi a criação de pequenas redes locais (LAN), posicionadas nos lugares estratégicos do país e coligadas por meio de redes de telecomunicação geográfica (WAN). Na eventualidade de uma cidade vir a ser destruída por um ataque nuclear, essa rede de redes conexas – Internet, isto é Inter Networking, literalmente, coligação entre redes locais distantes, garantiria a comunicação entre as remanescentes cidades coligadas.

Após a Guerra Fria, nas décadas de 1970 e 1980, a internet passou a ser um importante meio de comunicação no meio acadêmico das universidades dos Estados Unidos, principalmente após 1973 quando foi registrado o protocolo de controle da transmissão/protocolo internet, projeto desenvolvido por Vinton Cerf da Universidade da Califórnia.

Porém, foi somente no ano de 1990, que a internet começou a alcançar a população em geral. A década de 90 foi considerada a era da expansão quando começou a ser utilizada nas mais diversas classes sociais e não parou de evoluir.

Rosa (2002, p. 33) conceitua a internet da seguinte maneira:

> [...] a Internet é um conjunto de redes de computadores interligados pelo mundo inteiro, que têm em comum um conjunto de protocolos e serviços, possuindo a peculiaridade de funcionar pelo sistema de troca de pacotes, ou seja, as mensagens dividem-se em pacotes e cada pacote pode seguir uma rota distinta para chegar ao mesmo ponto. A Internet funciona graças aos protocolos ou sistemas de intercomunicação de programas, cujos protocolos mais importantes são o TCP (protocolo de controle de transferência) e o IP (Protocolo Internet), permitindo, assim, a utilização da Internet por computadores funcionando com qualquer Sistema Operacional: DOS, Windows, UNIX, MAC etc.

Essa rede mundial foi implantada comercialmente no Brasil apenas em meados dos anos 90, através da Norma nº 004 do Ministério das Telecomunicações[1], sendo inicialmente comercializada pela empresa Embratel.

[1] A norma nº 004 do Ministério das Telecomunicações foi aprovada em 1995 e regulava o uso dos meios da rede pública de telecomunicações para o provimento e utilização de serviços de conexão à internet.

Em 1996 já existiam cerca de 300 mil usuários da internet no Brasil. De acordo com a ABRANET (Associação Brasileira dos Provedores de Acesso, Serviços e Informações da Rede Internet), em 1997, esse número aumentou para 700 mil.

Conforme Paesani (2013), hoje em dia a estimativa de usuários brasileiros da internet ultrapassa oitenta milhões. Porém, ainda há mais de cem milhões de pessoas que não são usuários.

A internet é um meio tecnológico de suma importância, uma vez que as pessoas realizam através dela as mais diversas atividades, como compras, pesquisas, operações bancárias e comunicação, trazendo diversos outros benefícios.

É nesse cenário de popularização e avanços tecnológicos na área da informática que surgem os denominados crimes informáticos, que passam a preocupar a população quando começam a interferir nas relações sociais, antes seguras e pacíficas.

## 2.3 DIREITO E A ERA DIGITAL

Na atual sociedade em que vivemos é a tecnologia, internet e informática que causam as principais mudanças sociais. O acesso a esses meios estão cada vez mais abrangentes, e é através deles que os comportamentos e costumes da sociedade estão sendo ditados.

A nova sociedade de informação ultrapassa as barreiras culturais, políticas, sociais e econômicas, interligando usuários de todos os continentes. Hoje em dia as pessoas ficam protegidas atrás de uma tela de computador ou *smartphone*, passando a representar usuários anônimos com acesso a um turbilhão de informações.

Para Jesus e Milagre (2016), a convergência da tecnologia, a dinâmica da indústria e a queda nos preços dessas ferramentas, aliado ao enorme crescimento da internet são as molas propulsoras das recentes transformações sociais locais.

É indiscutível que o barateamento dos computadores nas últimas décadas está contribuindo para o largo acesso a informática e a internet por usuários do

mundo inteiro. As pessoas usam a tecnologia no dia-a-dia para diversas atividades, como para compras e vendas, pagamentos, acesso a informações e comunicação, muitas vezes fazendo desse meio o seu sustento pessoal.

Essa era digital traz consigo novos riscos e consequentemente a necessidade de uma regulação pelo direito. A sociedade sente a necessidade de formas de prevenção e de punição dos prejuízos causados através da rede mundial de computadores.

No Brasil, essas questões, no aspecto legislativo e operacional, encontram-se bastante deficientes. O direito ainda não forneceu respostas satisfatórias à sociedade. Conforme entendimento de Sydow (2015, p. 23):

> Por certo, há lacunas na parte geral e na parte especial do Direito Penal Brasileiro que merecem maior atenção legislativa e também mais detido estudo para se compreender melhor o uni- verso tratado, apesar das novas Leis ns. 12.735/2012 e 12.737/2012. Há tipos demandados pela nova doutrina que necessitam ser pensados diante da realidade informática brasileira para que a interpretação do Direito Penal não se torne falha, passando sensação de impotência estatal e impunidade aos agentes.

A sociedade, assim como a tecnologia, está em constante evolução, dessa forma, o direito deve acompanhar essa evolução, se adaptando a era da digital em que a humanidade vive atualmente.

São necessárias normas que protejam a sociedade em face dessa era tecnológica e dos riscos que ela traz consigo. Se não houver normas regulando essas questões, estabelece-se uma enorme insegurança jurídica.

As questões da era digital requerem a regulamentação nas mais diversas áreas do direito. Na área do direito civil quando se envolve fatos relacionados à compra, troca e venda realizadas via internet.

Na área do trabalho quando envolve contratações de trabalho realizadas virtualmente. Assim como o direito civil e o direito do trabalho, várias ramificações do direito podem vir a regulamentar as relações digitais.

O Direito Penal é um grande e importante instrumento de controle social, desta forma, os novos crimes surgidos na era digital são grandes desafios jurídicos para esse ramo do direito, necessitando urgente de uma eficaz regulamentação legislativa e um eficiente combate operacional.

Até pouco tempo os legisladores brasileiros não tratavam a informática como um bem que merecia muita relevância. O Direito penal só deve proteger os bens

juridicamente mais importantes, partindo dessa premissa, legislações que tratasse de crimes informáticos não foram aprovadas facilmente no Brasil.

As legislações informáticas existentes no Brasil ainda são embrionárias, e possuem muitas falhas técnicas, não oferecendo proteção ao bem jurídico informática da melhor maneira possível.

Onde há relevância econômica, é imprescindível que haja também relevância jurídica. Na sociedade de informação, dependente da internet, faz-se necessário essa proteção efetiva dos dados informáticos.

Na era atual o Direito deve ser preponderante, fazendo-se valer diante dos conflitos travados entre os usuários digitais. O Estado tem que ter controle do que acontece na sociedade para que as possíveis marginalidades que venham a surgir possam ser combatidas de forma eficaz.

## 2.4 CONCEITOS E CONTEXTO HISTÓRICO DOS CRIMES INFORMÁTICOS

As qualificações quanto aos crimes praticados na internet são inúmeras, “crimes cibernéticos”, “crimes informáticos”, “crimes de computador”, “crimes tecnológicos”, “crimes da era da informação”, “crimes da tecnologia da informação”, “crimes mediante computadores”, “cibercrimes”, “crimes eletrônicos”, “crimes digitais”, “crimes high-tech”, “tecnocrimes”, “netcrimes”, “crimes virtuais” e até mesmo “e-crimes”.

Segundo Jesus e Milagre (2016), no Brasil, o termo escolhido para denominar esses tipos de crimes foi “delitos informáticos”. Esse termo é utilizado nos países que adotam a língua espanhola e tem relação com o bem jurídico protegido, a informática e a informação.

Crimes informáticos são todas as condutas típicas, antijurídicas e culpáveis contra ou praticadas com o uso dos sistemas da informática.

Lima (2013, p. 13) conceitua esses crimes da seguinte forma:

> [...] temos que crimes de computador são qualquer conduta humana (omissiva ou comissiva) típica, antijurídica e culpável, em que a máquina computadorizada tenha sido utilizada e, de alguma forma, facilitado de sobremodo a execução ou a consumação da figura delituosa, ainda que cause um prejuízo a pessoas sem que necessariamente se beneficie o

> autor ou que, pelo contrário, produza um benefício ilícito a seu autor, embora não prejudique a vítima de forma direta ou indireta.

Dessa maneira, se o sistema informático for utilizado na conduta de um indivíduo que pratica uma ação ou omissão, desde que típica, antijurídica e culpável, esse indivíduo estará praticando um crime informático.

Essa nova realidade trazida pela era digital, proporciona um grande e rápido avanço dos crimes informáticos. Dessa forma, os criminosos virtuais podem cometer seus crimes das mais diversas maneiras e contra vítimas de qualquer lugar do planeta.

Os avanços tecnológicos se propagaram nacional e internacionalmente, consequentemente, se desenvolveu uma sociedade global de comunicação moldada virtualmente e capaz de realizar ações antes inimagináveis.

Todas essas inovações trouxeram uma necessidade de novas discussões sobre direitos já tutelados, como a comunicação, a privacidade, a informação, como também, trouxe a necessidade de grandes questionamentos sobre novos bens que também precisam ser tutelados, como a informática.

