UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO DE CIÊNCIAS JURÍDICAS
DEPARTAMENTO DE DIREITO

DEBORA CRISTINA DA SILVA

CIBERCRIMINALIDADE E A (IN) SUFICIÊNCIA LEGISLATIVA PÁTRIA PARA A REPRESSÃO DOS CRIMES COMETIDOS POR MEIO DA INTERNET

Florianópolis
2020

DEBORA CRISTINA DA SILVA

CIBERCRIMINALIDADE E A (IN) SUFICIÊNCIA LEGISLATIVA PÁTRIA PARA A REPRESSÃO DOS CRIMES COMETIDOS POR MEIO DA INTERNET

Trabalho de Conclusão de Curso submetido à banca examinadora da Universidade Federal de Santa Catarina - UFSC, como requisito parcial à obtenção do título de Bacharel em Direito.

Orientador: Prof. Dr. Matheus Felipe de Castro

Florianópolis

2020

RESUMO

O presente trabalho de conclusão de curso tem o objetivo de analisar o debate acerca das modalidades criminosas que surgem constantemente no ambiente virtual, devido ao crescimento da internet na sociedade moderna; as problemáticas que são enfrentadas pelos Estados soberanos na regulamentação do uso dessas tecnologias e na persecução penal dos cibercrimes; bem como a insuficiência da legislação pátria que regulamente os tipos penais e as formas de investigação e punição de tais delitos, juntamente com a necessidade de cooperação internacional sobre o tema. O problema da pesquisa é entender se há ou não a insuficiência da legislação nacional para regulamentar os meios de investigação e combate aos crimes cibernéticos, ou seja, analisar os problemas que o poder punitivo estatal enfrenta na persecução penal dessa modalidade criminosa e quais leis são aplicáveis à resolução desses problemas, analisando se tais legislações são suficientes. Para responder a essa pergunta, foi levantada a hipótese, ao final confirmada, de que a legislação brasileira é insuficiente e desatualizada, sendo incapaz de regulamentar com eficiência os meios de investigação, obtenção de prova e repressão dos crimes cometidos pela internet. O método de abordagem utilizado foi o dedutivo. O objetivo geral do trabalho foi verificar como o Estado brasileiro está aquém das necessidades legislativas para impor limites à criminalidade virtual, não acompanhando sua evolução e crescimento, falhando em proteger seus cidadãos de tais ataques. Nesse sentido, no primeiro capítulo, fez-se uma explanação acerca da abordagem histórica, visando demonstrar como ocorreu o surgimento da internet e, posteriormente, dos crimes que utilizam desse ambiente virtual como meio ou objeto delitivo. Buscando atestar que o uso da internet é meio idôneo para o cometimento de crimes, distinguiu-se a conceituação apresentada pela doutrina sobre as espécies de crimes informáticos, demonstrando, em seguida, a dificuldade encontrada pelos operadores do direito na investigação e repressão de tais crimes cometidos pela internet. Em seguida, no segundo capítulo, adentrou-se nas dificuldades que os Estados soberanos, como um todo, com enfoque no Estado brasileiro, possuem na regulamentação do uso da internet e no combate à criminalidade virtual, demonstrando a importância da obrigatoriedade legal do armazenamento dos registros de acesso dos usuários na rede mundial de computadores, relacionando tal necessidade com a controversa do direito à privacidade e da vedação ao anonimato. Enfim, com a análise do terceiro capítulo, buscou-se elucidar que, analisando as normas internas e internacionais sobre cibercrime e investigação criminal; as normas internacionais sobre o tema, a título de direito comparado; e a Convenção de Budapeste, conclui-se que a legislação brasileira é insuficiente e desatualizada para o combate ao crime cibernético. Ao final, a hipótese foi confirmada, no sentido de que a legislação pátria carece de modificação, atualização e complementação, devendo se atentar às características do ambiente virtual e dos crimes que ali são perpetrados, bem como a importância de buscar normas de cooperação internacional que visem o combate à cibercriminalidade para complementar a legislação e o aparato do poder punitivo estatal. A pesquisa tem relevância aos debates contemporâneos na medida em que traça os eixos a serem seguidos pelo Estado brasileiro para que consigam acompanhar a volatilidade dos meios informáticos e das ofensas aos direitos de terceiros que são materializadas nesse meio.

Palavras-chave: Cibercriminalidade. Insuficiência legislativa. Cooperação Internacional. Investigação Criminal. Direito Processual Penal.

ABSTRACT

The following final course assignment has the point to analyze the debate about the criminal modalities that constantly appear in the virtual environment, due to the growth of the internet in modern society; the problems faced by sovereign states in regulating the use of these technologies and in the criminal prosecution of cybercrimes; as well as the insufficiency of the national legislation that regulates the criminal types and the forms of investigation and punishment of such crimes, together with the need for international cooperation on the subject. The research problem is to understand whether or not national legislation is insufficient to regulate the means of investigating and combating cyber crimes, that is, analyzing the problems that the state punitive power faces in the criminal prosecution of this criminal modality and which laws are applicable solving these problems, analyzing whether such legislation is sufficient. To answer this question, the hypothesis was raised, at the end confirmed, that Brazilian legislation is insufficient and outdated, being unable to efficiently regulate the means of investigation, obtaining evidence and prosecuting crimes committed over the internet. The approach method used was deductive. The general objective of the work was to verify how the Brazilian State falls short of the legislative needs to impose limits on cyber crime, not following its evolution and growth, failing to protect its citizens from such attacks. In this meaning, in the first chapter, an explanation was made about the historical approach, aiming to demonstrate how the internet emerged and, later, the crimes that use this virtual environment as a criminal means or object. Seeking to attest that the use of the internet is suitable for the commission of crimes, the conceptualization presented by the doctrine on the types of computer crimes was distinguished, demonstrating, following by the difficulty found by the operators of the law in the investigation and repression of such crimes, committed over the internet. Then, in the second chapter, it entered into the difficulties that the sovereign states, as a whole, focusing on the Brazilian state, have in regulating the use of the internet and in combating cyber crime, demonstrating the importance of the legal obligation of storing data, user access records on the world wide web, relating this need to the controversial right to privacy and the prohibition of anonymity. Finally, with the analysis of the third chapter, it was sought to clarify that, analyzing the internal and international norms on cybercrime and criminal investigation; international standards on the subject, as a comparative law; and the Budapest Convention, it is concluded that Brazilian legislation is insufficient and outdated to combat cyber crime. In the end, the hypothesis was confirmed, in the sense that the national legislation needs modification, updating and complementation, paying attention to the characteristics of the virtual environment and the crimes that are perpetrated there, as well as the importance of seeking international cooperation standards that aims at combating cybercrime to complement legislation and the apparatus of state punitive power. The research has relevance to contemporary debates in that it traces the axes to be followed by the Brazilian State so that they are able to monitor the volatility of computer media and the offenses against the rights of third parties that are materialized in this medium.

Keywords: Cybercrime. Legislative failure. International cooperation. Criminal investigation. Criminal Procedural Law.

SUMÁRIO

INTRODUÇÃO

Não há como negar o desenvolvimento da tecnologia no mundo atual, especialmente o impacto que a informática apresentou na sociedade, seja no campo positivo da evolução do processo de comunicação e do encurtamento de distâncias entre as pessoas, seja no âmbito negativo, como no caso do aumento da criminalidade e, até, no surgimento de crimes propagados pela internet, até então desconhecidos.

Com o avanço dos meios de comunicação pela internet e o aumento cada vez mais crescente de usuários da rede mundial de computadores, a prática de crimes virtuais, conhecidos como cibercrimes, vem aumentando exponencialmente ao longo dos anos.

A internet propiciou um novo lócus de cometimento de crimes. Com a facilidade de poder ser acionada de qualquer lugar do mundo, a rede informática desestabilizou fronteiras e dificultou a atividade de persecução dos órgãos oficiais de controle.

Está enganado quem acredita que a internet é um espaço livre de leis, imperando o anonimato e a ilegalidade. Contudo, o direito ainda não se adaptou totalmente a estes novos tempos e isto se dá, em partes, em razão da própria natureza destas mudanças. A virtude da facilidade e velocidade com que as informações são trocadas, assim como o anonimato obtido através destes meios, dificultam o tratamento legal da matéria.

O presente trabalho visa analisar o atual cenário global dos danos causados pelos crescentes crimes praticados pela internet, bem como a dificuldade que os Estados soberanos enfrentam na investigação e punição desses delitos. Busca-se também analisar de forma detida a insuficiência legislativa brasileira sobre o tema, através da comparação com a legislação de outros países, bem como demonstrar os prejuízos causados por essa escassez de normas.

Nesse sentido, o presente trabalho, tendo como tema o Direito Processual Penal brasileiro, com enfoque aos crimes virtuais perpetrados por meio ou contra a internet e seus sistemas de dados, delimita como problema central a ser estudado justamente a legislação pátria brasileira e a discussão sobre sua insuficiência para regulamentar os meios de investigação e combate aos crimes cibernéticos.

A partir da suscitação de tal problema central, o trabalho, através de revisões bibliográficas demonstrando como se deu o surgimento dos crimes cometidos pela internet e suas espécies, além da dificuldade que os Estados soberanos enfrentam para investigar e punir tais tipos de delito, realizando um comparativo das legislações de países estrangeiros com a legislação brasileira que visam a repressão dos crimes cibernéticos,

pretende desenvolver a teoria de que a falta de legislação pátria que seja eficiente e atualizada para nortear a investigação e repressão dessa nova modalidade delitiva, bem como a escassez de uma cooperação internacional no mesmo sentido, causa sérios prejuízos aos Estados soberanos e à sociedade, na medida em que a impunidade gerada pela falta de legislação impulsiona o crescimento e aprimoramento da cibercriminalidade.

Assim, partindo dessa hipótese, utilizando como base teórica o pensamento positivista e fazendo uso do método dedutivo, por meio do procedimento de pesquisas bibliográfica, legislativa e jurisprudencial, desenvolve-se o presente trabalho de conclusão de curso.

O trabalho divide-se, então, em três capítulos, dentre os quais o primeiro tem por início uma abordagem histórica, visando demonstrar como ocorreu o surgimento da internet e, posteriormente, dos crimes que utilizam desse ambiente virtual como meio ou objeto delitivo. Para atestar que o uso da internet é meio idôneo para o cometimento de crimes, faz-se, inicialmente, a distinção e conceituação das espécies de crimes informáticos, demonstrando, em seguida, a dificuldade encontrada pelos operadores do direito na investigação e repressão de tais crimes cometidos pela internet.

Seguindo a cronologia do avançar do entendimento sobre a cibercriminalidade, o segundo capítulo tem por intuito a demonstração, por meio de estudos e pesquisas legislativas, da importância da obrigatoriedade legal do armazenamento dos registros de acesso dos usuários na rede mundial de computadores, indicando as leis que tratam sobre o tema, bem como a maneira que o regulamentam. Trazendo entendimentos legais, doutrinários e jurisprudenciais acerca da matéria, busca-se fazer a relação da importância de leis que obriguem o registro e armazenamento de tais dados, com a controversa do direito à privacidade e da vedação ao anonimato.

Por fim, o terceiro e último capítulo traz a problemática abordada no presente trabalho de forma mais específica. Neste ponto, analisa-se as normas internas e internacionais sobre cibercrime e investigação criminal. Para tal, estuda-se a Convenção de Budapeste, apresentando os temas abordados pelo referido diploma internacional e a importância e imprescindibilidade da adoção do mesmo pelo Brasil. Seguindo no tema, os estudos irão apontar para a legislação pátria brasileira que se ocupa do tema, bem como as normas sobre investigação criminal de delitos cometidos pela internet, quando se discutirá sobre a sua insuficiência para o combate ao crime cibernético.

1. O USO DA INTERNET COMO MEIO IDÔNEO PARA O COMETIMENTO DE CRIMES

1.1 SURGIMENTO DO CIBERCRIME

O surgimento da maior ferramenta utilizada no mundo nos dias atuais, segundo pesquisa da rede de notícias norte-americana CNN e do Instituto de Tecnologia de Massachussets, remonta ao período do auge da Guerra Fria, em meados do século XX. Nesse contexto histórico, em que duas grandes potências mundiais, Estados Unidos e União Soviética, disputavam uma corrida bélica, armamentista e espacial, visando conquistar poderes hegemônicos, foi que surgiu a internet, com objetivos primordialmente militares[1].

Receando ataques soviéticos, o Departamento de Defesa dos Estados Unidos (ARPA - Advanced Research Projects Agency) subsidiou uma grande pesquisa envolvendo universidades e centros de pesquisas norte-americanos, cujo objetivo central era desenvolver uma rede de comunicação confiável entre os centros militares desse Estado soberano, para garantir uma troca segura e ininterrupta de informações sigilosas do governo[2].

Os pesquisadores se depararam com o desafio de fazer com que, pela primeira vez, as redes de computadores das Forças Armadas, composta pelo Exército, Marinha e Aeronáutica, que tinham arquiteturas e modo de funcionamento próprios, completamente diferentes e incompatíveis entre si, pudessem se compatibilizar para realizar comunicações e interações de forma segura.[3]

Sob essas circunstancias, em 1969, surgiu o protótipo da primeira rede de internet, que ficou conhecida como ARPANET (Advanced Research Projects Agency Network).

---

[1] JUNIOR, Júlio Cesar Alexandre. **Cibercrime: um estudo acerca do conceito de crimes informáticos.** Revista Eletrônica da Faculdade de Direito de Franca. Disponível em <https://www.revista.direitofranca.br/index.php/refdf/article/view/602#:~:text=Cibercrime%20est%C3%A1%20associado%20ao%20%E2%80%9Cfen%C3%B3meno,12).>. Acesso em 14 de agosto de 2020.

[2] ANDRADE, Mariah Dourado de; BENTES, Dorinethe dos Santos; GUIMARAES, David Franklin da Silva. **Considerações sobre a aplicabilidade do direito penal acerca dos crimes virtuais.** Revista Vertentes do Direito. Disponível em <https://sistemas.uft.edu.br/periodicos/index.php/direito/article/view/4171#:~:text=O%20presente%20artigo%20busca%20compreender,Leis%20Penais%20regulando%20esse%20crime.>. Acesso em 14 de agosto de 2020.

[3] VALVERDE, Danielle Novaes de Siqueira. **Crimes Cibernéticos: a obrigatoriedade do registro de acesso à internet como forma de possibilitar a identificação do criminoso.** Revista da ESMAPE. Recife. v. 15. n. 32. p. 236. jul./dez. 2010.

A primeira conexão resultante dessas pesquisas interligava quatro universidades norte-americanas envolvidas no projeto, quais sejam: Universidade da Califórnia, em Los Angeles; Universidade da Califórnia, em Santa Bárbara; Universidade de Stanford e Universidade de Utah, em Salt Lake City.[4]

A primeira conexão internacional envolvendo a ARPANET ocorreu em 1973, ocasião em que Inglaterra e Noruega tiveram a oportunidade de se intercomunicar utilizando o novel sistema pela primeira vez.[5]

A denominação Internet foi atribuída tempo depois, em meados da década de 80, quando o sistema começou a apresentar proporções mundiais. No início, a expansão do inovador sistema de comunicação se deu de forma a interligar as demais universidades americanas, ampliando, posteriormente, seu acesso às demais universidades e centros de pesquisas sediados em outros países[6].

O principal objetivo do revolucionário sistema de comunicação em massa, desde o princípio, foi estabelecer uma rede segura para acesso às informações, de alcance universal. Com o sucesso da pesquisa e a expansão do programa, muitas adaptações ocorreram, contudo, o objetivo continuou o mesmo.

Com a democratização da internet, buscava-se que, em tese, todos os usuários ali presentes fossem anônimos e gozassem de igualdade na utilização desse espaço integrado, visando com isso garantir a maior velocidade, eficiência, equidade e, esperava-se, maior segurança nas relações interpessoais e negociais ali concretizadas. No entanto, a difusão e popularização da internet, aliado ao fácil acesso e amplo alcance desse meio, formaram um ambiente altamente favorável para o surgimento e propagação de ameaças.

A popularização da internet teve início na década de 90, com o início da exploração mercadológica do referido sistema, quando o cientista, físico e professor

---

[4] VALVERDE, Danielle Novaes de Siqueira. **Crimes Cibernéticos: a obrigatoriedade do registro de acesso à internet como forma de possibilitar a identificação do criminoso.** Revista da ESMAPE. Recife. v. 15. n. 32. p. 236. jul./dez. 2010.

[5] ANDRADE, Mariah Dourado de; BENTES, Dorinethe dos Santos; GUIMARAES, David Franklin da Silva. **Considerações sobre a aplicabilidade do direito penal acerca dos crimes virtuais.** Revista Vertentes do Direito. Disponível em <https://sistemas.uft.edu.br/periodicos/index.php/direito/article/view/4171#:~:text=O%20presente%20artigo%20busca%20compreender,Leis%20Penais%20regulando%20esse%20crime.>. Acesso em 14 de agosto de 2020.

[6] JUNIOR, Júlio Cesar Alexandre. **Cibercrime: um estudo acerca do conceito de crimes informáticos.** Revista Eletrônica da Faculdade de Direito de Franca. Disponível em <https://www.revista.direitofranca.br/index.php/refdf/article/view/602#:~:text=Cibercrime%20est%C3%A1%20associado%20ao%20%E2%80%9Cfen%C3%B3meno,12).>. Acesso em 14 de agosto de 2020.

britânico Tim Berners-Lee desenvolveu o serviço de World Wide Web, usualmente conhecido como “www”, criando, assim, o que se denominou de rede de acesso.[7]

Com a criação da teia mundial (World Wide Web – www), a ARPANET passou a ser chamada de internet e com certas melhorias em sua interface gráfica ficou mais acessível ao público em geral, tornando esse novo meio de comunicação popular.

A partir dessa inovação, a década de 90 foi o cenário do importante marco histórico popularmente conhecido como o “boom da internet”[8]. Nesse período a rede de acesso e comunicação se difundiu e universalizou. Como consequência desse crescente e lucrativo mercado, iniciou-se um constante e veloz aperfeiçoamento da internet e de novas tecnologias em software. Com o evidente crescimento da internet, passou-se a ter um crescimento exponencial do número de usuários dessa rede.

A primeira conexão à internet realizada no Brasil foi em 1991, por meio da fundação de Amparo à Pesquisa do Estado de São Paulo (Fapesp). A partir dessa primeira conexão à rede, as universidades brasileiras iniciaram negociações com o Governo dos Estados Unidos que envolviam o compartilhamento de informações.[9]

Em 1992 foi instituída a Rede Nacional de Ensino e Pesquisa (RNP), organização social ligada ao Ministério de Ciência, Tecnologia, Inovações e Comunicações do Governo Federal Brasileiro, a qual de fato moveu seus esforços no sentido de integralizar a internet ao Brasil e fomentar sua difusão na sociedade.[10]

Em 1997, criou-se as "redes locais de conexão" expandindo, dessa forma, o acesso a todo território nacional[11].

Na contemporaneidade, a internet passou a desempenhar um status significativo na sociedade em geral. Das relações interpessoais às negociais, passando pelas esferas do Governo, segurança pública, educação, saúde ou cultura, todas as ligações estabelecidas na sociedade atual passam, de alguma forma, pela informatização, sejam de dados ou da

---

[7] DIANA, Daniela. **História da internet.** Disponível em <https://www.todamateria.com.br/historia-da-internet/>. Acesso em 14 de agosto de 2020.
[8] DIANA, Daniela. **História da internet.** Disponível em <https://www.todamateria.com.br/historia-da-internet/>. Acesso em 14 de agosto de 2020.
[9] VALVERDE, Danielle Novaes de Siqueira. **Crimes Cibernéticos: a obrigatoriedade do registro de acesso à internet como forma de possibilitar a identificação do criminoso.** Revista da ESMAPE. Recife. v. 15. n. 32. p. 236. jul./dez. 2010.
[10] Rede Nacional de Ensino e Pesquisa. **Nossa História – RNP.** Disponível em <https://www.rnp.br/sobre/nossa-historia >. Acesso em 14 de agosto de 2020.
[11] DIANA, Daniela. **História da internet.** Disponível em <https://www.todamateria.com.br/historia-da-internet/>. Acesso em 14 de agosto de 2020.

própria comunicação. O que importa é que a internet desempenha uma função essencial e insubstituível na vida das pessoas.

A internet, no atual estágio que se encontra, desempenha papel que ultrapassa seus objetivos iniciais de comunicação, e seus objetivos intermediários de entretenimento, sendo hoje utilizada como uma das plataformas mais eficientes que impulsiona a economia mundial. Hodiernamente, os mecanismos disponíveis nesse espaço virtual percorrem desde os pequenos negócios virtuais, até as transações bilionárias de empresas multinacionais. Levando em consideração esse contexto socioeconômico desempenhado pela rede mundial de computadores, assim como todos os documentos sigilosos relacionados a esse cenário que ali estão armazenados, torna-se ainda mais perceptível os danos que podem advir de ameaças e ataques por meio da internet, e a amplitude dos prejuízos que essa insegurança pode ocasionar.

Os meios de tecnologias informacionais de comunicação tornaram-se, e tornam-se cada vez mais, elementos essenciais e indispensáveis à atividade humana para o seu desenvolvimento.

São inegáveis os benefícios que a informatização trouxe para os Governos e para a sociedade em geral, nos seus mais diversificados aspectos existentes. Contudo, em contrapartida, não se pode olvidar que esse meio de acesso volátil propiciou o aumento, e em certo grau o próprio surgimento, de uma série de crimes.

É o que se segue, nas palavras de Mendes e Vieira:

> [...] apesar das facilidades e benefícios oferecidos pela internet, esse cenário também é propício para a prática de crimes. Cada vez mais, os criminosos se valem desse meio para praticar os mais variados tipos de crime. Pois, com o advento da internet, os crimes já tipificados pelo Código Penal passaram a ser praticados também no meio virtual, assim como, surgiram novas modalidades de crimes que passaram a ser praticados nesse meio. [12]

Com as indiscutíveis e infindáveis vantagens proporcionadas pelos meios informáticos, principalmente pelo uso da internet, a sociedade ficou cada vez mais dependente desse espaço virtual, atrelando a ele quase todas suas informações e fazendo desse meio o local mais rápido e prático para resolver seus compromissos e problemas

[12] MENDES, Maria Eugenia Gonçalves; VIEIRA, Natália Borges. **Os Crimes Cibernéticos no Ordenamento Jurídico Brasileiro e a Necessidade de Legislação Específica.** Disponível em <http://www.gcpadvogados.com.br/artigos/os-crimes-ciberneticos-no-ordenamento-juridico-brasileiro-e-a-necessidade-de-legislacao-especifica-2>. Acesso em 14 de agosto de 2020.

cotidianos. Essa necessidade que se estabeleceu com o uso dos meios informáticos, ligados ou não à rede mundial de computadores, trouxe uma polêmica vulnerabilidade aos usuários, na medida em que estes, achando-se seguros, não tomam as devidas cautelas, tornando-se, assim, mais suscetíveis a ataques criminosos.

O uso constante e desmedido dos meios de comunicação em massa, tanto entre pessoas, como entre empresas, cria um ambiente de sujeição e instabilidades que proporciona a abertura de um novo campo para a atuação da criminalidade, com cada vez mais evidentes violações aos direitos fundamentais.

Essa conjuntura evidencia a impreterível discussão acerca dos crimes virtuais e suas nefastas consequências, que, não isoladas vezes, são ainda mais drásticas devido ao fato da internet ser um meio de fácil e rápida propagação de informações.

A internet, assim compreendida como patrimônio imaterial da sociedade atual, faz jus à proteção jurídica do Estado, em razão de sua importância no cenário mundial e de sua interligação direta com os direitos fundamentais da pessoa humana, visto que é por meio da internet que se cria o ambiente mais favorável para ameaçar e agredir tais direitos.

Acompanhado dos benefícios atrelados à disseminação dos computadores e demais hardwares, assim como do acesso à internet e aos cada vez mais sofisticados softwares existentes, surgiram crimes e criminosos altamente especializados na linguagem informática. Diversas terminologias foram desenvolvidas como sinônimos para referir-se às infrações penais realizadas através de dispositivos informáticos ligados à rede mundial de computadores, podendo-se mencionais, dentre os termos mais recorrentes: cibercrimes; crimes cibernéticos; crimes informáticos; crimes na internet; crimes virtuais; crimes digitais; crimes por computador; crimes telemáticos; crimes da era digital; crimes de alta tecnologia; crimes transnacionais; fraude informática; dentre outras nomenclaturas. A nomenclatura utilizada depende de cada pais e sua legislação, sendo que a adoção de uma nomenclatura não exclui a utilização de outras, já que todas são sinônimos da mesma ação delitiva.

Tais crimes, apesar de recém surgidos, propagam-se e crescem de forma incomensurável, o que torna árdua a tarefa de se proteger e prevenir de tais atos, além de serem de difícil controle, investigação e punição pelos Estados soberanos. Equitativamente ao surgimento e avanço diário das novas modalidades de interação entre os usuários, surgem os novos meios de praticar infrações penais.

> No que tange a conceituação, cibercrime (INTERPOL, 2015) é a atividade criminosa ligada diretamente a qualquer ação ou prática ilícita na Internet. Esse crime consiste em fraudar a segurança de computadores, sistema de comunicação e redes corporativas. Assim, o crime na internet, ou cibercrime, nada mais é do que uma conduta ilegal realizada por meio do uso do computador e da internet.[13]

No fim da década de 1990, na cidade de Lyon, na França, um subgrupo das nações do G8 se reuniu para debater sobre os graves crimes promovidos por meio de dispositivos eletrônicos conectados à internet, ou contra tais dispositivos. Nesta reunião foi criado o termo cibercrime (originalmente, em inglês, cybercrime), o qual é o termo mais comum para referir-se à tais infrações até os dias atuais. A mencionada categoria, denominada "Grupo de Lyon", utilizou o termo para informar, amplamente, as formas de crimes cometidos por meio da internet, enquanto debatiam sobre sua gravidade[14].

O termo cibercrime, assim como os diversos sinônimos existentes para tais atos criminosos, buscam referir-se às condutas atentatórias à direitos fundamentais e de grande monta de pessoas físicas e jurídicas, utilizando-se da internet e dos meios eletrônicos ligados a ela para a prática do crime, ou como objeto material do mesmo.

O uso inapropriado do âmbito virtual se subdivide em duas categorias distintas, quais sejam: ações prejudiciais atípicas e crimes virtuais[15].

As ações prejudiciais atípicas não possuem tipificação legal e, por isso, respeitando o princípio da estrita legalidade que rege o direito penal pátrio, tais condutas não são criminalizadas e não podem ser consideradas crimes sem que haja antes a tipificação da mesma pelos legisladores competentes. Contudo, tais atitudes, no mínimo, importunas, merecem uma resposta Estatal, já que lesionam o direito de terceiros. Por isso, é possível que as denominadas ações prejudicais atípicas cometidas pela internet sejam passiveis de processo e responsabilização no âmbito civil, visando proteger os inúmeros direitos ameaçados por essas práticas.

---

[13] NASCIMENTO, Samir de Paula. **Cibercrime: conceitos, modalidades e aspectos jurídicos-penais.** Disponível em <https://ambitojuridico.com.br/cadernos/internet-e-informatica/cibercrime-conceitos-modalidades-e-aspectos-juridicos-penais/>. Acesso em 14 de agosto de 2020.

[14] NASCIMENTO, Samir de Paula. **Cibercrime: conceitos, modalidades e aspectos jurídicos-penais.** Disponível em < https://ambitojuridico.com.br/cadernos/internet-e-informatica/cibercrime-conceitos-modalidades-e-aspectos-juridicos-penais/>. Acesso em 14 de agosto de 2020.

[15] ANDRADE, Mariah Dourado de; BENTES, Dorinethe dos Santos; GUIMARAES, David Franklin da Silva. **Considerações sobre a aplicabilidade do direito penal acerca dos crimes virtuais.** Revista Vertentes do Direito. Disponível em <https://sistemas.uft.edu.br/periodicos/index.php/direito/article/view/4171#:~:text=O%20presente%20artigo%20busca%20compreender,Leis%20Penais%20regulando%20esse%20crime.>. Acesso em 15 de agosto de 2020.

Em contrapartida, os crimes virtuais se dividem em crimes típicos da sociedade, porém agora realizados por meio de computadores, utilizando a internet como ferramenta para consumação dessas infrações penais. Ou, podem ser novos tipos delituosos, que tem como elementar do crime ou como o próprio objeto material do delito as informações armazenadas nesse ambiente virtual.

Quando da criação e democratização da internet, um de seus objetivos era o de tornar os seus usuários anônimos, não identificáveis, visando promover assim mais equidade entre as pessoas, destruindo barreiras socioeconômicas. Contudo, esse anonimato é a maior causa geradora da crescente criminalidade pela internet, devido à dificuldade de identificação de seus autores. Os crimes informáticos transcendem a esfera virtual e passam a afetar diretamente a vida das pessoas vítimas desses delinquentes cibernéticos, causando danos muitas vezes irreversíveis à pessoa, tendo em vista a rapidez da propagação de informações no mundo on-line.

Qualquer tecnologia criada não consegue desenvolver um método para garantir de forma efetiva a total segurança dos dados e usuários. Essa instabilidade proporcionou o surgimento e constante incremento de novos métodos criminosos, de forma que delinquentes especializados começaram a utilizar suas habilidades tecnológicas para descobrir meios de frustrar as barreiras de proteção criadas para os softwares e hardwares, visando cometer os mais diversos tipos de delitos.

Os casos de primeiros crimes virtuais em que se teve conhecimento aludem ao ano de 1960 e concentram-se na manipulação e sabotagem de sistemas de computadores. [16] Não obstante, foi apenas na década de 70 que os sujeitos ativos dessas infrações penais ganharam destaque e ficaram conhecidos, à época, como Hackers[17].

Em 1980, o objeto material dos crimes cometidos pela internet foi expandido, deixando de visar apenas o acesso para subtração, modificação ou destruição de dados contidos no ambiente virtual, passando a utilizar a internet como meio para o cometimento de outros crimes que já eram praticados de forma grave na sociedade, e que

---

[16] CARNEIRO, Adeneele Garcia. **Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação.** Âmbito Jurídico. Disponível em <http://www.ambito-juridico.com.br/site/index.php/?n_link=revista_artigos_leitura&artigo_id=11529&revista_caderno=17>. Acesso em 16 de agosto de 2020.

[17] ANDRADE, Mariah Dourado de; BENTES, Dorinethe dos Santos; GUIMARAES, David Franklin da Silva. **Considerações sobre a aplicabilidade do direito penal acerca dos crimes virtuais.** Revista Vertentes do Direito. Disponível em <https://sistemas.uft.edu.br/periodicos/index.php/direito/article/view/4171#:~:text=O%20presente%20artigo%20busca%20compreender,Leis%20Penais%20regulando%20esse%20crime.>. Acesso em 14 de agosto de 2020.

agora encontrariam uma forma mais fácil para sua propagação[18]. Desta forma, os cibercrimes deixaram de ter a internet apenas como objeto final do delito, para, também, utilizá-la como meio para consumação de outros crimes.

> Com a utilização de vírus, o criminoso conseguia obter acesso ao computador de suas vítimas. O advento da internet e a sua forma de concepção, que permite interconectar equipamentos ao arrepio da distância geográfica e do controle, aliado à facilidade de troca de informações entre usuários que nunca se viram, e provavelmente, nunca se verão, criou uma propícia para o estabelecimento de uma outra classe de programas com objetivos voltados para causar danos a terceiros. Um destes tipos de programas de computador é o chamado vírus. Vírus, então, nada mais são do que programas de computador intencionalmente desenvolvidos, em geral, com intenções maliciosas, de causar dano a um grupo específico de computadores ou à rede em geral.[19]

A introdução da internet na vida das pessoas se deu de maneira tal que as casas passaram a ser equipadas com computadores para que os membros da família pudessem estar sempre conectados à rede. As empresas começaram a utilizar dos mecanismos disponíveis no ambiente virtual para operar seus negócios e gerenciar seu pessoal, além de movimentar sua economia, realizar transações financeiras e armazenar seus dados sigilosos. Surgiram, ainda, os estabelecimentos especializados em prestar serviço de disponibilização de computadores com acesso à rede, como os cybercafés. Essa inclusão em massa dos mecanismos on-line no cotidiano das pessoas levou ao aumento significativo dos crimes cometidos pela internet.

Com o aumento dos casos de delitos praticados pela internet, a importância desse novo segmento da criminalidade foi evidenciada. Com estudos criminológicos mais aprofundados na área, passou-se a diferenciar as pessoas que possuem grande expertise no assunto conforme a finalidade que dão ao uso desses seus conhecimentos. Distinguiu-se, então, duas terminologias aplicáveis, quais sejam: Hackers e Crackers[20].

---

[18] ANDRADE, Mariah Dourado de; BENTES, Dorinethe dos Santos; GUIMARAES, David Franklin da Silva. **Considerações sobre a aplicabilidade do direito penal acerca dos crimes virtuais.** Revista Vertentes do Direito. Disponível em <https://sistemas.uft.edu.br/periodicos/index.php/direito/article/view/4171#:~:text=O%20presente%20artigo%20busca%20compreender,Leis%20Penais%20regulando%20esse%20crime.>. Acesso em 14 de agosto de 2020.

[19] SOUZA, Henry Leones De. VOLPE, Luiz Fernando Cassilhas. **Da ausência de legislação específica para os crimes virtuais.** Disponível em <https://egov.ufsc.br/portal/conteudo/da-aus%C3%AAncia-de-legisla%C3%A7%C3%A3o-espec%C3%ADfica-para-os-crimes-virtuais>. Acesso em 16 de agosto de 2020.

[20] NASCIMENTO, Samir de Paula. **Cibercrime: conceitos, modalidades e aspectos jurídicos-penais.** Disponível em < https://ambitojuridico.com.br/cadernos/internet-e-informatica/cibercrime-conceitos-modalidades-e-aspectos-juridicos-penais/>. Acesso em 16 de agosto de 2020.

Hacker, é a terminologia em inglês destinada a identificar as pessoas que possuem extremo conhecimento na área de tecnologia da informação e tecnologia da comunicação, voltando-se ao estudo e pesquisas de códigos de programação dos mais complexos softwares existentes. Essas pessoas utilizam do seu amplo conhecimento para identificar e resolver falhas nos sistemas, visando o aperfeiçoamento dos mesmos. Muitos desses indivíduos são profissionais na área, sendo contratados para isso.

De forma diametralmente oposta, os Crackers são indivíduos que também possuem grande conhecimento nas áreas de tecnologia da informação e tecnologia da comunicação, contudo, utilizam do seu vasto conhecimento para fins ilícitos, agindo de forma contrária à prevista em lei, criando e aperfeiçoando novos métodos criminosos, valendo-se do anonimato para tal e visando a obtenção de proveito pessoal de qualquer natureza. Pode-se utilizar ainda as denominações "Ciberpiratas" ou "Black Hat" para referir-se a esses criminosos. Os Crackers deram início ao uso do computador para fins ilícitos, criando uma nova modalidade de crimes.

A medida em que o computador deixou de ser apenas um meio de trabalho estático, assumindo uma posição altamente dinâmica na sociedade, as ameaças oriundas desse ambiente virtual passaram a chamar atenção e fazer jus à preocupação estatal, devendo ser criada e constantemente atualizada a adequada e obrigatória legislação contra os crimes virtuais.

Nesse sentido, vale lembrar, que os Estados Unidos, precursor no ramo da computação e criador da internet, foi o primeiro país a dar a devida importância para essas ameaças tecnológicas, tipificando pela primeira vez em 1978 crimes dessa natureza[21].

Apesar de a internet ser um instrumento que comporta e auxilia os mais diversos ramos e atividades da vida em sociedade, estima-se que os usuários comuns tenham acesso apenas à 0,18% da rede mundial de computadores, o que é chamado de Surface Web. Os outros 99,82% restantes estão inacessíveis para a maioria das pessoas.[22]

A Surface Web é a parte acessível da internet, aonde estão todas as funcionalidades que conhecemos. Essa região pode ser acessada através dos mecanismos de busca padrão. Contudo, conforme os dados acima demonstrados, apesar de conter

---

[21] SOUZA, Henry Leones De. VOLPE, Luiz Fernando Cassilhas. **Da ausência de legislação específica para os crimes virtuais.** Disponível em <https://egov.ufsc.br/portal/conteudo/da-aus%C3%AAncia-de-legisla%C3%A7%C3%A3o-espec%C3%ADfica-para-os-crimes-virtuais>. Acesso em 16 de agosto de 2020.

