FACULDADE DAMAS DA INSTRUÇÃO CRISTÃ
CURSO DE DIREITO

ANA LUIZA SIEPIERSKI

CRIMES CIBERNÉTICOS:
A POSSIBILIDADE DE RELATIVIZAÇÃO DO ANONIMATO

Recife
2016

ANA LUIZA SIEPIERSKI

CRIMES CIBERNÉTICOS:
A POSSIBILIDADE DE RELATIVIZAÇÃO DO ANONIMATO

Monografia apresentada à Faculdade Damas da Instrução Cristã como requisito parcial para obtenção do título de Bacharel em Direito.

Orientador(a): Professora Renata Celeste Sales e Silva

Recife
2016

Siepierski, Ana Luiza
Crimes cibernéticos: a posssiblidade de relativação do anonimato[a] Região. / Ana Luiza Siepierski. – Recife: O Autor, 2016.

48 f.; il.

Orientador(a): Prof[a]. Dr[a]. Renata Celeste Sales Silva.
Monografia (graduação) – Faculdade Damas da Instrução Cristã. Trabalho de conclusão de curso, 2016.

Inclui bibliografia.

1. Direito. 2. Crimes cibernéticos. 3. Anonimato. 4. Lei Carolina Dieckmann. I. Título.

34	**CDU (2.ed.)**	**Faculdade Damas**
340	**CDD (22.ed.)**	**TCC 2017-526**

FACULDADE DAMAS DA INSTRUÇÃO CRISTÃ
CURSO DE DIREITO

ANA LUIZA SIEPIERSKI

CRIMES CIBERNÉTICOS: A POSSIBILIDADE DE RELATIVIZAÇÃO DO ANONIMATO

Defesa Pública em Recife, _____de_____de_____.

BANCA EXAMINADORA:

Presidente:
_____

Orientador (a):
_____

Aos meus pais que nunca mediram esforços para auxiliar na minha jornada como estudante. Especialmente, para a conclusão desta graduação.

Agradeço, em especial, aos professores Ricardo Silva, Renata Celeste e Leonardo Siqueira que estiveram comigo contribuindo para a execução deste trabalho. Aos meus familiares e amigos por toda a paciência inesgotável.

RESUMO

O presente trabalho acadêmico é um estudo sobre os crimes cibernéticos e a possibilidade da relativização do anonimato. O tema é de grande relevância, uma vez que faz parte da nossa realidade, não recebendo, porém, o devido tratamento jurídico-doutrinário. A pesquisa foi baseada em livros, monografias e artigos, muitos fornecidos pela própria Internet. Primeiramente, o estudo abordou a evolução histórica dos crimes cibernéticos, apresentando a mudança de paradigma da evolução da tecnologia a partir da Revolução Industrial até os dias atuais. Sobre os delitos, o trabalho buscou conceituar e classificá-los demonstrando a sua abrangência. Em seguida, o estudo tratou dos aspectos legais dos delitos eletrônicos, fazendo menção à Convenção de Budapeste, bem como, à Lei nº 12.737/12. Por fim, o trabalho tratou da aplicação jurisprudencial e a questão do anonimato, expondo a dificuldade de se comprovar a materialidade e a autoria do crime. Das considerações finais, concluiu-se com a presente pesquisa, que nos casos excepcionais em que se legisla administrativamente para auxiliar na aplicação da lei penal, é possível restringir o alastramento dos crimes cibernéticos.

Palavras-chave: Crime cibernético, Internet, Anonimato.

ABSTRACT

The purpose of this academic paper is to study cybercrimes and the possibility of anonymity relativization. The theme is of great importance since it is part of our daily reality. Nevertheless, it does not receive the due legal-doctrinal treatment. The research is based on books, monographs, and articles, being many of them provided by the Internet itself. Firstly, the paper presents the historical development of cybercrimes. The approach considers the paradigm shift in technology evolution since the Industrial Revolution until today. Regarding the offences, they were conceptualized and classified, demonstrating their scope. Secondly, the study deals with the legal aspects of electronic offences, mentioning the Budapest Convention, as well as, the Law No 12.737/12. Finally, the study addresses the jurisprudential application and the issue of anonymity, exposing the difficulty in proving the crime materiality and authorship. Final consideration, concluded with this research that in exceptional cases where legislation administratively to assist in the application of criminal law, it is possible to restrict the spread of cyber crimes.