Os crimes informáticos surgiram, no mundo, na década de 1960. A comercialização e popularização da internet só ocorreram no Brasil na década de 90, e desde então surgiu no país os crimes virtuais.

Tem-se notícia dos primeiros crimes dessa espécie, no Brasil, entre 1997 e 1999. Foi então que a sociedade começou a sentir a necessidade de criação de leis versando sobre o assunto.

Em 1998, já se tem o julgamento do Habeas Corpus 76.689/PB, pelo Supremo Tribunal Federal (STF), referente a um caso de publicação de cena de sexo infanto-juvenil[2]. (BRASIL, 1998)

Nesse caso, havia sido imposta medida sócia-educativa de prestação de serviço a comunidade a dois adolescentes de quinze anos de idade por terem divulgado, através de uma rede BBS (*Bulleting Board System*)[3], imagens de crianças e adolescentes nus em práticas sexuais.

---

[2] O Habeas Corpus foi impetrado com a argumentação de que a representação deveria ser rejeitada e o processo trancado e arquivado. Na época, os pacientes alegaram que no ordenamento jurídico brasileiro, não havia qualquer previsão legal que coibisse a prática de inclusão de cenas pornográficas na internet.

[3] Bulleting Board System era um sistema informático que permitia uma conexão, por meio do telefone, a um sistema através do seu computador. Era como um provedor de web, porem, funcionava de

A grande maioria das vítimas dos crimes cibernéticos são pessoas comuns, que não tem noção da dimensão da rede em que estão inseridas, e nem dos riscos que o uso dessa rede pode proporcionar quando utilizada por outros usuários maliciosos.

O anonimato traz segurança para que os usuários da rede mundial de computadores ajam de forma delituosa, principalmente, diante da dificuldade de repressão, somada a ineficiência da legislação brasileira para tratar desses casos.

Com o grande avanço da tecnologia, o número de crimes cibernéticos praticados só vem aumentando e a legislação tornando-se ultrapassada diante de tanta modernidade.

O Direito como instrumento regulador da sociedade, deve acompanhar os avanços tecnológicos surgidos com a internet, se adaptando a essas mudanças de forma direta, com o intuito de trazer novas e eficazes soluções para os novos problemas, sob pena de perder o seu papel.

---

forma isolada, pois para duas pessoas se comunicarem através dos seus computadores era necessário colocar um computador para discar pra o telefone BBS do outro.

# 3 ASPECTOS JURÍDICOS DOS CRIMES INFORMÁTICOS

Todo o desenvolvimento dos equipamentos tecnológicos nas últimas décadas, assim como a possibilidade de conexão à internet, facilitou a vida de toda a população, proporcionando que essa realize atividades importantes através de uma tela digital.

Com toda essa evolução tecnológica e o surgimento de delitos nesse meio, perceber-se que o Código Penal é defasado quando se trata destes crimes que vão além do plano físico. Por se tratar de um código de 1940, na época de sua criação ainda não havia essa espécie de criminalidade.

Desta forma, faz-se necessária uma análise das recentes legislações elaboradas tratando da temática, assim como, um breve estudo de como alguns países tratam legislativamente a repressão desses crimes.

## 3.1 CLASSIFICAÇÃO DOS CRIMES INFORMÁTICOS

Os crimes informáticos possuem diversas classificações. Jesus e Milagre (2016) classificam esses crimes em próprios, impróprios, mistos e mediatos ou indiretos.

Os crimes informáticos próprios, ou puros, são aqueles que são praticados com o objetivo de atingir o computador do sujeito passivo, com atentado ao seu sistema e dados.

O bem jurídico tutelado, nos casos dos crimes informáticos classificados como próprios, é a própria tecnologia de informação. Nessa categoria de crime se encontra a invasão de dados de computadores, e sua respectiva alteração. A finalidade é atacar o *software*, *hardware*, dados, entre outros componentes do sistema do computador.

No caso dos crimes informáticos impróprios, há bens que são protegidos pelo Código Penal, e a tecnologia de informação é o meio utilizado pelo sujeito ativo para atingir esses bens.

Nesse caso, o bem jurídico tutelado é diverso do sistema informático, mas este é utilizado como instrumento para realização do delito. Enquadra-se nessa categoria os crimes de ameaça realizados através de rede mundial de computadores, assim como a veiculação de pornografia infantil.

Os crimes informáticos mistos são aqueles atacam a tecnologia de informação em si, mas também, afetam outros bens jurídicos diversos do informático. Neste caso, há execução de dois tipos penais diferentes.

Crime informático mediato ou indireto é o praticado com o objetivo da consumação de um crime não informático ao final. Quando o sujeito ativo do delito invade o dispositivo informático de um banco com o intuito de fazer uma transferência ilegal para sua conta bancária, estará praticando dois crimes, um crime cibernético, e outro patrimonial. De acordo com o princípio da consunção, o crime-fim absorverá o crime-meio, nesse caso, o agente só será punido pelo crime patrimonial.

## 3.2 SUJEITOS DOS CRIMES INFORMÁTICOS

A presença de um sujeito ativo virtual dificulta a imputação do crime ao real autor físico do delito. No mundo digital, temos agentes sentindo-se protegidos pela sensação de anonimato, e aproveitando-se da falta de conhecimento e precaução dos usuários que utilizam a rede mundial de computadores.

Há alguns anos atrás, o crime informático apenas era cometido por sujeitos com amplo e profundo conhecimento de informática, porém, com o passar dos anos, o acesso a informações e métodos de se cometer um crime no mundo digital se propagou, fazendo com que atualmente qualquer pessoa seja um possível criminoso virtual.

As pessoas mais leigas costumam denominar o criminoso virtual de forma errônea, chamando-o de *hacker. Hacker* é um grande conhecedor de sistemas informáticos, porém, não utiliza esse conhecimento para fins ilegítimos.

Os denominados *crackers* são os que utilizam seus conhecimentos tecnológicos para a execução de práticas delituosas. Existem várias outras

denominações para os mais diversos perfis de criminosos virtuais, de acordo com suas peculiaridades[4].

O sujeito passivo do crime informático é a pessoa ou ente que sofre os danos decorrentes da execução do delito. Muitas vezes, as vítimas dos crimes cibernéticos contribuem de forma substancial pra que o autor do delito consiga executá-lo.

A rede mundial de computadores atrai cada vez mais milhões de usuários, tornando-se indispensável na realização das mais diversas atividades dos seus dia-a-dia. Soma-se a estrutura dessa rede, a negligência e imprudência de muitos usuários, e se estará diante de um ambiente fértil a propagação desses delitos, tornando-os cada vez mais comuns e frequentes. Segundo entendimento de Sydow (2015, p. 208):

> Conforme exposto, a rede mundial de computadores mostra-se um ambiente propício constantemente para a execução de delitos informáticos, especialmente porque sua estrutura propicia a oportunidade, no sentido de que a contemporaneidade por si só traz a vítima para o ambiente e a vulneraliza.

Conforme o crime informático praticado, pode-se identificar o sujeito passivo, podendo ser pessoa física ou jurídica, haja vista que essa pode ter seus bens desviados ou informações sigilosas violadas. Geralmente, as grandes empresas que são vítimas desses crimes não fazem a devida comunicação à polícia receando uma publicidade que as prejudiquem.

## 3.3 DOS BENS JURIDICAMENTE PROTEGIDOS

Os bens são valores necessários à sociedade e, por esse motivo, os mais relevantes devem ser protegidos juridicamente pelo Direito Penal. Exemplo de bem juridicamente protegido pelo Direito Penal é a vida, a liberdade, a honra e o patrimônio.

O Direito Penal é um sistema de controle social imprescindível, este protege os bens jurídicos essenciais para a sociedade. Com a era da sociedade de

[4] *Carders* são pessoas que atuam na internet fraudando cartões de créditos. *Phreakrs* são o crackers da telefonia

informação surgiu então novas discussões acerca da necessidade de proteção dos direitos dos cidadãos em face desse mundo virtual.

A era digital trouxe consigo novos bens jurídicos a serem tutelados, como dados, documentos eletrônicos, hardwares, entre outros, uma vez que os crimes cibernéticos podem afetar os mais diversos bens. Crespo (2011, p. 56) assevera:

> Ao considerarmos as condutas ilícitas por meio da informática, verificamos a possibilidade de lesão a outros bens jurídicos. Assim, pode-se falar em condutas dirigidas a atingir não só aqueles valores que já gozam de proteção jurídica, como a vida, a integridade física, o patrimônio, a fé pública, mas, também as informações armazenadas (dados), a segurança dos sistemas de redes informáticas ou de telecomunicações.

De acordo com o princípio da Reserva Legal, previsto no art. 1º do Código Penal, nenhum fato poderá ser considerado crime, se assim não estiver disposto em lei. Nesse mesmo sentido dispõe o art. 5º, no seu inciso XXXIX, da Constituição Federal. Desta forma, com o avanço dos computadores, da internet e da tecnologia em geral, surge a necessidade do Direito Penal tutelar novos bens jurídicos decorrentes desta nova era, para que os crimes informáticos sejam eficazmente reprimidos.