[22] ESTRADA, Manuel Martin Pino. **Delitos na Web: à espera do marco civil da internet.** Revista Jurídica Consulex. Brasília. Ano XVII. n. 405. p. 36. 1 de dezembro/2013.

bilhões de páginas e instrumentos disponíveis aos usuários, essa parte da internet está muito aquém do seu verdadeiro tamanho.

A parte da internet criptografada tem o nome de Deep Web, essa região profunda da internet corresponde a mais de 90% do seu real espaço e é inacessível à maioria dos usuários, utilizando de criptografia de ponta para manter seu sigilo e o anonimato de quem a utiliza. Para conseguir acesso à Deep Web, é necessário a utilização de links diretos que possam levar a determinados fóruns de discussão, evitando o rastreamento padrão dos demais sites[23].

A criptografia utilizada na Deep Web faz com que a navegação não deixe rastros e os usuários ali presentes não possam ser identificados. Apesar disso, o acesso a essa parte oculta da internet não é proibido no Brasil, devendo-se analisar, contudo, a atividade ali praticada, já que esta sim pode ser ilegal[24].

Dentro do universo da Deep Web, encontra-se a Dark Web. Esta parte da internet é pouco conhecida e possui níveis altíssimos de dificuldade de acesso, que vão muito além da própria Deep Web.[25] Os navegadores padrões não conseguem acessar essa parte remota e secreta que existe na rede mundial de computadores. Além de que, para um usuário integrar o grupo criminoso que consegue acessar esse ambiente, ele precisará preencher diversos requisitos para ganhar a confiança dos outros usuários delinquentes, o que torna o acesso quase impossível.

Os altos níveis de proteção que são empregados para dificultar o acesso à Dark Web se justificam pelo conteúdo ali existente, além do tipo de atividades que são praticadas pelos seus usuários. Nesse ambiente, criam-se diversos fóruns para discussão, planejamento e execução dos mais variados tipos de crimes, em sua maioria absurdamente violentos e cruéis.

Apesar do atual conhecimento sobre essas atividades criminosas e da indispensabilidade e urgência do combate à tais práticas, os Estados soberanos não conseguem reprimir com eficiência esses crimes. Essa insuficiência das esferas do Poder Público em todo mundo se dá pela volatilidade da Internet, pelo anonimato de que se

---

[23] NASCIMENTO, Samir de Paula. **Cibercrime: conceitos, modalidades e aspectos jurídicos-penais.** Disponível em < https://ambitojuridico.com.br/cadernos/internet-e-informatica/cibercrime-conceitos-modalidades-e-aspectos-juridicos-penais/>. Acesso em 16 de agosto de 2020.

[24] NASCIMENTO, Samir de Paula. **Cibercrime: conceitos, modalidades e aspectos jurídicos-penais.** Disponível em < https://ambitojuridico.com.br/cadernos/internet-e-informatica/cibercrime-conceitos-modalidades-e-aspectos-juridicos-penais/>. Acesso em 16 de agosto de 2020.

[25] BARRETO, Alesandro Gonçalves. SANTOS, Hericson dos. **Deep Web: investigação no submundo da internet.** 1. Ed. Rio de Janeiro: Editora Brasport, 2019. p. 12.

valem os criminosos nesse ambiente e pela rapidez em que ocorrem os avanços tecnológicos.

1.2 ESPÉCIES DE CRIMES INFORMÁTICOS

A internet propiciou um novo lócus de cometimento de crimes. Com a facilidade de uso, a volatilidade dos dados e a acessibilidade em qualquer lugar do mundo, além do aparente anonimato dos usuários, essa rede informática que se modifica diariamente desestabilizou fronteiras e dificultou a atividade de persecução dos órgãos oficiais de controle e repressão.

Ainda hoje não há uma clara definição do que sejam crimes informáticos, visto que novos delitos e tipos de condutas surgem constantemente. Ademais, a internet pode ser tanto a ferramenta utilizada para a pratica da infração penal, quanto o próprio bem jurídico ofendido no delito perpetrado.

> Os crimes virtuais são todas as condutas típicas, antijurídicas e culpáveis praticadas com a utilização de computadores ou qualquer outro sistema de informática, sendo estes diversos e tendo como classificação mais aceita a distinção entre crimes cibernéticos puros/próprios ou impuros/impróprios, tendo o autor do crime como o agente ativo, popularmente conhecido como hacker ou cracker, e qualquer pessoa física ou jurídica ou uma entidade titular, pública ou privada, que sofra a ação ou sobre quem recaiu tal ação é o agente passivo do crime. [26]

Nos dias que correm, classificou-se esses delitos em dois grupos, quais sejam: crimes informáticos próprios e crimes informáticos impróprios.

1.2.1 CRIMES INFORMÁTICOS IMPRÓPRIOS

Os crimes virtuais impróprios, impuros ou virtuais comuns são os delitos comuns cometidos por meio de sistema de dados informatizados. Nessa categoria de cibercrimes, os meios digitais são utilizados como instrumento delitivo. Delitos informáticos dessa natureza se dão nos moldes de crimes já previstos na legislação.

O cometimento desses tipos delitivos não requer grandes conhecimentos técnicos especializados sobre computadores e infiltração de sistemas de dados. O bem

---

[26] WENDT, Emerson. JORGE, Higor Vinicius Nogueira. **Crimes Cibernéticos: ameaças e procedimentos de investigação.** 1. Ed. São Paulo: Editora Brasport, 2012. p. 65.

juridicamente protegido nesses casos não é a inviolabilidade da informação automatizada de dados, senão bens jurídicos diversos, tradicionais, já tipificados para punir ações atentatórias realizadas cotidianamente.

Quando a conduta do agente se amolda aos tipos de crimes virtuais impuros, essa ação lesiona, por intermédio de um computador, outros bens jurídicos, diversos dos informáticos, visando atingir o resultado naturalístico pretendido.

A maioria dos cibercrimes é impróprio, consistentes em realizar práticas ilícitas com o auxílio de um instrumento tecnológico, atingindo o meio jurídico já tipificado, praticando condutas já conhecidas, mas com *modos operandi* completamente inovador. Apesar de usarem a web como instrumento e, até, local de consumação desses delitos, os mesmos não permanecem necessariamente apenas no âmbito virtual, vindo a se exteriorizar e dar continuidade no mundo naturalístico. A exemplo disso temos o tráfico de drogas online e a promoção da pedofilia.

Conclui-se que, nessa classificação de ciberdelitos, o computador e a internet são utilizados como meio, instrumento, para realização de condutas ilícitas clássicas, a exemplo dos crimes contra a honra, contra o patrimônio e de falsa identidade, todos tipificados no Código Penal; pedofilia e pornografia infantil, tipificados no Estatuto da criança e do adolescente; crimes de racismo e terrorismo, punidos por legislação própria; dentre outros tantos.

De acordo com Damásio de Jesus:

> (...) Já os crimes eletrônicos impuros ou impróprios são aqueles em que o agente se vale do computador como meio para produzir resultado naturalístico, que ofenda o mundo físico ou o espaço 'real', ameaçando ou lesando outros bens, não-computacionais ou diversos da informática.[27]

Não obstante tais bens jurídicos visados no cometimento desses tipos de crimes já estarem protegidos no ordenamento, com as respectivas condutas atentatórias tipificadas, não se exclui a necessidade de também os delitos clássicos, quando praticados por instrumentos informáticos, a partir do espaço virtual, receberem tipificação própria e

[27]JESUS, Damásio De. ARAS, Vladmir. **Crimes de informática: Uma nova criminalidade**. Disponível em <https://jus.com.br/artigos/2250/crimes-de-informatica>. Acesso em 17 de agosto de 2020.

adequada às suas peculiaridades, visando garantir um efetivo exercício da jurisdição, limitando a necessidade do emprego de analogias para enquadrar essas condutas.

1.2.2 CRIMES INFORMÁTICOS PRÓPRIOS

De forma diversa dos delitos informáticos impróprios, cuja existência precede à revolução informática produzida pelos sistemas de dados e pelas respectivas conexões em rede, temos os delitos informáticos próprios ou puros, que nasceram através da informatização dos dados, constituindo crimes específicos dessa seara. Por sua individualidade, essa modalidade de crime virtual exige, ao contrário da primeira modalidade, conhecimentos técnicos especiais e avançados na área da computação e informação de dados, para que possam ser realizados.

Aqui, o ataque operado pela ação criminosa opera-se contra o próprio sistema de dados, atingindo-o quanto à privacidade e inviolabilidade das informações, à acessibilidade e disponibilidade e à veracidade das mesmas, lesando de forma ampla a seguridade informática.

Os delitos cibernéticos puros são mais raros, na medida em que requerem, obrigatoriamente, o uso do sistema informático não apenas como meio para a realização do crime, mas como o próprio objeto material visado com a conduta delituosa.

Inevitavelmente, nessas ações ocorrerão agressões diretas ao software do computador da vítima, propiciando o acesso à dados não autorizados, bem como à senhas e documentos, permitindo a alteração, inclusão e destruição dessas informações.

Como leciona o mestre Damásio de Jesus:

> Crimes eletrônicos puros ou próprios são aqueles que sejam praticados por computador e se realizem ou se consumem também em meio eletrônico. Neles, a informática (segurança dos sistemas, titularidade das informações e integridade dos dados, da máquina e periféricos) é o objeto jurídico tutelado. [28]

Os crimes informáticos puros constituem uma nova modalidade de crime, que crescem na medida em que a internet evolui e se expande. Diante da novidade do tema, e das alterações constantes dos meios informatizados, a legislação não consegue

[28] JESUS, Damásio De. ARAS, Vladmir. **Crimes de informática: Uma nova criminalidade**. Disponível em <https://jus.com.br/artigos/2250/crimes-de-informatica>. Acesso em 17 de agosto de 2020.

acompanhar a celeridade com que novas condutas lesivas surgem no ambiente virtual. Nesse cenário, diante da falta de legislação específica e completa para regulamentar o tema e punir tais atitudes lesivas, existem condutas que, apesar de causarem danos irreversíveis às vítimas, ainda são tidas como atípicas, não podendo ser punidas em decorrência do princípio da legalidade ou reserva legal que norteia de forma imperiosa o ordenamento jurídico brasileiro, especialmente em matéria penal.

Isso posto, nota-se que a doutrina especializada classifica os crimes virtuais de acordo com sua finalidade. Assim sendo, crimes virtuais impróprios são os cometidos por meio do sistema informático de dados. Em contrapartida, crimes virtuais próprios são os cometidos contra o sistema informático de dados.

Nesse aspecto, cumpre lembrar que não raras as vezes as modalidades de cibercrimes acima descritos, assim como os tipos penais relativos às atividades lesivas praticadas, irão se sobrepor, causando um concurso aparente de infrações penais. À vista disso, o direito penal brasileiro invoca as regras do concurso aparente de normas, previsto na parte geral do código penal brasileiro, para resolver, também aqui, essas questões de sobreposição de incidências penais. Rememorando que tais critérios se fundamentam na análise dos princípios da subsidiariedade; especialidade; consunção e alternatividade.

Atenta-se ao fato de que os delitos cibernéticos puros são caracterizados pela melhor doutrina brasileira como crimes formais, de consumação antecipada ou resultado cortado, na medida em que sua consumação se realiza no momento da prática da conduta criminosa, pouco importando a ocorrência do resultado no mundo naturalístico.[29]

A maioria dos criminosos virtuais é encorajada pela sensação de impunidade que a internet gera. Contudo, sejam nos crimes virtuais próprios ou impróprios, a maioria das utilizações da rede mundial de computadores deixa rastros, que, às vezes, chegam a ser maiores até do que nos crimes cometidos presencialmente. Esses vestígios deixados pelos criminosos constituem as informações que ficam registradas no acesso às redes de computadores, incluindo os dados de *Internet Protocol* (IP), que é o número identificador que o aparelho ou roteador de internet recebe ao se conectar à rede, além de sua localização e os dados cadastrais do usuário.

---

[29] SANTOS, Elaine Gomes dos. RIBEIRO, Raisa Duarte da Silva. **Restrições à liberdade de expressão e crimes cibernéticos: a tutela penal do discurso de ódio nas redes sociais.** Revista dos Tribunais. vol. 997. ano 107. p. 527. São Paulo: Editora RT. novembro 2018.

1.3 DIFICULDADE DE INVESTIGAÇÃO E REPRESSÃO DOS CRIMES COMETIDOS PELA INTERNET

Analisando a história da humanidade, sabe-se que o progresso é inerente ao homem e que a sociedade caminha no sentido da evolução e inovação constantes, sempre buscando avanços. Não se pode ignorar, todavia, que até os avanços possuem seu lado negativo, momento em que alguns se beneficiam do desconhecimento do novo para praticar condutas lesivas à terceiros. Nessa esteira, surgem os crimes virtuais.

Tem-se que a internet é considerada o maior e mais benéfico instrumento já desenvolvido até hoje, em razão da sua multifuncionalidade e dos incontáveis benefícios que ela proporciona[30]. Com a constante evolução social, há a continua disseminação da internet e dos meios de acesso à mesma. Com as vantagens dessa expansão, surgiram também novas demandas, as quais o Direito precisou se adaptar para conseguir cumprir sua finalidade precípua, qual seja, a proteção dos bens juridicamente tutelados.

Com a criação e sucessiva inovação dos meios e recursos tecnológicos, despontaram na sociedade novas formas de difusão de ameaças, através de novos meios para o cometimento de crimes conhecidos e, também, o surgimento de novas modalidades de crimes antes inexistentes.

A rápida evolução da internet e seus inerentes meios de comunicação ensejaram o surgimento de um novo lócus da criminalidade, por meio da qual os criminosos se valem da vulnerabilidade dos sistemas e dos próprios usuários dessa rede para cometer inúmeros delitos. O rápido surgimento de novas modalidades criminosas, o dinamismo da tecnologia de informação, aliado ao anonimato que impera na rede, criou um grande problema para os operadores do direito no processo de investigação, punição e repressão dos crimes cibernéticos, uma vez que as normas jurídicas que direcionam a atuação estatal não conseguem acompanhar a velocidade com que esses delitos evoluem.

Na velocidade em que os avanços tecnológicos ocorrem, se dá, também, de forma proporcional, o crescimento dos crimes cometidos através da rede mundial de computadores, devido à especialização dos criminosos nessa área. Contudo, os agentes responsáveis por solucionar e punir essas práticas não conseguem acompanhar essa rápida

---

[30] CRUZ, Diego; RODRIGUES, Juliana. **Crimes cibernéticos e a falsa sensação de impunidade.** Revista científica eletrônica do curso de direito. 13ª Ed. Disponível em <http://faef.revista.inf.br/imagens_arquivos/arquivos_destaque/iegWxiOtVJB1t5C_2019-2-28-16-36-0.pdf >. Acesso em 20 de agosto de 2020.

e dinâmica evolução. Nessa linha, apesar do crescente número de vítimas desses delitos virtuais, ainda é ínfimo o número de pessoas punidas por cometer esses crimes[31].

Em 2014, a Organização dos Estados Americanos (OEA), em conjunto com a empresa de segurança cibernética Symantec, divulgaram um relatório[32] no qual constavam dados apontando para o alarmante fato de que o Brasil está dentre os principais países da América Latina que mais geraram atividades nocivas pela internet. Em contrapartida, ainda temos o menor número de denúncias e consequentes punições desses delitos.

Diversas vezes os sujeitos passivos dos crimes virtuais não comunicam a pratica desses delitos aos órgãos e autoridades competentes, por incredulidade da resposta estatal. Essa sensação de insegurança e impunidade, que leva as vítimas a não denunciarem, vêm do reduzido número de casos solucionados e efetivamente reprimidos. As dificuldades práticas encontradas na atuação dos órgãos estatais responsáveis pela investigação, identificação e punição desses crimes, tornam cada vez mais difíceis a contenção desses delitos e delinquentes, gerando a desconfiança da sociedade e a incredibilidade estatal. A consequência direta desse fenômeno é o que a criminologia crítica chama de cifra negra da criminalidade, que corresponde ao índice de subnotificação de crimes às autoridades estatais, ou seja, refere-se ao percentual de delitos não comunicados formalmente à polícia e que não integram os dados estatísticos oficiais. As cifras negras, ou ocultas, da criminalidade geram o aumento dos delitos.

Segundo Tadeu Rover para a revista Consultor Jurídico (CONJUR): "Em 2016, mais de 42 milhões de brasileiros foram vítimas de crimes virtuais. Um aumento de 10% se comparado com o ano anterior, de acordo com dados da Norton, empresa de soluções de segurança cibernética".[33]

---

[31] FROTA, Jéssica Olivia Dias; PAIVA, Maria de Fátima Sampaio. **Crimes virtuais e as dificuldades para combatê-los.** Disponível em <https://flucianofeijao.com.br/novo/wp-content/uploads/2018/11/ARTIGO_CRIMES_VIRTUAIS_E_AS_DIFICULDADES_PARA_COMBATE_LOS.pdf >. Acesso em 20 de agosto de 2020.

[32] Symantec; Organizações dos Estados Americanos. Relatório 'Tendências de Cibersegurança na América Latina e no Caribe". 2014. Disponível em <http://www.symantec.com/content/en/us/enterprise/other_resources/b-cyber-security-trends-report-lamc-annex.pdf >. Acesso em 22 de agosto de 2020.

[33] ROVER, Tadeu. **Violência virtual: internet facilita crimes e dificulta investigação, estimulando a impunidade**. Disponível em <https://www.conjur.com.br/2017-fev-05/entrevista-daniel-burg-especialista-crimes-virtuais>. Acesso em 22 de agosto de 2020.

São inúmeros os problemas e dificuldades encontrados na persecução penal visando o combate e punição dos cibercrimes. Desde a polícia; Ministério Público; poder judiciário; até os legisladores e demais operadores do direito, encontram barreiras à sua atuação, as quais dificultam o exercício do *jus puniendi* e impulsionam a criminalidade.

As tecnologias de informação são dotadas de dinamismo e volatilidade, motivo pelo qual os crimes cibernéticos encontram incontáveis formas de serem praticados. Iniciada a persecução penal, através da investigação do crime virtual cometido, imperiosa se faz a imediata identificação do meio pelo qual tal crime foi praticado.

Essa identificação se faz fundamental para nortear a ação do órgão investigativo, pois conforme o meio adotado pelo cibercriminoso para execução do crime, diferentes serão as técnicas utilizadas para obtenção da autoria e materialidade do delito.

As dificuldades encontradas se iniciam no fato de que impera, no ordenamento jurídico brasileiro, a necessidade da comprovação, lastreada com provas robustas, de autoria e materialidade do delito, para que a sanção penal possa ser aplicada.

Caso não consiga ser comprovada a materialidade e autoria o juiz deverá absolver o réu, conforme traz o artigo 386 do Decreto-lei nº 3.689, de 3 de outubro de 1941(Código de Processo Penal):

> Art. 386. O juiz absolverá o réu, mencionando a causa na parte dispositiva, desde que reconheça: I - Estar provada a inexistência do fato; II - Não haver prova da existência do fato; III - Não constituir o fato infração penal; IV - Estar provado que o réu não concorreu para a infração penal; V - Não existir prova de ter o réu concorrido para a infração penal; VI – existirem circunstâncias que excluam o crime ou isentem o réu de pena, ou mesmo se houver fundada dúvida sobre sua existência; VII – não existir prova suficiente para a condenação.

Além de indispensável a prova de autoria e materialidade delitiva, é necessário que essas provas sejam adquiridas de forma lícita, em estrita obediência ao disposto em lei, em subordinação à um dos princípios mais importantes do Direito Penal, assim dizendo, o princípio da legalidade.

A prova de autoria do delito é o primeiro problema a ser resolvido na investigação dos crimes virtuais, além de ser um dos mais complexos, visto que, além do inicial anonimato do usuário da rede, dificilmente o agente criminoso utilizou a sua real identidade quando do cometimento do cibercrime. Esses fatores são o que tornam o endereço de protocolo de internet uma das evidencias de maior relevo dentro da investigação nesse ambiente. Ainda assim, conseguir esses dados é um processo penoso,

visto que está rodeado de exigências legais que devem ser estritamente respeitadas para não contaminar a prova obtida e, consequentemente, as provas dela derivadas.

Muitas vezes, para se chegar na localização e identificação do autor dos crimes, uma série de direitos fundamentais será violada, a exemplo da privacidade da pessoa, garantida pela Constituição Federal. A quebra de sigilo de dados será um meio utilizado de forma recorrente para se obter esses dados, devendo ser respeitadas as regras processuais para tal. Em alguns casos, ainda será necessário que as provas obtidas sejam submetidas à rigorosa perícia técnica para que, só então, ingressem no processo sendo capaz de lastrear uma condenação.

Os logs e o endereço IP (*internet protocol*) são as evidencias de maior relevo a serem perseguidas na investigação dos crimes informáticos, além de serem as provas que irão nortear toda a investigação. Essas informações estarão acompanhadas do registro da data, horário e fuso horário da conexão, além do respectivo número de protocolo de internet atribuído àquele acesso[34].

Quando se fala em tecnologia de informática, tem-se que os logs consistem no processo pelo qual os eventos praticados em um determinado acesso são registrados no sistema computacional, os quais permitirão a verificação dos atos praticados naquela ocasião.

Já quando se trata dos endereços de IP, estamos nos referindo ao registro criado toda vez que uma conexão é feita. Esses endereços de protocolos de internet podem ser estáticos ou dinâmicos.

Os IPs estáticos são comumente utilizados por grandes corporações como os órgãos públicos, universidades e empresas de grande porte. Esse tipo de IP não tem variação, ou seja, àquele usuário sempre se dará o mesmo protocolo de internet, independente de quantas conexões à rede forem realizadas por ele.

Já aos outros usuários, será atribuído o IP dinâmico, o qual terá uma identificação diferente concedida por seu provedor de acesso toda vez que for estabelecida uma conexão com a internet.

---

[34] DORIGON, Alessandro; SOARES, Renan Vinicius de Oliveira. **Crimes cibernéticos: dificuldades investigativas na obtenção de indícios da autoria e prova da materialidade.** Disponível em < https://jus.com.br/artigos/63549/crimes-ciberneticos-dificuldades-investigativas-na-obtencao-de-indicios-da-autoria-e-prova-da-materialidade>. Acesso em 22 de agosto de 2020.

De qualquer forma, independentemente do tipo de protocolo de internet atribuído ao usuário, se dinâmico ou estático, nunca nenhum número de IP será atribuído a mais de um usuário na mesma data, horário e fuso horário.

Assim sendo, vislumbra-se outra dificuldade prática para acesso à essas informações, pois, após se conseguir o número do IP mediante ordem judicial, ainda será necessário, caso se trate de um protocolo de internet dinâmico, que se tenha conhecimento da data, horário e fuso horário de acesso desse determinado IP, para que se possa solicitar aos provedores de acesso as informações sobre a identidade desse usuário.

Deste modo será indispensável ordem judicial escrita e fundamentada emitida por autoridade judiciária competente, dirigida aos provedores de acesso à internet, que faça referência a três indicadores, quais sejam: o número de *internet protocol* (IP), a data do acesso à rede e o horário e fuso horário deste acesso. Sendo que, mesmo já se tendo obtido o número do protocolo de internet, a nova decisão judicial que não faça referência cumulativa aos três indicadores supracitados, não é capaz de autorizar a quebra de sigilo dos dados telemáticos.

Iniciando as investigações, quando da busca pela autoria da atividade delitiva, a polícia esbarra em seu primeiro obstáculo, qual seja o artigo 5º, incisos X e XII da Constituição Federal Brasileira de 1988, que protege a privacidade e os dados. Desta forma, respeitando tais direitos constitucionalmente assegurados, o acesso aos dados de *logs* e protocolos de internet só poderão ser requeridos das empresas responsáveis mediante autorização judicial fundamentada, o que, inevitavelmente, leva a uma demora prejudicial ao êxito das investigações.

Nesse contexto, cabe mencionar que a polícia, após ter o conhecimento do meio utilizado pelo agente para pratica do crime, deve localizar qual o responsável pela hospedagem dos dados em questão, realizando, assim, dentro dos casos e na forma autorizada em lei, requerimento à autoridade judiciária competente pedindo a quebra de sigilo dos dados. A mesma deverá, então, expedir ordem judicial direcionada à empresa responsável pelos dados telemáticos, quando, só então, a autoridade investigativa terá acesso aos logs e endereços de IP. As empresas prestadoras de internet e os sites eventualmente utilizados para cometimento dos crimes deverão, à vista da ordem judicial, remeter à autoridade policial cópia das páginas requeridas que tenham relação com o fato criminoso, bem como acesso aos *logs*, que são os registros de modificações do conteúdo dessa determinada página, e o número do protocolo de internet utilizado naquela conexão, com a respectiva data de acesso, horário e fuso horário do mesmo.

Após conseguir o acesso àqueles dados, a autoridade policial irá precisar de uma nova ordem judicial determinando a quebra dos dados telemáticos, dessa vez dirigida aos provedores de acesso à internet, para que estes franqueiem o conhecimento pelos investigadores quanto às informações do usuário vinculadas ao número do IP anteriormente obtido.

Todo esse procedimento previsto em lei, que deverá ser minuciosamente respeitado, sob pena de invalidar toda a prova obtida, gera uma significativa demora às investigações, o que pode proporcionar irreparáveis prejuízos.

Como se não bastasse toda morosidade intrínseca ao procedimento que deve ser adotado com a devida reserva jurisdicional, há, ainda, empresas que se recusam a prestar auxílio ao Poder Público, mesmo perante ordem judicial. A título de exemplo temos a empresa WhatsApp, que se recusou obedecer à ordem da justiça brasileira para que prestasse informações sobre usuários investigados em processo criminal. Tal recusa gerou decisão judicial de bloqueio da referida rede social em todo território nacional, por tempo limitado, o que, posteriormente, foi dito inconstitucional em decisão do Supremo Tribunal Federal.[35]

Na sessão da primeira audiência pública da Comissão Parlamentar de Inquérito dos Crimes Cibernéticos, que ocorreu no dia 20/08/2014, foi amplamente discutida as dificuldades práticas sofridas na investigação e repressão dos cibercrimes, ficando evidente a dificuldade em rastrear, identificar e punir tais criminosos virtuais[36]. Tais dificuldades se iniciam no fato de que a velocidade com que os crimes na internet são cometidos, assim como a facilidade com que os vestígios dessas práticas criminosas se perdem, são incompatíveis com a morosidade para se conseguir o acesso aos dados que são indispensáveis ao prosseguimento e êxito das investigações.

O, à época, chefe do Serviço de Repressão aos Crimes Cibernéticos da Policia Federal, Delegado Elmer Coelho Vicente, advertiu que a polícia lida com duas grandes dificuldades. A primeira é que a maioria das empresas responsáveis pelos sites e aplicativos, bem como os provedores de acesso à rede, não aceitam requisições da polícia

---

[35]Consultor Jurídico. **STF derruba decisão judicial e libera volta do WhatsApp.** Disponível em <https://www.conjur.com.br/2016-jul-19/stf-derruba-decisao-judicial-libera-volta-whatsapp#:~:text=Por%20identificar%20viola%C3%A7%C3%B5es%20%C3%A0s%20liberdades,feira%20(19%2F7)>. Acesso em 22 de agosto de 2020.

[36] CANUTO, Luiz Cláudio. **CPI constata dificuldade em rastrear e punir crimes de internet.** Disponível em < https://www.camara.leg.br/noticias/467819-cpi-constata-dificuldade-em-rastrear-e-punir-crimes-de-internet/>. Acesso em 22 de agosto de 2020.

pela internet, o que contribui para lentidão das investigações e, consequentemente, mais chance de sua ineficácia. A segunda dificuldade, por sua vez, está no fato de que, após o Marco Civil da Internet (Lei nº 12.965, de 23 de abril de 2014), as empresas exigem ordem judicial para conceder informações, não bastando mais requisições da autoridade policial para a maioria das situações[37].

Os sites e provedores de acesso à rede são os locais em que as informações sobre a utilização da plataforma são registradas e armazenadas. Contudo, tais informações não são, em sua maioria, armazenadas por um longo período de tempo[38]. Assim sendo, fica claro que a demora para se obter os dados e, então, prosseguir nas investigações, gera danos irreparáveis como, por exemplo, a perda total dessas informações, o que compromete o trabalho do agente combatente.

Além da perda desses dados devido ao seu descarte, após um período, pelos próprios provedores responsáveis, as evidências dos crimes cibernéticos são altamente voláteis o que possibilita serem facilmente apagadas ou alteradas pelos próprios usuários. Gerando, desta forma, a destruição ou, no mínimo, modificação das provas do crime.

A imprescindível reserva jurisdicional; a demora de todo o procedimento necessário para o devido acesso aos dados e provas do delito virtual; somada, por vezes, à não colaboração das empresas responsáveis pelo ambiente virtual em que foi cometido o crime, geram uma enorme lentidão das investigações, problema este que, não raras as vezes, levam à prescrição do delito, sem que, ao menos, se consiga avanços significativos na fase inquisitória.

Além da autoria do crime, outro elemento imprescindível para uma condenação criminal, é a prova da materialidade delitiva. Após, seguidos todos os tramites legais, ser possível a identificação do criminoso através dos dados e informações fornecidos pelos sites e provedores de acesso, a investigação se dedicará à busca por provas da materialidade do crime virtual cometido pelo agente. Tendo isso em vista, a autoridade policial poderá requerer ao juiz competente que o mesmo expeça mandado de busca e apreensão em desfavor dos envolvidos no crime, para que, então, se possa apreender o

---

[37] CANUTO, Luiz Cláudio. **CPI constata dificuldade em rastrear e punir crimes de internet.** Disponível em < https://www.camara.leg.br/noticias/467819-cpi-constata-dificuldade-em-rastrear-e-punir-crimes-de-internet/>. Acesso em 22 de agosto de 2020.

[38] FROTA, Jéssica Olivia Dias; PAIVA, Maria de Fátima Sampaio. **Crimes virtuais e as dificuldades para combatê-los.** Disponível em <https://flucianofeijao.com.br/novo/wp-content/uploads/2018/11/ARTIGO_CRIMES_VIRTUAIS_E_AS_DIFICULDADES_PARA_COMBATE_LOS.pdf >. Acesso em 22 de agosto de 2020.

computador, equipamentos informáticos e demais documentos que possam servir à elucidação e prova do delito em análise.

Por vezes, será fundamental a realização de perícia técnica para produção de prova criminal hábil a lastrear uma condenação. Para que tal perícia possa ser realizada, na maioria das vezes, o perito precisará dispor do computador ou outro equipamento informático que seja objeto da análise. Contudo, novamente aqui, será fundamental o respeito à reserva jurisdicional, ou seja, será necessária autorização judicial por meio de mandado de busca e apreensão para que se consiga a máquina que será objeto da prova técnica.

Todo procedimento para se chegar à apreensão dos objetos necessários à prova causará uma incontestável demora, a qual poderá criar um ambiente propício para destruição dos equipamentos ou dos dados nele armazenados, desaparecendo as evidências que se busca.

Continuando discorrendo sobre os problemas encontrados quando o assunto são os crimes virtuais, chegamos ao *cloud computing*, ou computação nas nuvens, que se trata de um serviço disponível aos usuários da rede mundial de computadores por meio do qual o acesso e execução de arquivos e programas é realizado exclusivamente através da internet, ou seja, os dados visados pelo usuário não precisam estar em seu aparelho, o que permite a execução de diversas atividades sem que os arquivos estejam em seu computador ou qualquer outro equipamento informático utilizado, bastando apenas que se acesse a internet para tal, pois é "nas nuvens" que todos os arquivos e dados utilizados para essa atividade estão armazenados.[39]

Nesse tipo de acesso, qualquer arquivo e programa utilizado não estará vinculado ao computador do usuário, mas sim em servidores on-line que são criados exclusivamente para servir como hospedeiros, permitindo que os usuários desse serviço tenham acesso às informações ali contidas a qualquer tempo, em qualquer lugar e utilizando de qualquer equipamento conectado à rede.

A "nuvem", ou seja, o computador que hospeda de fato os arquivos, pode estar localizado em qualquer lugar do mundo. Assim sendo, o usuário pode estar no Brasil e

[39] DORIGON, Alessandro; SOARES, Renan Vinicius de Oliveira. **Crimes cibernéticos: dificuldades investigativas na obtenção de indícios da autoria e prova da materialidade.** Disponível em < https://jus.com.br/artigos/63549/crimes-ciberneticos-dificuldades-investigativas-na-obtencao-de-indicios-da-autoria-e-prova-da-materialidade>. Acesso em 22 de agosto de 2020.

acessar remotamente arquivos que estão armazenados em uma máquina localizada em qualquer outro país, não importando a distância.

Por óbvio, se sabe que esse tipo de serviço possui incontestáveis benefícios aos usuários, desde sua praticidade até a segurança dos dados ali armazenados. Entretanto, o *cloud computing* ocupa um lugar de destaque nas dificuldades para elucidação e punição dos cibercrimes, visto que é improvável, na maioria dos casos, que se consiga apreender um computador localizado em outro país. Isto pode inviabilizar, ou até mesmo tornar impossível, que se obtenha a prova da materialidade do delito.

A internet transcende fronteiras, liga usuários localizados em diferentes partes do mundo, permite a comunicação e troca de arquivos sem se preocupar com a distância física em que as pessoas estão. Por conseguinte, os crimes realizados por meio da internet adquiriram, também, essa característica. Os cibercrimes possibilitam que qualquer ameaça seja globalizada, tornando possível danos às vítimas que estão a qualquer distância imaginável dos autores do crime, bem como o concurso de agentes localizados em diferentes países. Isso se tornou possível através do uso dos recursos tecnológicos avançados, que permitem a preparação e execução de tais crimes mesmo a longas distancias.

A consumação de um crime praticado pela internet ocorre em todos os lugares do mundo em que essa conduta lesiva tenha se dado. Neste ponto se iniciam diversos problemas de competência e de conflito de normas. Dessarte, devido à natureza transnacional da internet e, consequentemente, dos delitos cometidos nela, se mostra urgente que haja cooperação internacional entre os Estados soberanos, para melhor interligar seus órgãos judiciários e investigativos quanto aos crimes informáticos que assolam às nações nos dias de hoje.

Toda mudança tecnológica vem acompanhada de uma evidente mudança cultural. Neste diapasão, o direito é diretamente influenciado por tais mudanças e tem o dever de se adaptar à nova realidade social. Levando em consideração o preconizado pelo artigo 5º, inciso XXXIX, da Constituição Federal Brasileira de 1988, que versa em sua melhor redação que "não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal", estabelecendo, assim, como direito fundamental inerente aos cidadãos o princípio da legalidade, imperioso se faz lembrar que é de extrema importância que o legislador brasileiro se debruce sobre as novas ameaças decorrentes do processo de inovação tecnológica, visando criar normas penais e processuais que englobem toda a problemática relativa aos cibercrimes, não deixando lacunas sobre o tema.

Nesse assunto, chegamos a mais uma dificuldade existente quando tratamos sobre os novos meios criminosos relativos à internet, qual seja, a falta de legislação adequada.

Respeitando o princípio da legalidade e as normas processuais para obtenção de provas, os operadores do direito em geral, com ênfase nos que atuam na fase investigativa, tropeçam na falta de normas aplicáveis aos casos de crimes virtuais em todas suas vertentes. A legislação brasileira sobre essa temática é, em sua esmagadora maioria, inexistente. Quando existe, contudo, contém falta de técnica legislativa adequada, dando margem a interpretações dúbias, dificultando sua aplicabilidade.[40]

O processo legislativo brasileiro, quando tenta ir ao encontro dessa problemática, visando criar normas que, de fato, consigam coibi-las, tipificando os crimes que estão surgindo e tentando facilitar as investigações dos mesmos, não consegue acompanhar a velocidade com que os meios informáticos, e as consequentes práticas criminosas relacionadas a eles, evoluem e se aperfeiçoam.

Não podemos nos enganar afirmando que a problemática está concentrada na falta de criação de tipos penais exclusivos aos crimes cibernéticos, pois, em sua excelência, o objeto material do crime virtual já é tutelado penalmente. A dificuldade se concentra em normas relativas ao procedimento cabível para apuração desses crimes, que devem levar em conta as peculiaridades do meio pelo qual tais delitos foram praticados.