Keywords: Cybercrimes, Internet, Anonymity.

SUMÁRIO

INTRODUÇÃO

Uma das transformações mais profundas que ocorreu nas últimas décadas foi o surgimento do "*personal computer*" (PC) – computador pessoal, traduzido para o português – juntamente com uma das suas principais conectividades: a Internet.

A web surgiu no ápice da Guerra Fria, a partir de um projeto militar norte-americano do Departamento de Defesa dos Estados Unidos. Foi através dela que as pessoas obtiveram nova forma de comunicação, novo modo de comercializar serviços e produtos que são entregues em qualquer lugar do mundo. Vantagens e benefícios que fazem aumentar o número de pessoas e companhias acessando a rede mundial de computadores desenfreadamente.

Ocorre que, com o passar do tempo, o aperfeiçoamento deste novo veículo de comunicação, cumulado com a facilidade de acesso à tecnologia, propiciou o surgimento de novas práticas ilícitas: os chamados crimes cibernéticos. Percebe-se pela prática de tais crimes que muitas são as pessoas que se utilizam das benesses da Internet, de forma a violar os direitos de outrem.

Estes delitos são praticados com frequência devido à rapidez com que eles podem ser realizados, em decorrência da dificuldade de encontrar o autor do ilícito e em razão do aperfeiçoamento constante deste na medida em que o Direito e as autoridades policiais apresentam uma evolução mais lenta para o combate destas condutas delituosas.

Levando-se em consideração que esses crimes de informática evoluem conforme ocorrem os avanços tecnológicos, existe grande necessidade de progresso do Direito e da atuação policial, bem como o desenvolvimento de ferramentas utilizadas por estes, para que os criminosos possam ser adequadamente punidos.

Sendo assim, o presente trabalho justifica-se pela necessidade de examinar a ambiguidade do anonimato, de forma a compreender até que ponto considera-se legítima sua existência ou não. Visto que, por um lado, é vedado constitucionalmente – conforme artigo 5º, inciso IV da Constituição Federal de 1988, *in verbis*: é livre a manifestação do pensamento, sendo vedado o anonimato – por outro, é compreendido como um direito a ser defendido garantindo a

liberdade de expressão daqueles que não querem se expor.

Isto posto, questiona-se: como criar mecanismos para coibir os crimes cibernéticos, face à liberdade de expressão?

Embora o anonimato seja vedado constitucionalmente, sendo livre a manifestação do pensamento, conforme artigo 5º, IV da CF/88, no mundo virtual há certa garantia, tendo em vista a dificuldade de se descobrir o autor do delito. À vista disso, acreditamos que há influência direta na prática dos crimes cibernéticos. O que leva a inúmeras discussões em Comissões Parlamentares de Inquérito, objetivando encontrar mecanismos que impeçam a prática dos crimes virtuais.

Como objetivo geral, este trabalho busca demonstrar o papel do anonimato na facilitação dos crimes cibernéticos e apontar possível relativização.

A pesquisa tem como objetivos específicos: conceituar e caracterizar o que são os crimes cibernéticos; analisar o anonimato e suas limitações, tendo por base o alcance da recente Lei 12.737/2012, denominada Lei Carolina Dieckmann; e, por fim, apresentar a possibilidade de um caminho para incidir contra o anonimato apenas nos casos dos crimes cibernéticos, preservando a liberdade de expressão da sociedade.

Almejando atingir o objetivo deste trabalho, utiliza-se o método hipotético-dedutivo. A análise deverá ser realizada por meio de pesquisas bibliográficas, de materiais já publicados, como livros, artigos científicos, periódicos, monografias, dissertações, teses, bem como pela Internet.

Assim sendo, o presente trabalho contém a estrutura de três capítulos:

No primeiro capítulo, estabelecem-se algumas noções básicas a respeito dos crimes cibernéticos. De forma a trazer algumas definições conceituando-o através de várias perspectivas, analisando sua evolução histórica.

No segundo capítulo, são analisados os aspectos legislativos do delito eletrônico, bem como a questão do anonimato e as suas limitações. Examinando sua vedação constitucional, de forma a avaliar até onde ele pode alcançar, haja vista a existência da Lei nº 12.737/2012, denominada Lei Carolina Dieckmann.