## 3.4 CRIMES INFORMÁTICOS E A LEGISLAÇÃO BRASILEIRA

O avanço diário da tecnologia faz com que surjam mais e mais espécies de crimes no mundo virtual, além de potencializar os já existentes. O Brasil levou bastante tempo para desenvolver uma legislação que tratasse dos crimes informáticos.

Faz-se necessário um breve estudo sobre as três principais legislações que abordam a temática, são elas a Lei Federal 12.737/2012, Lei Federal 12.735/2012 e Lei Federal 12.965/2014.

Porém, essas não são as únicas leis existentes que abordam o tema. Antes das leis acima mencionadas, houve a edição da Lei 9.983/2000, que acrescentou ao Código Penal os arts. 313-A e 313-B, que tratam dos crimes previdenciários cometidos através de computador.

No ordenamento jurídico também há a Lei 9.609/98 que dispõe sobre a proteção intelectual de programa de computador, se tratando de um dispositivo que visa combater a pirataria de softwares. Os arts. 241-A e 241-B do Estatuto da Criança e do Adolescente tratam de condutas envolvendo a obtenção e ou divulgação, através de sistema de informática ou telemáticos, de material pornográfico que contenham crianças e adolescentes.

A legislação brasileira específica sobre crimes informáticos ainda é bastante falha, necessitando de vários ajustes técnicos para que alcance uma satisfatória eficácia.

### 3.4.1 Lei Federal 12.737/2012: Lei Carolina Dieckmann

No Brasil, há um grande atraso quanto à criação de legislação que trate dessa espécie de crime. A mídia, assim como os legisladores, só deu maior importância ao tema quando, em 2012, *crackers* invadiram o computador da atriz brasileira Carolina Dieckmann e divulgaram suas fotos íntimas.

Antes de 2012 havia uma total ausência de legislação específica referente aos crimes cibernéticos, o que tornava ainda mais difícil a apuração desses crimes, uma vez que a legislação existente tipificava os crimes de forma geral.

A Lei 12.737/2012, conhecida como “Lei Carolina Dieckmann” trouxe importantes alterações ao Código Penal Brasileiro. Essa lei surgiu do projeto de Lei n. 2.793/2011, autoria do deputado Paulo Teixeira (PT- SP), e foi sancionada em 2 de dezembro de 2012 pela presidente Dilma Rousseff. A Lei 12.737/2012 acrescentou os arts. 154-A e 154-B e alterou os arts. 266 e 298, todos do Código Penal.

O art. 154-A tipificou o crime de invasão de dispositivo informático, fixando uma pena de detenção de 3 (três) meses a 1(um) ano e multa para quem 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. (BRASIL, 2012)

O art. 154-A do Código Penal visa proteger a liberdade individual, o direito a intimidade e a segurança da informação. Trata-se de um crime comum e formal, visto que pode ser praticado por qualquer pessoa e não depende de um resultado material, a mera invasão já tipifica o crime.

A forma qualificada do crime está prevista no seu § 3º e faz referência a violação de informações sigilosas, fixando uma pena de reclusão de 6 (seis) meses a 2 (dois) anos e multa, se a conduta não constituir crime mais grave. (BRASIL, 2012)

O art. 154-B estabeleceu como tipo de ação penal que julgará esse crime, a ação penal pública condicionada à representação, exceto nos casos do crime ser praticado em face da Administração Pública Direta ou Indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou em face de empresas concessionárias de serviços públicos, que será através de ação pública incondicionada.

A Lei 12.737/2012 alterou ainda o art. 266 do Código Penal. A antiga redação do art. 266 fazia referência apenas à interrupção ou perturbação de serviço telegráfico ou telefônico, com o advento da lei, acrescenta-se ao tipo penal a interrupção ou perturbação de serviço informático, telemático ou de informação de utilidade pública.

Esse tipo penal busca preservar o fornecimento dos serviços telegráficos, telefônicos, informáticos, telemáticos e de informação de utilidade pública de uma forma geral, em relação à coletividade. A pena é aplicada em dobro se o crime for cometido em ocasião de calamidade pública.

Esse crime está previsto no Título VIII do Código Penal Brasileiro, tratando-se de um crime contra a incolumidade pública. É crime que atinge um número indeterminado de pessoas.

Os arts. 297 e 298 do Código Penal tratam do crime de falsificação de documento. Se o documento for público, a pena fixada é de um a seis anos e multa (art.297), quando o documento falsificado for particular, a pena fixada é de reclusão de um a três anos e multa (art.298). A Lei 12.737/2012 acrescentou a esse último dispositivo penal o seu § 1º, equiparando o cartão de crédito e débito a um documento particular.

### 3.4.2 Lei Federal 12.735/ 2012: Lei Azeredo

Antes da criação da Lei 12.737/2012, foi aprovada com reservas a lei 12.735/2012, conhecida por Lei Azeredo, pois Eduardo Azeredo foi o seu relator no congresso[5], promovendo alterações no Código Penal, Código Penal Militar e na Lei 7.716/1989.

O projeto original da lei foi proposto em 1999, pelo deputado Luiz Piauhylin. Dos 23 artigos constantes no projeto 84/99, apenas quatro foram sancionados pela presidente, sendo que apenas dois possuem conteúdo penal. Foram retirados pontos considerados polêmicos

O art. 1º afirma que esta lei foi criada para alterar o Código Penal, o Código Penal Militar e a lei 7.716/2012, tipificando condutas realizadas através do uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares.

Embora esse artigo tenha tal redação, a Lei 12.735/2012 não criou nenhum novo tipo penal. Os arts. 2º e 3º da referida Lei foram vetados e o art. 4º prevê o seguinte:

> Art. 4º. Os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado. (BRASIL, 2012)

Em seu artigo 5º, a Lei 12.735/2012 modificou o inciso II do § 3º do art. 20 da Lei 7.776/1989, que define os crimes resultantes de preconceito de raça ou de cor. O art. 5º da Lei 12. 735/2012 prevê a possibilidade de o juiz determinar a cessação das transmissões radiofônicas, televisivas, eletrônicas ou da publicação por qualquer meio da prática, indução ou incitação à discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional.

[5] A Lei 12.735/2012 adveio do projeto de Lei n. 84/99 (89/2003), desta forma, nota-se embora não se desse tanta importância ao tema, há algum tempo já havia uma discussão sobre a necessidade de uma lei específica para os crimes cibernéticos.

### 3.4.3 Lei 12.965/2014: Marco Civil da Internet

A Lei 12.965/2014, conhecida como Marco Civil da internet Brasileira foi aprovada, e entrou em vigor em 2014, e é a lei que regula o uso da internet no país. Essa lei apresenta definições usadas no direito informático, prevê princípios, garantias, direito e deveres para as pessoas que adentram no mundo virtual.

A lei também determina diretrizes para atuação dos entes responsáveis pela matéria. Os princípios da disciplina do uso da internet estão firmados no art 3º da referida lei, e são eles:

> 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. (BRASIL, 2014)

As alterações constantes na sociedade e na tecnologia são de alta complexidade e multidisciplinar. Para se entender o direito penal informático é necessário que seja analisado os princípios, as garantias, os direitos e os deveres que abrangem todo o tema. Desta forma dispõe Sydow (2015, p. 274):

> [...] não há como se compreender a realidade do direito penal informático sem antes contar com algum normativo diretriz, verdadeiramente inaugurador desse ramo do Direito, que possua funções como gerador de nomenclaturas, demonstrador de papéis dos atores que frequentam a rede, escultor de princípios e garantias e iniciador de debates sobre o tema de modo amplo.

A Lei 12.965/2014, juntamente com as anteriormente estudadas, são complementares nas questões relativas à repressão dos crimes informáticos, por isso, se faz importante a análise de alguns pontos acerca do conteúdo desta primeira.

O art. 13 da Lei 12.965/2014 prevê o dever do administrador do sistema provedor de conexão à internet de manter os registros[6] de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1(um) ano, nos termos do regulamento.

Antes do advento dessa lei não havia qualquer regra no sentido de obrigar os administradores a guardarem esses registros, que são indispensáveis para apuração e atribuição da autoria dos crimes informáticos. Os provedores de internet só são obrigados a fornecer os dados registrados dos usuários através de uma ordem judicial.

O inciso III, do art 7º da referida Lei, dispõe que é assegurado ao usuário da internet a inviolabilidade e o sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial. Desta forma, é totalmente proibido, na esfera criminal, o grampo informático.

Não há o que se falar em responsabilidade civil dos provedores, segundo o art. 18, em decorrência de danos produzidos por conteúdo gerado por terceiro, exceto, como dispõe o art. 19, se o juiz emitir uma ordem, e o provedor não tomar as providências necessárias para tornar indisponível o conteúdo considerado infringente. (BRASIL, 2014)

## 3.5 LEGISLAÇÕES INFORMÁTICAS EM OUTROS PAÍSES

Soberania é a entidade que não possui nenhum superior externamente e nem igual internamente. Na comunidade internacional, temos uma relação horizontal entre os países, ou seja, uma relação de igualdade, porém, cada país tem sua soberania e autonomia interna, firmando suas próprias leis.