Saindo da problemática diretamente relacionada com a internet, mas ainda se debruçando sobre as dificuldades práticas encontradas no combate aos crimes virtuais, chegamos aos problemas estatais, iniciando pela falta de efetivo nos órgãos investigativos. A deficiência de investimentos nos órgãos policiais está presente em diversos aspectos, contudo, um dos mais prejudiciais é a falta de pessoal atuante nessa área. A notável escassez de policiais e peritos operantes na investigação de condutas delituosas virtuais, gera um acumulo de *notitia criminis,* sendo que essa demanda não consegue ser suprida pela ainda pequena quantidade de agentes estatais.[41] Nesta linha, conclui-se que se há falta de efetivo para investigar o todo, maior será ainda a dificuldade de se colocar pessoal especializado para atender apenas a demanda de crimes praticados

---

[40] DORIGON, Alessandro; SOARES, Renan Vinicius de Oliveira. **Crimes cibernéticos: dificuldades investigativas na obtenção de indícios da autoria e prova da materialidade.** Disponível em < https://jus.com.br/artigos/63549/crimes-ciberneticos-dificuldades-investigativas-na-obtencao-de-indicios-da-autoria-e-prova-da-materialidade>. Acesso em 22 de agosto de 2020.

[41] CRUZ, Diego; RODRIGUES, Juliana. **Crimes cibernéticos e a falsa sensação de impunidade.** Revista científica eletrônica do curso de direito. 13ª Ed. Disponível em <http://faef.revista.inf.br/imagens_arquivos/arquivos_destaque/iegWxiOtVJB1t5C_2019-2-28-16-36-0.pdf >. Acesso em 22 de agosto de 2020.

pela internet. O volume de investigações cresce paralelamente ao número de crimes praticados pela internet. Com isso, o efetivo das policias judiciárias e dos órgãos de perícia técnica precisam crescer na mesma proporção, para que se consiga maior êxito na repressão e investigação desses crimes.

Continuando nessa linha, devemos analisar ainda que o problema que se inicia com a falta de efetivo, se torna ainda maior quando analisamos a falta de capacitação técnica adequada do pessoal desses órgãos. As tecnologias de informação e comunicação possuem extrema complexidade e dinamismo, o que, em contrapartida, faz com que os órgãos legislativos, investigativos e judiciários não estejam adequadamente preparados e capacitados para lidar com essa nova criminalidade.[42]

As evidências deixadas pelos crimes virtuais são extremamente instáveis e, como já visto, podem ser facilmente perdidas, apagadas ou alteradas, em razão da sua volatilidade. Em virtude dessa característica dos cibercrimes, se faz necessário e imperioso que os agentes investigadores tenham cautela e conhecimento adequado para buscar e manusear tais dados, evitando-se que se corrompa as evidências e provas do crime informático.

A complexidade que envolve os dados na internet exige capacidade técnica adequada de quem irá perseguir as provas de um crime nesse meio, para garantir que ocorra a correta coleta e compreensão das evidências dos crimes desta natureza. Para isso, tem-se evidente o dever do Poder Público em investir na constante capacitação de seus agentes direcionados para essa área de atuação.

É fundamental também evidenciar a importância de se despender recursos para a criação de setores especializados em crimes virtuais dentro dos órgãos estatais, em especial na polícia judiciária e no poder judiciário. A criação de delegacias especializadas no combate aos crimes cibernéticos, bem como de varas nos tribunais especializadas nessa área, geraria um aperfeiçoamento do Estado para lidar com essa nova e crescente modalidade criminosa, além de conseguir tentar acompanhar sua constante e veloz mudança e evolução.

Entretanto, não é apenas a capacitação e qualificação técnicas dos agentes estatais que prejudica o processo de punição dos crimes cometidos pela internet, vez que mesmo

---

[42] DORIGON, Alessandro; SOARES, Renan Vinicius de Oliveira. **Crimes cibernéticos: dificuldades investigativas na obtenção de indícios da autoria e prova da materialidade.** Disponível em < https://jus.com.br/artigos/63549/crimes-ciberneticos-dificuldades-investigativas-na-obtencao-de-indicios-da-autoria-e-prova-da-materialidade>. Acesso em 22 de agosto de 2020.

quando o profissional possui o conhecimento que a complexidade das circunstancias exige, na generalidade dos casos o trabalho investigativo é frenado pela falta de equipamentos e meios técnicos adequados, inviabilizando as investigações dos crimes virtuais. Essa falta de meios essenciais à repressão de tais delitos, caracteriza uma flagrante falha do Estado, em seu sentido amplo.

Por conseguinte, o problema vislumbrado quanto aos crimes cibernéticos tem grande parte concentrada na falta de efetivo, no descaso com a qualificação e especialização dos agentes estatais e na escassez de tecnologia adequada. Desde a implementação da internet no território nacional, não houve investimentos e qualificação suficiente visando o combate das novas modalidades de crimes que já vinham sendo praticados nos países em que originalmente a internet se implementou.[43] A falta de meios adequados para perseguir esses delitos impulsiona o crescimento da criminalidade virtual.

Após discorrer sobre diversos problemas encontrados quando tratamos da investigação e do processo criminal por crimes virtuais, chegamos a maior adversidade neste tema, que impulsiona o crescimento destes tipos de delitos e é a principal causa da impunidade dos cibercriminosos, o anonimato.

A internet se tornou um ambiente altamente atrativo à prática de crimes devido à suas características, como a facilidade do cometimento desses atos; a volatilidade dos dados ali gerados; a possibilidade de perpetrar o ilícito penal em qualquer lugar que se encontre o agente ou a vítima; a sensação de anonimato e a aparente ausência de vigilância, o que impulsionam o cometimento de crimes nessas circunstâncias.

Como já exposto, em regra, a autoridade policial no bojo da investigação criminal, e com a indispensável autorização judicial de quebra de sigilo dos dados telemáticos, terá acesso aos *logs* e endereços de IP utilizados na conduta criminosa e, após isso, conseguiria a localização e identificação dos agentes delinquentes. Contudo, há diversas maneiras de fraudar esse tipo de evidência, tais como a utilização de servidores proxies, redes Wi-Fi abertas ou utilização de locais que comercializam o acesso à internet, conhecidos como Lan Houses e Cybercafés.

Os proxies são servidores que atuam como intermediários, solicitando, para seus clientes, recursos ou serviços de outros servidores. Desta forma, os proxies agem como

---

[43] CRUZ, Diego; RODRIGUES, Juliana. **Crimes cibernéticos e a falsa sensação de impunidade.** Revista científica eletrônica do curso de direito. 13ª Ed. Disponível em <http://faef.revista.inf.br/imagens_arquivos/arquivos_destaque/iegWxiOtVJB1t5C_2019-2-28-16-36-0.pdf >. Acesso em 22 de agosto de 2020.

uma “ponte” entre o usuário do serviço e o conteúdo acessado por este usuário na internet. Uma vez utilizado este recurso, o endereço de *internet protocol* que constará no banco de dados do site ou do provedor de acesso à rede será o do servidor proxy, e não o do usuário que efetivamente acessou àquela página da internet.[44]

Os servidores proxies, assim como a maioria das ferramentas na internet, foram criados visando a proteção dos usuários. Sua finalidade inicial era a de esconder o endereço de IP dos usuários para protegê-los de ameaças na rede ou evitar o furto de dados. Porém, esse tipo de ferramenta começou a ser utilizada para práticas maliciosas. A partir disso, começaram a ser criados servidores proxies destinados exclusivamente para fins ilícitos, visando justamente esconder a real identificação de seus usuários para dificultar a investigação dos crimes praticados por eles, obtendo, por conseguinte, a impunidade do criminoso.

Essa modalidade é denominada de proxy anônimo, sendo uma ferramenta muito utilizada para evitar que as atividades praticadas na internet deixem vestígios. Acessando a internet em favor do usuário, ocultando suas informações pessoais que poderiam o identificar, esses servidores garantem que haja o anonimato sobre o computador ou equipamento informático que deu origem ao evento na internet, ou sobre quem praticou as condutas lesivas na rede[45].

Há, ainda, a possibilidade de o usuário garantir que não haverá a sua identificação, por meio da utilização de uma cadeia de diferentes proxies. Desta forma, se houver alguma falha em um dos proxies da cadeia, os demais irão trabalhar para garantir que as informações do usuário fiquem ocultas, de forma que não haja falhas no processo de anonimato do sujeito que está utilizando esta ferramenta, assegurando que será, de fato, impossível rastrear o número de protocolo de internet da pessoa que fez o acesso.

As redes Wi-Fi abertas, por sua vez, consistem nos mais diversos tipos de locais que dão acesso gratuito à internet e podem ser conectados por qualquer pessoa, a qualquer momento e utilizando-se de qualquer tipo de dispositivo informático que permita acesso

---

[44] DORIGON, Alessandro; SOARES, Renan Vinicius de Oliveira. **Crimes cibernéticos: dificuldades investigativas na obtenção de indícios da autoria e prova da materialidade.** Disponível em < https://jus.com.br/artigos/63549/crimes-ciberneticos-dificuldades-investigativas-na-obtencao-de-indicios-da-autoria-e-prova-da-materialidade>. Acesso em 22 de agosto de 2020.

[45] DORIGON, Alessandro; SOARES, Renan Vinicius de Oliveira. **Crimes cibernéticos: dificuldades investigativas na obtenção de indícios da autoria e prova da materialidade.** Disponível em < https://jus.com.br/artigos/63549/crimes-ciberneticos-dificuldades-investigativas-na-obtencao-de-indicios-da-autoria-e-prova-da-materialidade>. Acesso em 22 de agosto de 2020.

à rede mundial de computadores[46]. Devido a sua finalidade de servir ao público em geral, esses tipos de conexões, frequentemente, não exigem nenhum cadastro ou identificação dos usuários que dela irão dispor, gerando aos cibercriminosos um ambiente favorável à pratica delitiva, pois a identificação e localização do responsável pelo acesso que deu origem à atividade lesiva será quase impossível, proporcionando maiores chances de impunidade.

Com a popularização da internet, diversas redes de comercialização de acesso virtual surgiram. Essa praticidade de se acessar à internet em qualquer local gerou uma nova dificuldade para identificar autores dos crimes virtuais, visto que, geralmente, não há o devido registro dos usuários que utilizam desses serviços de acesso à rede mundial de computadores que é disponibilizado nas Lan Houses e nos Cybercafés.

Cabe lembrar, ainda, que nos poucos casos em que essas empresas prestadoras desses tipos de serviços exigem o cadastro do cliente para que este possa realizar o acesso, o uso de documentos falsos é um meio muito utilizado para burlar esse precário controle.

Esses tipos de locais servem como um espaço favorável aos criminosos virtuais, o que dificulta que seja possível obter a autoria dos crimes cibernéticos ali perpetrados, já que tais estabelecimentos são abertos ao público, podendo ser utilizados por qualquer pessoa.

[46] DORIGON, Alessandro; SOARES, Renan Vinicius de Oliveira. **Crimes cibernéticos: dificuldades investigativas na obtenção de indícios da autoria e prova da materialidade.** Disponível em < https://jus.com.br/artigos/63549/crimes-ciberneticos-dificuldades-investigativas-na-obtencao-de-indicios-da-autoria-e-prova-da-materialidade>. Acesso em 22 de agosto de 2020.

2. OBRIGATORIEDADE DO ARMAZENAMENTO DOS REGISTROS DE ACESSO DOS USUÁRIOS NA REDE MUNDIAL DE COMPUTADORES

2.1 ANONIMATO COMO EXCEÇÃO NA INTERNET

2.1.1 O PANOPTISMO DE FOUCAULT E A EXPOSIÇÃO NA INTERNET

Não há como dissociar os acontecimentos na internet dos resultados no mundo concreto que eles causam. O mundo virtual deve ser tido como prolongamento da realidade.

Michel Foucault, notável filósofo dos anos 70, com fundamento em seus estudos sobre o panoptismo de Jeremias Bentham, foi o precursor nos estudos dos poderes dominantes presentes na sociedade moderna baseados na vigilância total. Aprofundou, de maneira crítica, o conceito benthamniano de panoptismo, que teria como objeto central a "visão do todo".[47]

Seguindo seus estudos, Foucault, em sua célebre obra "Vigiar e punir: nascimento da prisão", de 1976, relaciona o conceito de panoptismo com as instituições disciplinares, analisando o modelo de prisão do século 18 elaborado por Jeremy Bentham.[48]

A relação feita entre os estudos dos poderes através da política de vigilância total e o modelo adotado de encarceramento se fez devido à estrutura do mesmo. O modelo de prisão analisado, criado por Bentham, foi o de uma arquitetura em que as celas dos detentos eram dispostas de maneira a se formar um "anel" em torno de uma grande torre de vigilância. A forma com que as celas são construídas, somente com paredes laterais, garante que os encarcerados não consigam escapar da constante vigilância. Nesse panorama, os guardas ficam na torre central, de maneira que não podem ser vistos pelos presos, os quais, contudo, são vigiados na integralidade do tempo.[49]

---

[47] MAGELA, Nídia Cecília Mendes. ABREU, Bárbara França. GOMIDE, Caroline Carvalho. VIEIRA, Kely Bianca Teodoro. COSTA, Polyane Rodrigues. **Comunicação e sociedade: anonimato na internet.** Revista Expressão**.** Disponível em <http://www4.faculdadepromove.br/expressao/index.php/files/article/view/80/0>. Acesso em 06 de setembro de 2020.

[48] FOUCAULT, Michel. **Vigiar e Punir: nascimento da prisão**. Petrópolis: Editora Vozes, 1987.

[49] MAGELA, Nídia Cecília Mendes. ABREU, Bárbara França. GOMIDE, Caroline Carvalho. VIEIRA, Kely Bianca Teodoro. COSTA, Polyane Rodrigues. **Comunicação e sociedade: anonimato na internet.** Revista Expressão**.** Disponível em <http://www4.faculdadepromove.br/expressao/index.php/files/article/view/80/0>. Acesso em 06 de setembro de 2020.

Esse modelo arquitetônico utilizado por Bentham representava mais que uma simples proposta empírica de distribuição espacial dos corpos no interior de uma instituição total. Representava mesmo um modelo simbólico da sociedade da vigilância que ele imaginara, em seu utilitarismo, como um modelo de organização societal ótima.

Por isso, na sociedade tecnológica contemporânea, em especial na realidade discutida no presente trabalho, qual seja, a realidade virtual, fica claro que o conceito de panoptismo de Foucault, com adaptações, se aplica com perfeição ainda nos dias atuais. A problemática da "vigilância total", liberta do sentido meramente arquitetônico e assumindo um sentido simbólico, é atualmente ainda mais perceptível e constante.

> No panoptismo, o indivíduo é vigiado sem desejar, apesar de se sentir seguro com esse modelo de vigilância total e absoluta. No meio eletrônico, a mão é invertida. Quando uma pessoa entra em um site, para que ela possa interagir minimamente, como comentar um conteúdo em um blog, por exemplo, na maioria das vezes é preciso inserir seus dados. No acesso às redes sociais você também está o tempo todo sendo mapeado. A diferença é que agora muitas pessoas desejam ser monitoradas, ou fazem isso sem saber que estão sendo vigiadas.[50]

Ao utilizar a internet os usuários disponibilizam uma série de informações muito maiores do que imaginam. Essa exposição inevitável para se usar os recursos oferecidos no ambiente virtual tornam os usuários cada vez mais vulneráveis às ameaças e ataques criminosos, transformando-os em potênciais vítimas de crimes virtuais.

Os usuários das amplas redes conectadas à internet estão sob vigilância constante, mesmo que não percebam isso. Com a rápida evolução dos meios informáticos, a criminalidade virtual é aperfeiçoada de forma veloz, e utiliza de diversos meios para ter acesso aos dados das vítimas. Essa realidade se agrava à medida em que os recursos tecnológicos avançam e, em contrapartida, a maioria dos usuários não acompanham tal evolução. O desconhecimento das pessoas quanto à forma segura de utilização dos mecanismos na rede mundial de computadores, conhecido como analfabetismo virtual, facilita a ação criminosa, potencializando a prática dos crimes virtuais.

A educação informática da população é uma necessidade crescente e que deve ser incluída nas pautas dos governos. Os cidadãos, assumindo o papel de usuários das redes mundiais de compuptadores, estão predispostos ao monitoramento devido, e, em algumas

---

[50] GLOBO CIÊNCIA. **Modelo panóptico prega o poder por meio de vigilância total do homem**. Globo Ciência. Globo.com. 2012. Disponível em: <http://redeglobo.globo.com/globociencia/noticia/2012/03/modelo-panoptico-prega-o-poder-por-meio-da-vigilancia-total-do-homem.html>. Acesso em 06 de setembro de 2020.

situações, indevido e ilegal, de maneira constante. Desta forma, a vulnerabilidade da segurança e dos dados desses usuários torna a internet o ambiente perfeito aos ataques criminosos. Imprescindivel se torna o ensino e informações aos cidadãos sobre o uso correto e seguro da internet, e dos riscos que esse ambiente virtual pode apresentar, sob pena de retroagirmos na segurança da socidade enquanto a internet se torne o meio para impulsinar a criminalidade moderna.

2.1.2 A PROBLEMÁTICA DO ANONIMATO E SUA APLICAÇÃO NA REDE MUNDIAL DE COMPUTADORES

Anonimato pode ser definido como a qualidade ou condição de quem é anônimo, não identificável, seja pela ausência de nome ou de assinatura de quem fez algo. Seu principal objetivo é ocultar a identidade de alguém perante terceiros, pelos mais variados motivos.[51]

A Constituição Federal brasileira de 1891, inovando a ordem jurídica interna, positivou pela primeira vez a vedação ao anonimato.[52] A redação do seu artigo 72, §12, continha o seguinte mandamento: "Em qualquer assunto é livre a manifestação de pensamento pela imprensa ou pela tribuna, sem dependência de censura, respondendo cada um pelos abusos que cometer nos casos e pela forma que a lei determinar. Não é permitido o anonimato".

O legislador, ao dispor sobre a proibição ao anonimato no texto constitucional, objetivou regulamentar o exercício da liberdade de manifestação do pensamento e opinião, visando conter os abusos cometidos na exteriorização desse direito.[53]

Já com a promulgação da Constituição da República Federativa Brasileira em 1988, o veto constitucional ao anonimato ganhou destaque. Inserido no título dos direitos e garantias fundamentais, especificamente no art. 5º, IV, da Carta Magna, que trata dos

---

[51] PAGANELLI, Celso Jefferson Messias. **Anonimato e internet: análise do princípio constitucional frente às recentes decisões do STJ.** Revista Âmbito Jurídico**.** Disponível em <https://ambitojuridico.com.br/cadernos/direito-constitucional/anonimato-e-internet-analise-do-principio-constitucional-frente-as-recentes-decisoes-do-stj/>. Acesso em 06 de setembro de 2020.

[52] MORAES, Paulo Francisco Cardoso de. **A vedação constitucional do anonimato aplicada à internet: o papel do estado brasileiro na identificação dos usuários e responsabilização dos provedores.** Revista Âmbito Jurídico**.** Disponível em <https://ambitojuridico.com.br/edicoes/revista-91/a-vedacao-constitucional-do-anonimato-aplicada-a-internet-o-papel-do-estado-brasileiro-na-identificacao-dos-usuarios-e-responsabilizacao-dos-provedores/>. Acesso em 06 de setembro de 2020.

[53]BRASIL. Supremo Tribunal Federal. Informativo STF n° 286/2002. Disponível em <http://www.stf.jus.br//arquivo/informativo/documento/informativo286.htm> Acesso em 06 de setembro de 2020.

direitos e deveres individuais e coletivos, tidos como cláusulas pétreas, o texto da Lei Maior passou a envolver a liberdade de expressão e a garantia da privacidade e do sigilo dos dados, correlacionando esses direitos à vedação ao anonimato.

A nossa Constituição Federal assegura a liberdade de expressão, contudo, proíbe de maneira absoluta o anonimato na mesma. Essa proibição vai de encontro às legislações de outros países, como os Estados Unidos, em que a Primeira Emenda à Constituição Americana permite o anonimato, sendo que já foi decidido pela Suprema Corte que também se aplica à internet.[54] Essa proibição se opõe, ainda, ao próprio modo de operação da Internet, aonde impera o anonimato como regra.

O Ministro do Supremo Tribunal Federal, Carlos Mário da Silva Velloso, defendeu que aceitar condutas anônimas:

> (...) é conferir ao anônimo respeitabilidade que ele não tem, pois o homem sério não precisa esconder-se sob a capa do anonimato para dizer do caráter ou da conduta de alguém – é fazer tabula rasa do direito de defesa, já que é fácil, muito fácil, dizer que alguém não presta, que alguém tem mau procedimento, se se afasta a possibilidade desse alguém esclarecer as informações, realizar aquilo que é básico num Estado de Direito, que é o direito de defesa.[55]

O Ministro do Supremo Tribunal Federal, Celso de Mello, em seu voto no Mandado de Segurança 24.369-DF, em que foi relator, também defendeu a importância da vedação constitucional ao anonimato:

> O veto constitucional ao anonimato, como se sabe, busca impedir a consumação de abusos no exercício da liberdade de manifestação do pensamento, pois, ao exigir-se a identificação de quem se vale dessa extraordinária prerrogativa político-jurídica, essencial à própria configuração do Estado democrático de direito, visa-se, em última análise, a possibilitar que eventuais excessos, derivados da prática do direito à livre expressão, sejam tornados passíveis de responsabilização, "a posteriori", tanto na esfera civil, quanto no âmbito penal.[56]

---

[54] PAGANELLI, Celso Jefferson Messias. **Anonimato e internet: análise do princípio constitucional frente às recentes decisões do STJ.** Revista Âmbito Jurídico**.** Disponível em < https://ambitojuridico.com.br/cadernos/direito-constitucional/anonimato-e-internet-analise-do-principio-constitucional-frente-as-recentes-decisoes-do-stj/>. Acesso em 06 de setembro de 2020.

[55] BRASIL. Supremo Tribunal Federal. Recurso Extraordinário n° 125.556/PR. p. 517. Disponível em <http://www.stf.jus.br/> Acesso em 06 de setembro de 2020.

[56] BRASIL. Supremo Tribunal Federal. Informativo STF n° 393/2005. Disponível em <http://www.stf.jus.br/arquivo/informativo/documento/informativo393.htm> Acesso em 06 de setembro de 2020.

Nossa Constituição foi promulgada em 1988 e, já naquela época, tratava sobre o anonimato e a necessidade de sua vedação, isso antes de se imaginar o alcance da comunicação de dados e ideias que seria proporcionado pela Internet. Esse fato torna evidente a importância e amplitude da problemática relativa à abrangência e forma de aplicação dessa questão na atualidade e, em especial, no ambiente virtual, considerando sempre a necessária preservação da livre expressão e demais liberdades inerentes a esse meio, que, além de direitos constitucionalmente previstos, são elementos essenciais à rede mundial de computadores e ao seu pleno funcionamento.

A despeito da proibição constitucional ao anonimato, há diversas situações em que o mesmo é lícito. Muitas vezes, mais do que simplesmente permitida, essa prática é necessária para o pleno exercício de outros direitos. Isso é possível pois não há nenhuma prerrogativa constitucional que tenha plena abrangência, não há direito absoluto que se sobrepõe face aos outros direitos, gerando, assim, conflito de normas, que é aceitável e deve ser resolvido com base na ponderação entre os direitos conflitantes no caso concreto.

Em um Estado democrático de Direito, aonde se pretende assegurar as liberdades inerentes à cidadania, a anonímia não se faz apenas necessária, em algumas situações ela se faz indispensável. Há eventos no cotidiano da população em que as pessoas não querem, ou até mesmo não devem ser identificadas para, assim, terem seus mais diversificados direitos garantidos.

O anonimato como condição *sine qua non* para concretização de objetivos lícitos está presente em diversos exemplos, a se citar as pessoas que buscam auxilio em grupos de autoajuda como os alcoólicos anônimos; as pesquisas em que não se deve citar os participantes para se garantir a veracidade dos dados colhidos; a busca por ajuda de profissionais como advogados e médicos; as ações visando proteger as testemunhas de um crime; os atos para se evitar perseguições políticas e as próprias denúncias anônimas aos órgãos públicos, o que é perfeitamente permitido pelo ordenamento jurídico e auxilia os órgãos de persecução penal e até as instâncias administrativas do Estado no seu controle interno.[57] Esses são alguns exemplos de situações em que o anonimato é perfeitamente possível, estando de acordo com os demais direitos protegidos.

---

[57] MORAES, Paulo Francisco Cardoso de. **A vedação constitucional do anonimato aplicada à internet: o papel do estado brasileiro na identificação dos usuários e responsabilização dos provedores.** Revista Âmbito Jurídico**.** Disponível em <https://ambitojuridico.com.br/edicoes/revista-91/a-vedacao-constitucional-do-anonimato-aplicada-a-internet-o-papel-do-estado-brasileiro-na-identificacao-dos-usuarios-e-responsabilizacao-dos-provedores/>. Acesso em 06 de setembro de 2020.

Analisando o descrito, se torna evidente que haverá o conflito ou colisão entre o anonimato e diversos princípios e garantias, assim como entre esses. À vista disso, será necessária uma análise minuciosa do caso concreto, se fazendo a ponderação entre os direitos conflitantes mediante a aplicação do princípio da proporcionalidade. A partir desse juízo no caso concreto será feita a restrição de algum direito em face do outro, a qual "pode ocorrer mesmo sem autorização expressa do constituinte sempre que se fizer necessária à concretização do princípio da concordância prática entre ditames constitucionais".[58]

Tendo em vista que o anonimato se torna legitimo em diversas situações, conclui-se que a vedação constitucional ao mesmo se restringe aos fatos em que houver a manifestação do pensamento. Enquanto a pessoa se valer do anonimato apenas dentro do âmbito de proteção aos seus direitos de privacidade, intimidade e sigilo, sem que sua conduta fira direitos de terceiros, imperioso se faz respeitar essa garantia que lhe é assegurada, inferindo que o anonimato não será vedado se não ocorrer a manifestação de pensamento de alguma forma.[59]

Esse raciocínio se aplica integralmente à internet. No uso cotidiano da rede mundial de computadores e de suas diversas ferramentas disponibilizadas, é licito o anonimato do usuário quando não ultrapassar seu âmbito de privacidade e intimidade, em outras palavras, o anonimato na rede será possível caso não viole a esfera de proteção de direitos de terceiros.

> Um simples navegar anônimo através da Internet é estritamente legal, pois que no correr da navegação não se faz essencial a manifestação de pensamento. Se uma pessoa desejar visitar *websites* comprometedores (de que natureza forem) sem se identificar, nenhum argumento legal poderá ser aduzido contra ela – seja de natureza civil ou penal.[60]

Neste assunto, há a necessidade de se distinguir os conceitos de anonimato, previsto na Constituição Federal de 1988, em seu art. 5º, IV, e privacidade, direito

---

[58] BRANCO, Paulo Gustavo Gonet; COELHO, Inocêncio Mártires; MENDES, Gilmar Ferreira. **Curso de Direito Constitucional.** 4ª. ed. São Paulo: Saraiva, 2008. p. 435.

[59] MORAES, Paulo Francisco Cardoso de. **A vedação constitucional do anonimato aplicada à internet: o papel do estado brasileiro na identificação dos usuários e responsabilização dos provedores.** Revista Âmbito Jurídico**.** Disponível em < https://ambitojuridico.com.br/edicoes/revista-91/a-vedacao-constitucional-do-anonimato-aplicada-a-internet-o-papel-do-estado-brasileiro-na-identificacao-dos-usuarios-e-responsabilizacao-dos-provedores/>. Acesso em 06 de setembro de 2020.

[60] NETO, Amaro Moraes e Silva. **Privacidade na Internet: um enfoque jurídico**. Bauru, São Paulo: EDIPRO, 2001. p. 106-107.

igualmente previsto na Constituição Federal, no texto do art. 5º, X, quando tratamos desses assuntos no uso da internet.

A análise deve ser feita de forma didática a partir da interação feita com os sistemas e bancos de dados quando se acessa alguma página na internet. Ao acessarmos as ferramentas disponíveis na internet, como os sites, em regra isso será feito de forma anônima, vez que estamos protegidos pelo direito constitucional à privacidade, intimidade e ao sigilo. No entanto, se dentro desse mesmo local na web for inserido algum tipo de conteúdo, incidirá aqui a proibição constitucional ao anonimato, visto que a expressão de qualquer pensamento ou opinião é um direito assegurado pela Carta Magna, contudo é indiscutivelmente proibido que isso seja feito de forma que não se possa identificar o autor de tal fato.[61]

Se não há a manifestação de opinião pelo usuário e se o mesmo não entra na órbita de proteção dos direitos de terceiros, ameaçando-os ou lesando-os, sua prerrogativa à privacidade e ao sigilo de seus dados deve ser respeitada.

Por óbvio, diversos dados são arrecadados pelos servidores e empresas na internet enquanto os usuários realizam suas atividades on-line, e, através dessa captação de dados, são feitas diversas análises estatísticas sobre o acesso, permitindo a verificação do que mais é consumido pelo público na rede, e por cada usuário especificamente, com vistas a impulsionar o mercado financeiro on-line. No entanto, isso deve ser feito sem que o usuário seja identificado, sem que qualquer informação pessoal a respeito do mesmo seja armazenada ou divulgada, preservando assim sua privacidade.[62]

Depreende-se, assim, que o anonimato está proibido pela Constituição Federal, contudo, essa proibição só se apresenta válida quando houver a livre manifestação do pensamento, vez que a partir desse momento o exercício desse direito torna o conteúdo da ideia do agente disponível a terceiros, podendo, assim, influir na esfera jurídica alheia, violando direitos de outrem, situações essas em que será cabível reparação do dano eventualmente causado e responsabilização do autor do mesmo.

---

[61] PAGANELLI, Celso Jefferson Messias. **Anonimato e internet: análise do princípio constitucional frente às recentes decisões do STJ.** Revista Âmbito Jurídico**.** Disponível em <https://ambitojuridico.com.br/cadernos/direito-constitucional/anonimato-e-internet-analise-do-principio-constitucional-frente-as-recentes-decisoes-do-stj/>. Acesso em 06 de setembro de 2020.

[62] PAGANELLI, Celso Jefferson Messias. **Anonimato e internet: análise do princípio constitucional frente às recentes decisões do STJ.** Revista Âmbito Jurídico**.** Disponível em <https://ambitojuridico.com.br/cadernos/direito-constitucional/anonimato-e-internet-analise-do-principio-constitucional-frente-as-recentes-decisoes-do-stj/>. Acesso em 06 de setembro de 2020.

> Todos têm liberdade para falar o que quiser, porém, precisam responder legalmente por suas palavras, principalmente nos casos em que houver calúnia, injúria e/ou difamação. O presente exposto é evidente no artigo 5º da Constituição Federal que diz ser vedado o anonimato. Ou seja, não se pode proferir algo que venha a ofender a outrem e depois renegar o que foi falado. Deve-se arcar sempre com as consequências daquilo que é dito e saber ouvir o que o outro tem a dizer por lhe ser garantido o direito de resposta.[63]

Corroborando a importância de se entender que o anonimato em diversas situações é meio essencial à garantia da efetividade de outros direitos, Paulo Gustavo Gonet Branco expõe que o "sigilo das comunicações é não só um corolário da garantia da livre expressão de pensamento; exprime também aspecto tradicional do direito à privacidade e à intimidade".[64]

O direito à privacidade, entendido como uma garantia fundamental do cidadão e instituído como cláusula pétrea devido sua evidente importância na sociedade, merece destaque e atenção, principalmente quando aplicado ao ambiente virtual, onde se torna um elemento essencial ao funcionamento e objetivo da rede.

Privacidade é o direito que a pessoa tem de controlar em qual medida poderá, ou não, haver a exposição de informações e dados sobre si, bem como de que forma, e se isso poderá ser disponibilizado a terceiros.[65] É um direito subjetivo fundamental dos cidadãos.[66]

Quando há o conflito entre o anonimato e a privacidade, deverá ser analisado se o sujeito que agindo anonimamente o fez dentro do uso do seu direito à privacidade, intimidade e sigilo e se não violou o direito de outrem.

> O direito à privacidade, concebido como uma tríade de direitos – direito de não ser monitorado, direito de não ser registrado e direito de não ser reconhecido (direito de não ter registros pessoais publicados) – transcende, pois, nas

---

[63] PIRES, Maísa Rezende. **O equilíbrio necessário para que a liberdade de expressão coexista com outros direitos**. Revista Âmbito Jurídico. Caderno Constitucional. Ano XIV, nº 95, Dezembro/2011. Disponível em <http://www.ambito-juridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=10790&revista_cadern o=9>. Acesso em 06 de setembro de 2020.

[64] BRANCO, Paulo Gustavo Gonet; COELHO, Inocêncio Mártires; MENDES, Gilmar Ferreira. **Curso de Direito Constitucional**. 4ª. ed. São Paulo: Saraiva, 2008. p. 435.

[65] PAGANELLI, Celso Jefferson Messias. **Anonimato e internet: análise do princípio constitucional frente às recentes decisões do STJ.** Revista Âmbito Jurídico**.** Disponível em <https://ambitojuridico.com.br/cadernos/direito-constitucional/anonimato-e-internet-analise-do-principio-constitucional-frente-as-recentes-decisoes-do-stj/>. Acesso em 06 de setembro de 2020.

[66] MORAES, Paulo Francisco Cardoso de. **A vedação constitucional do anonimato aplicada à internet: o papel do estado brasileiro na identificação dos usuários e responsabilização dos provedores.** Revista Âmbito Jurídico**.** Disponível em <https://ambitojuridico.com.br/edicoes/revista-91/a-vedacao-constitucional-do-anonimato-aplicada-a-internet-o-papel-do-estado-brasileiro-na-identificacao-dos-usuarios-e-responsabilizacao-dos-provedores/>. Acesso em 06 de setembro de 2020.

> sociedades informacionais, os limites de mero direito de interesse privado para se tornar um dos fundamentos do Estado Democrático de Direito.[67]

As relações estabelecidas pelo uso da Internet garantem às partes envolvidas, sejam os usuários ou os próprios provedores de acesso e criadores das ferramentas disponíveis nas redes, a privacidade de seus dados e ações como uma prerrogativa inerente ao próprio ambiente virtual. O direito à privacidade é constitucionalmente assegurado à todos, e se relaciona diretamente com o direito à inviolabilidade do domicilio, da correspondência, da comunicação e dos dados.[68]

Contudo, não obstante a importância de assegurar esses direitos fundamentais previstos na Constituição Federal, não se pode invocar o direito à privacidade para legitimar condutas anônimas que manifestem expressões e pensamentos de seus autores, pois isso não possui respaldo legal.

Como já discutido anteriormente, haverá, não raras as vezes, um conflito de normas e princípios a ser resolvido na questão envolvendo o anonimato e as outras garantias constitucionais. Por vezes, o anonimato é legitimo e pode ser necessário para a plena execução de outros direitos, contudo, em diversas situações o anonimato será o meio utilizado para violação de importantes direitos de terceiros. Nesse contexto, muitos são os direitos que podem ser violados diretamente com a permissão do anonimato, havendo, ainda, um direito que pode ser lesado indiretamente pelo mesmo, qual seja o direito de acesso à justiça, que é corolário do princípio da inafastabilidade da apreciação jurisdicional, previsto no art. 5º, XXXV, da Constituição Federal de 1988, cuja redação expõe que: "a lei não excluirá da apreciação do Poder Judiciário lesão ou ameaça a direito".[69]

Por óbvio, caso não haja a identificação do autor do fato, devido ao seu anonimato, impossível será que a pessoa lesada possa recorrer ao Estado buscando a satisfação de

---

[67] VIANNA, Túlio. **Transparência Pública, Opacidade Privada**. Rio de Janeiro: Editora Revan. 2006. p. 84.

[68] MORAES, Paulo Francisco Cardoso de. **A vedação constitucional do anonimato aplicada à internet: o papel do estado brasileiro na identificação dos usuários e responsabilização dos provedores.** Revista Âmbito Jurídico**.** Disponível em <https://ambitojuridico.com.br/edicoes/revista-91/a-vedacao-constitucional-do-anonimato-aplicada-a-internet-o-papel-do-estado-brasileiro-na-identificacao-dos-usuarios-e-responsabilizacao-dos-provedores/>. Acesso em 06 de setembro de 2020.

[69] MORAES, Paulo Francisco Cardoso de. **A vedação constitucional do anonimato aplicada à internet: o papel do estado brasileiro na identificação dos usuários e responsabilização dos provedores.** Revista Âmbito Jurídico**.** Disponível em <https://ambitojuridico.com.br/edicoes/revista-91/a-vedacao-constitucional-do-anonimato-aplicada-a-internet-o-papel-do-estado-brasileiro-na-identificacao-dos-usuarios-e-responsabilizacao-dos-provedores/>. Acesso em 06 de setembro de 2020.

seus direitos e a reparação do dano sofrido, seja na esfera civil, penal ou administrativa, o que é intolerável em um Estado Democrático de Direito.