Por fim, no terceiro capítulo, são apresentadas aplicações jurisprudenciais e a possibilidade de relativização do anonimato. Demonstrando as dificuldades de provar a materialidade e autoria do fato, bem como, os conflitos de competência jurisdicional e territorial dos delitos de informática.

2. CRIMES CIBERNÉTICOS: CONCEITUAÇÃO E EVOLUÇÃO

Inicialmente, é importante estabelecer, neste trabalho, como se deu a evolução histórica da Internet, para, então, buscar uma definição objetiva e clara do que é o crime cibernético.

A Internet surge como um instrumento facilitador para a consecução de crimes, visto que, em muitos casos, o agente delituoso não precisa utilizar de nenhum instrumento físico que seja ou violento ou ameaçador para realização daqueles, bastando apenas o computador e o conhecimento técnico, ou não, para concretizar as condutas delitivas.

Assim, na medida em que a Internet concentra, processa e transfere qualquer tipo de informação e dados, ela também se transformou em um meio eficaz para a realização de crimes ou certas condutas que agridem bens relevantes do homem.

Sucede que, ao tempo em que a rede mundial de computadores evolui e ganha determinada proporção, dá espaço aos denominados crimes cibernéticos, que serão estudados e classificados adiante.

2.1. A Mudança de Paradigma e o Surgimento dos Delitos Eletrônicos

Em primeiro plano, o mundo experimentou um conjunto de mudanças revolucionárias que ocorreram na Europa entre os séculos XVIII e XIX, cuja denominação se deu por Revolução Industrial. Esta trouxe avanço substancial na transformação de vida do homem do campo para o homem da cidade.

A Revolução Industrial passou basicamente por três etapas. Caracterizou-se, primeiramente, pela produção artesanal, no qual o artesão era dono da matéria-prima e dos instrumentos de produção. Com o aperfeiçoamento das máquinas a vapor, a continuação da Revolução foi impulsionada.

O segundo momento das transformações ocorridas na Europa Ocidental, entre o período de 1860 a 1900, ganha rosto com a produção manufatureira, alcançando outros países como Alemanha, França, Itália, Rússia. As divisões de trabalho começaram a surgir, de modo que a velocidade da produção aumentou

substancialmente.

Por fim, a terceira fase da Revolução Industrial é o momento em que surgem as máquinas industriais, que, por sua vez, substituíram trabalhadores e ferramentas. Aqueles tornam-se meros operários submetidos ao ritmo frenético dos instrumentos revolucionários. Assim, dá-se início a uma nova era: a era da tecnologia.

Por volta da década de 60, em meio a tantas transformações surgiu a Internet. O advento da rede mundial de computadores se deu, primeiramente, por uma necessidade militar, tendo em vista o cenário da Guerra Fria, servindo como base de apoio para as comunicações feitas entre as forças de ataque norte americano em casos de investidas inimigas que pudessem pôr em risco as informações captadas e emitidas pelos meios convencionais.

A ideia de uma rede interligada surgiu com o objetivo de proteger os computadores do governo norte americano, notadamente como medida preventiva para o caso de um eventual ataque nuclear contra o país. O domínio da tecnologia e a própria utilização da rede permaneceram restritos às áreas militar e universitária, e somente com o surgimento da Rede Minitel, na França, no final da década de 70 e início da década de 80, é que o sistema passou a ser disponibilizado também para o comércio.

No século XXI tais tecnologias se tornaram a coluna vertebral da sociedade, o mundo já não via barreiras, sendo possível estar virtualmente em qualquer lugar e em qualquer momento.

De acordo com o livro Sociedade da Informação no Brasil – Livro Verde, elaborado pelo Ministério da Ciência e Tecnologia do Brasil, a Internet é definida como:

> Um sistema de redes de computadores - uma rede de redes - que pode ser utilizado por qualquer pessoa, em qualquer parte do mundo, onde haja um ponto de acesso, e que oferece um amplo leque de serviços básicos, tais como correio eletrônico, acesso livre ou autorizado a informações em diversos formatos digitais e transferência de arquivos [1].

[1] Ministério da Ciência e Tecnologia (Org.). **Sociedade da informação no Brasil Livro Verde**. Brasília: 2000.