Alguns países são bem avançados no que se diz respeito a legislações sobre crimes informáticos. O direito comparado nos permite adentrar na realidade das

[6] Quando um usuário se conecta a internet é gerado um endereço IP (*internet protocol*), esse IP é um conjunto de protocolos, ou seja, de padrões de comunicação. Com base no número IP fornecido através de ordem judicial, pode-se descobrir qual o provedor de acesso responsável e requerer os dados cadastrais do usuário que se conectou a internet com aquele IP, para então se descobrir a suposta autoria do delito.

legislações dos outros países, para que então seja analisado o que se tem de relevante.

Faz-se necessário, então, uma breve análise sobre aspectos legislativos relacionados aos crimes informáticos em alguns países.

### 3.5.1 Estados Unidos

Foi um dos países pioneiros a legislar sobre crimes informáticos, tanto no âmbito estadual, como no federal. Uma das primeiras leis foi a federal Computer System Protection Act - Lei de Proteção aos Sistemas Computacionais, de 1981, logo em seguida foi criada a *Electronic Funds Transfer Act* - Lei de Transferência Eletrônica de Fundos, de 1982 e a principal lei sobre os delitos virtuais do país foi a Computer Fraud and Act - Lei de Fraude e Abuso Computacional, de 1986.

Houve alterações nessas legislações e atualmente existem no país outras leis fragmentadas e iniciativas que tratam do assunto.

Nos Estados Unidos também há uma lei chamada de *A Children's Online Privacy Protection Act* – Lei de Proteção da Privacidade das Crianças On-line, a finalidade da lei é regular as informações pessoais que são fornecidas pelos menores de 13 anos aos sites comerciais na internet. Uma das regras impostas aos operadores dos sites é que é necessário obter a autorização dos pais das crianças menores de 13 anos para coleta, uso e divulgações de dados pessoais.

### 3.5.2 Itália

No início dos anos 90 o direito italiano sofreu alterações estruturais em sua legislação penal, sendo editado o Decreto Legislativo n.51, de 29 de dezembro de 1992, e Lei n. 547, de 23 de dezembro de 1993, onde foram inseridos alguns crimes cibernéticos.

Na Itália há um título no Código Penal que tutela a inviolabilidade de domicílio, e nesse título há o art.615 que trata de acesso ilegal a sistemas informáticos,

posteriormente, no art. 617 é tratada a interceptação e interrupção de comunicações informáticas.

O Código Penal Italiano também criminaliza a danificação do funcionamento de sistemas informáticos com intuito de obter ilegalmente informações, dados e lucros.

### 3.5.3 França

Na França há uma Lei chamada Hadopi que visa punir o compartilhamento ilegal na rede de arquivos protegidos por direitos autorais. Se comprovada a violação da lei pelo usuário, ele recebe uma advertência por e-mail, se uma segunda violação vier a ocorrer, o usuário receberá uma nova advertência por e-mail e uma carta explicando as possíveis consequências de uma próxima violação.

A lei previa a possível suspensão da internet do violador reincidente, porém, essa disposição foi revogada no ano de 2013. Da aprovação da lei, até a revogação do dispositivo que previa a suspensão da internet, tem-se relato de apenas um caso de usuário que teve sua internet suspensa.

A França foi um dos países pioneiros em desenvolver legislação específica para proteger a propriedade intelectual.

### 3.5.4 Espanha

Na Espanha vigora uma lei de regulamentação da internet, conhecida como Sinde-Wert, criada com o intuito de fortalecer a vigilância dos conteúdos dispostos na rede, para fins de diminuir a pirataria.

A criação dessa lei tem um viés econômico. Diante da crise financeira em que passava o país, a lei foi criada dentro de um plano econômico, para aumento do controle das informações que circulam na web e dificultam a exploração econômica da propriedade imaterial.

O Código Penal da Espanha é do ano de 1995, e ao passar do tempo já foi alterado diversas vezes, prevendo, hoje em dia, dispositivos relativos aos crimes informáticos.

# 4 DESAFIOS ENFRENTADOS NO COMBATE A CRIMINALIDADE VIRTUAL

A criação de leis técnicas e específicas é imprescindível para o combate dos crimes informáticos. Embora já tenha havida a elaboração de uma lei específica no ordenamento jurídico brasileiro, esta se mostrou falha. Na verdade, as leis aqui já estudadas tipificam apenas uma pequena parcela das possibilidades de cometimento de delito virtual e carecem de termos técnicos adequados.

A tecnologia avança em uma velocidade enorme, diariamente novas formas de se cometer um delito informático surgem e a legislação não consegue acompanhar toda essa evolução.

A preparação técnica dos órgãos investigativos também possui grande importância na apuração do delito e imputação da autoria. No Brasil, um país extenso e populoso, onde os índices da criminalidade virtual só crescem, se tem um despreparo enorme das autoridades investigativas, e algumas poucas unidades de delegacias especializadas.

A insuficiência das leis específicas, as práticas investigativas antigas e ineficientes, e o suposto anonimato que a rede de internet oferece ao sujeito, contribuem para que ultimamente os números referentes às práticas delitivas na internet só tenham aumentado.

Para uma eficaz repressão dos crimes informáticos é necessária uma constante atualização de todos os setores envolvidos, desde uma legislação moderna, a uma equipe investigativa preparada e conhecedora das tecnologias utilizadas pelos *crackers.*

## 4.1 CRÍTICAS A LEGISLAÇÃO BRASILEIRA INFORMÁTICA

A Lei 12.737/2012 é a principal lei brasileira quando se trata de crimes informáticos. Antes de a referida lei ser aprovada, já havia há algum tempo um debate sobre a necessidade de aprovação de alguma lei que regulamentasse esses crimes.

Quando a atriz global Carolina Dieckmann teve seu computador invadido e fotos íntimas divulgadas, deu-se repercussão ao fato e a população começou a pressionar a aprovação de uma lei tratando desses crimes.

Devido a grande pressão popular, a Lei 12.737/2012 teve a sua tramitação acelerada e dessa forma percebe-se algumas falhas, como a ausência de um glossário constando a definição de termos técnicos presentes, o que pode vir a dificultar a sua aplicação.

Em uma análise dos artigos da lei 12. 737/2012 é necessário se fazer alguns questionamentos. O caput do art. 154-A, que trata da invasão de dispositivos informáticos, dispõe o seguinte (BRASIL, 2012):

> 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. (destaque nosso)

A expressão “invadir” repassa uma ideia de força e violência, ou seja, nem toda aproximação que o agente tiver com o sistema informático será considerado invasão, mas, muitas vezes, um mero acesso. Dessa forma, se for levar em consideração o termo utilizado, só seria considerado crime se a invasão ao dispositivo fosse feita através do uso da força. Por pressupor uma ação de agressividade, o termo “invasão” não é o tecnicamente mais correto.

Outra crítica que é feita a Lei é em relação ao fato de que quando estabelece que a invasão tenha que se dar mediante violação indevida de mecanismo de segurança, fica-se a indagação de quais são os mecanismos que se enquadram como seguros e como seria essa proteção.

Quando não há um mecanismo de segurança, a conduta é atípica. Segundo Jesus e Milagre (2016), há uma corrente que defende que se houver uma segurança, mas esta for ineficaz, também não haverá tipicidade, uma vez que a ineficiência se equipararia a uma ausência. Em sentido contrário, há também uma corrente que defende que havendo um mecanismo de segurança, independente de este ser eficaz ou não, haveria a tipicidade da conduta.

Esse mecanismo de segurança deve ser considerado um bloqueio que existe para que o invasor tenha dificuldade de acessar os dados contidos no dispositivo informático alheio.

Quanto as penas cominadas, têm pouco efeito intimidador, pois são pequenas e aplicadas pelos juizados especiais criminais.

Em relação à Lei 12.735/2012, Lei Azeredo, quando estabeleceu em seu art. 4º que os órgãos da polícia judiciária estruturarão setores e equipes especializadas no combate a crimes informáticos, fez uma preposição, não obrigando os entes federados a cumpri-lo. O decreto regulamentar previsto nesta lei nunca chegou a ser editado. (BRASIL, 2012)

## 4.2 DIFICULDADE DE IDENTIFICAÇÃO DO AUTOR DE UM CRIME INFORMÁTICO

Os sujeitos que praticam os crimes informáticos não possuem um padrão ou perfil, podendo o crime ser praticado até por um agente com pouca habilidade. Porém, o que se percebe é que o que prevalece são sujeitos com um razoável ou amplo conhecimento informático, principalmente aqueles que praticam delitos que envolve intrusão e programação.

Para se propor uma ação penal, necessita-se de no mínimo provas da materialidade e indícios de autoria. Dessa forma, um dos maiores obstáculos para punição adequada do autor do delito informático é justamente a sua identificação, principalmente, devido a sua ausência física.

Uma das provas mais relevantes para se chegar ao autor do delito é o endereço IP, mas, embora seja importante, não é suficiente. O endereço IP é a identificação da conexão do usuário com a internet, e quando se descobre o endereço IP, pode-se descobrir de qual máquina surgiu a prática delitiva, porém, não significa que necessariamente irá se identificar o autor.

Os criminosos, muitas vezes, se utilizam de métodos para burlar esse endereço IP. A utilização de *proxies* é um dos métodos utilizados maliciosamente pelos criminosos virtuais e, se trata de serviços utilizados com a finalidade de ocultar o IP, fazendo com que a autoridades investigativas tenha dificuldade de se chegar a quem praticou a conduta.