2.1.3 ANONÍMIA ABSOLUTA E RELATIVA

Em diversos julgados o Supremo Tribunal Federal se deparou com o tema do anonimato, ocasiões em que teve que se ater à discussão desse tema detalhadamente.

Na ocasião em que o Presidente do Tribunal de Contas da União negou o fornecimento da identificação do autor de uma denúncia que originou processo para apurar atos de servidor responsável pela gestão de recursos públicos federais, foi impetrado mandado de segurança contra essa negativa. No julgamento do remédio constitucional em questão, o Ministro Relator Carlos Velloso, em seu voto, iniciou a discussão sobre a anonímia absoluta e relativa, afirmando que a prática do anonimato pode se dar de forma plena ou parcial, tese esta que foi adotada pelo Tribunal.[70]

O anonimato pode se dar de forma absoluta quando o anônimo preserva essa qualidade perante todos, ou seja, absolutamente ninguém consegue identifica-lo de nenhuma maneira. Já em sua vertente relativa, o anônimo consegue conservar essa condição de anonimato apenas em relação a determinados sujeitos, mas não em relação a outros.[71] Explico, enquanto no anonimato absoluto ninguém consegue identificar o sujeito, no anonimato relativo apenas determinadas pessoas não o conseguem identificar, contudo, em relação a outras esse sujeito é plenamente identificável.

A anonímia absoluta, também conhecida como anonímia própria, é aquela em que ninguém sabe quem é o sujeito que está se valendo do anonimato para utilizar seu direito à liberdade de expressão, o que é inconstitucional. Nesses casos, não é possível nem à vítima ou pessoa lesada de alguma maneira, nem aos provedores de acesso à internet ou provedores responsáveis pelos serviços disponibilizados na rede, a identificação do sujeito ativo da conduta anônima. Nessas situações em que o anonimato é absoluto,

---

[70] BRASIL. Supremo Tribunal Federal. MS 24.405-4-DF. Rel. Min. Carlos Velloso. Disponível em <http://www.stf.jus.br/>. Acesso em 06 de setembro de 2020.

[71] MORAES, Paulo Francisco Cardoso de. **A vedação constitucional do anonimato aplicada à internet: o papel do estado brasileiro na identificação dos usuários e responsabilização dos provedores.** Revista Âmbito Jurídico**.** Disponível em <https://ambitojuridico.com.br/edicoes/revista-91/a-vedacao-constitucional-do-anonimato-aplicada-a-internet-o-papel-do-estado-brasileiro-na-identificacao-dos-usuarios-e-responsabilizacao-dos-provedores/>. Acesso em 06 de setembro de 2020.

proceder-se-á à responsabilização objetiva ou subjetiva dos provedores, conforme o caso.[72]

A anonímia relativa, por sua vez, é conhecida como anonimato impróprio. Diz respeito às situações em que a conduta de certa pessoa é não identificável relativamente a alguém, ou a algum grupo específico. Contudo, essa mesma pessoa que praticou tal ato é plenamente identificável para terceiros. Assim sendo, conclui-se que na anonímia relativa o sujeito ativo pode ser anônimo relativamente a certa pessoa, mas não conserva essa característica em relação a outra. Esse tipo de anonimato respeita a vedação constitucional, uma vez que permite a identificação do agente quando ele exerce sua manifestação de pensamento. Essa identificação, que pode ser feita por algumas pessoas, ocorre pois o agente teve que informar seus dados ou porque ele deixou vestígios quando de sua ação.[73]

Não importa o meio que permitiu a identificação do agente, sendo um meio de obtenção de prova lícito é plenamente aceitável para o responsabilizar. No contexto virtual das condutas exercidas na internet, os provedores de acesso, serviço e conteúdo, devem deter a capacidade de identificar quem cometeu determinadas condutas.[74]

Portanto, o usuário dos mecanismos disponibilizados na internet está anônimo perante os demais usuários, salvo se houver atos volitivos de identificação, ou situações em que inexoravelmente a identificação será obrigatória. Contudo, em relação aos provedores de acesso à rede e suas ferramentas de uso, o anonimato não deverá ocorrer e, para isso, esses provedores devem agir de forma diligente para garantir a identificação e armazenamento dos dados de seus usuários, de forma a respeitar, porém, o direito à privacidade. Quando se faça necessário, respeitando às regras do devido processo legal, os provedores que possuem os dados sob sua guarda deverão operar a quebra do sigilo e

---

[72] MORAES, Paulo Francisco Cardoso de. **A vedação constitucional do anonimato aplicada à internet: o papel do estado brasileiro na identificação dos usuários e responsabilização dos provedores.** Revista Âmbito Jurídico**.** Disponível em <https://ambitojuridico.com.br/edicoes/revista-91/a-vedacao-constitucional-do-anonimato-aplicada-a-internet-o-papel-do-estado-brasileiro-na-identificacao-dos-usuarios-e-responsabilizacao-dos-provedores/>. Acesso em 06 de setembro de 2020.

[73] MORAES, Paulo Francisco Cardoso de. **A vedação constitucional do anonimato aplicada à internet: o papel do estado brasileiro na identificação dos usuários e responsabilização dos provedores.** Revista Âmbito Jurídico**.** Disponível em < https://ambitojuridico.com.br/edicoes/revista-91/a-vedacao-constitucional-do-anonimato-aplicada-a-internet-o-papel-do-estado-brasileiro-na-identificacao-dos-usuarios-e-responsabilizacao-dos-provedores/>. Acesso em 06 de setembro de 2020.

[74] MORAES, Paulo Francisco Cardoso de. **A vedação constitucional do anonimato aplicada à internet: o papel do estado brasileiro na identificação dos usuários e responsabilização dos provedores.** Revista Âmbito Jurídico**.** Disponível em <https://ambitojuridico.com.br/edicoes/revista-91/a-vedacao-constitucional-do-anonimato-aplicada-a-internet-o-papel-do-estado-brasileiro-na-identificacao-dos-usuarios-e-responsabilizacao-dos-provedores/>. Acesso em 06 de setembro de 2020.

fornecer essas informações ao requerente, se assim o determinar o juiz competente. “Do contrário, o anonimato seria perpetuado e isso é vedado pela constituição, principalmente se houver violação dos direitos de alguém”.[75]

2.1.4 O ANONIMATO NO AMBIENTE VIRTUAL

A privacidade é encarada como o direito mais importante no ambiente virtual, sendo uma das características imprescindíveis ao pleno funcionamento dos recursos que ali se encontram disponíveis. Paralelamente, as taxas de crimes cibernéticos crescem desenfreadamente, assim como os mecanismos existentes para o cometimento desses e de novos crimes.[76]

Essas práticas lesivas a direitos alheios que, não raras as vezes, chegam a ser criminosas, devem ser combatidas de modo a responsabilizar e punir seus agentes, reprimindo a impunidade, garantindo o pleno exercício dos direitos individuais e coletivos, protegendo os cidadãos e, indiretamente, o próprio Estado Democrático de Direito, que é a base do Estado Republicano brasileiro.[77]

Em seus primórdios, um dos objetivos iniciais da internet era garantir o anonimato de seus usuários. Essa prerrogativa visava garantir que os usuários, uma vez não identificáveis, pudessem utilizar de melhor maneira os recursos provenientes da internet, garantindo-se a igualdade entre todos no ambiente virtual.[78] Entretanto, com o surgimento

---

[75] MORAES, Paulo Francisco Cardoso de. **A vedação constitucional do anonimato aplicada à internet: o papel do estado brasileiro na identificação dos usuários e responsabilização dos provedores.** Revista Âmbito Jurídico**.** Disponível em <https://ambitojuridico.com.br/edicoes/revista-91/a-vedacao-constitucional-do-anonimato-aplicada-a-internet-o-papel-do-estado-brasileiro-na-identificacao-dos-usuarios-e-responsabilizacao-dos-provedores/>. Acesso em 06 de setembro de 2020.

[76] MORAES, Paulo Francisco Cardoso de. **A vedação constitucional do anonimato aplicada à internet: o papel do estado brasileiro na identificação dos usuários e responsabilização dos provedores.** Revista Âmbito Jurídico**.** Disponível em <https://ambitojuridico.com.br/edicoes/revista-91/a-vedacao-constitucional-do-anonimato-aplicada-a-internet-o-papel-do-estado-brasileiro-na-identificacao-dos-usuarios-e-responsabilizacao-dos-provedores/>. Acesso em 08 de setembro de 2020.

[77] MORAES, Paulo Francisco Cardoso de. **A vedação constitucional do anonimato aplicada à internet: o papel do estado brasileiro na identificação dos usuários e responsabilização dos provedores.** Revista Âmbito Jurídico**.** Disponível em <https://ambitojuridico.com.br/edicoes/revista-91/a-vedacao-constitucional-do-anonimato-aplicada-a-internet-o-papel-do-estado-brasileiro-na-identificacao-dos-usuarios-e-responsabilizacao-dos-provedores/>. Acesso em 08 de setembro de 2020.

[78] ANDRADE, Mariah Dourado de; BENTES, Dorinethe dos Santos; GUIMARAES, David Franklin da Silva. **Considerações sobre a aplicabilidade do direito penal acerca dos crimes virtuais.** Revista Vertentes do Direito. Disponível em <https://sistemas.uft.edu.br/periodicos/index.php/direito/article/view/4171#:~:text=O%20presente%20artigo%20busca%20compreender,Leis%20Penais%20regulando%20esse%20crime.>. Acesso em 14 de agosto de 2020.

e o absurdo crescimento dos delitos perpetrados pela internet e contra seus mecanismos de uso, a prerrogativa do anonimato teve que ser relativizada e reavaliada no cenário social em que passou a se encontrar, analisando essa questão sob a égide da Constituição Federal de 1988 e as leis infraconstitucionais posteriores.

A internet da forma como foi criada inicialmente, pretendendo que seus usuários não fossem identificados, se contrapões em diversas situações ao que determina a Carta Magna, como já discorrido anteriormente neste trabalho. Não obstante, apesar da vedação constitucional ao anonimato, o mesmo ainda é uma das principais causas dos crimes virtuais, visto que sua utilização facilita a impunidade dos delitos praticados na rede.

É importante que se garanta o respeito à privacidade; à intimidade; ao sigilo e livre manifestação do pensamento nas redes informáticas, visto que são garantias constitucionais. Contudo, isso deve ser feito de maneira proporcional, buscando a proteção dos direitos de terceiros e de maneira que não se viole os direitos fundamentais e os direitos humanos.

Relembramos que nesse assunto a maior problemática gira em torno dos sistemas que lidam com redes anônimas, conhecidas como Deep Web e Dark Web. Devido ao fato de que suas páginas não são localizadas pelos mecanismos usuais de buscas e de que seus programas possuem criptografia de ponta, o anonimato dentro desses ambientes é real, o que torna, quase sempre, impossível a identificação de seus usuários. Esses fatores, e a sensação de garantia de impunidade que os mesmos geram, propiciam que os mais diversos tipos imagináveis de crimes sejam planejados e executados nesse ambiente.[79]

Nossa sociedade, entendida como democrática, consagra o pluralismo de ideias e pensamentos, assim como o respeito e a tolerância, como necessidades vitais à convivência entre as pessoas. Nesse contexto, a liberdade de expressão é essencial e "compreende não somente as informações consideradas como inofensivas, indiferentes ou favoráveis, mas também as que possam causar transtornos, resistência, inquietar pessoas".[80]

Corroborando a importância do direito à liberdade de expressão, a Declaração Universal dos Direitos do Homem, em seu artigo 19, dispõe que "todo o homem tem

---

[79] MAGELA, Nídia Cecília Mendes. ABREU, Bárbara França. GOMIDE, Caroline Carvalho. VIEIRA, Kely Bianca Teodoro. COSTA, Polyane Rodrigues. **Comunicação e sociedade: anonimato na internet.** Revista Expressão**.** Disponível em <http://www4.faculdadepromove.br/expressao/index.php/files/article/view/80/0>. Acesso em 08 de setembro de 2020.

[80] MORAES, Alexandre de. **Constituição do Brasil interpretada e legislação constitucional**. 4. ed. – São Paulo: Atlas, 2004. p 207.

direito à liberdade de opinião e expressão; este direito inclui a liberdade de, sem interferências, ter opiniões e de procurar, receber e transmitir informações e ideias por quaisquer meios, independentemente de fronteiras".[81]

O Brasil é signatário da Declaração Universal dos Direitos do Homem.[82] A Constituição Federal Brasileira de 1988 garante, em seu art. 5º, IV, que "é livre a manifestação do pensamento, sendo vedado o anonimato". O texto fundamental ainda protege essa liberdade em diversas outras passagens, visto o quão importante é este direito.

Devemos, aqui, citar alguns artigos que, direta ou indiretamente, garantem essa liberdade primordial aos cidadãos, quais sejam: o art. 5º, X, que em seu texto garante que "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação"; o art. 5º, XIV, que dispõe ser "assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional"; o art. 220 que protege esse direito quando dispõe que "a manifestação do pensamento, a criação, a expressão e a informação, sob qualquer forma, processo ou veículo não sofrerão qualquer restrição, observado o disposto nesta Constituição", bem como em seus §1º e §2º que determinam que "nenhuma lei conterá dispositivo que possa constituir embaraço à plena liberdade de informação jornalística em qualquer veículo de comunicação social, observado o disposto no art. 5º, IV, V, X, XIII e XIV" e que "é vedada toda e qualquer censura de natureza política, ideológica e artística", respectivamente; todos da Constituição Federal Brasileira de 1988.

Conforme leciona Alexandre de Moraes: "O Estado democrático defende o conteúdo essencial da manifestação da liberdade, que é assegurado tanto sob o aspecto positivo, ou seja, proteção da exteriorização da opinião, como sob o aspecto negativo, referente à proibição da censura".[83] A liberdade de expressão, assim entendida como um direito fundamental inerente à pessoa humana, pretende em seu efeito inibir as censuras estatais.[84]

---

[81] **Declaração Universal dos Direitos do Homem**. Disponível em < http://pfdc.pgr.mpf.mp.br/atuacao-e-conteudos-de-apoio/legislacao/direitos-humanos/declar_dir_homem.pdf>. Acesso em 08 de setembro de 2020.

[82] SIMONSEN, André Wallace. **Privacidade e anonimidade na internet.** Disponível em <https://jus.com.br/artigos/32143/privacidade-e-anonimidade-na-internet>. Acesso em 08 de setembro de 2020.

[83] MORAES, Alexandre de. **Direito constitucional**. 15. Ed. – São Paulo: Atlas, 2004. p. 74

[84] BRANCO, Paulo Gustavo Gonet; COELHO, Inocêncio Mártires; MENDES, Gilmar Ferreira. **Curso de Direito Constitucional.** 4ª. ed. São Paulo: Saraiva, 2008. p. 404.

Essa liberdade, não obstante seu caráter essencial, será mitigada sempre que preciso se houver colisões entre ela e outros direitos fundamentais ou valores constitucionais diversos.[85] A proibição constitucional à censura não constitui óbice para que o indivíduo seja responsabilizado civil, penal ou administrativamente pelas consequências que gerou com seus atos.

Nítido se faz que não é permitido a ninguém alegar seu direito à liberdade de expressão como forma de contrariar a vedação constitucional ao anonimato. Sabemos que nenhum princípio é absoluto, e por essa mesma razão deverá haver sopesamento dos que conflitarem e forem concernentes à mesma matéria.[86] É o que se depreende do seguinte julgado:

> Liberdade de expressão. Garantia constitucional que não se tem como absoluta. Limites morais e jurídicos. O direito à livre expressão não pode abrigar, em sua abrangência, manifestações de conteúdo imoral que implicam ilicitude penal. As liberdades públicas não são incondicionais, por isso devem ser exercidas de maneira harmônica, observados os limites definidos na própria CF (CF, art. 5º, § 2º, primeira parte). O preceito fundamental de liberdade de expressão não consagra o 'direito à incitação ao racismo', dado que um direito individual não pode constituir-se em salvaguarda de condutas ilícitas, como sucede com os delitos contra a honra. Prevalência dos princípios da dignidade da pessoa humana e da igualdade jurídica. (HC 82.424, Rel. p/ o ac. Min. Presidente Maurício Corrêa, julgamento em 17-9-2003, Plenário, DJ de 19-3-2004.)[87]

Acertado é que a liberdade de expressão não será protegida se for exercida se valendo do anonimato para tal, em especial se for materializada em condutas que lesem outros direitos, com ênfase naqueles indisponíveis.

Não há direito absoluto, até mesmo os direitos elencados como fundamentais possuem limites explícitos e implícitos na própria constituição.[88] O Ministro Gilmar Mendes ao se debruçar sobre o tema esclarece que *stricto sensu* as colisões se referem à contraposição entre direitos fundamentais, sejam eles idênticos ou diversos. Já *lato sensu*,

---

[85] BRANCO, Paulo Gustavo Gonet ; COELHO, Inocêncio Mártires ; MENDES, Gilmar Ferreira. **Curso de Direito Constitucional.** 4ª. ed. São Paulo: Saraiva, 2008. p. 403.

[86] PAGANELLI, Celso Jefferson Messias. **Anonimato e internet: análise do princípio constitucional frente às recentes decisões do STJ.** Revista Âmbito Jurídico**.** Disponível em <https://ambitojuridico.com.br/cadernos/direito-constitucional/anonimato-e-internet-analise-do-principio-constitucional-frente-as-recentes-decisoes-do-stj/>. Acesso em 08 de setembro de 2020.

[87] BRASIL. Supremo Tribunal Federal. HC 82.424. Rel. p/ o ac. Min. Presidente Maurício Corrêa. Disponível em <http://www2.stf.jus.br/portalStfInternacional/cms/verConteudo.php?sigla=portalStfJurisprudencia_pt_br&idConteudo=185077&modo=cms>. Acesso em 08 de setembro de 2020.

[88] BRASIL. Supremo Tribunal Federal. Ação Direita de Inconstitucionalidade n° 1969-2007. Rel. Min. Ricardo Lewandosvik. p. 16. Disponível em <http://www.stf.jus.br/>. Acesso em 08 de setembro de 2020.

envolvem a contraposição entre direitos fundamentais e outros princípios ou valores diversos.[89]

A vedação ao anonimato para o exercício do direito à liberdade de expressão surge como forma de cautela antecipada do constituinte originário, visto que já se podia verificar que tal liberdade estaria em potencial conflito com os demais direitos assegurados.[90]

2.2 LEGISLAÇÃO BRASILEIRA COMPARADA À LEGISLAÇÃO ESTRANGEIRA SOBRE O TEMA

A internet se vale de um protocolo comum para interligar uma rede de computadores dispersos pelo mundo, objetivando viabilizar a comunicação, compartilhamento e intercâmbio de dados variados.[91]

Através do protocolo comum utilizado na rede mundial de computadores, cada computador interligado deverá ter sua respectiva identificação, que possibilite sua singularização perante os demais, para que haja a correta identificação de cada aparelho e seu respectivo usuário.[92]

O protocolo comum utilizado na internet para interconectar e identificar as redes interligadas é denominado de TCP/IP (*Transmission Control Protocol* e *Internet Protocol)*. Por meio desses protocolos os diversos acessos à rede são interligados, formando a rede mundial de computadores.[93] Os dois protocolos têm as seguintes

---

[89] BRANCO, Paulo Gustavo Gonet ; COELHO, Inocêncio Mártires ; MENDES, Gilmar Ferreira. **Curso de Direito Constitucional.** 4ª. ed. São Paulo: Saraiva, 2008. p. 376.

[90] MORAES, Paulo Francisco Cardoso de. **A vedação constitucional do anonimato aplicada à internet: o papel do estado brasileiro na identificação dos usuários e responsabilização dos provedores.** Revista Âmbito Jurídico**.** Disponível em <https://ambitojuridico.com.br/edicoes/revista-91/a-vedacao-constitucional-do-anonimato-aplicada-a-internet-o-papel-do-estado-brasileiro-na-identificacao-dos-usuarios-e-responsabilizacao-dos-provedores/>. Acesso em 08 de setembro de 2020.

[91] MORAES, Paulo Francisco Cardoso de. **A vedação constitucional do anonimato aplicada à internet: o papel do estado brasileiro na identificação dos usuários e responsabilização dos provedores.** Revista Âmbito Jurídico**.** Disponível em < https://ambitojuridico.com.br/edicoes/revista-91/a-vedacao-constitucional-do-anonimato-aplicada-a-internet-o-papel-do-estado-brasileiro-na-identificacao-dos-usuarios-e-responsabilizacao-dos-provedores/>. Acesso em 14 de setembro de 2020.

[92] MORAES, Paulo Francisco Cardoso de. **A vedação constitucional do anonimato aplicada à internet: o papel do estado brasileiro na identificação dos usuários e responsabilização dos provedores.** Revista Âmbito Jurídico**.** Disponível em < https://ambitojuridico.com.br/edicoes/revista-91/a-vedacao-constitucional-do-anonimato-aplicada-a-internet-o-papel-do-estado-brasileiro-na-identificacao-dos-usuarios-e-responsabilizacao-dos-provedores/>. Acesso em 14 de setembro de 2020.

[93] MORAES, Paulo Francisco Cardoso de. **A vedação constitucional do anonimato aplicada à internet: o papel do estado brasileiro na identificação dos usuários e responsabilização dos provedores.** Revista Âmbito Jurídico**.** Disponível em < https://ambitojuridico.com.br/edicoes/revista-91/a-vedacao-

funções: “O IP cuida do endereçamento, enquanto o TCP cuida da transmissão dos dados e correção de erros”.[94]

Mediante os protocolos de internet gerados em uma conexão, as provedoras de acesso à internet terão a possibilidade de identificar a máquina da qual partiu determinada ação na rede, isso se dá através do rastreamento do *internet protocol* (IP).

Se faz oportuno recordar que o rastreamento do protocolo de internet e a identificação do usuário são formas de quebra de sigilo de dados. Os serviços de internet, segundo a legislação brasileira, estão contidos na definição de serviços de telecomunicações e lidam com dados sigilosos. Portanto, o acesso a tais dados e o rastreamento do endereço físico e da identidade de determinado usuário, por meio do protocolo de internet e demais dados de que a provedora de acesso tem conhecimento, requer uma imprescindível autorização judicial, em respeito ao direito à privacidade e sigilo das comunicações e dos dados, que é garantido constitucionalmente.[95]

Muitas ações ilegais e, também, criminosas são praticadas através da internet. Em diversas ocasiões o Poder Público busca impelir aos servidores de acesso e de conteúdo a responsabilidade por apagar e bloquear todos os tipos de conteúdos ilegais que possam sobrevir ao acesso à rede. Contudo, obviamente, isso só será possível em relação a determinados conteúdos que estejam no servidor, como os claramente ilegais. É tecnicamente impossível aos provedores identificar todos os conteúdos ilegais e bloqueá-los.[96]

Essa impossibilidade de se estabelecer a obrigação aos provedores de que não haja conteúdos ilegais em seus servidores, bem como a necessidade de se determinar a responsabilidade do autor do fato ilegal, possibilitando, ainda, sua punição quando ocorrerem atos criminosos por meio de suas condutas na internet, demonstra a

---

constitucional-do-anonimato-aplicada-a-internet-o-papel-do-estado-brasileiro-na-identificacao-dos-usuarios-e-responsabilizacao-dos-provedores/>. Acesso em 14 de setembro de 2020.

[94] MORIMOTO, Carlos Eduardo. **Termos técnicos GdH**. Disponível em <http://www.guiadohardware.net/termos/tcp-ip>. Acesso em 15 de setembro de 2020.

[95] MORAES, Paulo Francisco Cardoso de. **A vedação constitucional do anonimato aplicada à internet: o papel do estado brasileiro na identificação dos usuários e responsabilização dos provedores.** Revista Âmbito Jurídico**.** Disponível em < https://ambitojuridico.com.br/edicoes/revista-91/a-vedacao-constitucional-do-anonimato-aplicada-a-internet-o-papel-do-estado-brasileiro-na-identificacao-dos-usuarios-e-responsabilizacao-dos-provedores/>. Acesso em 14 de setembro de 2020.

[96] PEREIRA, Eduardo Baker Valls. **Crimes informacionais: da compatibilidade internacional do ordenamento jurídico nacional e da proposta de reforma.** Revista IBCCRIM. n. 112. 2015.

indispensabilidade e importância de haver medidas para que ocorra a identificação do agente dessas condutas maliciosas.[97]

Diante dessa problemática, surge a necessidade de se estabelecer a obrigatoriedade de registro e guarda dos dados de acesso dos usuários à rede como forma de possibilitar a identificação dos autores dessas condutas prejudiciais a direitos alheios, garantindo que não haja o anonimato para pratica de crimes e que seja possível a punição dos infratores, através do devido processo legal.

Nesta senda, a legislação pátria vem se movendo no sentido de estabelecer a necessidade do registro e, especialmente, da guarda desses dados, objetivando a possibilidade de eventual identificação dos cybercriminosos quando se fizer necessário.[98]

Em nível distrital e municipal, há as iniciativas do Distrito Federal, com a Lei Distrital nº 3.437/2004 e do município de Recife, com a Lei Municipal nº 17.572/2009, ambas lidando com a questão da obrigatoriedade de registro e armazenamento do acesso de usuários nas redes mundiais de computadores.[99]

A nível estadual merecem destaques as iniciativas legislativas concernentes ao tema dos Estados de São Paulo, Lei 12.228/2006; Amapá, Lei 1.047/2006; Paraíba, Lei 8.134/2006; Alagoas, Lei 6.891/2007; Espirito Santo, Lei 8.777/2007; Rio de Janeiro, Lei 5.132/2007; Rio Grande do Sul, Lei 12.698/2007; Amazonas, Lei 3.173/2007 e Lei 3.351/2008; Piauí, Lei 5.747/2008; Bahia, Lei 11.608/2009; Paraná, Lei 16.241/2009; Pernambuco, Lei 14.001/2009 e Santa Catarina, com sua respectiva Lei 14.890/2009.[100]

O Estado de Santa Catarina, por meio de sua Lei Estadual nº 14.890/2009, inovou seu ordenamento disciplinando sobre regras e meios de controle de acesso à internet pelas empresas de *lan houses*. Por meio da respectiva Lei Estadual criou-se a obrigação desses estabelecimentos adotarem o controle de seus clientes por meio de sistema de monitoramento em vídeo, por câmeras de vigilância. Estabeleceu-se, ainda, a necessidade de cadastro dos usuários de seus serviços, bem como o registro de dados e a guarda dos

---

[97] PEREIRA, Eduardo Baker Valls. **Crimes informacionais: da compatibilidade internacional do ordenamento jurídico nacional e da proposta de reforma.** Revista IBCCRIM. n. 112. 2015.
[98] VALVERDE, Danielle Novaes de Siqueira. **Crimes Cibernéticos: a obrigatoriedade do registro de acesso à internet como forma de possibilitar a identificação do criminoso.** Revista da ESMAPE. Recife. v. 15. n. 32. p. 243. jul./dez. 2010.
[99] VALVERDE, Danielle Novaes de Siqueira. **Crimes Cibernéticos: a obrigatoriedade do registro de acesso à internet como forma de possibilitar a identificação do criminoso.** Revista da ESMAPE. Recife. v. 15. n. 32. p. 243. jul./dez. 2010.
[100] VALVERDE, Danielle Novaes de Siqueira. **Crimes Cibernéticos: a obrigatoriedade do registro de acesso à internet como forma de possibilitar a identificação do criminoso.** Revista da ESMAPE. Recife. v. 15. n. 32. p. 243. jul./dez. 2010.

mesmo por um período de 02 anos, observando a necessária correlação do cadastro com o computador, horário de início e término do respectivo acesso.[101]

Já o Estado de São Paulo, no ano de 2006, através da Lei 12.228, instituiu a obrigação legal aos estabelecimentos que comercializam internet por meio da locação de máquinas e pontos de acesso, a exemplo das *lan houses* e *cybercafés*, de realizar o cadastro e manter o registro atualizado de todos seus clientes que utilizem de seus serviços para acesso à rede. Os registros desses dados devem ficar armazenados por um período de, no mínimo, 60 meses, sob pena de multa estabelecida na citada lei.[102]

Esse cadastro deve conter o nome completo do cliente, sua data de nascimento, número do registro geral (RG), endereço e telefone atualizados. As empresas de comercialização de máquinas para acesso à rede devem ter a atenção de registrar corretamente, ainda, os horários iniciais e finais de conexão em cada acesso, bem como qual o aparelho utilizado pelo cliente devidamente identificado.[103]

Em Recife, as empresas que trabalham nessa área de comercialização de terminais para acesso à internet ficaram obrigadas, pela Lei Municipal 17.572/2009, a estabelecer o controle dos usuários por meio do cadastro de seus clientes e dos dados de acesso com o dia, hora e terminal utilizados. Essas informações devem ser mantidas por um período não inferior a 12 meses, conforme disposição legal.[104]

No Poder Legislativo Federal, antes da criação do Marco Civil da Internet, Lei nº 12.965, de 23 de abril de 2014, não havia legislação concernente ao tema. Nesse cenário, o Poder Executivo Federal passou a editar resoluções, dentro de sua competência, para tentar amenizar os problemas decorrentes da falta de legislação sobre o registro e guarda dos dados dos usuários e dos acessos à internet pelos provedores.[105]

---

[101] VALVERDE, Danielle Novaes de Siqueira. **Crimes Cibernéticos: a obrigatoriedade do registro de acesso à internet como forma de possibilitar a identificação do criminoso.** Revista da ESMAPE. Recife. v. 15. n. 32. p. 244. jul./dez. 2010.

[102] VALVERDE, Danielle Novaes de Siqueira. **Crimes Cibernéticos: a obrigatoriedade do registro de acesso à internet como forma de possibilitar a identificação do criminoso.** Revista da ESMAPE. Recife. v. 15. n. 32. p. 243 - 244. jul./dez. 2010.

[103] FOLHA ONLINE. **Lan house começa a cadastrar clientes em SP**. Disponível em <http://www1.folha.uol.com.br/folha/informatica/ult124u19642.shtml>. Acesso em 15 de setembro de 2020.

[104] VALVERDE, Danielle Novaes de Siqueira. **Crimes Cibernéticos: a obrigatoriedade do registro de acesso à internet como forma de possibilitar a identificação do criminoso.** Revista da ESMAPE. Recife. v. 15. n. 32. p. 244. jul./dez. 2010.

[105] DORIGON, Alessandro; SOARES, Renan Vinicius de Oliveira. **Crimes cibernéticos: dificuldades investigativas na obtenção de indícios da autoria e prova da materialidade.** Disponível em < https://jus.com.br/artigos/63549/crimes-ciberneticos-dificuldades-investigativas-na-obtencao-de-indicios-da-autoria-e-prova-da-materialidade>. Acesso em 15 de setembro de 2020.

Os dados de acesso à rede devem ser registrados pelos servidores dos provedores de acesso e de conteúdo através dos denominados *logs.* Com o advento do Marco Civil da Internet, passou-se a estabelecer o prazo de 06 meses para que os provedores armazenassem os registros de acesso, devendo mantê-los, obrigatoriamente, sob sigilo, o qual só poderá ser relativizado mediante ordem judicial escrita e fundamentada de quebra de sigilo de dados, emanada por autoridade judiciaria competente.[106] É o que se depreende da redação do art. 15 da referida lei:

> Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento.

O Marco Civil da Internet, Lei 12.965/2014, ainda estipula o prazo de 01 ano para a guarda dos registros de conexão. É o que aponta o seu art. 13:

> Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento.

Analisando a redação do referido artigo 13 do Marco Civil da Internet, infere-se que o texto legal obriga apenas os administradores de sistemas autônomos a realizarem a guarda dos dados de conexão. Isto posto, somente aqueles que possuem o Número de Sistema Autônomo (ASN) é que teriam o dever de realizar o armazenamento dos dados de acesso. Nesse cenário criado pela lei, os demais provedores de menor porte não são caracterizados como serviço autônomo de provedores de acesso, não se enquadrando na obrigação legal de armazenamento dos dados.[107]

Porém, anteriormente à entrada em vigor do Marco Civil da Internet, a Agência Nacional de Telecomunicações (ANATEL) publicou a Resolução nº 614/2013, estabelecendo novas regras ao Serviço de Comunicação Multimídia (SCM). Dentre essas novas diretrizes, a Resolução estabelece o período mínimo de 01 ano para guarda dos

---

[106] VALVERDE, Danielle Novaes de Siqueira. **Crimes Cibernéticos: a obrigatoriedade do registro de acesso à internet como forma de possibilitar a identificação do criminoso.** Revista da ESMAPE. Recife. v. 15. n. 32. p. 245. jul./dez. 2010.

[107] DORIGON, Alessandro; SOARES, Renan Vinicius de Oliveira. **Crimes cibernéticos: dificuldades investigativas na obtenção de indícios da autoria e prova da materialidade.** Disponível em < https://jus.com.br/artigos/63549/crimes-ciberneticos-dificuldades-investigativas-na-obtencao-de-indicios-da-autoria-e-prova-da-materialidade>. Acesso em 15 de setembro de 2020.

dados de acesso à rede pelas prestadoras de serviços. Portanto, conclui-se que, de acordo com a Resolução da ANATEL sobre o tema, todos os provedores de acesso que detenham SCM estão obrigados a realizar o registro e armazenamentos dos *logs* de conexão à internet. Contudo, discute-se a derrogabilidade ou não desta resolução ante a entrada em vigor do Marco Civil da Internet.[108]

Revendo o prazo de obrigatoriedade do armazenamento dos dados de acesso, teve início no Senado Federal, em 2008, o Projeto de Lei do Senado nº 494/2008, que tem como finalidade estabelecer ações de repressão aos crimes sexuais praticados contra crianças e adolescentes por meio da internet. Este Projeto de Lei, após ser aprovado em 2015 no Senado Federal, sua casa de origem, foi remetido para votação na Câmara dos Deputados, local em que deu origem ao Projeto de Lei nº 2.514/2015. O principal objetivo deste Projeto de Lei, que está em votação até hoje, é estabelecer a obrigatoriedade do registro e armazenamentos dos dados de acesso à rede pelo período de 03 anos, prazo superior ao atual período estabelecido pelo Marco Civil da Internet.[109]

O Marco Civil da Internet corrobora a regra constitucional, estabelecendo que o usuário tem direito ao anonimato em suas conexões à rede, contudo este anonimato deverá ser relativizado pelo armazenamento dos dados de acesso, garantindo a correta identificação do agente nos casos em que suas condutas violarem os direitos de terceiros.[110]

Cabe ressaltar, aqui, que o Projeto de Lei do novo Código de Processo Penal se omite sobre o tema, que é tão relevante na sociedade moderna, não trazendo qualquer referência à obrigatoriedade de armazenamento dos registros de acesso e dos dados dos usuários da rede mundial de computadores. "Referente à internet, o projeto limita-se a prever, no título relativo às medidas cautelares pessoais, o bloqueio de endereço eletrônico".[111]

---

[108] DORIGON, Alessandro; SOARES, Renan Vinicius de Oliveira. **Crimes cibernéticos: dificuldades investigativas na obtenção de indícios da autoria e prova da materialidade.** Disponível em < https://jus.com.br/artigos/63549/crimes-ciberneticos-dificuldades-investigativas-na-obtencao-de-indicios-da-autoria-e-prova-da-materialidade>. Acesso em 15 de setembro de 2020.

[109] DORIGON, Alessandro; SOARES, Renan Vinicius de Oliveira. **Crimes cibernéticos: dificuldades investigativas na obtenção de indícios da autoria e prova da materialidade.** Disponível em < https://jus.com.br/artigos/63549/crimes-ciberneticos-dificuldades-investigativas-na-obtencao-de-indicios-da-autoria-e-prova-da-materialidade>. Acesso em 15 de setembro de 2020.

[110] VALVERDE, Danielle Novaes de Siqueira. **Crimes Cibernéticos: a obrigatoriedade do registro de acesso à internet como forma de possibilitar a identificação do criminoso.** Revista da ESMAPE. Recife. v. 15. n. 32. p. 246. jul./dez. 2010.

[111] VALVERDE, Danielle Novaes de Siqueira. **Crimes Cibernéticos: a obrigatoriedade do registro de acesso à internet como forma de possibilitar a identificação do criminoso.** Revista da ESMAPE. Recife. v. 15. n. 32. p. 247. jul./dez. 2010.

Deve-se atentar, neste ponto, ao concernente tema conexo à questão, qual seja, a responsabilidade criminal do representante dos provedores de acesso. A título de exemplo, temos os casos previstos no Estatuto da Criança e do Adolescente, que na redação de seu art. 241-A, incluído pela Lei 11.829 de 2008, dispõe[112]:

> Art. 241-A. Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa. § 1 º-Nas mesmas penas incorre quem: I – assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens de que trata o caput deste artigo; II – assegura, por qualquer meio, o acesso por rede de computadores às fotografias, cenas ou imagens de que trata o caput deste artigo. § 2 º–As condutas tipificadas nos incisos I e II do § 1 º-deste artigo são puníveis quando o responsável legal pela prestação do serviço, oficialmente notificado, deixa de desabilitar o acesso ao conteúdo ilícito de que trata o caput deste artigo.