Outro método utilizado pelos autores dos delitos informáticos é o de realizar suas ações através de *lan houses*. As *lan houses* são estabelecimentos comerciais que permitem que seus clientes tenham acesso a computadores ligados a internet.

Geralmente, essas *lan houses* não fazem registros e não possuem um controle de quais os clientes tem acesso a seus computadores, desta forma, quando a polícia consegue identificar o IP do qual decorreu a conduta delituosa e esse IP decorre desses estabelecimentos, terá dificuldade de identificar qual usuário utilizou a máquina e praticou a conduta.

Os crackers também se utilizam de *wifi*s (redes de internet sem fio) livres, ou seja, desprotegidos de senhas, que estão presentes nas faculdades, nos shoppings e em outros locais públicos, tornando, também, difícil a identificação do autor do delito que for cometido através dessas conexões.

Os indícios desse tipo de crime possuem algumas peculiaridades. Normalmente são bem instáveis, podendo ser apagadores, alterados e até perdidos.

### 4.2.1 Deep Web

A internet que a maioria das pessoas tem acesso é chamada de *surface web*, é a que está disponível para o público em geral. É indexada por buscadores convencionais, como o *google* e *yahoo*.

A *deep web*, sigla inglesa que significa internet profunda, é considerada uma zona invisível da internet que comporta sites que não são passíveis de serem encontrados através dos mecanismos convencionais de busca. Dessa forma, ao usuário que tem acesso a *Deep Web* é proporcionado uma suposta privacidade e anonimato.

O conteúdo disponível na *deep web* não é de fácil acesso para qualquer internauta e os donos dos sites mantém um anonimato. Para ter acesso a *deep web* é necessário utilizar programas específicos e códigos secretos.

A *deep web* é utilizada para as mais diversas finalidades, muitas pessoas e instituições decidem usá-la devido a privacidade, utilizando-a para hospedar arquivos sigilosos.

Porém, a *deep web* também é um território fértil para que os pedófilos, assassinos, vendedores de drogas e hackers propaguem seus crimes. O território da *deep web* dominado pelos criminosos é conhecido como *Dark Web* (internet sombria).

Na *dark web* se encontra sites vendendo drogas ilícitas, anúncios de assassinos de aluguel, vídeos de pedofilia, fóruns de tortura, contato entre terroristas, propagação de vírus, fraudes de sistemas bancários, entre outras práticas criminosas.

O navegador TOR (*The Onion Router*) é o mais utilizado para acessar a *deep web*. Este navegador tem a função de dificultar e embaralhar a identidade dos computadores quando estão navegando na *deep web*.

Segundo Franco e Magalhães (2015), os maiores defensores do TOR são os grupos que defendem a liberdade de expressão, devido à possibilidade de se comunicar anonimamente, sem interceptações, beneficiando os que lutam contra regimes ditatoriais.

Embora não seja impossível, a identificação de um autor de delito informático que utilizou a *deep web* para praticá-lo é bem difícil, uma vez que os navegadores utilizados tem a função de dificultar o rastreamento do IP de onde a conduta foi praticada.

## 4.3 COMPETÊNCIA PARA JULGAMENTO

Para Capez (2015), jurisdição é uma função que o estado exerce com exclusividade, através do Poder Judiciário, de forma a aplicar normas jurídicas a um caso concreto. É o poder de solucionar um caso concreto.

Competência é, então, a medida da jurisdição. É a atribuição que o magistrado tem de exercer a jurisdição, resolvendo o conflito de um caso.

A doutrina tradicional distribui a competência em razão da matéria, em razão da pessoa e em razão do local. A competência em matéria de processo penal está disciplinada nos arts. 69 e seguintes do Código de Processo Penal.

Para se fixar a competência em razão da matéria, é necessário analisar se o julgamento compete à justiça comum, que engloba a justiça estadual e a federal, ou especializada, que engloba as justiças militar, eleitoral e trabalhista.

Os arts. 106 a 110 da CRFB/88 fixam a competência da Justiça Federal. No caso de não se enquadrar em nenhuma das causas competentes da Justiça Federal, ou das justiças especializadas, a competência residual é da Justiça Estadual. (BRASIL, 1988)

Em julgamento do Habeas Corpus 121.23 - Distrito Federal, foi decida a competência da Justiça Estadual para processar e julgar o crime de incitação a discriminação cometido por meio da internet. Muito embora o impetrante tenha usado o argumento que a competência seria da Justiça Federal, decorrente do art.109, V da CRFB/88, alegando que se tratava de um crime previsto em tratado ou convenção internacional, que, quando iniciada a execução no País, o resultado possa ter ocorrido no estrangeiro, no caso em questão, as ofensas foram dirigidas a uma pessoa determinada, não ultrapassando as fronteiras nacionais. Dessa forma decidiu a primeira turma do STF (2014) no julgamento do referido HC:

> EMENTA: HABEAS CORPUS. ALEGAÇÃO DE VÍCIO PROCIDIMENTAL. COMPETÊNCIA PARA PROCESSAR E JULGAR CRIME DE INCITAÇÃO À DISCRIMINAÇÃO COMETIDO POR MEIO DA INTERNET. OFENSAS DIRIGIDAS A PESSOAS DETERMINADAS. . Não se declara a nulidade do ato processual que não houver influído na decisão da causa. 2. É da Justiça estadual a competência para processar e julgar o crime de incitação à discriminação racial por meio da internet cometido contra pessoas determinadas e cujo resultado não ultrapassou as fronteiras territoriais brasileiras. 3. Ordem denegada. (STF - HC: 121283 DF, Relator: Min. ROBERTO BARROSO, Data de Julgamento: 29/04/2014, Primeira Turma, Data de Publicação: DJe-091 DIVULG 13-05-2014 PUBLIC 14-05-2014).

Quanto à competência em razão do lugar, essa possui algumas controvérsias quando se trata de crimes informáticos. Em relação ao lugar do crime, o art. 6º do Código Penal estabelece que o lugar em que o crime foi praticado é aquele em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado. Desta forma, em um delito de invasão de dispositivo, o juízo competente para julgar seria o do lugar onde estava o dispositivo invadido.

Porém, quando se trata de crime contra honra cometido via internet, há divergências jurisprudenciais sobre qual seria o juízo competente para julgar o caso. Em um caso de ofensa feita pela rede social *Facebook,* a segunda Câmara Criminal

do Tribunal de Justiça do Paraná (2015) entendeu que a competência para apreciar a matéria era do local onde a vítima e terceiros tomaram conhecimento dos fatos ofensivos:

> DECISÃO: ACORDAM os Magistrados integrantes da Segunda Câmara Criminal do Egrégio Tribunal de Justiça do Paraná, à unanimidade, em conhecer parcialmente do recurso, e, nessa parte, dar-lhe provimento. EMENTA: RECURSO EM SENTIDO ESTRITO. CRIMES CONTRA A HONRA PRATICADOS PELA INTERNET. ANÁLISE SOBRE A COMPETÊNCIA PARA APRECIAR A MATÉRIA. APLICAÇÃO DA REGRA DO ART. 70 DO CÓDIGO DE PROCESSO PENAL. TEORIA DO RESULTADO. LOCAL ONDE A VÍTIMA E TERCEIROS TOMARAM CONHECIMENTO DOS FATOS, EM TESE, OFENSIVOS, AINDA QUE AS PUBLICAÇÕES NO FACEBOOK TENHAM OCORRIDO EM LOCAL DIVERSO. RECURSO PARCIALMENTE CONHECIDO, E, NESSA PARTE, PROVIDO. **Aplica-se a regra do art. 70 do Código de Processo Penal (lugar da consumação) nos crimes contra a honra, cometidos pela Internet (na rede social Facebook), tendo em vista que o conteúdo, em tese, ofensivo, pode ser publicado de qualquer lugar, contudo causam ofensas à honra da vítima na comunidade em que ela vive**. I.
> (TJPR - 2ª C.Criminal - RSE - 1397104-5 - Região Metropolitana de Maringá - Foro Central de Maringá - Rel.: José Mauricio Pinto de Almeida - Unânime - - J. 08.10.2015). (destaque nosso).