Como se observa do texto legal, as figuras equiparas desse crime são voltadas aos provedores de acesso e de conteúdo. Contudo, como ordena o próprio §2º do referido artigo, tais condutas só serão puníveis quando o responsável legal pela prestação do serviço, oficialmente notificado, deixa de desabilitar o acesso ao conteúdo ilícito de que trata o caput deste artigo, sendo uma verdadeira condição objetiva de punibilidade.

A legislação brasileira vem movendo-se no sentido de preocupar-se em garantir meios para que o autor de determinada conduta ilegal possa ser devidamente identificado e responsabilizado por suas ações ilegais ou criminosas, contudo, isso ainda caminha a passos lentos. Tendo em vista que as leis brasileiras ainda não garantem completamente meios coercitivos para obrigar o cadastro e armazenamento dos dados necessários a correta identificação do usuário da rede que deu ensejo ao fato violador de direitos alheios, doutrina e jurisprudência tendem a tentar amenizar esse problema para a vítima, objetivando que a mesma não esteja completamente desamparada quando da busca por seus direitos. Nesse sentido, criam-se teses para que os provedores de acesso ou de conteúdo sejam responsabilizados nos casos em que não se puder identificar o autor da conduta. Isso terá embasamento no fato de que os provedores não foram diligentes em

---

[112] VALVERDE, Danielle Novaes de Siqueira. **Crimes Cibernéticos: a obrigatoriedade do registro de acesso à internet como forma de possibilitar a identificação do criminoso.** Revista da ESMAPE. Recife. v. 15. n. 32. p. 244. jul./dez. 2010.

sua responsabilidade de coletar dados e armazená-los devidamente, impossibilitando, assim, por sua omissão, a identificação do usuário que violou direitos de outrem.[113]

A pessoa que foi lesada em seus direitos tem a prerrogativa de buscar a reparação dos mesmos e a responsabilização adequada de quem os violou. Caso não haja a possibilidade de identificar o autor da conduta ilegal que ocorreu por meio da internet, por omissão dos provedores de acesso e de conteúdo, doutrina e jurisprudência garantem que a vítima poderá pleitear seus direitos contra o próprio provedor omitente, que será responsabilizado pela conduta ilegal de seu usuário, devido a sua falta de diligência. Em contrapartida, se o provedor conseguir indicar quem é o autor do fato ilegal, tendo registrado e armazenado os dados necessários para tal e os disponibilizar mediante autorização judicial de quebra de sigilo de dados, ficará isento de responsabilidade.[114]

Diante do exposto, conclui-se que a responsabilidade penal, civil ou administrativa, conforme o caso, por atos praticados por meio da internet, poderá recair sobre: os usuários da internet que deram ensejo ao ato ilegal, quando possível sua identificação por meio dos dados de acesso armazenados pelos devidos responsáveis; os provedores de acesso à rede ou provedores de conteúdo, quando os mesmos não mantém o devido e adequado controle dos usuários que utilizam de seus serviços, ou, ainda, poderá recair sobre as pessoas físicas proprietárias de redes privadas de acesso à internet que não tenham mantido diligência quanto à sua proteção para que terceiros não identificados a utilizassem indevidamente.[115]

A identificação do usuário da internet pode ocorrer em dois momentos distintos. A primeira identificação cabe ao provedor de acesso à rede, que, sendo responsável pela transmissão de dados, deverá realizar e ter sob sua guarda o registro do número de *internet protocol* (IP), localização, data, horário e fuso horário do respectivo acesso. O segundo

---

[113] MORAES, Paulo Francisco Cardoso de. **A vedação constitucional do anonimato aplicada à internet: o papel do estado brasileiro na identificação dos usuários e responsabilização dos provedores.** Revista Âmbito Jurídico**.** Disponível em <https://ambitojuridico.com.br/edicoes/revista-91/a-vedacao-constitucional-do-anonimato-aplicada-a-internet-o-papel-do-estado-brasileiro-na-identificacao-dos-usuarios-e-responsabilizacao-dos-provedores/>. Acesso em 16 de setembro de 2020.

[114] MORAES, Paulo Francisco Cardoso de. **A vedação constitucional do anonimato aplicada à internet: o papel do estado brasileiro na identificação dos usuários e responsabilização dos provedores.** Revista Âmbito Jurídico**.** Disponível em < https://ambitojuridico.com.br/edicoes/revista-91/a-vedacao-constitucional-do-anonimato-aplicada-a-internet-o-papel-do-estado-brasileiro-na-identificacao-dos-usuarios-e-responsabilizacao-dos-provedores/>. Acesso em 16 de setembro de 2020.

[115] MORAES, Paulo Francisco Cardoso de. **A vedação constitucional do anonimato aplicada à internet: o papel do estado brasileiro na identificação dos usuários e responsabilização dos provedores.** Revista Âmbito Jurídico**.** Disponível em <https://ambitojuridico.com.br/edicoes/revista-91/a-vedacao-constitucional-do-anonimato-aplicada-a-internet-o-papel-do-estado-brasileiro-na-identificacao-dos-usuarios-e-responsabilizacao-dos-provedores/>. Acesso em 16 de setembro de 2020.

momento da identificação do usuário ocorrerá no que tange aos provedores de serviços e conteúdos na rede, esses serão capazes de indicar, além do endereço de *internet protocol* (IP), localização, data, horário e fuso horário do acesso aos seus sites ou serviços, o conteúdo em si que foi inserido em seu servidor pelo usuário.[116]

A identificação do usuário deve ser feita nessas duas etapas, de forma conjunta. Isso será de grande importância, visto que a identificação pelos provedores de acesso à rede pode levar à correta identificação do agente e sua localização, já as informações prestadas pelos provedores de conteúdo e de serviços são pressupostos para a constatação da materialidade da conduta do usuário, pois tratam do próprio conteúdo em si da ação do mesmo e que podem ser facilmente apagados se não forem devidamente registrados pelos provedores.[117]

A relação jurídica direta proveniente do acesso à internet e do uso dos serviços e plataformas ali disponibilizados, se dá entre os usuários da rede e os provedores de acesso, de conteúdo ou de serviços.[118] Estabelecer a natureza dessa relação jurídica firmada é imprescindível para se determinar qual a responsabilidade das provedoras.

Os provedores de acesso à internet, quando devidamente licenciados, são caracterizados como fornecedores de serviços, por conseguinte, estão inclusos na definição do art. 3º do Código de Defesa do Consumidor. Também se aplicará a regra do referido artigo do Código de Defesa do Consumidor aos provedores de serviço, visto que estabelecerão uma atividade negocial com os consumidores na rede. Serão, ainda, classificados como fornecedores de serviços os provedores de conteúdo quando os mesmos desenvolverem atividades econômicas no fornecimento de seu objeto de trabalho, ou seja, quando disponibilizarem o conteúdo mediante pagamento ou qualquer outra vantagem patrimonial. Nesses casos, ficará caracterizada uma relação de consumo

---

[116] MORAES, Paulo Francisco Cardoso de. **A vedação constitucional do anonimato aplicada à internet: o papel do estado brasileiro na identificação dos usuários e responsabilização dos provedores.** Revista Âmbito Jurídico**.** Disponível em <https://ambitojuridico.com.br/edicoes/revista-91/a-vedacao-constitucional-do-anonimato-aplicada-a-internet-o-papel-do-estado-brasileiro-na-identificacao-dos-usuarios-e-responsabilizacao-dos-provedores/>. Acesso em 16 de setembro de 2020.

[117] MORAES, Paulo Francisco Cardoso de. **A vedação constitucional do anonimato aplicada à internet: o papel do estado brasileiro na identificação dos usuários e responsabilização dos provedores.** Revista Âmbito Jurídico**.** Disponível em <https://ambitojuridico.com.br/edicoes/revista-91/a-vedacao-constitucional-do-anonimato-aplicada-a-internet-o-papel-do-estado-brasileiro-na-identificacao-dos-usuarios-e-responsabilizacao-dos-provedores/>. Acesso em 16 de setembro de 2020.

[118] MIRAGEM, Bruno. **Responsabilidade por danos na sociedade de informação e proteção do consumidor: desafios atuais da regulação jurídica da Internet**. Revista de Direito do Consumidor: RDC. São Paulo. ano 18. n. 70. p. 50. abr.-jun. 2009.

entre o respectivo provedor e o usuário da internet, incidindo, por consequência, as regras de proteção ao consumidor previstas na legislação especifica.[119]

Contudo, se estivermos lidando com um provedor de conteúdos que esteja apenas exercendo sua atividade sem nenhuma finalidade econômica ou negocial, publicando conteúdos como forma de manifestação do seu direito à liberdade de expressão, teremos a incidência das normas do Código Civil quanto a sua responsabilidade.[120]

Nos casos em que houver exercício da atividade comercial, em que se caracterizará a relação de consumo, incidindo, assim, as regras pertinentes do Código de Defesa do Consumidor, a responsabilidade dos provedores de acesso, serviços ou conteúdo será objetiva.[121]

> No caso dos provedores de acesso e dos provedores de conteúdo em que exista atividade de intermediação de produtos e serviços, caracterizando intervenção profissional e organizada no mercado de consumo, tratam-se de situações a justificar a incidência do art. 14 do CDC na hipótese de danos ao consumidor, dando causa à responsabilidade objetiva do fornecedor.[122]

Em contrapartida, quando se tratar de provedores de conteúdo que não imprimirem nenhum tipo de atividade negocial com o usuário, estaremos diante de caso de aplicação das normas do Código Civil para estabelecer sua responsabilidade. Neste cenário, quando houver danos causados pelos usuários desses provedores e os mesmos não identificarem quem foi o responsável por esses atos ilegais, teremos a aplicação da responsabilidade por atos ilícitos, de natureza subjetiva, nos termos do art. 186 c/c art. 927, *caput*, do Código Civil de 2002.[123]

---

[119] MORAES, Paulo Francisco Cardoso de. **A vedação constitucional do anonimato aplicada à internet: o papel do estado brasileiro na identificação dos usuários e responsabilização dos provedores.** Revista Âmbito Jurídico**.** Disponível em <https://ambitojuridico.com.br/edicoes/revista-91/a-vedacao-constitucional-do-anonimato-aplicada-a-internet-o-papel-do-estado-brasileiro-na-identificacao-dos-usuarios-e-responsabilizacao-dos-provedores/>. Acesso em 16 de setembro de 2020.

[120] MORAES, Paulo Francisco Cardoso de. **A vedação constitucional do anonimato aplicada à internet: o papel do estado brasileiro na identificação dos usuários e responsabilização dos provedores.** Revista Âmbito Jurídico**.** Disponível em <https://ambitojuridico.com.br/edicoes/revista-91/a-vedacao-constitucional-do-anonimato-aplicada-a-internet-o-papel-do-estado-brasileiro-na-identificacao-dos-usuarios-e-responsabilizacao-dos-provedores/>. Acesso em 16 de setembro de 2020.

[121] MIRAGEM, Bruno. **Responsabilidade por danos na sociedade de informação e proteção do consumidor: desafios atuais da regulação jurídica da Internet**. Revista de Direito do Consumidor: RDC. São Paulo. ano 18. n. 70. p. 50. abr.-jun. 2009.

[122] MIRAGEM, Bruno. **Responsabilidade por danos na sociedade de informação e proteção do consumidor: desafios atuais da regulação jurídica da Internet**. Revista de Direito do Consumidor: RDC. São Paulo. ano 18. n. 70. p. 50. abr.-jun. 2009.

[123] MIRAGEM, Bruno. **Responsabilidade por danos na sociedade de informação e proteção do consumidor: desafios atuais da regulação jurídica da Internet**. Revista de Direito do Consumidor: RDC. São Paulo. ano 18. n. 70. p. 50. abr.-jun. 2009.

Devido a importância do tema, se mostra relevante uma análise das legislações internacionais sobre o assunto. A nível de Tratado Internacional, ganhou destaque as disposições concernentes contidas na Convenção de Budapeste. O art. 16 da referida convenção sobre o cybercrime dá poderes às autoridades competentes para que as mesmas tenham a prerrogativa de exigir o registro e a conservação pelos meios que julgarem convenientes e obter quaisquer informações e dados relativos aos acessos à rede, desde que haja fundadas razões para a referida autoridade acreditar que tais dados estão suscetíveis de perda ou alteração iminente.[124]

A Convenção ainda garante às autoridades competentes o poder de exigir dos provedores o armazenamento dos dados e informações pertinentes pelo período de tempo que julgarem necessário, estabelecendo, apenas, um limite máximo de 90 dias. Neste período em que as provedoras estariam obrigadas a armazenar com segurança tais dados, o Ministério Público ou a polícia justificariam ao magistrado a necessidade e imprescindibilidade de seu acesso a essas informações, requerendo o respectivo mandado judicial para quebra do sigilo dos dados.[125]

Quanto à legislação estrangeria, a título de comparação, inicia-se com as regras concernentes ao tema previstas nos Estados Unidos. Neste país, não há a obrigatoriedade de armazenamento dos registros e dados de acesso pelos provedores. Esta obrigação é tema de debates no Congresso desde 2008, mas ainda não há uma decisão definitiva sobre.[126]

O FBI (*Federal Bureau of Investigation*) propugna desde 2005 pela adoção de regras que obriguem os provedores a registrar e armazenar os dados de acesso e pleiteia que esse armazenamento seja feito por um período de, no mínimo, 02 anos. Em contrapartida, os provedores de acesso, serviços e conteúdos argumentam pela não obrigatoriedade, embasada no direito à privacidade.[127]

---

[124] VALVERDE, Danielle Novaes de Siqueira. **Crimes Cibernéticos: a obrigatoriedade do registro de acesso à internet como forma de possibilitar a identificação do criminoso.** Revista da ESMAPE. Recife. v. 15. n. 32. p. 239. jul./dez. 2010.

[125] VALVERDE, Danielle Novaes de Siqueira. **Crimes Cibernéticos: a obrigatoriedade do registro de acesso à internet como forma de possibilitar a identificação do criminoso.** Revista da ESMAPE. Recife. v. 15. n. 32. p. 239. jul./dez. 2010.

[126] VALVERDE, Danielle Novaes de Siqueira. **Crimes Cibernéticos: a obrigatoriedade do registro de acesso à internet como forma de possibilitar a identificação do criminoso.** Revista da ESMAPE. Recife. v. 15. n. 32. p. 240. jul./dez. 2010.

[127] VALVERDE, Danielle Novaes de Siqueira. **Crimes Cibernéticos: a obrigatoriedade do registro de acesso à internet como forma de possibilitar a identificação do criminoso.** Revista da ESMAPE. Recife. v. 15. n. 32. p. 240. jul./dez. 2010.

Ainda sobre os Estados Unidos, o anonimato se aplica aos usuários da internet neste país, visto que o entendimento jurisprudencial é de que a Primeira Emenda à Constituição Americana, que garante a liberdade de expressão e o direito ao anonimato, se aplica, também, aos atos praticados na rede mundial de computadores. Apesar disso, o ordenamento jurídico em questão não proíbe o monitoramento do acesso e da comunicação realizada pela internet.[128]

Outro país que adota a não exigência do registro e armazenamento dos dados de acesso e conteúdo na internet, é Cingapura. Aqui também é garantido o anonimato aos usuários.[129]

Contrariamente à política anteriormente mencionada, se opondo ao acesso amplo e irrestrito dos usuários na internet, se encontram as legislações de países como a China, Croácia, Índia e Paquistão.[130]

"A política Chinesa para a internet é baseada na lei e na segurança e amparada no princípio do uso correto, voltado a criar um ambiente harmônico, saudável e de promoção do progresso social e econômico".[131]

Há, na China, um rigoroso sistema de controle dos acessos e dos conteúdos publicados na rede. Esse controle é realizado pelos órgãos governamentais. A legislação chinesa veda o anonimato e obriga os provedores a realizarem o registro e o armazenamento dos dados de acesso pelo período de até 60 dias. Após esse período determinado para o armazenamento dessas informações, elas deverão ser disponibilizadas aos órgãos de segurança e à Procuradoria do Povo, objetivando a manutenção da segurança nacional e eventuais investigações de crimes.[132]

---

[128] VALVERDE, Danielle Novaes de Siqueira. **Crimes Cibernéticos: a obrigatoriedade do registro de acesso à internet como forma de possibilitar a identificação do criminoso.** Revista da ESMAPE. Recife. v. 15. n. 32. p. 240. jul./dez. 2010.

[129] VALVERDE, Danielle Novaes de Siqueira. **Crimes Cibernéticos: a obrigatoriedade do registro de acesso à internet como forma de possibilitar a identificação do criminoso.** Revista da ESMAPE. Recife. v. 15. n. 32. p. 241. jul./dez. 2010.

[130] VALVERDE, Danielle Novaes de Siqueira. **Crimes Cibernéticos: a obrigatoriedade do registro de acesso à internet como forma de possibilitar a identificação do criminoso.** Revista da ESMAPE. Recife. v. 15. n. 32. p. 241. jul./dez. 2010.

[131] VALVERDE, Danielle Novaes de Siqueira. **Crimes Cibernéticos: a obrigatoriedade do registro de acesso à internet como forma de possibilitar a identificação do criminoso.** Revista da ESMAPE. Recife. v. 15. n. 32. p. 241. jul./dez. 2010.

[132] VALVERDE, Danielle Novaes de Siqueira. **Crimes Cibernéticos: a obrigatoriedade do registro de acesso à internet como forma de possibilitar a identificação do criminoso.** Revista da ESMAPE. Recife. v. 15. n. 32. p. 241. jul./dez. 2010.

Lidando de forma rigorosa com o tema, o Governo Chinês, por meio do órgão da Diretoria do Escritório de Informação do Conselho de Estado, se manifestou no sentido de criar a obrigação legal aos usuários de utilizarem seu nome verdadeiro nas redes.[133]

Neste país, quanto a responsabilidade pelos atos lesivos causados através da internet, se decidiu que a responsabilidade é solidária entre o usuário e o próprio provedor.[134]

Na Croácia, a legislação que trata sobre o assunto é a lei sobre Comunicações Eletrônicas, publicada em 24 de junho de 2008.[135] Por esta lei fica determinado que é obrigatório o registro e armazenamento dos dados de acesso dos usuários na internet pelo período de, no máximo, 12 meses e com a estrita finalidade de investigação e processo por ilícitos penais que atentem contra a defesa e a segurança nacional.[136] A regra geral adotada é de que o anonimato é vedado.[137]

Na Índia, há a obrigatoriedade de registro e armazenamento dos dados de acesso pelo período de 01 ano. Há grande preocupação do país quanto ao controle em estabelecimentos de comercializam acesso à rede, como as *lan houses* e os *cybercafés*. Em Bombaim, cidade na Índia, a própria polícia realiza o monitoramento nesses locais, cadastrando os usuários que irão utilizar dos pontos de acesso comercializados.[138] "Além disso, o funcionamento de um *cybercafé* depende de licença especial e os seus proprietários estão obrigados a instalar filtros nos computadores, de modo a bloquear pornográfica ou outro tipo de material considerado ofensivo".[139]

---

[133] VALVERDE, Danielle Novaes de Siqueira. **Crimes Cibernéticos: a obrigatoriedade do registro de acesso à internet como forma de possibilitar a identificação do criminoso.** Revista da ESMAPE. Recife. v. 15. n. 32. p. 241. jul./dez. 2010.

[134] VALVERDE, Danielle Novaes de Siqueira. **Crimes Cibernéticos: a obrigatoriedade do registro de acesso à internet como forma de possibilitar a identificação do criminoso.** Revista da ESMAPE. Recife. v. 15. n. 32. p. 241. jul./dez. 2010.

[135] VALVERDE, Danielle Novaes de Siqueira. **Crimes Cibernéticos: a obrigatoriedade do registro de acesso à internet como forma de possibilitar a identificação do criminoso.** Revista da ESMAPE. Recife. v. 15. n. 32. p. 241. jul./dez. 2010.

[136] VALVERDE, Danielle Novaes de Siqueira. **Crimes Cibernéticos: a obrigatoriedade do registro de acesso à internet como forma de possibilitar a identificação do criminoso.** Revista da ESMAPE. Recife. v. 15. n. 32. p. 241-242. jul./dez. 2010.

[137] VALVERDE, Danielle Novaes de Siqueira. **Crimes Cibernéticos: a obrigatoriedade do registro de acesso à internet como forma de possibilitar a identificação do criminoso.** Revista da ESMAPE. Recife. v. 15. n. 32. p. 242. jul./dez. 2010.

[138] VALVERDE, Danielle Novaes de Siqueira. **Crimes Cibernéticos: a obrigatoriedade do registro de acesso à internet como forma de possibilitar a identificação do criminoso.** Revista da ESMAPE. Recife. v. 15. n. 32. p. 242. jul./dez. 2010.

[139] VALVERDE, Danielle Novaes de Siqueira. **Crimes Cibernéticos: a obrigatoriedade do registro de acesso à internet como forma de possibilitar a identificação do criminoso.** Revista da ESMAPE. Recife. v. 15. n. 32. p. 242. jul./dez. 2010.

O Paquistão é mais um país que começou a legislar sobre os temas concernentes ao uso da internet. Após episódios terroristas sofridos no país, em que não foi possível a identificação dos agentes criminosos, a regulamentação dos acessos através dos *cybercafés* passou a ser considerada assunto de segurança nacional, dando ensejo à criação de normas para obrigar a instituição de um rígido sistema de controle e armazenamento de dados dos clientes e seus respectivos acessos à rede.[140]

Na Dinamarca também há leis que obrigam o registro e armazenamento dos dados e informações concernentes ao uso da internet pelo período de 01 ano. Contudo, os provedores são responsáveis por dados de acesso, mas não o são quanto aos conteúdos transmitidos pelos usuários. O armazenamento não se estende às informações transmitidas no uso da rede. Quanto ao anonimato, entende-se que, nesse país, é possível quando o acesso à internet for realizado via telefonia pré-paga.[141]

Em Omã, na Península Arábica, há a necessidade de armazenamento dos downloads feitos pelos usuários da internet pelo período de 03 meses e o acesso anônimo na rede é ilegal.[142]

Por fim, na nossa análise comparativa, temos a Arábia Saudita que obriga a guarda dos *logs* e demais dados de acesso à rede pelo período de 06 meses. A responsabilidade é bem delineada, respondendo o usuário por seus atos na internet e os provedores sendo responsáveis apenas pela identificação dos mesmos, sendo que se não o fizer corretamente responderá por sua omissão, mas não pelos atos do usuário.[143]

2.3 OBRIGATORIEDADE DE ARMAZENAMENTO DE DADOS PELOS ESTABELECIMENTOS QUE COMERCIALIZAM A LOCAÇÃO DE TERMINAIS DE COMPUTADORES

[140] VALVERDE, Danielle Novaes de Siqueira. **Crimes Cibernéticos: a obrigatoriedade do registro de acesso à internet como forma de possibilitar a identificação do criminoso.** Revista da ESMAPE. Recife. v. 15. n. 32. p. 242. jul./dez. 2010.
[141] VALVERDE, Danielle Novaes de Siqueira. **Crimes Cibernéticos: a obrigatoriedade do registro de acesso à internet como forma de possibilitar a identificação do criminoso.** Revista da ESMAPE. Recife. v. 15. n. 32. p. 242. jul./dez. 2010.
[142] VALVERDE, Danielle Novaes de Siqueira. **Crimes Cibernéticos: a obrigatoriedade do registro de acesso à internet como forma de possibilitar a identificação do criminoso.** Revista da ESMAPE. Recife. v. 15. n. 32. p. 243. jul./dez. 2010.
[143] VALVERDE, Danielle Novaes de Siqueira. **Crimes Cibernéticos: a obrigatoriedade do registro de acesso à internet como forma de possibilitar a identificação do criminoso.** Revista da ESMAPE. Recife. v. 15. n. 32. p. 243. jul./dez. 2010.

Considerando que o direito ao anonimato é vedado no uso da liberdade de expressão, e que essa é limitada quando em contraposição com outros direitos, cria-se a necessidade de se identificar os agentes que infringem tais regras, para poder responsabilizá-los por suas ações. A partir dessa premissa, nasce a discussão sobre a obrigatoriedade do armazenamento de dados que sejam suficientes para identificar o usuário por trás de uma conduta ilegal, e as formas como isso será feito de maneira que seja suficiente e eficaz, mas que respeite os direitos e liberdades dos cidadãos no Estado Democrático de Direito.

A identificação dos chamados cybercriminosos, ou seja, as pessoas que se utilizam da internet e de suas facilidades para permanecerem às margens da lei, é dificultada pela deficiência legislativa sobre o assunto. À medida em que as leis do país não conseguem regular de maneira concreta e especifica o tema, criam-se lacunas que tornam o trabalho investigativo e o dever punitivo do Estado falhos, visto não se conseguir, em muitos casos, nem a identificação do agente criminoso, impulsionando a própria criminalidade virtual.[144]

As atuais iniciativas legislativas locais que analisamos ao longo do tópico anterior deste trabalho, demonstram a crescente necessidade de regulamentação do tema, visto a importância prática que o registro e guarda dos dados de acesso e de cadastro dos usuários têm para proteção de outros direitos que, eventualmente, sejam atingidos por condutas de usuários na rede. Contudo, a abrangência limitada que as leis locais possuem fazem com que sejam insuficientes para lidar com o problema, causando, ainda, dificuldades quanto às divergências na forma de legislar sobre o tema de região para região.[145]

Como analisado anteriormente, percebe-se que há iniciativas legislativas em âmbito federal visando a regulamentação sobre a obrigatoriedade e o tempo de registro e guarda dos *logs* de acesso e cadastro de usuários quando de sua utilização à rede mundial de computadores. Contudo, é manifesto que tais iniciativas ainda estão muito aquém do necessário para lidar com tamanha problemática.

As leis ainda são insuficientes, seja quanto a amplitude de suas normas, que não chegam a regulamentar o problema por inteiro, estando deficientes no aspecto do poder

---

[144] VALVERDE, Danielle Novaes de Siqueira. **Crimes Cibernéticos: a obrigatoriedade do registro de acesso à internet como forma de possibilitar a identificação do criminoso.** Revista da ESMAPE. Recife. v. 15. n. 32. p. 249. jul./dez. 2010.

[145] VALVERDE, Danielle Novaes de Siqueira. **Crimes Cibernéticos: a obrigatoriedade do registro de acesso à internet como forma de possibilitar a identificação do criminoso.** Revista da ESMAPE. Recife. v. 15. n. 32. p. 249. jul./dez. 2010.

extroverso do Estado de obrigar os mais diversos segmentos à um registro completo de informações sobre o acesso e sobre o próprio usuário; seja quanto à definição de um tempo suficiente para que tais dados fiquem armazenados com segurança pelos responsáveis pelo registro e guarda; seja pela carência de normas que regulamentem e padronizem a forma de registro e armazenamento desses dados, garantindo a confiabilidade dos mesmos para sua utilização no processo cível ou penal que os necessitar para constituir prova, ou pela falta de leis que tratem sobre a obrigatoriedade de colaboração das empresas e provedores com o Poder Público.

Atualmente, pela redação da Lei nº 12.965, de 23 de abril de 2014**,** conhecida como Marco Civil da Internet, há a obrigatoriedade do registro de acesso pelo prazo de 06 meses e do registro de conexão à rede pelo período de 01 ano, devendo os provedores responsáveis pelo registro e armazenamento desses dados mantê-los sob sigilo que só poderá ser quebrado mediante ordem judicial emanada por autoridade judiciária competente.[146]

Relativo ao tempo de armazenamento dos dados obtidos em uma conexão à internet e de seus respectivos usuários, há oposição entre os provedores de acesso e conteúdo e o Poder Público, em especial as instituições policiais.[147] Ambos os lados possuem argumentos distintos quanto à guarda dos *logs* e o período que deve ser obrigatória essa conservação.

Os provedores, que são os responsáveis pelo registro e guarda dos dados relativos ao acesso à rede ou ao conteúdo nela publicado, alegam que é demasiadamente oneroso o custo para implementar meios seguros de registro e guarda dos dados de acesso, em especial se o tempo de armazenamento desses dados for muito longo, o que, segundo eles, é inviável. Tais empresas propugnam pela não obrigatoriedade do registro e guarda dos *logs* e dados de acesso e conteúdo, e alegam que se tal obrigação for imposta, o armazenamento deve ser feito por um curto período, para evitar custos excessivos às provedoras responsáveis.[148]

---

[146] VALVERDE, Danielle Novaes de Siqueira. **Crimes Cibernéticos: a obrigatoriedade do registro de acesso à internet como forma de possibilitar a identificação do criminoso.** Revista da ESMAPE. Recife. v. 15. n. 32. p. 245. jul./dez. 2010.

[147] VALVERDE, Danielle Novaes de Siqueira. **Crimes Cibernéticos: a obrigatoriedade do registro de acesso à internet como forma de possibilitar a identificação do criminoso.** Revista da ESMAPE. Recife. v. 15. n. 32. p. 245. jul./dez. 2010.

[148] VALVERDE, Danielle Novaes de Siqueira. **Crimes Cibernéticos: a obrigatoriedade do registro de acesso à internet como forma de possibilitar a identificação do criminoso.** Revista da ESMAPE. Recife. v. 15. n. 32. p. 245. jul./dez. 2010.

O Poder Público, por sua vez, preocupado com a efetiva concretização do *jus puniendi estatal*, nos casos de crimes cometidos pela internet, ou preocupados com a responsabilização dos autores de outros atos ilegais que lesionam direitos de terceiros, apresentam argumentos contrários às reclamações dos provedores de acesso e conteúdo. Os órgãos do Poder Público ressaltam a importância e imprescindibilidade do registro dos dados completos de acesso e de identificação dos usuários à rede mundial de computadores, e o armazenamento desses dados por período de tempo suficiente à constituição de prova do ato ilegal ou criminoso praticado.[149]

Na fase da persecução penal relativa à investigação criminal realizada por órgão com competência de polícia judiciária, respeitado o que preceitua a Constituição Federal de 1988, em seu artigo 144, as polícias judiciárias alegam que o prazo estabelecido pelo Marco Civil da Internet é absurdamente curto, o que, na prática, dificulta e, por vezes, até impossibilita a efetiva investigação dos crimes cometidos pela internet, gerando impunidade.[150]

Um dos argumentos apresentados à crítica do tempo de obrigatoriedade do armazenamento dos dados é de que, em muitas situações, o tempo que decorre até o conhecimento pela vítima do fato criminoso supera em muito o tempo estabelecido para o armazenamento dos dados que, na maioria das vezes, são as provas de autoria e materialidade do respectivo crime.[151]

Outro problema que leva às instituições policiais a requererem e argumentarem por um tempo maior de obrigatoriedade do armazenamento seguro dos dados e *logs* de acesso, conteúdo e identificação dos usuários da internet, é o fato de que, nos casos práticos, muitas vezes a investigação se depara com crimes de alta complexidade, como os que envolvem o crime organizado e, em tais situações, os fatos criminosos vão sendo conhecidos apenas durante o decorrer das investigações o que pode levar meses, senão

---

[149] VALVERDE, Danielle Novaes de Siqueira. **Crimes Cibernéticos: a obrigatoriedade do registro de acesso à internet como forma de possibilitar a identificação do criminoso.** Revista da ESMAPE. Recife. v. 15. n. 32. p. 245. jul./dez. 2010.

[150] VALVERDE, Danielle Novaes de Siqueira. **Crimes Cibernéticos: a obrigatoriedade do registro de acesso à internet como forma de possibilitar a identificação do criminoso.** Revista da ESMAPE. Recife. v. 15. n. 32. p. 245. jul./dez. 2010.

[151] VALVERDE, Danielle Novaes de Siqueira. **Crimes Cibernéticos: a obrigatoriedade do registro de acesso à internet como forma de possibilitar a identificação do criminoso.** Revista da ESMAPE. Recife. v. 15. n. 32. p. 245. jul./dez. 2010.

anos, a depender do crime perpetrado. Nesses casos, por óbvio, a destruição dos dados leva à frustração das investigações e à impunidade dos criminosos.[152]

Ademais, o prazo preconizado para a guarda dos registros dos dados relativos aos acessos à rede esbarra na questão dos prazos prescricionais dos crimes praticados contra ou por meio da internet. Indiretamente, esse prazo para o armazenamento afeta o direito de punir do Estado, induzindo ao entendimento de que o prazo prescricional relativo a tais crimes será o tempo previsto para o armazenamento dos dados, qual seja, 06 meses, em regra. Esse entendimento se dá pois se o Estado não agir dentro desse período em que os dados estão disponíveis para serem acessados, ficará impedido, faticamente, de cumprir seu dever na proteção dos direitos lesados.[153]

Devido aos fortes argumentos apresentados visando demostrar a insuficiência do tempo estabelecido para o armazenamento dos dados e os problemas que isso pode gerar na defesa dos direitos ameaçados e lesados por atos de terceiros na internet, teve início, em 2008, o Projeto de Lei do Senado nº 494/2008, visando estabelecer a obrigatoriedade do armazenamento dos dados registrados por um período de tempo maior que o atualmente estabelecido. Em 2015, esse Projeto de Lei aprovado no Senado Federal foi enviado à Câmara dos Deputados para votação, local em que ainda se encontra pendente de deliberação e sob o número 2.514/2015. Essa iniciativa legislativa busca estabelecer a obrigatoriedade do registro e armazenamentos dos dados de acesso à rede pelo período de 03 anos.[154]

Desta forma, a proposta atual é de que haja a obrigatoriedade de armazenamento dos *logs* e dados de acesso, conteúdo e dados cadastrais dos usuários por um período de 03 anos, período que está de acordo com o estabelecido na cláusula terceira do Termo de Mútua Cooperação[155] firmado entre os principais provedores do Brasil; o Senado Federal,

---

[152] VALVERDE, Danielle Novaes de Siqueira. **Crimes Cibernéticos: a obrigatoriedade do registro de acesso à internet como forma de possibilitar a identificação do criminoso.** Revista da ESMAPE. Recife. v. 15. n. 32. p. 245. jul./dez. 2010.

[153] POLICIA FEDERAL. **Contribuição da Policia Federal para o Marco Civil da Internet.** Disponível em <http://culturadigital.br/marcocivil/2010/05/31/contribuicao-da-policia-federal-para-o-marco-civil-da-internet/>. Acesso em 29 de setembro de 2020.

[154] DORIGON, Alessandro; SOARES, Renan Vinicius de Oliveira. **Crimes cibernéticos: dificuldades investigativas na obtenção de indícios da autoria e prova da materialidade.** Disponível em < https://jus.com.br/artigos/63549/crimes-ciberneticos-dificuldades-investigativas-na-obtencao-de-indicios-da-autoria-e-prova-da-materialidade>. Acesso em 01 de outubro de 2020.

[155] VALVERDE, Danielle Novaes de Siqueira. **Crimes Cibernéticos: a obrigatoriedade do registro de acesso à internet como forma de possibilitar a identificação do criminoso.** Revista da ESMAPE. Recife. v. 15. n. 32. p. 246. jul./dez. 2010.

por meio de sua Comissão Parlamentar de Pedofilia; o Comitê Gestor da Internet[156]; o Ministério Público Federal; Ministérios Públicos Estaduais; Polícia Federal e a Sociedade Civil[157].

Quando se trata da obrigatoriedade do registro dos dados relativos a um acesso à rede, deve-se atentar que é necessário que os dados sejam coletados de forma ampla e completa. Somente o registro do endereço de *internet protocol*, o conhecido IP, não é suficiente para uma concreta identificação dos agentes de atos lesivos à direitos alheios.

Os provedores e empresas que lidam com o acesso e conteúdo da internet, quando se vêm obrigadas a realizarem a coleta desses dados e o armazenamento seguro dos mesmos, alegam que o simples número de endereço de IP é o suficiente. Tal narrativa visa economizar nos meios e tecnologias adequadas que deverão ser empregados para garantir a efetiva e real identificação dos usuários e registros dos seus acessos, e os custos com o armazenamento de tais informações. Contudo, a argumentação de que o registro e guarda dos endereços de IP são suficientes para correta identificação do usuário não é válida e não tem aceitação pelos operadores do direito, sendo, inclusive, afastada pelos tribunais americanos em suas decisões.[158]

Outro problema que invalida o argumento de que o registro e guarda dos números de endereço de *internet protocol* são suficientes são as tecnologias *proxy*, já apresentadas nesse trabalho. Vale lembrar, neste ponto, no que consiste tal tecnologia. O *proxy*, como mencionado anteriormente, é um sistema que fará a mediação entre o usuário e o endereço final da internet que o mesmo busca acessar, gerando um endereço único de IP para todos os usuários que se valerem do *proxy* para utilizar a rede. Desta forma, o endereço de IP encontrado em uma conexão que se utilizou deste programa será o número de *internet protocol* do *proxy* e não do real usuário, que permanecerá anônimo. Vislumbra-se, com isso, a insuficiência do endereço de IP para identificação do agente que cometeu a conduta danosa.[159]

---

[156] RABANEDA, Fabiano. **Os logs de acesso e sua guarda pelos provedores.** Disponível em <http://www.nic.br/imprensa/clipping/2010/midia165.htm>. Acesso em 01 de outubro de 2020.