Em sentido contrário, o Tribunal Regional Eleitoral de São Paulo (2013), em um caso de crimes contra honra praticados via rede social *Facebook,* durante campanha eleitoral, entendeu ser a competência do local de onde partiu a publicação das ofensas e não do local onde residiam os eleitores a quem se pretendia divulgar as ofensas contra a honra da vítima:

> CONFLITO NEGATIVO DE COMPETÊNCIA. INQUÉRITO POLICIAL. CRIMES CONTRA A HONRA COM FINALIDADE ELEITORAL PRATICADOS ATRAVÉS DA INTERNET (FACEBOOK). CRITÉRIO DO LOCAL DE ONDE PARTIU O ATO DE PUBLICAÇÃO. PRECEDENTES STJ [CC 200901364221, TERCEIRA SEÇÃO, DJE DE 25/05/2010; CC 201202148611, TERCEIRA SEÇÃO, DJE DE 12/12/2012). AUTORES DIVERSOS. INEXISTÊNCIA DE ELEMENTOS QUE INDIQUEM CONEXÃO. DESMEMBRAMENTO DO INQUÉRITO POLICIAL MANTIDO. CONFLITO JULGADO IMPROCEDENTE. 1. TRATA-SE DE CONFLITO NEGATIVO DE COMPETÊNCIA INSTAURADO PELO JUÍZO DA 3ª ZONA ELEITORAL (SÃO PAULO) EM FACE DO JUÍZO DA 217ª (MAUÁ) EM RAZÃO DE CRIMES CONTRA A HONRA PRATICADOS, DURANTE A CAMPANHA ELEITORAL, POR MEIO DE PERFIL FALSO DA REDE SOCIAL FACEBOOK 3. HOUVE A IDENTIFICAÇÃO DOS PRETENSOS AUTORES, ATRAVÉS DOS NÚMEROS DE SEUS PROTOCOLOS DE INTERNET (IP'S). 4. **JUÍZO SUSCITANTE QUE CONSIDERA COMO LOCAL DO RESULTADO DO CRIME AQUELE ONDE RESIDEM OS ELEITORES A QUEM SE PRETENDIA DIVULGAR AS OFENSAS CONTRA A HONRA DA VÍTIMA. PRECEDENTES DO SUPERIOR TRIBUNAL DE JUSTIÇA QUE CONSIDERAM COMO TAL O LOCAL DE ONDE PARTIU A PUBLICAÇÃO DAS OFENSAS.** 5. NECESSIDADE DE DESMEMBRAMENTO DO INQUÉRITO POLICIAL. 6. CONFLITO JULGADO IMPROCEDENTE. (TRE-SP - CJ: 14819 SP, Relator: LUIZ

> GUILHERME DA COSTA WAGNER JUNIOR, Data de Julgamento: 12/11/2013, Data de Publicação: DJESP - Diário da Justiça Eletrônico do TRE-SP, Data 19/11/2013). (destaque nosso).

Neste mesmo sentido entendeu o Superior Tribunal de Justiça (2013):

> PENAL. CONFLITO DE COMPETÊNCIA. CRIME DE RACISMO PRATICADO POR INTERMÉDIO DE MENSAGENS TROCADAS EM REDE SOCIAL DA INTERNET. USUÁRIOS DOMICILIADOS EM LOCALIDADES DISTINTAS. INVESTIGAÇÃO DESMEMBRADA. CONEXÃO INSTRUMENTAL. EXISTÊNCIA. COMPETÊNCIA FIRMADA PELA PREVENÇÃO EM FAVOR DO JUÍZO ONDE AS INVESTIGAÇÕES TIVERAM INÍCIO. 1. **A competência para processar e julgar o crime de racismo praticado na rede mundial de computadores estabelece-se pelo local de onde partiram as manifestações tidas por racistas**. Precedente da Terceira Seção. 2. No caso, o procedimento criminal (quebra de sigilo telemático) teve início na Seção Judiciária de São Paulo e culminou na identificação de alguns usuários que, embora domiciliados em localidades distintas, trocavam mensagens em comunidades virtuais específicas, supostamente racistas. O feito foi desmembrado em outros treze procedimentos, distribuídos a outras seções judiciárias, sob o fundamento de que cada manifestação constituía crime autônomo. 3. Não obstante cada mensagem em si configure crime único, há conexão probatória entre as condutas sob apuração, pois a circunstância em que os crimes foram praticados - troca de mensagens em comunidade virtual - implica o estabelecimento de uma relação de confiança, mesmo que precária, cujo viés pode facilitar a identificação da autoria. 4. Caracterizada a conexão instrumental, firma-se a competência pela prevenção, no caso, em favor do Juízo Federal de São Paulo - SJ/SP,onde as investigações tiveram início. Cabendo a este comunicar o resultado do julgamento aos demais juízes federais para onde os feitos desmembrados foram remetidos, a fim de que restituam os autos, ressalvada a existência de eventual sentença proferida (art. 82 do CPP). 5. Conflito conhecido para declarar a competência do Juízo Federal da 9ª Vara Criminal da Seção Judiciária de São Paulo, o suscitante. (STJ - CC: 116926 SP 2011/0091691-2, Relator: Ministro SEBASTIÃO REIS JÚNIOR, Data de Julgamento: 04/02/2013, S3 - TERCEIRA SEÇÃO, Data de Publicação: DJe 15/02/2013) (destaque nosso).

Com o advento de toda a tecnologia e a possibilidade de se conectar a uma rede mundial de internet, as pessoas tem a possibilidade de estarem virtualmente em vários locais ao mesmo tempo através dessa rede. Toda essa noção de ciberespaço modificou a concepção clássica de território, uma vez que as informações contidas na internet desconhecem os limites fronteiriços, suscitando divergências de entendimentos como os acima mencionados e trazendo novos desafios para os operadores do direito.

O Brasil adota a teoria da territorialidade, ou seja, irá se aplicar a lei brasileira nos casos ocorridos no país. O que ocorrer além dos limites do território nacional resulta em uma revisão dos acordos feitos entre o Brasil e os outros países.

Se um crime é cometido no estrangeiro, não se aplicará a norma brasileira. Porém, se o crime informático cometido no exterior for praticado por um brasileiro, e a vítima estiver no Brasil, a competência será brasileira, desde que o agente que cometeu o delito adentre no território nacional e a conduta por ele praticada seja considerada crime em ambos os países.

## 4.4 DESAFIOS PRESENTES NAS INVESTIGAÇÕES DOS CRIMES INFORMÁTICOS

A existência de leis específicas tipificando de forma adequada os crimes cibernéticos é essencial, porém, não é o único aspecto necessário para que se tenha uma efetiva punição dos autores desses delitos.

Para que se tenham resultados positivos na persecução penal é necessária uma estrutura investigativa que contenha profissionais preparados e capacitados para enfrentar os desafios que esses crimes tecnológicos representam.

Os órgãos responsáveis pelas investigações na persecução penal desses crimes no Brasil é a Polícia Civil em âmbito estadual, e a Polícia Federal em âmbito federal.

Essas equipes investigativas precisam ter conhecimentos técnicos sobre esse mundo digital para que possam realizar procedimentos efetivos. Caso contrário, dificilmente a persecução penal logrará êxito e o autor do delito será reprimido pela conduta criminosa.

De acordo com Cerqueiro e Rocha (2015), o procedimento utilizado na persecução penal desses crimes informáticos costuma ser o mesmo utilizado na persecução dos crimes comuns, porém, a mudança consiste em uma parcela da investigação que exige amplo conhecimento de internet, engenharia de software, eletrônica, redes de comunicação e computação.

Um dos desafios da repressão a esses crimes consiste justamente nessa necessidade de uma equipe tecnicamente preparada. É necessário que as autoridades responsáveis pelas investigações tenham acesso a uma equipe especializada, que possuam equipamentos tecnológicos avançados.

A tecnologia avança a cada dia que passa e junto com esse avanço, os criminosos estão cada vez mais especializados, desenvolvendo novas técnicas para praticarem seus crimes, desta forma, a capacitação e treinamento dos agentes investigativos tem que ser permanente para que haja uma paridade de conhecimentos técnicos entre estes e os autores dos delitos.

Segundo o delegado da Polícia Civil do Rio Grande do Sul, Wendt (2015), apenas 13 Estados brasileiros possuem órgãos policiais especializados no combate a crimes informáticos, que são estes: Bahia, Espírito Santo, Maranhão, Mato Grosso, Minhas Gerais, Pará, Paraná, Pernambuco, Piauí, Rio de Janeiro, São Paulo, Sergipe e Tocantins.

Ou seja, muitos Estados brasileiros enfrentam os crimes informáticos sem sequer possuir uma polícia judiciária especializada e tecnicamente preparada para isto.

A prova eletrônica é também uma das maiores barreiras na investigação a esses crimes diante da dificuldade de obtê-las. Essas provas virtuais, para que possam ser consideradas confiáveis e aceitas judicialmente, precisam passar por perícias técnicas e a demora em obtê-las para que sejam periciadas acabam tornando-as, muitas vezes, obsoletas, diante de suas características peculiares, como a facilidade em ser modificada e até apagada.

Para que se tenha acesso aos elementos que são essenciais para se chegar à autoria do delito, é necessário que o provedor de acesso, de serviço ou de internet os disponibilizem, porém, as empresas não aceitam a requisição de informações feita apenas pela polícia.

Após a entrada em vigor do Marco Civil da Internet, que estabelece nos incisos II e III, do art. 7º, que ao usuário é assegurado o direito de inviolabilidade e sigilo do fluxo de suas comunicações pela internet e de suas comunicações privadas armazenadas, salvo por ordem judicial, as empresas cedem os dados apenas por intermédio de uma ordem judicial, dessa forma, muitas vezes, para a polícia obter as informações necessárias leva algum tempo, retardando as investigações.

Wendt (2013) informa que não raramente, mesmo após a ordem judicial, as empresas retardam o fornecimento das informações até por mais de sessenta dias. A polícia, então, tem que solicitar uma requisição de cumprimento da ordem judicial sob pena de incidirem em crime de desobediência.

Outro desafio está na questão da transnacionalidade desses crimes. Com a globalização e o advento da rede mundial de internet, os criminosos podem fazer de vítimas pessoas de qualquer lugar do globo terrestre, assim como praticar esses delitos através de sistemas que estão hospedados em outros países.

Dessa forma, para que as investigações policiais logrem êxito, é necessária uma cooperação internacional. Conseguir as informações desses provedores de serviços e internet que estão localizados fora do país não é uma missão fácil, uma vez que não estão subordinados às leis brasileiras.

De acordo com Jesus e Milagre (2016), para que se tenha acesso aos dados dos usuários que se utilizaram desses serviços fornecidos por provedores localizados no exterior, normalmente, faz-se meio da carta rogatória, tratando-se de um meio demorado que atrasa as investigações.

Existe um Departamento de Recuperação de Ativos e Cooperação Internacional (DRCI), departamento do Ministério da Justiça, que faz o intermédio entre o órgão judicial brasileiro e o do outro país envolvido. Porém, conseguir informações através dessa intervenção também é um método moroso e pode levar a impunidade dos criminosos, uma vez que, com a demora, os indícios podem ser excluídos e as provas destruídas. Jesus e Milagre (2016, p. 180) discorrem sobre o desafio em que consiste a cooperação internacional:

> Deste modo, a cooperação internacional ainda é um desafio para a eficácia do combate ao crime eletrônico. os provedores, como “portas” de entrada e saída da internet, são os primeiros a ter a possibilidade de apurar dados de usuários que sejam seus clientes. não bastasse, no que tange a provimento de aplicações e serviços, é notório que os serviços mais utilizados no Brasil pertencem a grandes provedores de conteúdo com sede no exterior (alguns, sequer com filiais físicas no Brasil). Neste contexto, em defesas envolvendo processos de quebras de sigilo de seus usuários, no Brasil, quase sempre argumentam que não estão sujeitos à jurisdição brasileira, apresentando inclusive a “lei do país sede”. Muito embora tal argumentação seja desconsiderada pelo judiciário na grande maioria dos casos, ainda preocupa a questão do provedor no exterior que não tem filial no Brasil. nestes casos, é importante que a cooperação internacional efetivamente se desenvolva.

Já existem convenções e tratados feitos entre países do mundo inteiro a respeito do combate a esses crimes, porém, a cooperação internacional ainda é fraca, e os criminosos tiram vantagens desse fato atacando países que tornam o rastreamento dos crimes mais difícil. Cada país tem suas próprias regras sobre como cooperar.

Entre os desafios enfrentados pela polícia, está a dificuldade de interceptação dos dados informáticos. A interceptação telemática é uma forma de se adquirir provas na persecução penal dos crimes informáticos, regida pela Lei 9.296/96. Ao contrário da interceptação telefônica que é amplamente utilizada e produz resultados positivos, a interceptação telemática tem um processo técnico mais complexo. Cerqueira e Rocha (2013, p. 152) explicam como funciona essa espécie de interceptação:

> O processo técnico para se realizar uma interceptação telemática é complexo e há situações para as quais ainda não existe solução na tecnologia. Dependendo da provedora de acesso, pode ser possível executar a interceptação do sinal de comunicação remotamente, isto é, em uma dependência policial. Pode haver a necessidade de instalação de computador dedicado e especialmente configurado nas dependências da empresa provedora, com posterior busca e análise dos arquivos gravados referentes ao tráfego. E há casos em que simplesmente não é possível realizar a interceptação por absoluta falta de viabilidade técnica.

Não é admitida a interceptação telemática quando a prova a ser colhida puder ser obtida através de outro meio, ou quando ao fato que está sendo investigado para uma futura punição seja cominada uma pena de detenção.

A tecnologia se reinventa a cada momento, fazendo surgir serviços inovadores. O *cloud computing* é uma espécie de serviço que permite que seus usuários tenham acesso a arquivos, programas e demais funcionalidades de um computador pessoal, através da internet, utilizados aplicativos como o *Dropbox*, *Google Drive*, *ICloud*, entre outros.

O acesso a esses arquivos e programas pode se dar de qualquer lugar, através de qualquer aparelho, desde que conectado a internet. Ou seja, esses dados estão em uma “nuvem” virtual, hospedado em computadores que tem essa função, e não nos computadores dos usuários.

Os servidores que armazenam os dados podem estar localizados no Brasil ou em qualquer outro país, o que pode dificultar a investigação de crimes que tenham relação com esse tipo de serviço em decorrência dos impasses que essa relações transnacionais trazem, como já foi relatado anteriormente.

Embora esse seja um avanço tecnológico que traz benefícios para seus usuários, pode ser também considerado mais um desafio para a polícia responsável pelas investigações dos crimes cibernéticos. Cerqueira e Rocha (2015, p. 156) dispõem:

> A tecnologia continua avançando e disponibilizando mais conectividade, portabilidade e equipamentos cada vez mais potentes, mais rápidos, reduzindo dia após dia a distância entre estados, países e continentes. Lamentavelmente, contudo, a evolução tecnológica não traz só benefícios.

Os desafios enfrentados na persecução penal dos crimes informáticos são variados e para que esta produza resultados satisfatórios é necessária uma atualização constante dos operadores do direito em todas as esferas, devendo se dispensado muito estudo e aperfeiçoamento. Da mesma forma se faz essencial uma legislação sem falhas técnicas.

Alguns países já despertaram para o cenário tecnológico atual e toda a criminalidade que vem se desenvolvendo neste. Esses países já possuem toda uma estruturação investigativa e legislativa para combater esses crimes informáticos.

O Brasil, embora já tenha despertado para a importância de se modernizar e se especializar no combate a esses delitos específicos, ainda caminha em passos lentos, necessitando de um grande treinamento e capacitação dos setores periciais, do aumento de núcleos especializados e do aperfeiçoamento técnico da legislação específica.

## 5 CONSIDERAÇÕES FINAIS

A tecnologia avançou muito nas últimas décadas, se tornando elemento essencial na vida das pessoas. Em meio a todo esse ambiente digital, utilizado pela maioria das pessoas com boa-fé, como ferramenta útil para as atividades do dia-a-dia, existem pessoas que utilizam essa tecnologia como uma ferramenta para praticar seus crimes e tornar os usuários menos precavidos suas vítimas.

Esse trabalho teve por objetivo analisar os principais aspectos relacionados aos crimes informáticos que influenciam diretamente na eficácia de sua repressão, o qual foi alcançado por meio de extensa pesquisa bibliográfica.

Foram analisadas as principais legislações brasileiras que abordam essa temática dos crimes informáticos, que são a Lei 12.735/2012, Lei 12.737/2012 e Lei 12.965/2014. Constatou-se que a existência dessas leis já configura um importante avanço na repressão desses delitos, tendo em vista que antes eram regulados pelo Código Penal, um código antigo e que foi elaborado para tratar de delitos físicos e não virtuais.

Muito embora a criação dessas leis seja considerada um avanço importante, observou-se que são tecnicamente falhas e que ainda precisam de muitos ajustes para que tenham a eficácia necessária.

Constatou-se, também, que um dos principais desafios enfrentados na persecução penal desses crimes é a identificação do autor do delito, devido às peculiaridades que o mundo virtual possui. Um importante passo para a identificação do autor do delito é a descoberta do endereço IP da máquina de onde partiu a ação delituosa, porém, nem sempre a identificação da máquina significa que irá ser identificado o autor.

Muitos autores dos delitos fazem uso de proxies, que são serviços utilizados para ocultar o endereço IP, entre outras artimanhas para se esquivarem das investigações policiais. Dessa forma, percebeu-se que os sujeitos ativos, principalmente dos delitos mais complexos, estão cada vez mais preparados tecnologicamente, tornando-se um grande desafio para os investigadores policiais a sua identificação.

Há importantes aspectos que retardam as investigações policiais desses crimes. Analisou-se que muitas vezes os provedores de internet utilizados pelos

autores dos delitos estão localizados no exterior, e há uma grande demora em conseguir os dados dos usuários com esses provedores, uma vez que alegam não estarem subordinados à jurisdição brasileira, tornando, geralmente, as provas obsoletas.

Contudo, o maior desafio na persecução penal desses crimes está na deficiência dos órgãos investigativos. Há uma enorme carência de equipe técnica devidamente preparada e atualizada para o combate dos crimes em meio à tecnologia.

Embora alguns Estados brasileiros possuam órgãos de investigação especializados, apenas 11 Estados, ainda não é suficiente diante da enorme população do país e do crescimento alarmante que esse tipo de crime está tendo.

Desse modo, há uma urgente necessidade de preparação técnica dos profissionais incumbidos pela investigação e repressão desses crimes; de um investimento financeiro para aquisição de máquinas avanças e eficientes capazes de auxiliar os investigadores na identificação dos autores desses delitos. Também é necessária a expansão dos núcleos policiais especializados, para que a população de todos os estados do país se beneficie.

É possível concluir que embora já tenha havido alguns avanços com relação à legislação e aos órgãos investigativos, o país ainda necessita avançar mais nesses e em outros aspectos, para que a repressão a esses crimes seja eficaz, possibilitando aos usuários da internet uma maior sensação de segurança.