[157] MALTA, Magno. **Termo de Mútua Cooperação.** Disponível em <http://www.safernet.org.br/site/sites/default/files/Teles.pdf>. Acesso em 01 de outubro de 2020.

[158] PAGANELLI, Celso Jefferson Messias. **Anonimato e internet: análise do princípio constitucional frente às recentes decisões do STJ.** Revista Âmbito Jurídico**.** Disponível em <https://ambitojuridico.com.br/cadernos/direito-constitucional/anonimato-e-internet-analise-do-principio-constitucional-frente-as-recentes-decisoes-do-stj/>. Acesso em 01 de outubro de 2020.

[159] PAGANELLI, Celso Jefferson Messias. **Anonimato e internet: análise do princípio constitucional frente às recentes decisões do STJ.** Revista Âmbito Jurídico**.** Disponível em <https://ambitojuridico.com.br/cadernos/direito-constitucional/anonimato-e-internet-analise-do-principio-constitucional-frente-as-recentes-decisoes-do-stj/>. Acesso em 01 de outubro de 2020.

As empresas e provedores de acesso e conteúdo, utilizando o argumento de que o simples endereço de IP é suficiente para identificação dos atos e dos agentes que causam danos na internet à direitos de terceiros, desrespeitam o preconizado pela Constituição Federal de 1988, que estabelece a vedação ao anonimato e o direito de acesso à justiça, garantido pelo princípio da inafastabilidade da apreciação jurisdicional.

O endereçamento de IP não é suficiente para identificar condutas e seus agentes, tão pouco para constituir prova de autoria de infrações penais, visto que tal dado não identifica pessoas, mas sim dispositivos, quando muito conseguem fazê-lo com precisão.[160]

O aparelho eletrônico em si não é suficiente para identificar, com precisão, quem é o proprietário do equipamento que está realizando a conexão à rede. Com isso, se torna necessário que haja uma identificação pessoal do usuário, com seu cadastro informando seus dados pessoais, sendo que para isso serão necessárias tecnologias que tentem garantir a verificação do uso de documentos e informações verdadeiras pelo agente que tente acessar a rede. Além disso, será necessário o registro do local, dia, horário e fuso horário da conexão, para, somente com esses dados, poder ser realizada a identificação da máquina de origem dos dados de conexão e de seu respectivo usuário conectado à internet naquela ocasião.[161]

Como elencado anteriormente, por diversos motivos a identificação de uma máquina, através de seu número de endereço de *internet protocol*, não basta. Isso se dá devido ao fato de que, mesmo sendo possível identificar o aparelho eletrônico que originou determinada conexão à rede, ainda assim não haverá a identificação precisa de quem de fato foi o usuário e real responsável por um ato ilegal, não sendo suficiente para caracterização da prova de autoria de uma conduta lesiva ou de uma infração penal, sendo impossível responsabilizar alguém dessa forma.

Além das redes públicas de acesso e dos próprios programas que impedem a identificação do real endereço de IP do usuário, temos ocasiões em que será difícil de haver a identificação do real responsável, mesmo se tratando de redes privadas. A

---

[160] PAGANELLI, Celso Jefferson Messias. **Anonimato e internet: análise do princípio constitucional frente às recentes decisões do STJ.** Revista Âmbito Jurídico**.** Disponível em < https://ambitojuridico.com.br/cadernos/direito-constitucional/anonimato-e-internet-analise-do-principio-constitucional-frente-as-recentes-decisoes-do-stj/>. Acesso em 01 de outubro de 2020.

[161] MORAES, Paulo Francisco Cardoso de. **A vedação constitucional do anonimato aplicada à internet: o papel do estado brasileiro na identificação dos usuários e responsabilização dos provedores.** Revista Âmbito Jurídico**.** Disponível em < https://ambitojuridico.com.br/edicoes/revista-91/a-vedacao-constitucional-do-anonimato-aplicada-a-internet-o-papel-do-estado-brasileiro-na-identificacao-dos-usuarios-e-responsabilizacao-dos-provedores/>. Acesso em 01 de outubro de 2020.

exemplo disso, há os casos em que em uma residência, pensão ou mesmo repúblicas em que várias pessoas, da mesma família ou não, moram juntas e dividem a mesma internet, sendo, muitas vezes, impossível se identificar quem foi o responsável por determinada conexão. Nesse exemplo, ainda teremos a problemática que envolve crianças e adolescentes, inimputáveis, que residem no mesmo local que adultos, onde todos se valem da mesma internet, sendo improvável que haja uma forma de se demonstrar quem realizou efetivamente o acesso à rede naquela ocasião específica que lesionou algum direito.[162]

Nesse sentido, no direito comparado, considerando que o endereço de *internet protocol* identifica máquinas e não pessoas, caminham as decisões da Suprema Corte dos Estados Unidos, que consideram o endereço de IP prova insuficiente para, sozinho, demonstrar a responsabilidade de alguém perante um ato ilegal.[163]

A maior problemática enfrentada quando o assunto é a identificação dos usuários responsáveis por ações criminosas ou que lesam direitos de terceiros se valendo da internet para tal, ou mesmo ações contra a internet e banco de dados, são as redes públicas de acesso. Nas redes públicas de acesso à internet, que são disponibilizadas nos mais variados locais e estabelecimentos públicos ou acessíveis ao público, qualquer pessoa pode se conectar à rede e exercer qualquer atividade nela se valendo da rede sem fio e sem a necessidade de prévio registro ou cadastro de seus dados em servidores ou provedores para tal, tornando praticamente impossível o reconhecimento deste usuário para sua responsabilização.[164]

Com a popularização da internet, se torna cada vez mais comum, e de mais fácil acesso, locais em que haja a disponibilização gratuita de redes sem fio de conexão, visando a promoção de políticas sociais de inclusão de todos os níveis da população, sem distinções. Esses tipos de acesso carecem de controle, não se exigindo, na grande maioria dos casos, nenhum tipo de cadastro prévio do usuário e, ainda, quando exigido, não há o controle quanto aos dados apresentados pelo sujeito, não se podendo garantir que tais

---

[162] PAGANELLI, Celso Jefferson Messias. **Anonimato e internet: análise do princípio constitucional frente às recentes decisões do STJ.** Revista Âmbito Jurídico**.** Disponível em <https://ambitojuridico.com.br/cadernos/direito-constitucional/anonimato-e-internet-analise-do-principio-constitucional-frente-as-recentes-decisoes-do-stj/>. Acesso em 01 de outubro de 2020.

[163] PAGANELLI, Celso Jefferson Messias. **Anonimato e internet: análise do princípio constitucional frente às recentes decisões do STJ.** Revista Âmbito Jurídico**.** Disponível em <https://ambitojuridico.com.br/cadernos/direito-constitucional/anonimato-e-internet-analise-do-principio-constitucional-frente-as-recentes-decisoes-do-stj/>. Acesso em 01 de outubro de 2020.

[164] VALVERDE, Danielle Novaes de Siqueira. **Crimes Cibernéticos: a obrigatoriedade do registro de acesso à internet como forma de possibilitar a identificação do criminoso.** Revista da ESMAPE. Recife. v. 15. n. 32. p. 250. jul./dez. 2010.

informações são verdadeiras. Nesse aspecto, a utilização das redes públicas de acesso à internet torna, praticamente, nulas as possibilidades de identificação do usuário.[165]

Os problemas relativos a identificação do usuário que comete condutas ilegais ou, até mesmo, criminosas por meio da internet se tornam ainda mais complexos quando tais ações são cometidas pela conexão à rede realizada em locais que comercializam o acesso, como as *lan houses* e os *cybercafés.* Como já discutido amplamente em capítulos anteriores deste trabalho, a legislação brasileira carece de leis que regulamentem, obriguem e fiscalizem o registro de clientes usuários da rede mundial de computadores nesses locais. Apesar de haverem propostas legislativas pontuais sobre o tema, que, frisa-se, ainda são insuficientes, a grande maioria dos estabelecimentos não realiza nenhum tipo de controle sobre seus clientes, tornando impossível a identificação do usuário e sua responsabilização ou punição.[166]

> A conclusão que se chega, é que o endereço IP não é uma forma confiável de se identificar uma pessoa, principalmente se for com o propósito de responsabilizar alguém por um ato ilícito, em virtude da fragilidade que o sistema representa como um todo, intrinsecamente, e também por conta das tecnologias disponíveis que permitem a ocultação do responsável, lembrando ainda, das vulnerabilidades encontradas em diversas redes que permitem o uso indiscriminado por pessoas que não estariam autorizadas.[167]

Nesta senda, concluímos pela imprescindibilidade e urgência de iniciativas legislativas movidas no sentido de regulamentar, obrigar e implementar uma forte fiscalização quanto aos registros e armazenamento dos dados de acesso à rede, de forma ampla e completa, sem deixar lacunas que propiciem o anonimato e a impunidade, especialmente relativo aos registro de cadastro dos dados dos usuários, e não apenas das máquinas, e à maneiras de se certificar que os dados e documentos informados são, de fato, verdadeiros.

---

[165] PAGANELLI, Celso Jefferson Messias. **Anonimato e internet: análise do princípio constitucional frente às recentes decisões do STJ.** Revista Âmbito Jurídico**.** Disponível em <https://ambitojuridico.com.br/cadernos/direito-constitucional/anonimato-e-internet-analise-do-principio-constitucional-frente-as-recentes-decisoes-do-stj/>. Acesso em 01 de outubro de 2020.

[166] VALVERDE, Danielle Novaes de Siqueira. **Crimes Cibernéticos: a obrigatoriedade do registro de acesso à internet como forma de possibilitar a identificação do criminoso.** Revista da ESMAPE. Recife. v. 15. n. 32. p. 249. jul./dez. 2010.

[167] PAGANELLI, Celso Jefferson Messias. **Anonimato e internet: análise do princípio constitucional frente às recentes decisões do STJ.** Revista Âmbito Jurídico**.** Disponível em <https://ambitojuridico.com.br/cadernos/direito-constitucional/anonimato-e-internet-analise-do-principio-constitucional-frente-as-recentes-decisoes-do-stj/>. Acesso em 01 de outubro de 2020.

3. NORMAS INTERNAS E INTERNACIONAIS SOBRE CIBERCRIME E INVESTIGAÇÃO CRIMINAL

A internet como se conhece hoje se tornou um instrumento imprescindível nas relações interpessoais e negociais modernas, tal característica impulsiona seu constante avanço e adaptação às necessidades de seus usuários.

A internet transcende fronteiras, não conhece limites, é capaz de interconectar pessoas de todas as partes do mundo, tornando possível os mais diversos tipos de comunicações, ignorando, em diversos aspectos, a distância geográfica que se impõe. Como leciona Assis Medeiros: "não há fronteiras demarcadas no ambiente cibernético. Isso derruba um dos principais pilares do chamado Estado Moderno".[168]

Com o avanço da tecnologia surgiram novas modalidades de crimes que, sem demora, também aderiram à transnacionalidade como uma de suas características principais, passando as ameaças a serem globalizadas.

Devido à natureza transnacional da internet, e dos crimes cometidos por meio desse ambiente virtual, se torna crescente a necessidade de se estabelecer uma cooperação internacional entre os órgãos judiciários e investigativos de diferentes países voltada ao combate dessas práticas delituosas, visando a redução das burocracias existentes no processo de investigação e julgamento de tais delitos que lesam diversos Estados soberanos em sua prática.[169]

A cooperação internacional entre os órgãos que lidam com a persecução penal nos países ao redor do mundo se faz, hoje, medida imprescindível e insubstituível no combate à tais ameaças globalizadas, visto que não há outra forma de enfrentamento eficaz aos crimes cibernéticos que ultrapassam os limites geográficos dos Estados. A cibercriminalidade desconhece fronteiras em um mundo que é politicamente dividido, o que torna a cooperação internacional medida necessária para se estabelecer regras e meios para que essas diferentes nações possam se unir visando a repressão das crescentes

---

[168] MEDEIROS, Assis. **Hackers: entre a ética e a criminalização**. Florianópolis: Visual Books. p. 147. 2002.

[169] DORIGON, Alessandro; SOARES, Renan Vinicius de Oliveira. **Crimes cibernéticos: dificuldades investigativas na obtenção de indícios da autoria e prova da materialidade.** Disponível em <https://jus.com.br/artigos/63549/crimes-ciberneticos-dificuldades-investigativas-na-obtencao-de-indicios-da-autoria-e-prova-da-materialidade>. Acesso em 19 de outubro de 2020.

ameaças virtuais. Se assim não for, não haverá um meio eficaz para se acompanhar e reprimir a evolução dos crimes tecnológicos.[170]

Visto a importância que os tratados e convenções sobre cooperação internacional visando o combate aos crimes cibernéticos possuem, se torna evidente que o Brasil deve se atentar a necessidade de estabelecer acordos de cooperação e se tornar signatário de tratados concernentes ao tema, em especial a Convenção sobre o Cibercrime, de 2001, conhecida como Convenção de Budapeste, que é hoje o principal tratado internacional sobre o assunto. [171]

3.1 CONVENÇÃO DE BUDAPESTE

As ferramentas *on-line* possibilitam que diversas atividades do cotidiano sejam exercidas com a facilidade do ambiente virtual, contudo, essas mesmas ferramentas, a depender da forma com que são usadas, podem colocar em risco bens e direitos de indivíduos e, também, de Estados. Visando o combate à essas ameaças virtuais, em âmbito internacional, foi criada a Convenção sobre os cibercrimes.[172]

A transnacionalidade característica dos crimes virtuais alterou a resposta normativa exigida no âmbito da persecução penal desses delitos. As lesões que são perpetradas com os delitos virtuais e os problemas que os mesmos geram ao poder punitivo dos Estados soberanos levaram à necessidade de uma resposta eficaz do Poder Público e à redefinição dos meios adequados para o combate a esses crimes, com respostas estatais para além do território de cada nação. A Convenção de Budapeste sobre o cibercrime demonstrou o alto grau de preocupação das nações com essas novas modalidades criminosas.

Após o conhecido episódio terrorista de 11 de setembro de 2001, nos Estados Unidos, a Comunidade Europeia promoveu a Convenção sobre o cibercrime, que ocorreu

---

[170] CAVALCANTE, Fachinelli**. Crimes cibernéticos**: **noções básicas de investigação e ameaças na internet.** Disponível em: <https://jus.com.br/artigos/25743/crimes-ciberneticos>. Acesso em 19 de outubro de 2020.

[171] DORIGON, Alessandro; SOARES, Renan Vinicius de Oliveira. **Crimes cibernéticos: dificuldades investigativas na obtenção de indícios da autoria e prova da materialidade.** Disponível em <https://jus.com.br/artigos/63549/crimes-ciberneticos-dificuldades-investigativas-na-obtencao-de-indicios-da-autoria-e-prova-da-materialidade>. Acesso em 19 de outubro de 2020.

[172] SOUZA, Gills Lopes Macêdo; PEREIRA, Dalliana Vilar. **A CONVENÇÃO DE BUDAPESTE E AS LEIS BRASILEIRAS.** Disponível em <https://www.mpam.mp.br/centros-de-apoio-sp-947110907/combate-ao-crime-organizado/doutrina/574-a-convencao-de-budapeste-e-as-leis-brasileiras>. Acesso em 19 de outubro de 2020.

em Budapeste, capital da Hungria, e teve como intuito alcançar a padronização universal quanto à repressão aos crimes virtuais, considerando a sua principal característica, a transnacionalidade.[173]

Em 23 de novembro de 2001, na cidade de Budapeste, foram abertos os debates e as assinaturas que levaram à criação, pelo Conselho da Europa, da maior Convenção internacional sobre crimes cibernéticos, que ficou concedida como Convenção de Budapeste sobre o cibercrime, a qual entrou em vigor na ordem jurídica internacional em 01 de julho de 2004, após as cinco ratificações exigidas.[174] Por meio desta Convenção foi instituída a expressão cibercrime no ordenamento internacional, o qual ainda se dedicou a tipificar os principais delitos cometidos no ambiente virtual.175

A Convenção de Budapeste sobre os crimes virtuais e sua Minuta do Relatório Explicativo foram adotados pelo Comitê de Ministros do Conselho da Europa na Sessão 109 de 08 de novembro de 2001.[176]

A referida Convenção internacional sobre crimes cibernéticos é o único tratado internacional sobre o tema que possui normas de direito penal e processual penal voltados a definir medidas conjuntas entre os países signatários para tipificação, investigação e enfrentamento dos crimes praticados por meio e contra a internet.[177] O objetivo principal da Convenção de Budapeste sobre o cibercrime é promover e possibilitar a cooperação internacional para o combate aos crimes informáticos. "A convenção prioriza uma política criminal comum, com o objetivo de proteger a sociedade contra a criminalidade no ciberespaço, designadamente, através da adoção de legislação adequada e da melhoria da cooperação internacional".[178]

---

[173] VALVERDE, Danielle Novaes de Siqueira. **Crimes Cibernéticos: a obrigatoriedade do registro de acesso à internet como forma de possibilitar a identificação do criminoso.** Revista da ESMAPE. Recife. v. 15. n. 32. p. 239. jul./dez. 2010.

[174] ROMANO, Rogério Tadeu. **CONVENÇÃO DE BUDAPESTE E CIBERCRIMES**. Disponível em <https://jus.com.br/artigos/72969/convencao-de-budapeste-e-cibercrimes>. Acesso em 19 de outubro de 2020.

[175] SOUZA, Gills Lopes Macêdo; PEREIRA, Dalliana Vilar. **A CONVENÇÃO DE BUDAPESTE E AS LEIS BRASILEIRAS.** Disponível em <https://www.mpam.mp.br/centros-de-apoio-sp-947110907/combate-ao-crime-organizado/doutrina/574-a-convencao-de-budapeste-e-as-leis-brasileiras>. Acesso em 19 de outubro de 2020.

[176] ROMANO, Rogério Tadeu. **CONVENÇÃO DE BUDAPESTE E CIBERCRIMES**. Disponível em <https://jus.com.br/artigos/72969/convencao-de-budapeste-e-cibercrimes>. Acesso em 19 de outubro de 2020.

[177] Procuradoria-Geral da República. **MPF defende adesão do Brasil à Convenção de Budapeste em audiência pública na Câmara.** Disponível em <http://www.mpf.mp.br/pgr/noticias-pgr/mpf-defende-adesao-do-brasil-a-convencao-de-budapeste-em-audiencia-publica-na-camara>. Acesso em 19 de outubro de 2020.

[178] Secretaria Geral da Presidência da República. **Brasil é convidado a aderir à Convenção do Conselho da Europa contra a Criminalidade Cibernética**. Disponível em <https://www.gov.br/secretariageral/pt-

A cooperação prevista nesse instrumento de direito público internacional prevê normas processuais, designando meios de obtenção de provas, e normas de direito material, que se exprimem na criação de tipos penais puníveis nas atividades praticadas no ambiente virtual. Têm-se, assim, o primeiro instrumento jurídico transnacional de regulamentação da internet, que servirá de caminho e parâmetro a ser adotado nas legislações dos países signatários, além de influenciar a doutrina e decisões jurisprudenciais de países não signatários, visto sua importância sobre o tema.[179]

> Segundo seu Preâmbulo, a Convenção prioriza uma política criminal comum, com o objetivo de proteger a sociedade contra a criminalidade no ciberespaço, designadamente, através da adoção de legislação adequada e da melhoria da cooperação internacional e reconhece a necessidade de uma cooperação entre os Estados e a indústria privada.[180]

A Convenção de Budapeste ainda enfatiza, em seu escopo inicial, o obrigatório respeito: à Convenção para a Proteção dos Direitos do Homem e das Liberdades Fundamentais do Conselho da Europa (1950); ao Pacto Internacional sobre os Direitos Civis e Políticos da ONU (1966); à Convenção das Nações Unidas sobre os Direitos da Criança (1989) e à Convenção da Organização Internacional do Trabalho sobre as Piores Formas do Trabalho Infantil (1999).[181]

Na sua parte destinada à regulamentar normas de direito material, o principal destaque da Convenção é que ela define cibercrimes, tipificando-os como infrações contra sistemas e dados informáticos; infrações relacionadas com computadores; infrações relacionadas com o conteúdo, quando incrimina a pornografia infantil; e infrações relacionadas com a violação de direitos autorais.[182]

---

br/noticias/2020/julho/brasil-e-convidado-a-aderir-a-convencao-do-conselho-da-europa-contra-a-criminalidade-cibernetica>. Acesso em 19 de outubro de 2020.

[179] KAMINSKI, Omar. **Conheça o Tratado Internacional contra crimes na Internet.** Revista Consultor Jurídico. Disponível em <https://www.conjur.com.br/2001-nov-4/convencao_lanca_tratado_internacional_cibercrimes>. Acesso em 19 de outubro de 2020.

[180] SOUZA, Gills Lopes Macêdo; PEREIRA, Dalliana Vilar. **A CONVENÇÃO DE BUDAPESTE E AS LEIS BRASILEIRAS.** Disponível em <https://www.mpam.mp.br/centros-de-apoio-sp-947110907/combate-ao-crime-organizado/doutrina/574-a-convencao-de-budapeste-e-as-leis-brasileiras>. Acesso em 19 de outubro de 2020.

[181] SOUZA, Gills Lopes Macêdo; PEREIRA, Dalliana Vilar. **A CONVENÇÃO DE BUDAPESTE E AS LEIS BRASILEIRAS.** Disponível em <https://www.mpam.mp.br/centros-de-apoio-sp-947110907/combate-ao-crime-organizado/doutrina/574-a-convencao-de-budapeste-e-as-leis-brasileiras>. Acesso em 19 de outubro de 2020.

[182] SOUZA, Gills Lopes Macêdo; PEREIRA, Dalliana Vilar. **A CONVENÇÃO DE BUDAPESTE E AS LEIS BRASILEIRAS.** Disponível em <https://www.mpam.mp.br/centros-de-apoio-sp-947110907/combate-ao-crime-organizado/doutrina/574-a-convencao-de-budapeste-e-as-leis-brasileiras>. Acesso em 19 de outubro de 2020.

Não obstante a tipificação de crimes contida na Convenção, tal instrumento internacional recomenda que os países signatarios adotem, ainda, medidas legislativas internas para tipificar e criminalizar outros crimes cibernéticos "tais como infrações contra a confidencialidade, integridade e disponibilidade de sistemas informáticos e dados informáticos, infrações relacionadas com computadores, infrações relacionadas com conteúdo e infrações relacionadas com a violação do direito de autor e direitos conexos".[183]

Além da preocupação com a padronização referente à tipificação de crimes no que se refere às previsões relativas aos cibercrimes, a Convenção de Budapeste se debruça, ainda, nos aspectos processuais da matéria, buscando que as autoridades e orgãos competentes possuam medidas bem regulamentadas e definidas de colaboração em toda a persecução penal dos crimes virtuais, visando implementar e estabelecer mecanismos rápidos e eficazes de cooperação internacional.[184]

Em matéria processual penal, a Convenção trata de importantes temas relativos à persecução penal e à busca por meios de obtenção de provas, tais como identificação, guarda, armazenamento e conservação de dados informáticos; busca e apreensão de dados virtuais localizados em servidores locais e internacionais, entre tantos outros procedimentos.[185] O documento internacional em comento prevê, ainda, a possibilidade de utilização pelos países signatários de serviços informáticos de busca remota em tempo real; interceptação e confisco de dados em trânsito ou armazenados, inclusive para fins de prova judicial; bloqueio de acesso de terceiros; além da possibilidade de se determinar a remoção de dados dos sistemas.[186]

Neste importante documento ainda há tratativas sobre competência no âmbito da cooperação internacional entre os países signatários. Contudo, tal questão é tratada de maneira flexível na medida em que deixa a critério das partes envolvidas a possibilidade

---

[183] Secretaria Geral da Presidência da República. **Brasil é convidado a aderir à Convenção do Conselho da Europa contra a Criminalidade Cibernética**. Disponível em <https://www.gov.br/secretariageral/pt-br/noticias/2020/julho/brasil-e-convidado-a-aderir-a-convencao-do-conselho-da-europa-contra-a-criminalidade-cibernetica>. Acesso em 19 de outubro de 2020.

[184] ROMANO, Rogério Tadeu. **CONVENÇÃO DE BUDAPESTE E CIBERCRIMES**. Disponível em <https://jus.com.br/artigos/72969/convencao-de-budapeste-e-cibercrimes>. Acesso em 19 de outubro de 2020.

[185] SOUZA, Gills Lopes Macêdo; PEREIRA, Dalliana Vilar. **A CONVENÇÃO DE BUDAPESTE E AS LEIS BRASILEIRAS.** Disponível em <https://www.mpam.mp.br/centros-de-apoio-sp-947110907/combate-ao-crime-organizado/doutrina/574-a-convencao-de-budapeste-e-as-leis-brasileiras>. Acesso em 20 de outubro de 2020.

[186] KAMINSKI, Omar. **Conheça o Tratado Internacional contra crimes na Internet**. Revista Consultor Jurídico**.** Disponível em <https://www.conjur.com.br/2001-nov-4/convencao_lanca_tratado_internacional_cibercrimes>. Acesso em 20 de outubro de 2020.

de eleger a jurisdição mais adequada para o procedimento legal no caso concreto.[187] "Caso não haja Tratado ou Convenção firmados entre as partes a respeito de assistência mútua e reciprocidade, a Convenção de Budapeste prevê a prevalência da norma Convencional sobre a jurisdição e regulamentação locais."[188]

Quanto ao tema concernente à extradição na cooperação internacional sobre os cibercrimes, a Convenção de Budapeste prevê que tal medida se sujeita às condições previstas pelo direito interno do país requerido ou pelos tratados de extradição aplicáveis.[189]

A Convenção de Budapeste sobre crimes cibernéticos objetiva a cooperação internacional em sentido amplo entre seus países signatários, garantindo que os mesmos adotem medidas legislativas domésticas para repressão ao crime virtual, bem como demais ações preventivas e repressivas em âmbito internacional para o combate às ameaças e ofensas perpretadas na internet e por meio desta como ferramenta.[190]

Atualmente a Convenção já possui mais de 60 Estados-partes signatários, entre eles cita-se: Albânia, Armênia, Áustria, Bélgica, Bulgária, Croácia, Ilha de Chipre, Estônia, Finlândia, França, Alemanha, Grécia, Hungria, Itália, Letônia, Moldova, Holanda, Noruega, Polônia, Portugal, Romênia, Espanha, Suíça, República Iugoslava da Macedônia, Ucrânia e Inglaterra. Dentre os países não-membros do Conselho Europeu, houve a adesão à Convenção pelo Canadá, Japão, África do Sul, Estados Unidos e outros Estados soberanos.[191] Além dos países membros, o documento conta com outros 10 países observadores.[192]

---

[187] SOUZA, Gills Lopes Macêdo; PEREIRA, Dalliana Vilar. **A CONVENÇÃO DE BUDAPESTE E AS LEIS BRASILEIRAS.** Disponível em <https://www.mpam.mp.br/centros-de-apoio-sp-947110907/combate-ao-crime-organizado/doutrina/574-a-convencao-de-budapeste-e-as-leis-brasileiras>. Acesso em 20 de outubro de 2020.

[188] KAMINSKI, Omar. **Conheça o Tratado Internacional contra crimes na Internet**. Revista Consultor Jurídico**.** Disponível em <https://www.conjur.com.br/2001-nov-4/convencao_lanca_tratado_internacional_cibercrimes>. Acesso em 20 de outubro de 2020

[189] SOUZA, Gills Lopes Macêdo; PEREIRA, Dalliana Vilar. **A CONVENÇÃO DE BUDAPESTE E AS LEIS BRASILEIRAS.** Disponível em <https://www.mpam.mp.br/centros-de-apoio-sp-947110907/combate-ao-crime-organizado/doutrina/574-a-convencao-de-budapeste-e-as-leis-brasileiras>. Acesso em 20 de outubro de 2020.

[190] KAMINSKI, Omar. **Conheça o Tratado Internacional contra crimes na Internet**. Revista Consultor Jurídico**.** Disponível em <https://www.conjur.com.br/2001-nov-4/convencao_lanca_tratado_internacional_cibercrimes>. Acesso em 20 de outubro de 2020.

[191] KAMINSKI, Omar. **Conheça o Tratado Internacional contra crimes na Internet**. Revista Consultor Jurídico**.** Disponível em <https://www.conjur.com.br/2001-nov-4/convencao_lanca_tratado_internacional_cibercrimes>. Acesso em 20 de outubro de 2020.

[192] Secretaria Geral da Presidência da República. **Brasil é convidado a aderir à Convenção do Conselho da Europa contra a Criminalidade Cibernética**. Disponível em <https://www.gov.br/secretariageral/pt-br/noticias/2020/julho/brasil-e-convidado-a-aderir-a-convencao-do-conselho-da-europa-contra-a-criminalidade-cibernetica>. Acesso em 20 de outubro de 2020.

Quando de sua criação e abertura às assinaturas pelos Estados signatários, o Brasil não aderiu à Convenção de Budapeste sobre os crimes virtuais, não sendo um dos países membros. Devido a sua não assinatura quando da criação do referido documento internacional, não se tornando um signatário, atualmente, como bem enfatiza o Secretário-Geral do Ministério das Relações Exteriores/Itamaraty, Samuel Pinheiro Guimarães, o Brasil não pode apenas aderir à Convenção se assim o quiser. Há a necessidade do país não signatário da referida Convenção internacional ser convidado pelo Comitê de Ministros do Conselho Europeu à assinar o documento, para que assim possa se tornar membro de tal Convenção, conforme determina o artigo 37, do texto original da Convenção de Budapeste, que trata sobre a adesão à Convenção.[193]

A Convenção de Budapeste sobre o cibercrime serve de orientação aos países, signatários ou não, que busquem desenvolver legislações internas contra a criminalidade virtual. Não obstante, o fato de um país não ser parte da referida Convenção não exclui a possibilidade do mesmo criar legislações pátrias visando a tipificação e combate dos crimes cometidos na internet ou por seu meio.[194]

Em julho de 2019 teve início uma série de tratativas entre o governo brasileiro e o Conselho da Europa, oportunidade em que o Brasil manifestou sua intenção em aderir ao instrumento internacional sobre a criminalidade cibernética.[195]

> Trata-se de iniciativa decorrente de trabalho de coordenação interinstitucional, constituído para esse fim, entre o Ministério das Relações Exteriores, a Polícia Federal (PF) e o Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional (DRCI) – ambos do Ministério da Justiça e Segurança Pública –, o Gabinete de Segurança Institucional da Presidência da República, a Agência Brasileira de Inteligência e o Ministério Público Federal. O Ministro da Justiça e Segurança Pública, Sergio Moro, fez o pedido com base em pareceres técnicos da PF e do DRCI.[196]

---

[193] SOUZA, Gills Lopes Macêdo; PEREIRA, Dalliana Vilar. **A CONVENÇÃO DE BUDAPESTE E AS LEIS BRASILEIRAS.** Disponível em <https://www.mpam.mp.br/centros-de-apoio-sp-947110907/combate-ao-crime-organizado/doutrina/574-a-convencao-de-budapeste-e-as-leis-brasileiras>. Acesso em 20 de outubro de 2020.

[194] SOUZA, Gills Lopes Macêdo; PEREIRA, Dalliana Vilar. **A CONVENÇÃO DE BUDAPESTE E AS LEIS BRASILEIRAS.** Disponível em <https://www.mpam.mp.br/centros-de-apoio-sp-947110907/combate-ao-crime-organizado/doutrina/574-a-convencao-de-budapeste-e-as-leis-brasileiras>. Acesso em 20 de outubro de 2020.

[195] Ministério das Relações Exteriores. **Processo de adesão à Convenção de Budapeste - Nota Conjunta do Ministério das Relações Exteriores e do Ministério da Justiça e Segurança Pública**. Disponível em <http://www.itamaraty.gov.br/pt-BR/notas-a-imprensa/21146-processo-de-adesao-a-convencao-de-budapeste-nota-conjunta-do-ministerio-das-relacoes-exteriores-e-do-ministerio-da-justica-e-seguranca-publica>. Acesso em 20 de outubro de 2020.

[196] Ministério das Relações Exteriores. **Processo de adesão à Convenção de Budapeste - Nota Conjunta do Ministério das Relações Exteriores e do Ministério da Justiça e Segurança Pública**. Disponível em <http://www.itamaraty.gov.br/pt-BR/notas-a-imprensa/21146-processo-de-adesao-a-convencao-de-

Em dezembro de 2019 o Comitê de Ministros do Conselho da Europa convidou o Brasil a aderir à Convenção do Conselho da Europa contra a Criminalidade Cibernética, conhecida como Convenção de Budapeste.[197] O convite possui validade por 03 anos.[198]

A adesão a esse acordo de cooperação internacional proporcionará às autoridades e órgãos brasileiros que lidam com a persecução penal dos crimes informáticos, acesso de forma mais ampla e ágil às provas eletrônicas e demais elementos informativos sob jurisdição estrangeira, além de tornar mais efetiva a cooperação jurídica internacional visando combater tais delitos.[199]

Em julho de 2020, foi encaminhado ao Congresso Nacional o texto da Convenção sobre o Cibercrime para que seja discutido a sua aprovação e posterior adesão brasileira ao instrumento de cooperação internacional.[200]

Para a adesão à Convenção de Budapeste, o Brasil precisará adotar providências legais internas. Entretanto, enquanto conclui os trâmites legais à assinatura da Convenção internacional, o país já pode participar das reuniões sobre a Convenção e seus protocolos, como observador.[201] A iniciativa de adesão do Brasil à Convenção de Budapeste sobre a criminalidade virtual vem ao encontro dos objetivos da Lei nº 12.965/2014, conhecido como Marco Civil da Internet, visando meios adequados à persecução penal dos crimes cibernéticos.

---

budapeste-nota-conjunta-do-ministerio-das-relacoes-exteriores-e-do-ministerio-da-justica-e-seguranca-publica>. Acesso em 20 de outubro de 2020.

[197] Ministério das Relações Exteriores. **Processo de adesão à Convenção de Budapeste - Nota Conjunta do Ministério das Relações Exteriores e do Ministério da Justiça e Segurança Pública**. Disponível em <http://www.itamaraty.gov.br/pt-BR/notas-a-imprensa/21146-processo-de-adesao-a-convencao-de-budapeste-nota-conjunta-do-ministerio-das-relacoes-exteriores-e-do-ministerio-da-justica-e-seguranca-publica>. Acesso em 20 de outubro de 2020.

[198] Secretaria Geral da Presidência da República. **Brasil é convidado a aderir à Convenção do Conselho da Europa contra a Criminalidade Cibernética**. Disponível em <https://www.gov.br/secretariageral/pt-br/noticias/2020/julho/brasil-e-convidado-a-aderir-a-convencao-do-conselho-da-europa-contra-a-criminalidade-cibernetica>. Acesso em 20 de outubro de 2020.

[199] Ministério das Relações Exteriores. **Processo de adesão à Convenção de Budapeste - Nota Conjunta do Ministério das Relações Exteriores e do Ministério da Justiça e Segurança Pública**. Disponível em <http://www.itamaraty.gov.br/pt-BR/notas-a-imprensa/21146-processo-de-adesao-a-convencao-de-budapeste-nota-conjunta-do-ministerio-das-relacoes-exteriores-e-do-ministerio-da-justica-e-seguranca-publica>. Acesso em 20 de outubro de 2020.

[200] Secretaria Geral da Presidência da República. **Brasil é convidado a aderir à Convenção do Conselho da Europa contra a Criminalidade Cibernética**. Disponível em <https://www.gov.br/secretariageral/pt-br/noticias/2020/julho/brasil-e-convidado-a-aderir-a-convencao-do-conselho-da-europa-contra-a-criminalidade-cibernetica>. Acesso em 20 de outubro de 2020.

[201] SOUZA, Gills Lopes Macêdo; PEREIRA, Dalliana Vilar. **A CONVENÇÃO DE BUDAPESTE E AS LEIS BRASILEIRAS.** Disponível em <https://www.mpam.mp.br/centros-de-apoio-sp-947110907/combate-ao-crime-organizado/doutrina/574-a-convencao-de-budapeste-e-as-leis-brasileiras>. Acesso em 20 de outubro de 2020.

Dada as características inerentes à internet e, consequentemente, à criminalidade virtual, o combate ao crime cibernético deve ser efetivado de modo rápido, a fim de interromper crimes em curso e possibilitar a elucidação exitosa dos delitos já praticados, preservando as provas que, se não obtidas rapidamente e de maneira correta, podem se perder definitivamente.

Não obstante a criação da Lei nº 12.965 de 2014, Marco Civil da Internet, que se preocupa em regulamentar importantes pontos relativos à persecução penal dos crimes virtuais, a criminalidade digital transcende fronteiras, o que faz ser imprescindível o constante aprimoramento de cooperação internacional entre os países que, em um caso concreto, possam ser lesados ou possam ser o local em que a prova de tal delito deve ser obtida. Nesse cenário, surge a Convenção de Budapeste sobre a cibercriminalidade.[202]

A necessidade de adesão, pelo Brasil, à Convenção de Budapeste, é visando a utilização desse instrumento internacional para, junto com o Marco Civil da Internet, suplementar a legislação nacional que ainda é deficiente na matéria, estabelecendo na seara criminal parâmetros mais concretos para a persecução penal dos crimes virtuais.[203]

A Procuradora da República, Fernanda Teixeira Souza Domingos, coordenadora do departamento de combate ao cibercrime no Ministério Público Federal, e Aristides Moura, da área de *Law Enforcement* da Microsoft Brasil, afirmam que o Brasil teve grande avanço nos temas relativos à internet e às ameaças provenientes do ambiente virtual nos últimos anos, em especial com a criação do Marco Civil da Internet e da Lei Geral de Proteção de Dados. Contudo, tais especialistas asseguram que as medidas legislativas brasileiras ainda são insuficientes e, por isso, a adesão à Convenção de Budapeste se mostra fundamental para o avanço no combate ao crime cibernético.[204]

A importância da adesão do Brasil à Convenção de Budapeste é indiscutível, visto que, se tornando signatário do referido acordo de cooperação internacional, o país entrará em um regime internacional de combate ao cibercrime, facilitando, assim, a comunicação

---

[202] Secretaria Geral da Presidência da República. **Brasil é convidado a aderir à Convenção do Conselho da Europa contra a Criminalidade Cibernética**. Disponível em <https://www.gov.br/secretariageral/pt-br/noticias/2020/julho/brasil-e-convidado-a-aderir-a-convencao-do-conselho-da-europa-contra-a-criminalidade-cibernetica>. Acesso em 21 de outubro de 2020.

[203] **Brasil adere à Convenção de Budapeste e se posiciona contra crimes cibernéticos**. Disponível em <https://diariodoturismo.com.br/brasil-adere-a-convencao-de-budapeste-e-se-posiciona-contra-crimes/>. Acesso em 21 de outubro de 2020.

[204] **Brasil adere à Convenção de Budapeste e se posiciona contra crimes cibernéticos**. Disponível em <https://diariodoturismo.com.br/brasil-adere-a-convencao-de-budapeste-e-se-posiciona-contra-crimes/>. Acesso em 21 de outubro de 2020.

e colaboração com outros países que sofrem das mesmas práticas ilícitas, mas que possuem legislações e regras de persecução penal diferentes.[205]

3.2 A LEGISLAÇÃO INTERNA E SUA INSUFICIÊNCIA PARA O COMBATE AO CRIME CIBERNÉTICO

O Direito penal possui um caráter dúplice, qual seja: servir a sociedade, protegendo-a de condutas danosas; e servir às pessoas, limitando a atuação punitiva estatal. A isso se dá o nome de garantismo, em sua vertente negativa e positiva. Enquanto o garantismo negativo veda os excessos do Estado, o garantismo positivo veda uma proteção insuficiente da coletividade. Suas utilidades, que são igualmente garantidas pela Constituição Federal, fazem com que o Direito penal não seja um fim em si mesmo.

O Direito penal, respeitando seu princípio da subsidiariedade, deve se ater à proteção de bens jurídicos penalmente tutelados, os quais devem estar ligados aos valores da realidade social que, em um dado momento histórico-cultural, são alterados, em especial quando há uma ruptura com o modelo social existente.

O mundo moderno e suas permanentes evoluções requerem do Direito um acompanhamento atento às mudanças e transformações ocorridas na sociedade, notadamente no que atine ao ramo da informática, que se encontra em constante desenvolvimento.

Hoje em dia, outra adversidade em que se esbarra os operadores do direito é a legislação aplicável aos casos de crimes cibernéticos, pois, em sua maioria, são inexistentes, e quando existem são insuficientes e possuem defeitos que levam à interpretações dúbias e à dificuldade de sua aplicabilidade.[206]

Não obstante os incessantes avanços tecnológicos, com o constante surgimento de novos recursos no ambiente virtual, os legisladores, juristas e doutrinadores brasileiros

---

[205] SOUZA, Gills Lopes Macêdo; PEREIRA, Dalliana Vilar. **A CONVENÇÃO DE BUDAPESTE E AS LEIS BRASILEIRAS.** Disponível em <https://www.mpam.mp.br/centros-de-apoio-sp-947110907/combate-ao-crime-organizado/doutrina/574-a-convencao-de-budapeste-e-as-leis-brasileiras>. Acesso em 21 de outubro de 2020.

[206] DORIGON, Alessandro; SOARES, Renan Vinicius de Oliveira. **Crimes cibernéticos: dificuldades investigativas na obtenção de indícios da autoria e prova da materialidade.** Disponível em < https://jus.com.br/artigos/63549/crimes-ciberneticos-dificuldades-investigativas-na-obtencao-de-indicios-da-autoria-e-prova-da-materialidade>. Acesso em 25 de outubro de 2020.

ainda caminham a passos lentos quando se fala de normas atinentes ao combate à criminalidade cibernética.[207]

No cenário legislativo pátrio, a Lei nº 11.829, de 25 de novembro de 2008, que alterou o Estatuto da Criança e do Adolescente, Lei 8.069 de 1990, foi um dos primeiros movimentos do Poder Legislativo visando o combate aos crimes virtuais.[208] Tal lei buscou suprir a lacuna legislativa até então existente, definindo e tipificando condutas especificas relacionadas à pornografia infantil na internet, aprimorando o combate à produção, venda e distribuição de pornografia infantil, bem como criminalizando a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia no ambiente virtual.[209] A falta de legislação especifica sobre o tema propiciava a impunidade dos agentes que armazenavam em seus computadores vídeos e fotos relacionados à pornografia infantil.[210]

O ordenamento jurídico brasileiro teve importantes e notáveis progressos referentes à legislação aplicável aos cibercrimes. Até o ano de 2012 não havia nenhuma lei especifica que tratasse sobre a punição e demais assuntos penais referentes aos crimes virtuais próprios, existindo apenas lei regulamentadora para os crimes cibernéticos impróprios. Contudo, após situações que pressionaram o legislativo a tratar da matéria, foram publicadas duas leis que se referiam a assuntos atinentes à criminalidade virtual, quais sejam às leis 12.735/2012 e 12.737/2012. Tais leis tipificaram condutas, visando à criminalização e punição dos crimes virtuais, bem como instituíram mecanismos apropriados para investigação de tais delitos.[211]

Importante destacar, ainda, a promulgação da Lei n° 12.965/2014, conhecida como Marco Civil da Internet, que trouxe diversos dispositivos atinentes ao tema e que,

---

[207] VALVERDE, Danielle Novaes de Siqueira. **Crimes Cibernéticos: a obrigatoriedade do registro de acesso à internet como forma de possibilitar a identificação do criminoso.** Revista da ESMAPE. Recife. v. 15. n. 32. p. 234-235. jul./dez. 2010.

[208] DORIGON, Alessandro; SOARES, Renan Vinicius de Oliveira. **Crimes cibernéticos: dificuldades investigativas na obtenção de indícios da autoria e prova da materialidade.** Disponível em <https://jus.com.br/artigos/63549/crimes-ciberneticos-dificuldades-investigativas-na-obtencao-de-indicios-da-autoria-e-prova-da-materialidade>. Acesso em 25 de outubro de 2020.

[209] VALVERDE, Danielle Novaes de Siqueira. **Crimes Cibernéticos: a obrigatoriedade do registro de acesso à internet como forma de possibilitar a identificação do criminoso.** Revista da ESMAPE. Recife. v. 15. n. 32. p. 244. jul./dez. 2010.

[210] DORIGON, Alessandro; SOARES, Renan Vinicius de Oliveira. **Crimes cibernéticos: dificuldades investigativas na obtenção de indícios da autoria e prova da materialidade.** Disponível em <https://jus.com.br/artigos/63549/crimes-ciberneticos-dificuldades-investigativas-na-obtencao-de-indicios-da-autoria-e-prova-da-materialidade>. Acesso em 25 de outubro de 2020.

[211] NASCIMENTO, Talles Leandro Ramos. **Crimes cibernéticos.** Conteúdo Jurídico. Disponível em <https://conteudojuridico.com.br/consulta/Artigos/52512/crimes-ciberneticos>. Acesso em 25 de outubro de 2020.

apesar de sua feição civil, também influenciaram diretamente no aspecto penal da investigação dos crimes virtuais.[212]

3.2.1 LEI 12.735/2012

Proposto pelo Senador Eduardo Azeredo, em substituição aos antecessores projetos de lei 89/2003, 76/2000 e 137/2000,[213] a Lei 12.735/2012, que ficou conhecida como Lei Azeredo, foi sancionada em 30 de novembro de 2012, e buscou tipificar condutas realizadas mediante uso de sistemas eletrônicos digitais ou seus similares, ou que sejam praticadas contra os sistemas informatizados e seus equivalentes.[214]

O artigo 1º da Lei 12.735/2012 possui o mesmo texto de sua ementa, ambos preveem a tipificação de condutas praticadas no ambiente virtual. Os artigos 2º e 3º da citada lei tratavam, respectivamente, sobre os delitos de falsificação de cartão de crédito, o qual já possuía tipificação prevista no Código Penal, e do crime de delito em favor no inimigo, que já possui previsão no Código Penal Militar, ambos artigos foram vetados quando da sanção da lei.[215]

Já em seu artigo 4º, a Lei Azeredo tratou de aspectos processuais penais, com a criação de órgãos especializados para o combate aos crimes desenvolvidos no ambiente virtual. A criação de órgãos específicos, com um corpo técnico especializado e capacitado para atuar na área, se justificou pelo fato de que o início das ações investigativas, em sua maioria, se dá com a localização e manuseio de computadores e equipamentos informáticos, e dos dados ali armazenados, o que requer técnica dos agentes responsáveis.[216]

---

[212] NASCIMENTO, Talles Leandro Ramos. **Crimes cibernéticos.** Conteúdo Jurídico. Disponível em <https://conteudojuridico.com.br/consulta/Artigos/52512/crimes-ciberneticos>. Acesso em 25 de outubro de 2020.

[213] SOUZA, Gills Lopes Macêdo; PEREIRA, Dalliana Vilar. **A CONVENÇÃO DE BUDAPESTE E AS LEIS BRASILEIRAS.** Disponível em <https://www.mpam.mp.br/centros-de-apoio-sp-947110907/combate-ao-crime-organizado/doutrina/574-a-convencao-de-budapeste-e-as-leis-brasileiras>. Acesso em 26 de outubro de 2020.

[214] NASCIMENTO, Talles Leandro Ramos. **Crimes cibernéticos.** Conteúdo Jurídico. Disponível em <https://conteudojuridico.com.br/consulta/Artigos/52512/crimes-ciberneticos>. Acesso em 25 de outubro de 2020.

[215] NASCIMENTO, Talles Leandro Ramos. **Crimes cibernéticos.** Conteúdo Jurídico. Disponível em <https://conteudojuridico.com.br/consulta/Artigos/52512/crimes-ciberneticos>. Acesso em 25 de outubro de 2020.

[216] NASCIMENTO, Talles Leandro Ramos. **Crimes cibernéticos.** Conteúdo Jurídico. Disponível em <https://conteudojuridico.com.br/consulta/Artigos/52512/crimes-ciberneticos>. Acesso em 25 de outubro de 2020.

Por fim, o artigo 5º modificou a redação do §3º do Art. 20 da Lei nº 7.716/1989 que define crimes resultantes de preconceito de raça ou de cor, visando impedir, com essa alteração, que as novas tecnologias fossem utilizadas como meio para disseminação do preconceito e intolerância racial.[217]

3.2.2 LEI 12.737/2012

A Lei 12.737/2012 teve seu projeto apresentado pelo Deputado Federal Paulo Teixeira[218], e foi promulgada em 30 de novembro de 2012[219], após ter seu tramite acelerado em razão da grande pressão midiática que propugnava pela rápida regulamentação dos crimes virtuais, após a invasão, subtração e distribuição na internet de fotografias íntimas da atriz Carolina Dieckmann, que teve sua conta de e-mail invadida por cibercriminosos.[220] Após esse episódio criminoso, tal lei ficou conhecida socialmente como Lei Carolina Dieckmann e foi considerada um grande avanço legislativo sobre o tema.[221]

A Lei 12.737/2012, inovou o ordenamento jurídico pátrio à medida em que tipificou novos delitos em seu texto, expandindo a legislação sobre crimes virtuais.[222] Esta lei introduziu no Código Penal os artigos seguintes: art. 154-A, que trata da invasão de dispositivo informático; art. 266, §1º, que tipifica a interrupção ou perturbação de

---

[217] NASCIMENTO, Talles Leandro Ramos. **Crimes cibernéticos.** Conteúdo Jurídico. Disponível em <https://conteudojuridico.com.br/consulta/Artigos/52512/crimes-ciberneticos>. Acesso em 25 de outubro de 2020.

[218] SANTOS, Elaine Gomes dos. RIBEIRO, Raisa Duarte da Silva. **Restrições à liberdade de expressão e crimes cibernéticos: a tutela penal do discurso de ódio nas redes sociais.** Revista dos Tribunais. vol. 997. ano 107. p. 533. São Paulo: Editora RT. novembro 2018.

[219] DORIGON, Alessandro; SOARES, Renan Vinicius de Oliveira. **Crimes cibernéticos: dificuldades investigativas na obtenção de indícios da autoria e prova da materialidade.** Disponível em < https://jus.com.br/artigos/63549/crimes-ciberneticos-dificuldades-investigativas-na-obtencao-de-indicios-da-autoria-e-prova-da-materialidade>. Acesso em 25 de outubro de 2020.

[220] SANTOS, Elaine Gomes dos. RIBEIRO, Raisa Duarte da Silva. **Restrições à liberdade de expressão e crimes cibernéticos: a tutela penal do discurso de ódio nas redes sociais.** Revista dos Tribunais. vol. 997. ano 107. p. 533. São Paulo: Editora RT. novembro 2018.

[221] DORIGON, Alessandro; SOARES, Renan Vinicius de Oliveira. **Crimes cibernéticos: dificuldades investigativas na obtenção de indícios da autoria e prova da materialidade.** Disponível em < https://jus.com.br/artigos/63549/crimes-ciberneticos-dificuldades-investigativas-na-obtencao-de-indicios-da-autoria-e-prova-da-materialidade>. Acesso em 25 de outubro de 2020.

[222] NASCIMENTO, Talles Leandro Ramos. **Crimes cibernéticos.** Conteúdo Jurídico. Disponível em <https://conteudojuridico.com.br/consulta/Artigos/52512/crimes-ciberneticos>. Acesso em 25 de outubro de 2020.

serviço telemático ou de informação de utilidade pública e o art. 298, §1º, sobre a falsificação de cartão.[223]

Detalhando a lei 12.737/2012, temos que seu artigo 2º é o de maior importância, pois propiciou grande avanço ao ordenamento jurídico no que se refere aos crimes virtuais, quando tipificou as condutas referentes à "invasão de dispositivo informático". Tal artigo incluiu os artigos 154-A e 154-B no Código Penal Brasileiro.[224]

> Art. 154-A - Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita. Pena: detenção, de 3 (três) meses a 1 (um) ano, e multa.

Infere-se da análise do referido artigo de lei, que este tipo penal tem como objetivo incriminar a conduta de quem invade, adultera ou destrói a privacidade digital de outrem, lesando seu direito através da violação de mecanismos de segurança. Porém, vale ressaltar a necessidade expressa por lei de que haja um mecanismo de segurança no sistema do aparelho eletrônico da vítima, sob pena de não se encaixar no crime ora estudado.[225]

Denota-se que o referido artigo, incluído no Código Penal pela lei 12.737/2012, busca suprimir condutas criminosas baseadas na invasão de dispositivo informático alheio, conectado ou não à internet, criminalizando o acesso sem permissão, condicionando, contudo, a invasão à uma violação indevida e concreta de mecanismos de segurança que devem, obrigatoriamente, existir para que haja a configuração deste crime, e com o fim de obter, adulterar ou destruir dados ou informações sem autorização do titular do dispositivo ou para instalar vulnerabilidades em dispositivo alheio, visando obter, com isso, vantagem ilícita de qualquer natureza.[226]

---

[223] PEREIRA, Eduardo Baker Valls. **Crimes informacionais: da compatibilidade internacional do ordenamento jurídico nacional e da proposta de reforma.** Revista IBCCRIM. n. 112. 2015.

[224] NASCIMENTO, Talles Leandro Ramos. **Crimes cibernéticos.** Conteúdo Jurídico. Disponível em <https://conteudojuridico.com.br/consulta/Artigos/52512/crimes-ciberneticos>. Acesso em 25 de outubro de 2020.

[225] SANTOS, Elaine Gomes dos. RIBEIRO, Raisa Duarte da Silva. **Restrições à liberdade de expressão e crimes cibernéticos: a tutela penal do discurso de ódio nas redes sociais.** Revista dos Tribunais. vol. 997. ano 107. p. 533. São Paulo: Editora RT. novembro 2018.

[226] SANTOS, Elaine Gomes dos. RIBEIRO, Raisa Duarte da Silva. **Restrições à liberdade de expressão e crimes cibernéticos: a tutela penal do discurso de ódio nas redes sociais.** Revista dos Tribunais. vol. 997. ano 107. p. 533. São Paulo: Editora RT. novembro 2018.

No seu parágrafo 2°, o art. 154-A do Código Penal demostra a preocupação dos legisladores em punir de modo mais severo quando a invasão também atingir a esfera patrimonial da vítima, prevendo uma causa de aumento de pena de 1/6 a 1/3, que deverá ser analisada pelo magistrado na terceira fase da dosimetria da pena, se houver prejuízo econômico à vítima resultante da invasão do equipamento informático da mesma.[227]

O artigo 154-B do Código penal estabelece que a ação penal para o crime de "invasão de dispositivo informático" será pública condicionada à representação da vítima. Não obstante, prevê como exceção à essa regra os casos em que o delito for cometido contra a administração pública direta ou indireta, quando a ação passa a ser pública incondicionada.[228]

Também é de grande importância o artigo 3º da Lei 12.737/2012 que altera os delitos tipificados nos artigos 266 e 298 do Código Penal. No art. 266, a alteração incluiu "na descrição do tipo o serviço informático, telemático ou de informação de utilidade pública, passando a ser caracterizado crime a sua interrupção"[229]. Por fim, no art. 298 do Código Penal a alteração produzida pela Lei 12.737/2012 se deu com a inclusão do delito de falsificação de cartão, a qual anteriormente só era punida com a utilização do cartão falsificado, na forma do delito de estelionato.[230]

Deste modo, a criação dos referidos diplomas legais pela Lei 12.737/2012, "Lei Carolina Dieckmann", buscou preencher a lacuna normativa existente, objetivando a repressão e punição, de maneira mais efetiva, da prática desses ilícitos no ambiente virtual.[231]

3.2.3 LEI 12.965/2014

---

[227] NASCIMENTO, Talles Leandro Ramos. **Crimes cibernéticos.** Conteúdo Jurídico. Disponível em <https://conteudojuridico.com.br/consulta/Artigos/52512/crimes-ciberneticos>. Acesso em 25 de outubro de 2020.

[228] NASCIMENTO, Talles Leandro Ramos. **Crimes cibernéticos.** Conteúdo Jurídico. Disponível em <https://conteudojuridico.com.br/consulta/Artigos/52512/crimes-ciberneticos>. Acesso em 25 de outubro de 2020.

[229] NASCIMENTO, Talles Leandro Ramos. **Crimes cibernéticos.** Conteúdo Jurídico. Disponível em <https://conteudojuridico.com.br/consulta/Artigos/52512/crimes-ciberneticos>. Acesso em 25 de outubro de 2020.

[230] NASCIMENTO, Talles Leandro Ramos. **Crimes cibernéticos.** Conteúdo Jurídico. Disponível em <https://conteudojuridico.com.br/consulta/Artigos/52512/crimes-ciberneticos>. Acesso em 25 de outubro de 2020.

[231] NASCIMENTO, Talles Leandro Ramos. **Crimes cibernéticos.** Conteúdo Jurídico. Disponível em <https://conteudojuridico.com.br/consulta/Artigos/52512/crimes-ciberneticos>. Acesso em 25 de outubro de 2020.

Anteriormente à entrada em vigor do Marco Civil da Internet, não haviam leis brasileiras que dispusessem de maneira completa sobre o tema, havendo apenas resoluções editadas pelo Poder Executivo nesse sentido, tentando amenizar a lacuna legislativa existente quanto aos problemas legais encontrados no ambiente virtual e no uso de suas plataformas.[232]

Marco Civil da internet é como ficou conhecida a Lei 12.965, de 23 de abril de 2014, que teve seu anteprojeto elaborado pelo Ministério da Justiça e cria diretrizes, além de estabelecer princípios, garantias, direitos e deveres, para o uso da rede mundial de computadores no Brasil, que devem ser aplicados aos usuários, governo e provedores de serviços e acessos.[233]

Importante destacar que a referida lei, objetivando promover a utilização ética dos instrumentos virtuais, buscou consolidar os direitos dos usuários da internet no país, em especial a inviolabilidade da intimidade e vida privada, sem, contudo, tipificar qualquer conduta.[234] O Marco Civil da Internet "tratou de um conjunto de normas que regulamentasse o uso da internet, tendo como princípios a neutralidade da rede, a privacidade do usuário e a liberdade de expressão"[235].

A proposta de lei que resultou na criação da Lei 12.965/2014 teve início em 2009, com a apresentação do projeto de lei nº 2.126/2011. O texto do projeto de lei, que foi posteriormente convertido no Marco Civil da Internet, foi submetido à consulta pública em diversas cidades do país, sendo que diversas sugestões atinentes ao tema foram objeto de discussão pelo Poder Legislativo e as principais foram incorporadas ao final do texto legal.[236]

A liberdade de expressão e vedação à censura é tema de grande importância tratado na referida lei, sendo que o caput do art. 2° e seu art. 19 se reservam a garantir

---

[232] DORIGON, Alessandro; SOARES, Renan Vinicius de Oliveira. **Crimes cibernéticos: dificuldades investigativas na obtenção de indícios da autoria e prova da materialidade.** Disponível em <https://jus.com.br/artigos/63549/crimes-ciberneticos-dificuldades-investigativas-na-obtencao-de-indicios-da-autoria-e-prova-da-materialidade>. Acesso em 28 de outubro de 2020.

[233] VALVERDE, Danielle Novaes de Siqueira. **Crimes Cibernéticos: a obrigatoriedade do registro de acesso à internet como forma de possibilitar a identificação do criminoso.** Revista da ESMAPE. Recife. v. 15. n. 32. p. 245. jul./dez. 2010.

[234] SANTOS, Elaine Gomes dos. RIBEIRO, Raisa Duarte da Silva. **Restrições à liberdade de expressão e crimes cibernéticos: a tutela penal do discurso de ódio nas redes sociais.** Revista dos Tribunais. vol. 997. ano 107. p. 529. São Paulo: Editora RT. novembro 2018.

[235] NASCIMENTO, Talles Leandro Ramos. **Crimes cibernéticos.** Conteúdo Jurídico. Disponível em <https://conteudojuridico.com.br/consulta/Artigos/52512/crimes-ciberneticos>. Acesso em 28 de outubro de 2020.

[236] NASCIMENTO, Talles Leandro Ramos. **Crimes cibernéticos.** Conteúdo Jurídico. Disponível em <https://conteudojuridico.com.br/consulta/Artigos/52512/crimes-ciberneticos>. Acesso em 28 de outubro de 2020.

expressamente esses direitos. No mesmo sentido, o art. 3º, I, do Marco Civil da Internet, prevê como princípios do uso da internet no Brasil a liberdade de expressão, comunicação e manifestação do pensamento. Nesta mesma perspectiva, os incisos I, II, III, VII e VIII do art. 7º, se atentam ao direito à privacidade, garantindo aos usuários das redes virtuais "a inviolabilidade da intimidade e vida privada, preservação do sigilo de comunicações transmitidas ou armazenadas, não fornecimento de dados coletados pela internet sem prévio consentimento do usuário, bem como o dever de informar ao usuário acerca da coleta de dados sobre si, desde que haja justificativa para tal"[237].

Este assunto ganha tal importância na Lei 12.965/2014 que seu art. 10 também se reserva a estabelecer que "a guarda e a disponibilização dos registros de conexão e de acesso à aplicações de internet devem ser realizadas com respeito a intimidade, vida privada, honra e imagem das pessoas direta ou indiretamente envolvidas"[238].

O polêmico e importante tema referente ao registro e guarda dos *logs* de acesso dos usuários à rede também é tratado no Marco Civil da Internet, visto que seu artigo 14 estabelece que os provedores de acesso e conteúdo na internet não podem guardar registros de acesso sem prévio consentimento do usuário. Já o seu artigo 13, ainda lidando com o relevante tema do registro e guarda dos *logs* de acesso, impõe a obrigação da guarda dos registros de acesso dos usuários pelo período mínimo de um ano.[239]

A lei ora estudada ainda se ateve às regras para estabelecer a responsabilidade civil dos provedores de internet quando houver ofensa aos direitos da personalidade das pessoas, os quais poderão ser responsabilizados, por exemplo, pelos danos decorrentes dos conteúdos publicados em suas plataformas caso não os removam após ordem judicial.[240]

Por fim, importante mencionar que o art. 29 e seu parágrafo único, estabelecem "o direito do usuário de internet de instalar em seu computador pessoal programas

---

[237] NASCIMENTO, Talles Leandro Ramos. **Crimes cibernéticos.** Conteúdo Jurídico. Disponível em <https://conteudojuridico.com.br/consulta/Artigos/52512/crimes-ciberneticos>. Acesso em 28 de outubro de 2020.

[238] NASCIMENTO, Talles Leandro Ramos. **Crimes cibernéticos.** Conteúdo Jurídico. Disponível em <https://conteudojuridico.com.br/consulta/Artigos/52512/crimes-ciberneticos>. Acesso em 28 de outubro de 2020.

[239] NASCIMENTO, Talles Leandro Ramos. **Crimes cibernéticos.** Conteúdo Jurídico. Disponível em <https://conteudojuridico.com.br/consulta/Artigos/52512/crimes-ciberneticos>. Acesso em 28 de outubro de 2020.

[240] NASCIMENTO, Talles Leandro Ramos. **Crimes cibernéticos.** Conteúdo Jurídico. Disponível em <https://conteudojuridico.com.br/consulta/Artigos/52512/crimes-ciberneticos>. Acesso em 28 de outubro de 2020.

destinados ao controle parental, ou seja, do conteúdo entendido como impróprio aos filhos menores"[241].

Em breve síntese, pode-se afirmar que o Marco Civil da Internet é uma espécie de Constituição da internet, que procurou estabelecer, de diversas formas, os direitos e deveres dos usuários das redes informáticas, dos provedores de acesso e de conteúdo, bem como do próprio Estado.

Embora o Marco Civil da Internet, Lei 12.965/2014, tenha sido aprovado e entrado em vigor em 2014, sendo a principal lei concernente ao tema, sua proteção que deve ser feita por meio da norma penal ainda não foi efetivada como deveria. Temas como a inviolabilidade da intimidade e da vida privada e a inviolabilidade e o sigilo do fluxo de comunicações, ainda estão tratadas apenas no art. 7º da referida lei. De forma idêntica, sucede com a Lei de Proteção de Dados, Lei 13.709, de 14 de agosto de 2018, regulamentadora do Marco Civil da Internet, que não se atenta às inovações legislativas necessárias quanto à proteção de bens jurídicos por meio da norma incriminadora.[242]

3.2.4 CÓDIGO PENAL

Ainda é deficiente a tipificação atinente à criminalidade cibernética própria no ordenamento jurídico brasileiro. Há apenas alguns poucos cibercrimes propriamente ditos previstos na legislação, como o artigo 154-A do Código Penal, já estudado anteriormente neste trabalho, incluído na seção dos crimes contra a inviolabilidade de segredos, pela Lei 12.737/2012.[243] Sob o *nomen juris* de "invasão de dispositivo informático", o tipo penal protege a seguridade informática e a integridade e privacidade dos dados.[244]

Se unem ao artigo 154-A do Código Penal, integrando a pequena lista de delitos informáticos próprios previstos no ordenamento jurídico brasileiro, os artigos 313-A, que

---

[241] NASCIMENTO, Talles Leandro Ramos. **Crimes cibernéticos.** Conteúdo Jurídico. Disponível em <https://conteudojuridico.com.br/consulta/Artigos/52512/crimes-ciberneticos>. Acesso em 28 de outubro de 2020.

[242] GUARAGNI, Fábio André. RIOS, Rodrigo Sanchez. **Novas tendências de combate aos crimes cibernéticos: cooperação internacional e perspectivas na realidade brasileira contemporânea.** Revista de Estudos Criminais. Porto Alegre, v. 18, n. 73. p. 181. 2019.

[243] GUARAGNI, Fábio André. RIOS, Rodrigo Sanchez. **Novas tendências de combate aos crimes cibernéticos: cooperação internacional e perspectivas na realidade brasileira contemporânea.** Revista de Estudos Criminais. Porto Alegre, v. 18, n. 73. p. 179. 2019.

[244] GUARAGNI, Fábio André. RIOS, Rodrigo Sanchez. **Novas tendências de combate aos crimes cibernéticos: cooperação internacional e perspectivas na realidade brasileira contemporânea.** Revista de Estudos Criminais. Porto Alegre, v. 18, n. 73. p. 180. 2019.

criminaliza a inserção de dados falsos em sistema de dados da Administração Pública e 313-B, que tipifica a modificação ou alteração não autorizada de dados em sistema da Administração Pública, ambos delitos funcionais contra os sistemas de dados do Estado, que foram inseridos no Código Penal pela Lei nº 9.983, de 14 de julho de 2000. Soma-se a eles o artigo 266, § 1º, do Código Penal, referente ao crime contra a disponibilidade dos dados.[245]

3.2.5 PROJETO DE LEI 8.045/2010

O projeto de lei do novo Código de Processo Penal, Projeto de Lei nº 8.045/2010, não busca tratar de maneira eficaz os importantes temas concernentes ao ambiente virtual e à cibercriminalidade. O projeto não menciona em nenhum de seus artigos a obrigatoriedade do registro e guarda dos *logs* de acesso à internet, tampouco a obrigatoriedade de cadastro dos usuários da rede.[246] "Referente à internet, o projeto limita-se a prever, no título relativo às medidas cautelares pessoais, o bloqueio de endereço eletrônico"[247].

Complementando as leis referidas no presente trabalho que abordam a problemática do ambiente virtual, sua regulamentação e a consequente criminalidade que ali surge, cabe mencionar outros diplomas normativos que tratam de alguns temas específicos, como: a Lei nº 9.296/1996 que disciplinou a interceptação de comunicação telemática ou informática, o que se aplica aos crimes cometidos no ambiente virtual ou por seu meio; a Lei nº 9.609/1998, que trata da proteção da propriedade intelectual do programa de computador; a Lei nº 9.983/2000, que tipificou os crimes relacionados ao acesso indevido a sistemas informatizados da Administração Pública; e a Lei nº 12.034/2009, que delimita os direitos e deveres dentro da rede mundial, durante as campanhas eleitorais.[248]

---

[245] GUARAGNI, Fábio André. RIOS, Rodrigo Sanchez. **Novas tendências de combate aos crimes cibernéticos: cooperação internacional e perspectivas na realidade brasileira contemporânea.** Revista de Estudos Criminais. Porto Alegre, v. 18, n. 73. p. 181. 2019.

[246] VALVERDE, Danielle Novaes de Siqueira. **Crimes Cibernéticos: a obrigatoriedade do registro de acesso à internet como forma de possibilitar a identificação do criminoso.** Revista da ESMAPE. Recife. v. 15. n. 32. p. 247. jul./dez. 2010.

[247] VALVERDE, Danielle Novaes de Siqueira. **Crimes Cibernéticos: a obrigatoriedade do registro de acesso à internet como forma de possibilitar a identificação do criminoso.** Revista da ESMAPE. Recife. v. 15. n. 32. p. 247. jul./dez. 2010.

[248] NASCIMENTO, Talles Leandro Ramos. **Crimes cibernéticos.** Conteúdo Jurídico. Disponível em <https://conteudojuridico.com.br/consulta/Artigos/52512/crimes-ciberneticos>. Acesso em 28 de outubro de 2020.

Embora é notável o avanço legislativo quanto ao enfrentamento aos cibercrimes no Brasil, a legislação pátria ainda está muito aquém da necessária para a devida regulamentação do uso do ambiente virtual e de suas plataformas e da repressão aos crescentes crimes virtuais em sua vertente própria e imprópria.[249]

3.3 A FALTA DE NORMAS SOBRE INVESTIGAÇÃO CRIMINAL DE DELITOS COMETIDOS PELA INTERNET

A era digital em que o mundo se encontra propicia o fenômeno conhecido como globalização, as novas tecnologias trouxeram inúmeros benefícios aos adeptos do ambiente virtual, contudo, essa era tecnológica também veio acompanhada de malefícios, como a criação de uma nova modalidade criminosa, surgindo, assim, os crimes cibernéticos. Além dos bens jurídicos individuais, a criminalidade informática passou a atingir, ainda, os bens jurídicos difusos, causando um crescente dano à sociedade.[250]

O número de usuários da internet cresce paralelamente ao seu contínuo avanço. Atualmente, a internet é considerada o maior sistema de comunicabilidade global, isso se dá pelos vastos recursos que a mesma dispõe aos seus usuários.[251]

Hoje, o Brasil ocupa o quarto lugar no *ranking* dos países com o maior número de usuários da internet, segundo dados da Conferência das Nações Unidas sobre Comércio e Desenvolvimento. Importante destacar que a criminalidade cibernética se expande proporcionalmente à quantidade de usuários dessa rede virtual.[252]

Os crimes virtuais se difundem e se aprimoram rapidamente, já a legislação que trata sobre o tema, juntamente com a persecução penal do mesmo, é lenta e morosa, não

---

[249] NASCIMENTO, Talles Leandro Ramos. **Crimes cibernéticos.** Conteúdo Jurídico. Disponível em <https://conteudojuridico.com.br/consulta/Artigos/52512/crimes-ciberneticos>. Acesso em 28 de outubro de 2020.
[250] FOGLIATTO, Juliana. **Os crimes cibernéticos e os meios que a polícia utiliza para a identificação dos criminosos.** Disponível em <https://jus.com.br/artigos/77225/os-crimes-ciberneticos-e-os-meios-que-a-policia-utiliza-para-a-identificacao-dos-criminosos>. Acesso em 30 de outubro de 2020.
[251] SANCHES, Ademir Gasques. ANGELO, Ana Elisa de. **Insuficiência das leis em relação aos crimes cibernéticos no Brasil.** Disponível em <https://jus.com.br/artigos/66527/insuficiencia-das-leis-em-relacao-aos-crimes-ciberneticos-no-brasil>. Acesso em 30 de outubro de 2020.
[252] SANCHES, Ademir Gasques. ANGELO, Ana Elisa de. **Insuficiência das leis em relação aos crimes cibernéticos no Brasil.** Disponível em <https://jus.com.br/artigos/66527/insuficiencia-das-leis-em-relacao-aos-crimes-ciberneticos-no-brasil>. Acesso em 30 de outubro de 2020.

acompanhando a nova criminalidade que se impõe no ambiente virtual. O direito deve evoluir equitativamente aos crimes, sobretudo os crimes virtuais.[253]

Levando em consideração a crescente criminalidade que surge no ambiente virtual e suas características próprias, foi criada, em parceria com o Ministério Público Federal, em 20 de dezembro de 2005, a Safernet, que é uma "associação civil de direito privado, com atuação nacional, sem fins lucrativos ou econômicos, sem vinculação político partidária, religiosa ou racial"[254], que tem como objetivo a "promoção e defesa dos Direitos Humanos na Internet no Brasil"[255].