Por fim, esse estudo é relevante por evidenciar, além dos aspectos jurídicos inerentes a matéria dos crimes cibernéticos, os desafios enfrentados na sua repressão, trazendo os principais empasses que as autoridades responsáveis enfrentam e contribuindo para incrementar o conhecimento pertinente à matéria no campo acadêmico e profissional, uma vez que se trata de tema tão importante e debatido atualmente.

# REFERÊNCIAS

ANDRADE, Leonardo**. Cybercrimes na deep web:** as dificuldades jurídicas de determinação de autoria nos crimes virtuais. Disponível em: <https://jus.com.br/artigos/39754/cybercrimes-na-deep-web-as-dificuldades-juridicas-de-determinacao-de-autoria-nos-crimes-virtuais>. Acesso em: 10 jan. 2017.

BRASIL. Tribunal de Justiça do Estado do Paraná. **RECURSO EM SENTIDO ESTRITO. CRIMES CONTRA A HONRA PRATICADOS PELA INTERNET.ANÁLISE SOBRE A COMPETÊNCIA PARA APRECIAR A MATÉRIA. APLICAÇÃO DA REGRA DO ART. 70 DO CÓDIGO DE PROCESSO PENAL. TEORIA DO RESULTADO. LOCAL ONDE A VÍTIMA E TERCEIROS TOMARAM CONHECIMENTO DOS FATOS, EM TESE, OFENSIVOS, AINDA QUE AS PUBLICAÇÕES NO FACEBOOK TENHAM OCORRIDO EM LOCAL DIVERSO. RECURSO PARCIALMENTE CONHECIDO, E, NESSA PARTE, PROVIDO.** (TJ-PR - RSE: 13971045 PR 1397104-5 (Acórdão), Relator: José Mauricio Pinto de Almeida, Data de Julgamento: 08/10/2015, 2ª Câmara Criminal, Data de Publicação: DJ: 1678 28/10/2015) Disponível em:< https://tj-pr.jusbrasil.com.br/jurisprudencia/249461167/recurso-em-sentido-estrito-rse-13971045-pr-1397104-5-acordao>. Acesso em: 15 fev. 2017.

_____. **Código de Processo Penal**. Disponível em:<http://www.planalto.gov.br/ccivil_03/decreto-lei/Del3689.htm>. Acesso em: 10 dez. 2016.

_____. **Código Penal**. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm>. Acesso em: 20 dez. 2016

_____. **Comissão dos Deputados CPI – Crimes Cibernéticos (relatório**). Disponível em: <http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=1447125>. Acesso em: 10 dez. 2016.

_____. **Constituição da República Federativa do Brasil**. Disponível em: <http://www.planalto.gov.br/ccivil_03/Constituicao/ Constituicao.htm>. Acesso em: 20 dez. 2016

_____. **Informativo 326 - Crimes na Internet – Competência.** Disponível em: <http://www.criminal.mppr.mp.br/modules/conteudo/conteudo.php?conteudo=1474>. Acesso em: 10 jan.2017.

_____. **Lei nº 12.735, de 30 de Novembro de 2012**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12735.htm>. Acesso em: 27 ago. 2016.

_____. **Lei nº 12.737, de 30 de Novembro de 2012.** Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 07 nov. 2016.

_____. **Lei nº 12.965, de 23 de Abril de 2014**. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 27 ago. 2016.

_____. Superior Tribunal de Justiça. **PENAL. CONFLITO DE COMPETÊNCIA. CRIME DE RACISMO PRATICADO PORINTERMÉDIO DE MENSAGENS TROCADAS EM REDE SOCIAL DA INTERNET.USUÁRIOS DOMICILIADOS EM LOCALIDADES DISTINTAS. INVESTIGAÇÃODESMEMBRADA. CONEXÃO INSTRUMENTAL. EXISTÊNCIA. COMPETÊNCIA FIRMADAPELA PREVENÇÃO EM FAVOR DO JUÍZO ONDE AS INVESTIGAÇÕES TIVERAMINÍCIO**. Disponível em:< https://stj.jusbrasil.com.br/jurisprudencia/23052425/conflito-de-competencia-cc-116926-sp-2011-0091691-2-stj>. Acesso em: 15 fev. 2017.

_____. Supremo Tribunal Federal. **HABEAS CORPUS. ALEGAÇÃO DE VÍCIO PROCIDIMENTAL. COMPETÊNCIA PARA PROCESSAR E JULGAR CRIME DE INCITAÇÃO À DISCRIMINAÇÃO COMETIDO POR MEIO DA INTERNET. OFENSAS DIRIGIDAS A PESSOAS DETERMINADAS.** (STF - HC: 121283 DF, Relator: Min. ROBERTO BARROSO, Data de Julgamento: 29/04/2014, Primeira Turma, Data de Publicação: DJe-091 DIVULG 13-05-2014 PUBLIC 14-05-2014). Disponível em:< https://stf.jusbrasil.com.br/jurisprudencia/25078330/habeas-corpus-hc-121283-df-stf?ref=juris-tabs>. Acesso em: 10 dez.2017.

_____. Tribunal Regional Eleitoral de São Paulo. **CONFLITO NEGATIVO DE COMPETÊNCIA. INQUÉRITO POLICIAL. CRIMES CONTRA A HONRA COM FINALIDADE ELEITORAL PRATICADOS ATRAVÉS DA INTERNET (FACEBOOK).** [...].(TRE-SP - CJ: 14819 SP, Relator: LUIZ GUILHERME DA COSTA WAGNER JUNIOR, Data de Julgamento: 12/11/2013, Data de Publicação: DJESP - Diário da Justiça Eletrônico do TRE-SP, Data 19/11/2013). Disponível em: <https://tre-sp.jusbrasil.com.br/jurisprudencia/120123972/conflito-de-jurisdicao-cj-14819-sp>. Acesso em: 15 fev. 2017.

CAPEZ, Fernando. **Curso de processo penal.** 23. ed. São Paulo: Saraiva, 2016.

CERQUEIRA, Silvio Castro; ROCHA, Claudinor. Crimes cibernéticos: desafios da investigação. **Aslegis,** Brasilia, v. 1, n. 49, p.131-161, maio 2013.

CONTE, Christiany Pegorari. Jurisdição e competência nos crimes informáticos. **Revista Brasileira de Meio Ambiente Digital e Sociedade da Informação,** São Paulo, v. 1, n. 1, p.49-208, abr. 2014.

CRESPO, Marcelo Xavier de Freitas. **Crimes digitais**. 1. ed. São Paulo: Saraiva, 2011.

FIORILLO, Celso Antônio Pacheco; CONTE, Christiany Pegorari. **Crimes no meio ambiente digital e a sociedade de informação.** 2. ed. São Paulo: Saraiva, 2016.

FRANCO, Deivison Pinheiro; MAGALHÃES, Suyanne Ramos. **A darkweb: navegando no lado obscuro da internet**. Amazônia em Foco**,** Castanhal, v. 4, n. 6, p.18-133, jan 2015.

JESUS, Damásio de; MILAGRE, José Antonio. **Manual de crimes informáticos.** São Paulo: Saraiva, 2016.

LIMA, Paulo Marco Ferreira. **Crimes de computador e segurança computacional.** 2. ed. São Paulo: Atlas, 2011.

LINS, Bernardo Felipe Estelita. A evolução da internet: uma perspectiva histórica. In: **Cadernos ASLEGIS,** nº 48. Brasília: ASLEGIS, 2015.

LOPES JUNIOR, Aury. **Direito processual penal.** 13. ed. São Paulo: Saraiva, 2016.

MACEDO, Patrícia Alves. **Crimes Virtuais frente à falta de Legislação e Educação Ambiental**. Disponível em: <https://goo.gl/7UQaaY>. Acesso em: 16 dez. 2016.

NETO, Cícero Alves de Sousa; SANTOS, SANTOS, Matheus. **Crimes cibernéticos:** generalidades e perspectiva da legislação brasileira. Disponível em: <https://periodicos.ufrn.br/transgressoes/article/viewFile/6664/5161>. Acesso em: 10 jan. 2017.

NUCCI, Guilherme de Souza. **Manual de processo penal e execução penal.** 13. ed. Rio de Janeiro: Forense, 2016.

PAESANI, Liliana Minardi. **Dirieito e internet:** Liberdade de informação, privacidade e responsabilidade civil. 6. ed. São Paulo: Atlas, 2013.

ROSA, Fabrízio. **Crimes de Informática**. 1. ed. Campinas: Bookseller, 2002.

ROSSINI, Augusto. **Informática, Telemática e Direito Penal**. São Paulo: Memória Jurídica Editora, 2004.

SYDOW, Spencer Toth. **Crimes informáticos e suas vítimas.** 2. ed. São Paulo: Saraiva, 2015.

WENDT, Emerson. **Lista dos Estados que possuem Delegacias de Polícia de combate aos Crimes Cibernéticos**. Disponível em:< http://www.emersonwendt.com.br/2010/07/lista-dos-estados-com-possuem.html> Acesso em: 20 jan.2017.

_____. **Inteligência cibernética:** a insegurança virtual no brasil. São Paulo: Delfos Editora Digital, 2011.

_____, JORGE, Higor Vinicius Nogueira. **Crimes cibernéticos:** ameaças e procedimentos de investigação. 2. ed. Rio de Janeiro: Brasport, 2013.