Tal organização não governamental foi criada como meio para encorajar as denúncias sobre crimes cibernéticos. As *notitia criminis* são recebidas de maneira eletrônica, através do site da Safernet, são, posteriormente, encaminhadas à análise e, se comprovada sua materialidade, são encaminhas ao Ministério Público e a Polícia Federal para os competentes procedimentos legais cabíveis.[256]

Conforme preconiza o texto legal da Lei 12.735/12, a polícia judiciária deve criar, dentro de seu órgão, setores especializados no combate à criminalidade virtual, visando uma atenção específica e capacitada no que tange à investigação dessa modalidade ímpar de crimes. Apesar de expressamente previsto pela citada Lei, que já conta com muitos anos desde sua entrada em vigor, apenas alguns Estados da Federação já implementaram tais setores por meio de delegacias especializadas em crimes virtuais.[257]

A importância da implementação de delegacias especializadas no combate à cibercriminalidade está relacionada com o aperfeiçoamento dos agentes responsáveis pela investigação de tais delitos, que precisam estar preparados para lidar com um ambiente que se modifica e se aprimora constantemente. Delegacias não especializadas em crimes virtuais não estão capacitadas para atender a demanda e peculiaridades de tais delitos.[258]

---

[253] FOGLIATTO, Juliana. **Os crimes cibernéticos e os meios que a polícia utiliza para a identificação dos criminosos.** Disponível em <https://jus.com.br/artigos/77225/os-crimes-ciberneticos-e-os-meios-que-a-policia-utiliza-para-a-identificacao-dos-criminosos>. Acesso em 30 de outubro de 2020.

[254] SAFERNET. Disponível em <https://new.safernet.org.br/content/institucional>. Acesso em 30 de outubro de 2020.

[255] SAFERNET. Disponível em <https://new.safernet.org.br/content/institucional>. Acesso em 30 de outubro de 2020.

[256] FOGLIATTO, Juliana. **Os crimes cibernéticos e os meios que a polícia utiliza para a identificação dos criminosos**. Disponível em <https://jus.com.br/artigos/77225/os-crimes-ciberneticos-e-os-meios-que-a-policia-utiliza-para-a-identificacao-dos-criminosos>. Acesso em 30 de outubro de 2020.

[257] FOGLIATTO, Juliana. **Os crimes cibernéticos e os meios que a polícia utiliza para a identificação dos criminosos.** Disponível em <https://jus.com.br/artigos/77225/os-crimes-ciberneticos-e-os-meios-que-a-policia-utiliza-para-a-identificacao-dos-criminosos>. Acesso em 30 de outubro de 2020.

[258] FOGLIATTO, Juliana. **Os crimes cibernéticos e os meios que a polícia utiliza para a identificação dos criminosos**. Disponível em <https://jus.com.br/artigos/77225/os-crimes-ciberneticos-e-os-meios-que-a-policia-utiliza-para-a-identificacao-dos-criminosos>. Acesso em 30 de outubro de 2020.

O trabalho investigativo realizado pelos agentes e autoridades policiais no que se refere aos crimes virtuais deve ser ainda mais rápido e preciso, visto que dependem de elementos para caracterizar a autoria e materialidade delitiva que podem se perder facilmente devido à volatilidade dos dados e do fato que tais dados, que devem ser armazenados por provedores e instituições responsáveis, não permanecem armazenados por longo período de tempo. Importante lembrar que devido às características desse ambiente, os dados podem se perder facilmente se não houver uma manipulação correta dos mesmos. Devido à necessidade de vasto conhecimento especializado no ambiente virtual e nos crimes que ali se originam, o percentual de êxito nas investigações dos cibercrimes nas delegacias não especializadas é muito baixo, gerando impunidade e impulsionando tal criminalidade.[259]

É imprescindível que haja uma reestruturação no que tange aos conhecimentos informáticos dos agentes estatais responsáveis por lidar com os crimes virtuais, em especial na fase de investigação de tais delitos, devendo se priorizar a criação de setores especializados dentro dos órgãos competentes, para que os agentes que lidam com tais práticas criminosas sejam capacitados para conhecer o ambiente virtual e as ferramentas que os criminosos se utilizam nesse ambiente, permitindo que o Estado esteja pronto para realmente combater a crescente criminalidade cibernética.[260]

O trabalho investigativo da polícia judiciária quando se trata de crimes virtuais segue o mesmo rito previsto no Código de Processo Penal para as outras modalidades criminosas. Contudo, os crimes informáticos são diferentes por natureza, tendo características e meios de execução próprios, necessitando de legislação diferenciada para sua investigação.[261]

A investigação dos cibercrimes é feita através de uma análise técnica dos dados de conexão, buscando elementos que comprovem a autoria e materialidade dos crimes perpetrados por meio da rede mundial de computadores. Buscando evitar a perda dos elementos de autoria e materialidade delitiva, bem como dos dados que poderão constituir as provas do crime virtual, é necessário que a investigação seja diferenciada, que leve em

---

[259] FOGLIATTO, Juliana. **Os crimes cibernéticos e os meios que a polícia utiliza para a identificação dos criminosos**. Disponível em <https://jus.com.br/artigos/77225/os-crimes-ciberneticos-e-os-meios-que-a-policia-utiliza-para-a-identificacao-dos-criminosos>. Acesso em 30 de outubro de 2020.

[260] FOGLIATTO, Juliana. **Os crimes cibernéticos e os meios que a polícia utiliza para a identificação dos criminosos.** Disponível em <https://jus.com.br/artigos/77225/os-crimes-ciberneticos-e-os-meios-que-a-policia-utiliza-para-a-identificacao-dos-criminosos>. Acesso em 30 de outubro de 2020.

[261] FOGLIATTO, Juliana. **Os crimes cibernéticos e os meios que a polícia utiliza para a identificação dos criminosos.** Disponível em <https://jus.com.br/artigos/77225/os-crimes-ciberneticos-e-os-meios-que-a-policia-utiliza-para-a-identificacao-dos-criminosos>. Acesso em 30 de outubro de 2020.

consideração as características dos cibercrimes e do ambiente em que os mesmos são executados.[262]

Não é correto que a investigação dos crimes virtuais seja regida da mesma forma e pelas mesmas leis que regulamentam a investigação dos demais crimes, fazer isso é ignorar as notáveis diferenças existentes entre essas diversas modalidades criminosas e levar, em muitos casos, a investigação de crimes virtuais ao fracasso.

As poucas normas penais existentes tratando sobre a criminalidade virtual, em sua maioria, são vagas e imprecisas, levando a interpretações dúbias e à necessidade de complementação por outras normas. Por exemplo, a alteração no Código Penal promovida pela Lei 12.737/2012, que tipificou alguns cibercrimes, trouxe uma tipificação vaga, fazendo com que tais artigos necessitassem de complementação de outras normas, criando, assim, normas penais em branco.[263]

É necessário que as leis que tratem de tal tema, que é novo e possui diversas alterações constantemente, trate de maneira mais concreta e explicativa sobre os temas concernentes à criminalidade virtual em todas suas vertentes, não deixando espaço para interpretações duvidosas e inseguranças jurídicas.

De fato, é inegável que as investigações dos crimes virtuais esbarram na falta de legislação adequada sobre o tema, o que dificulta o combate à essa criminalidade. A existência de um Marco Civil da Internet, de uma lei de proteção de dados e de algumas esparsas leis atinentes ao tema não é suficiente, principalmente quando seu texto não é claro ao tratar da matéria, criando lacunas na lei.[264]

"Busca-se enquadrar as ilicitudes nas figuras penais típicas, porém, o Código Penal vigente é de 1940, desta forma, não abarca determinados comportamentos da sociedade moderna"[265], e nem poderia, visto que à época não se tinha como prever a crescente estrutura do ambiente virtual e a forma como ele seria usado para a criação de

---

[262] FOGLIATTO, Juliana. **Os crimes cibernéticos e os meios que a polícia utiliza para a identificação dos criminosos.** Disponível em <https://jus.com.br/artigos/77225/os-crimes-ciberneticos-e-os-meios-que-a-policia-utiliza-para-a-identificacao-dos-criminosos>. Acesso em 30 de outubro de 2020.
[263] FOGLIATTO, Juliana. **Os crimes cibernéticos e os meios que a polícia utiliza para a identificação dos criminosos.** Disponível em <https://jus.com.br/artigos/77225/os-crimes-ciberneticos-e-os-meios-que-a-policia-utiliza-para-a-identificacao-dos-criminosos>. Acesso em 30 de outubro de 2020.
[264] FOGLIATTO, Juliana. **Os crimes cibernéticos e os meios que a polícia utiliza para a identificação dos criminosos.** Disponível em <https://jus.com.br/artigos/77225/os-crimes-ciberneticos-e-os-meios-que-a-policia-utiliza-para-a-identificacao-dos-criminosos>. Acesso em 30 de outubro de 2020.
[265] SANCHES, Ademir Gasques. ANGELO, Ana Elisa de. **Insuficiência das leis em relação aos crimes cibernéticos no Brasil.** Disponível em <https://jus.com.br/artigos/66527/insuficiencia-das-leis-em-relacao-aos-crimes-ciberneticos-no-brasil>. Acesso em 30 de outubro de 2020.

novos tipos penais, além de novos meios de execução para os antigos delitos já conhecidos na sociedade.

Além das condutas que não estão tipificadas, o que leva ao necessário uso de analogia pelos operadores do direito, há condutas que já estão previstas e são conhecidas como crimes virtuais impróprios. Contudo, por mais que tais condutas estejam tipificadas no Código Penal, por serem delitos já conhecidos e praticados também fora do ambiente virtual, quando ocorrem no meio eletrônico ganham novas proporções, vez que sua reparação se torna complexa, pois "cessar por completo algo que está na rede beira a impossibilidade"[266]. É necessário que isso seja levado em consideração, pois tais crimes, ainda que já tipificados, merecem atenção diferenciada na sua punição, visto que, geralmente, causam danos ainda maiores à suas vítimas.

O Brasil possui uma legislação escassa e insuficiente sobre os crimes virtuais, tanto na tipificação dos delitos, quanto nas normas processuais referentes à persecução penal dos mesmos. Essa falta de legislação adequada faz com que o Poder Judiciário tente encontrar soluções imediatas para resolver os casos em análise, porém tais medidas não sanam o problema de forma permanente e eficaz. Tal carência legislativa impulsiona a criminalidade virtual e leva crackers e até mesmo criminosos não especializados na área a propiciar consideráveis e, por vezes, irreparáveis danos.[267]

A carência legislativa especifica sobre a cibercriminalidade presente no cenário pátrio impulsiona o crescimento da criminalidade virtual e, em muitos casos, gera a impunidade dos criminosos que utilizam desse ambiente para cometer os mais diversos delitos. Isso ocorre, pois, diversas condutas criminosas que são criadas pelos cibercriminosos sequer possuem tipificação, e as que possuem, não raras as vezes, são repletas de lacunas e interpretações dúbias.[268]

O avanço das tecnologias e, consequentemente, dos crimes virtuais, faz com que seja prioridade, em um Estado Democrático de Direito que se preocupa com seus cidadãos, a criação de legislações específicas que contenham normas de direito material e processual, objetivando tipificar as condutas criminosas e regulamentar a investigação

---

[266] SANCHES, Ademir Gasques. ANGELO, Ana Elisa de. **Insuficiência das leis em relação aos crimes cibernéticos no Brasil.** Disponível em <https://jus.com.br/artigos/66527/insuficiencia-das-leis-em-relacao-aos-crimes-ciberneticos-no-brasil>. Acesso em 30 de outubro de 2020.

[267] SANCHES, Ademir Gasques. ANGELO, Ana Elisa de. **Insuficiência das leis em relação aos crimes cibernéticos no Brasil.** Disponível em <https://jus.com.br/artigos/66527/insuficiencia-das-leis-em-relacao-aos-crimes-ciberneticos-no-brasil>. Acesso em 30 de outubro de 2020.

[268] SANCHES, Ademir Gasques. ANGELO, Ana Elisa de. **Insuficiência das leis em relação aos crimes cibernéticos no Brasil.** Disponível em <https://jus.com.br/artigos/66527/insuficiencia-das-leis-em-relacao-aos-crimes-ciberneticos-no-brasil>. Acesso em 30 de outubro de 2020.

e persecução penal dos crimes virtuais, tendo em observância todas suas características e peculiaridades.

Importante que nesse processo legislativo, os legisladores se atentem às penas que serão cominadas à tais delitos, levando em consideração os resultados danosos que estes produzem à vítima e à sociedade em geral.[269]

À vista disso, a criação de leis competentes e bem definidas é imprescindível para o combate à cibercriminalidade.

[269] SANCHES, Ademir Gasques. ANGELO, Ana Elisa de. **Insuficiência das leis em relação aos crimes cibernéticos no Brasil.** Disponível em <https://jus.com.br/artigos/66527/insuficiencia-das-leis-em-relacao-aos-crimes-ciberneticos-no-brasil>. Acesso em 30 de outubro de 2020.

CONCLUSÃO

É inegável o modo que a tecnologia se desenvolve e se torna imprescindível aos mais diversos setores no mundo atual. Devemos atentarmos, especialmente, aos impactos que a informática causa na sociedade moderna, seja no campo positivo da evolução do processo de comunicação e de realização das mais variadas tarefas, seja no âmbito negativo, como no caso do aumento da criminalidade e surgimento de crimes propagados pela internet.

Nesse ponto, denomina-se crime de informática, ou cibercrimes, toda ação típica, antijurídica e culpável, cometida contra ou pela utilização de processamento automático de dados ou sua transmissão. A internet propiciou um novo lócus de cometimento de crimes. Com a facilidade de poder ser acionada de qualquer lugar do mundo, a rede informática desestabilizou fronteiras e dificultou a atividade de persecução de órgãos oficiais de controle.

O direito ainda não se adaptou totalmente à sociedade moderna e isto se dá, em partes, devido a própria natureza das mudanças que ocorrem diariamente e de maneira cada vez mais rápida. A virtude da facilidade e velocidade com que as informações são trocadas, assim como o anonimato obtido através destes meios, dificultam o tratamento legal da matéria.

Inobstante aos benefícios que a internet propicia, os usuários da rede mundial de computadores se valem das características da mesma para beneficiarem-se da facilidade deste meio virtual e cometer ilícitos, prejudicando direitos alheios. Diante da dificuldade de investigar crimes dessa natureza, os agentes utilizam do anonimato que impera na rede para praticar condutas ilícitas ou, na sua maioria, criminosas, dificultando a apuração de sua autoria.

A identificação dos cibercriminosos se torna tarefa ainda mais complexa devido à ausência de normas que obriguem de maneira efetiva provedores de acesso e de conteúdos a armazenar registros e logs de atividades na rede mundial de computadores, por certo período de tempo, gerando um ambiente propício ao anonimato desses criminosos.

A importância de leis que obriguem de fato a guarda dos registros de acesso dos usuários à internet, bem como dos dados relativos às atividades do mesmo nestes acessos, por período de tempo que seja proporcional e suficiente, além de fiscalizar o cumprimento dessas regras pelos responsáveis pelo registro e guarda, se dá pois estes dados são necessários para possibilitar a identificação dos autores de crimes praticados por meio do

ambiente virtual, tornando o anonimato exceção e não regra, na rede mundial de computadores.

A escassez legislativa sobre o tema torna ainda mais difícil a identificação do autor do fato, bem como a colheita de provas de materialidade, prejudicando a investigação de tais infrações penais e toda a persecução penal relativa à mesma.

Os cibercrimes são delitos que crescem tão ou mais rapidamente que a própria tecnologia. De partida, reforça-se que os delitos informáticos são classificados pela doutrina especializada como: impróprios, quando cometidos por meio do sistema informático de dados; ou próprios, quando cometidos contra o sistema informático de dados.

Os crimes cibernéticos, seja em sua vertente própria ou impropria, tem como característica primordial o fato de, na maioria das vezes, não encontrar fronteiras para seu cometimento. O seu caráter transnacional, portanto, demanda um esforço muito maior do Estado nacional em promover atos de cooperação para combater a criminalidade virtual, a fim de permitir sua persecução e punição, tanto a nível policial quanto judicial.

Uma simples aproximação à temática dos crimes praticados por meio virtual conduz à constatação de sua transnacionalidade. A importância que essa característica, que é própria da cibercriminalidade, possui, conduz ao fato de que os crimes virtuais imperam entre as prioridades da cooperação internacional a partir da fase de investigação preliminar.

Os problemas que os sistemas e as redes de informática causam ao poder punitivo, como um todo, importam na necessária redefinição do alcance e dos limites para além do território pátrio dos poderes estatais atinentes ao combate às novas práticas delituosas.

A transnacionalidade e globalidade da rede, e seu uso para prática de delitos contra a estrutura de dados, bem como por meio dela, exigem o fomento das mecânicas de cooperação jurídica internacional. Nesse sentido, em 2001, foi criado pelo Conselho da Europa um organismo internacional destinado à promoção da democracia e proteção dos direitos humanos, tal instrumento ficou conhecido como Convenção de Budapeste, que está em vigor desde 2004. A Convenção estabelece uma rede de cooperação internacional, visando uma padronização acerca dos termos envolvidos na tipificação de crimes cibernéticos e dos meios utilizados para investigar e processar tais delitos.

A internet e a criminalidade que proveio desse meio geraram novos desafios políticos-criminais colocados frente à norma pátria. Essa realidade exige do sistema criminal, como um todo, novas respostas, não alcançadas pela política criminal em vigor

e nem pelos tipos penais e normas processuais já existentes no ordenamento jurídico vigente. Trata-se de desafio imposto ao Estado e todo seu aparato de justiça, que supera a criminalidade territorial. Esse quadro altera a resposta normativa exigida tanto no plano da prevenção quanto no da investigação e persecução penal.

Apesar do avanço da tecnologia, do surgimento frequente de novos recursos e aplicativos na internet, os legisladores, juristas e doutrinadores brasileiros caminham a passos lentos na direção da construção de normas que alcancem o cibercrime, não conseguindo acompanhar a evolução da sociedade e, tampouco, o rápido aperfeiçoamento da criminalidade virtual.

Os projetos de lei que tramitam no Congresso Nacional, bem como as leis já em vigor que podem ser aplicadas ao tema, não conseguem refletir as necessidades atuais do combate ao crime cibernético, carecendo de modernização conceitual e abrangência que supere a velocidade do avanço da tecnologia.

Projetos de lei e modificações legislativas concernentes ao delicado tema da criminalidade informática, devem ser analisados criticamente e com propostas de mudanças concretas no texto legislativo, levando em consideração as características próprias do ambiente virtual, para que, assim, tais leis estejam adequadas às necessidades práticas, ao ordenamento jurídico nacional e internacional.

A dificuldade de investigação, identificação dos criminosos, punição e até a falta de tipificação desses novos delitos, faz com que os Estados tendam a falhar na garantia da proibição da proteção deficiente quanto aos seus cidadãos.

REFERÊNCIAS

ANDRADE, Mariah Dourado de. BENTES, Dorinethe dos Santos. GUIMARAES, David Franklin da Silva. **Considerações sobre a aplicabilidade do direito penal acerca dos crimes virtuais.** Revista Vertentes do Direito. Disponível em <https://sistemas.uft.edu.br/periodicos/index.php/direito/article/view/4171#:~:text=O%20presente%20artigo%20busca%20compreender,Leis%20Penais%20regulando%20esse%20crime.>. Acesso em 15 de agosto de 2020.

BARRETO, Alesandro Gonçalves. SANTOS, Hericson dos. **Deep Web: investigação no submundo da internet.** 1. Ed. Rio de Janeiro: Editora Brasport, 2019.

BRASIL. Supremo Tribunal Federal. **Informativo STF n° 286/2002.** Disponível em <http://www.stf.jus.br//arquivo/informativo/documento/informativo286.htm>. Acesso em 06 de setembro de 2020.

BRASIL. Supremo Tribunal Federal. **Informativo STF n° 393/2005.** Disponível em <http://www.stf.jus.br/arquivo/informativo/documento/informativo393.htm>. Acesso em 06 de setembro de 2020.

BRASIL. Supremo Tribunal Federal. **Recurso Extraordinário n° 125.556/PR.** Disponível em <http://www.stf.jus.br/>. Acesso em 06 de setembro de 2020.

BRASIL. Supremo Tribunal Federal. **MS 24.405-4-DF.** Rel. Min. Carlos Velloso. Disponível em <http://www.stf.jus.br/>. Acesso em 06 de setembro de 2020.

BRASIL. Supremo Tribunal Federal. **HC 82.424.** Rel. p/ o ac. Min. Presidente Maurício Corrêa. Disponível em <http://www2.stf.jus.br/portalStfInternacional/cms/verConteudo.php?sigla=portalStfJurisprudencia_pt_br&idConteudo=185077&modo=cms>. Acesso em 08 de setembro de 2020.

BRASIL. Supremo Tribunal Federal. **Ação Direita de Inconstitucionalidade n° 1969-2007.** Rel. Min. Ricardo Lewandosvik. Disponível em <http://www.stf.jus.br/>. Acesso em 08 de setembro de 2020.

Brasil adere à Convenção de Budapeste e se posiciona contra crimes cibernéticos. Disponível em <https://diariodoturismo.com.br/brasil-adere-a-convencao-de-budapeste-e-se-posiciona-contra-crimes/>. Acesso em 16 de outubro de 2020.

BRANCO, Paulo Gustavo Gonet. COELHO, Inocêncio Mártires. MENDES, Gilmar Ferreira. **Curso de Direito Constitucional.** 4ª. ed. São Paulo: Saraiva, 2008.

CARNEIRO, Adeneele Garcia. **Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação.** Âmbito Jurídico. Disponível em <http://www.ambito-juridico.com.br/site/index.php/?n_link=revista_artigos_leitura&artigo_id=11529&revista_caderno=17>. Acesso em 16 de agosto de 2020.

CANUTO, Luiz Cláudio. **CPI constata dificuldade em rastrear e punir crimes de internet.** Disponível em <https://www.camara.leg.br/noticias/467819-cpi-constata-dificuldade-em-rastrear-e-punir-crimes-de-internet/>. Acesso em 22 de agosto de 2020.

CAVALCANTE, Fachinelli**. Crimes cibernéticos**: **noções básicas de investigação e ameaças na internet.** Disponível em <https://jus.com.br/artigos/25743/crimes-ciberneticos>. Acesso em 19 de outubro de 2020.

Consultor Jurídico. **STF derruba decisão judicial e libera volta do WhatsApp.** Disponível em <https://www.conjur.com.br/2016-jul-19/stf-derruba-decisao-judicial-libera-volta-whatsapp#:~:text=Por%20identificar%20viola%C3%A7%C3%B5es%20%C3%A0s%20liberdades,feira%20(19%2F7)>. Acesso em 22 de agosto de 2020.

CRUZ, Diego. RODRIGUES, Juliana. **Crimes cibernéticos e a falsa sensação de impunidade.** Revista científica eletrônica do curso de direito. 13ª Ed. Disponível em <http://faef.revista.inf.br/imagens_arquivos/arquivos_destaque/iegWxiOtVJB1t5C_2019-2-28-16-36-0.pdf >. Acesso em 22 de agosto de 2020.

DIANA, Daniela. **História da internet.** Disponível em <https://www.todamateria.com.br/historia-da-internet/>. Acesso em 14 de agosto de 2020.

Declaração Universal dos Direitos do Homem. Disponível em <http://pfdc.pgr.mpf.mp.br/atuacao-e-conteudos-de-apoio/legislacao/direitos-humanos/declar_dir_homem.pdf>. Acesso em 08 de setembro de 2020.

DORIGON, Alessandro. SOARES, Renan Vinicius de Oliveira. **Crimes cibernéticos: dificuldades investigativas na obtenção de indícios da autoria e prova da materialidade.** Disponível em <https://jus.com.br/artigos/63549/crimes-ciberneticos-dificuldades-investigativas-na-obtencao-de-indicios-da-autoria-e-prova-da-materialidade>. Acesso em 22 de agosto de 2020.

ESTRADA, Manuel Martin Pino. **Delitos na Web: à espera do marco civil da internet.** Revista Jurídica Consulex. Brasília. Ano XVII. n. 405. 1 de dezembro/2013.

FOUCAULT, Michel. **Vigiar e Punir: nascimento da prisão**. Petrópolis: Editora Vozes, 1987.

FOGLIATTO, Juliana. **Os crimes cibernéticos e os meios que a polícia utiliza para a identificação dos criminosos.** Disponível em <https://jus.com.br/artigos/77225/os-crimes-ciberneticos-e-os-meios-que-a-policia-utiliza-para-a-identificacao-dos-criminosos>. Acesso em 30 de outubro de 2020.

FOLHA ONLINE. **Lan house começa a cadastrar clientes em SP**. Disponível em <http://www1.folha.uol.com.br/folha/informatica/ult124u19642.shtml>. Acesso em 15 de setembro de 2020.

FROTA, Jéssica Olivia Dias. PAIVA, Maria de Fátima Sampaio. **Crimes virtuais e as dificuldades para combatê-los.** Disponível em <https://flucianofeijao.com.br/novo/wp-

content/uploads/2018/11/ARTIGO_CRIMES_VIRTUAIS_E_AS_DIFICULDADES_PARA_COMBATE_LOS.pdf >. Acesso em 22 de agosto de 2020.

GLOBO CIÊNCIA. **Modelo panóptico prega o poder por meio de vigilância total do homem**. Globo Ciência. Globo.com. 2012. Disponível em <http://redeglobo.globo.com/globociencia/noticia/2012/03/modelo-panoptico-prega-o-poder-por-meio-da-vigilancia-total-do-homem.html>. Acesso em 06 de setembro de 2020.

GUARAGNI, Fábio André. RIOS, Rodrigo Sanchez. **Novas tendências de combate aos crimes cibernéticos: cooperação internacional e perspectivas na realidade brasileira contemporânea.** Revista de Estudos Criminais. Porto Alegre, v. 18, n. 73. 2019.

JESUS, Damásio De. ARAS, Vladmir. **Crimes de informática: Uma nova criminalidade**. Disponível em <https://jus.com.br/artigos/2250/crimes-de-informatica>. Acesso em 17 de agosto de 2020.

JUNIOR, Júlio Cesar Alexandre. **Cibercrime: um estudo acerca do conceito de crimes informáticos.** Revista Eletrônica da Faculdade de Direito de Franca. Disponível em <https://www.revista.direitofranca.br/index.php/refdf/article/view/602#:~:text=Cibercrime%20est%C3%A1%20associado%20ao%20%E2%80%9Cfen%C3%B3meno,12).>. Acesso em 14 de agosto de 2020.

KAMINSKI, Omar. **Conheça o Tratado Internacional contra crimes na Internet**. Revista Consultor Jurídico**.** Disponível em <https://www.conjur.com.br/2001-nov-4/convencao_lanca_tratado_internacional_cibercrimes>. Acesso em 16 de outubro de 2020.

MALTA, Magno. **Termo de Mútua Cooperação.** Disponível em <http://www.safernet.org.br/site/sites/default/files/Teles.pdf>. Acesso em 01 de outubro de 2020.

MAGELA, Nídia Cecília Mendes. ABREU, Bárbara França. GOMIDE, Caroline Carvalho. VIEIRA, Kely Bianca Teodoro. COSTA, Polyane Rodrigues. **Comunicação e sociedade: anonimato na internet.** Revista Expressão**.** Disponível em <http://www4.faculdadepromove.br/expressao/index.php/files/article/view/80/0>. Acesso em 06 de setembro de 2020.

MENDES, Maria Eugenia Gonçalves. VIEIRA, Natália Borges. **Os Crimes Cibernéticos no Ordenamento Jurídico Brasileiro e a Necessidade de Legislação Específica.** Disponível em <http://www.gcpadvogados.com.br/artigos/os-crimes-ciberneticos-no-ordenamento-juridico-brasileiro-e-a-necessidade-de-legislacao-especifica-2>. Acesso em 14 de agosto de 2020.

MEDEIROS, Assis. **Hackers: entre a ética e a criminalização**. Florianópolis: Visual Books. 2002.

Ministério Público Federal. 2ª Câmara De Coordenação e Revisão. **Crimes Cibernéticos**. Coletânea de artigos. Volume 3. Brasília. 2018. Disponível em

<http://www.mpf.mp.br/atuacao-tematica/ccr2/publicacoes/coletaneas-de-artigos/coletanea_de_artigos_crimes_ciberneticos>. Acesso em 16 de outubro de 2020.

Ministério das Relações Exteriores. **Processo de adesão à Convenção de Budapeste - Nota Conjunta do Ministério das Relações Exteriores e do Ministério da Justiça e Segurança Pública**. Disponível em <http://www.itamaraty.gov.br/pt-BR/notas-a-imprensa/21146-processo-de-adesao-a-convencao-de-budapeste-nota-conjunta-do-ministerio-das-relacoes-exteriores-e-do-ministerio-da-justica-e-seguranca-publica>. Acesso em 16 de outubro de 2020.

MIRAGEM, Bruno. **Responsabilidade por danos na sociedade de informação e proteção do consumidor: desafios atuais da regulação jurídica da Internet**. Revista de Direito do Consumidor: RDC. São Paulo. ano 18. n. 70. abr.-jun. 2009.

MORAES, Alexandre de. **Constituição do Brasil interpretada e legislação constitucional**. 4. ed. São Paulo: Atlas, 2004.

MORAES, Alexandre de. **Direito constitucional**. 15. Ed. São Paulo: Atlas, 2004.

MORAES, Paulo Francisco Cardoso de. **A vedação constitucional do anonimato aplicada à internet: o papel do estado brasileiro na identificação dos usuários e responsabilização dos provedores.** Revista Âmbito Jurídico**.** Disponível em <https://ambitojuridico.com.br/edicoes/revista-91/a-vedacao-constitucional-do-anonimato-aplicada-a-internet-o-papel-do-estado-brasileiro-na-identificacao-dos-usuarios-e-responsabilizacao-dos-provedores/>. Acesso em 06 de setembro de 2020.

MORIMOTO, Carlos Eduardo. **Termos técnicos GdH**. Disponível em <http://www.guiadohardware.net/termos/tcp-ip>. Acesso em 15 de setembro de 2020.

NASCIMENTO, Samir de Paula. **Cibercrime: conceitos, modalidades e aspectos jurídicos-penais.** Disponível em <https://ambitojuridico.com.br/cadernos/internet-e-informatica/cibercrime-conceitos-modalidades-e-aspectos-juridicos-penais/>. Acesso em 14 de agosto de 2020.

NASCIMENTO, Talles Leandro Ramos. **Crimes cibernéticos.** Conteúdo Jurídico. Disponível em <https://conteudojuridico.com.br/consulta/Artigos/52512/crimes-ciberneticos>. Acesso em 25 de outubro de 2020.

NETO, Amaro Moraes e Silva. **Privacidade na Internet: um enfoque jurídico**. Bauru, São Paulo: EDIPRO, 2001.

PAGANELLI, Celso Jefferson Messias. **Anonimato e internet: análise do princípio constitucional frente às recentes decisões do STJ.** Revista Âmbito Jurídico**.** Disponível em <https://ambitojuridico.com.br/cadernos/direito-constitucional/anonimato-e-internet-analise-do-principio-constitucional-frente-as-recentes-decisoes-do-stj/>. Acesso em 06 de setembro de 2020.

PEREIRA, Eduardo Baker Valls. **Crimes informacionais: da compatibilidade internacional do ordenamento jurídico nacional e da proposta de reforma.** Revista IBCCRIM. n. 112. 2015.

PIRES, Maísa Rezende. **O equilíbrio necessário para que a liberdade de expressão coexista com outros direitos**. Revista Âmbito Jurídico. Caderno Constitucional. Ano XIV, nº 95, Dezembro/2011. Disponível em <http://www.ambito-juridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=10790&revista_caderno=9>. Acesso em 06 de setembro de 2020.

POLICIA FEDERAL. **Contribuição da Policia Federal para o Marco Civil da Internet.** Disponível em <http://culturadigital.br/marcocivil/2010/05/31/contribuicao-da-policia-federal-para-o-marco-civil-da-internet/>. Acesso em 29 de setembro de 2020.

Procuradoria-Geral da República. **MPF defende adesão do Brasil à Convenção de Budapeste em audiência pública na Câmara.** Disponível em <http://www.mpf.mp.br/pgr/noticias-pgr/mpf-defende-adesao-do-brasil-a-convencao-de-budapeste-em-audiencia-publica-na-camara>. Acesso em 16 de outubro de 2020.

RABANEDA, Fabiano. **Os logs de acesso e sua guarda pelos provedores.** Disponível em <http://www.nic.br/imprensa/clipping/2010/midia165.htm>. Acesso em 01 de outubro de 2020.

Rede Nacional de Ensino e Pesquisa. **Nossa História – RNP.** Disponível em <https://www.rnp.br/sobre/nossa-historia >. Acesso em 14 de agosto de 2020.

ROMANO, Rogério Tadeu. **CONVENÇÃO DE BUDAPESTE E CIBERCRIMES**. Disponível em <https://jus.com.br/artigos/72969/convencao-de-budapeste-e-cibercrimes>. Acesso em 16 de outubro de 2020.

ROVER, Tadeu. **Violência virtual: internet facilita crimes e dificulta investigação, estimulando a impunidade.** Disponível em <https://www.conjur.com.br/2017-fev-05/entrevista-daniel-burg-especialista-crimes-virtuais>. Acesso em 22 de agosto de 2020.

SANTOS, Elaine Gomes dos. RIBEIRO, Raisa Duarte da Silva. **Restrições à liberdade de expressão e crimes cibernéticos: a tutela penal do discurso de ódio nas redes sociais.** Revista dos Tribunais. vol. 997. ano 107. São Paulo: Editora RT. novembro 2018.

SANCHES, Ademir Gasques. ANGELO, Ana Elisa de. **Insuficiência das leis em relação aos crimes cibernéticos no Brasil.** Disponível em <https://jus.com.br/artigos/66527/insuficiencia-das-leis-em-relacao-aos-crimes-ciberneticos-no-brasil>. Acesso em 30 de outubro de 2020.

SAFERNET. Disponível em <https://new.safernet.org.br/content/institucional>. Acesso em 30 de outubro de 2020.

Secretaria Geral da Presidência da República. **Brasil é convidado a aderir à Convenção do Conselho da Europa contra a Criminalidade Cibernética**. Disponível em <https://www.gov.br/secretariageral/pt-br/noticias/2020/julho/brasil-e-convidado-a-aderir-a-convencao-do-conselho-da-europa-contra-a-criminalidade-cibernetica>. Acesso em 16 de outubro de 2020.

SIMONSEN, André Wallace. **Privacidade e anonimidade na internet.** Disponível em <https://jus.com.br/artigos/32143/privacidade-e-anonimidade-na-internet>. Acesso em 08 de setembro de 2020.

SOUZA, Henry Leones de. VOLPE, Luiz Fernando Cassilhas. **Da ausência de legislação específica para os crimes virtuais.** Disponível em <https://egov.ufsc.br/portal/conteudo/da-aus%C3%AAncia-de-legisla%C3%A7%C3%A3o-espec%C3%ADfica-para-os-crimes-virtuais>. Acesso em 16 de agosto de 2020.

SOUZA, Gills Lopes Macêdo; PEREIRA, Dalliana Vilar. **A CONVENÇÃO DE BUDAPESTE E AS LEIS BRASILEIRAS.** Disponível em <https://www.mpam.mp.br/centros-de-apoio-sp-947110907/combate-ao-crime-organizado/doutrina/574-a-convencao-de-budapeste-e-as-leis-brasileiras>. Acesso em 16 de outubro de 2020.

Symantec. Organizações dos Estados Americanos. **Relatório 'Tendências de Cibersegurança na América Latina e no Caribe".** 2014. Disponível em <http://www.symantec.com/content/en/us/enterprise/other_resources/b-cyber-security-trends-report-lamc-annex.pdf >. Acesso em 22 de agosto de 2020.

VALVERDE, Danielle Novaes de Siqueira. **Crimes Cibernéticos: a obrigatoriedade do registro de acesso à internet como forma de possibilitar a identificação do criminoso.** Revista da ESMAPE. Recife. v. 15. n. 32. jul./dez. 2010.

VIANNA, Túlio. **Transparência Pública, Opacidade Privada**. Rio de Janeiro: Editora Revan. 2006.

WENDT, Emerson. JORGE, Higor Vinicius Nogueira. **Crimes Cibernéticos: ameaças e procedimentos de investigação.** 1. Ed. São Paulo: Editora Brasport, 2012.