Marco Antonio Zanellato acredita que, independente da definição adotada para a rede mundial de computadores:

> (...) Três elementos caracterizam a Internet: (a) é uma cadeia de redes (réseau de réseaux); (b) em escala mundial; (c) cujos equipamentos informáticos expressam a mesma linguagem e utilizam as mesmas técnicas para fazer circular a informação [2].

Neste sentido, conclui-se o conceito de Internet como uma rede de computadores, integrada por outras redes menores, comunicando-se entre si. Em outras palavras, os computadores comunicam-se através de um endereço IP, onde é trocada uma gama de informações.

Ocorre que, existe uma quantidade enorme de informações pessoais disponíveis na rede, ficando à disposição de milhares de pessoas que possuem acesso à Internet. E, quando não disponíveis pelo próprio usuário, são procuradas por outros que buscam na web o cometimento de crimes, são os denominados Crimes Virtuais.

Pierre Lévy, filósofo, sociólogo e pesquisador em ciência da informação e da comunicação, estuda o impacto da Internet na sociedade, as humanidades digitais e o virtual. Pierre é um dos maiores estudiosos sobre a Internet, busca analisar e explicar as interações entre a web e a sociedade. Atualmente, é um dos principais filósofos da mídia.

O filósofo mais influente na área da tecnologia, em uma de suas obras[3], caracterizando o contexto contemporâneo de cibercultura, já havia identificado um crescente aumento no uso da rede por parte das pessoas que utilizavam a Internet, tendo em vista o desenvolvimento de novas tecnologias e interfaces de comunicação sem fio.

Estava certo Pierre Lévy frente ao cenário atual. Hoje a Internet está disponível em vários dispositivos portáteis, das mais diferentes formas; milhares de pessoas permanecem por vezes mais tempo navegando na Internet do que vivendo o mundo real, mídias sociais, leitura de livros, videoconferências.

Uma nova sociedade surge marcada pelo individualismo, que vive atrás

---

[2] ZANELLATO, Marco Antonio. **Condutas Ilícitas na Sociedade Digital**. São Paulo: 2002.
[3] LEMOS, André; LÉVY, Pierre. **O futuro da Internet: em direção a uma ciberdemocracia**. São Paulo: 2010.

do computador. Novas relações jurídicas também eclodem, de modo que o Direito deve se adequar, trazendo soluções para os litígios que venham a ocorrer dentro do ambiente virtual.

É fato que a rede mundial de computadores, isto é, a Internet, é o meio de comunicação em massa mais difundida na população nos últimos anos, haja vista sua capacidade infindável e, muitas vezes, ilimitada de facilitar e modernizar a vida das pessoas que convivem em uma sociedade.

É unânime o entendimento de que a web é resultado de uma evolução tecnológica proporcionada pela sociedade de massa. O setor de telecomunicações que mais cresce no país é o da Internet banda larga, que proporciona o tráfego de dados em rede de alta velocidade.

A troca de correspondências, pesquisas, movimentação das contas bancárias, o contato com pessoas do outro lado do mundo em tempo real, comprar produtos sem sair de casa, eram atos inimagináveis aos internautas de hoje.

No âmbito do Direito Penal, o uso da Internet veio acompanhado de diferentes condutas passíveis de causar lesão a diversos bens jurídicos. Conforme lembra Alexandre Jean Daoun:

> Os benefícios da modernidade e celeridade alcançados com a rede mundial trazem, na mesma proporção, a prática de ilícitos penais que vêm confundindo não só as vítimas como também os responsáveis pela persecução penal [4].

Desse modo, o surgimento da rede mundial de computadores facilitou veementemente o relacionamento entre as pessoas, físicas ou jurídicas, seja no sentido pessoal ou comercial. Todavia, se de um lado a Internet é utilizada para proporcionar tais benefícios, de outro não deixa de ser acionada na realização de práticas ilícitas.

Na nova era da tecnologia os criminosos não saem às ruas armados, expondo-se. Ao contrário, acobertam-se por trás do anonimato. Anonimato este que é garantido, em sua maioria, no cometimento dos crimes cibernéticos, tendo em vista a utilização dos computadores como meio para a prática do delito.

---

[4] DAOUN, Alexandre Jean. **Os novos crimes de informática**. 2016. Disponível em: <http://www.egov.ufsc.br/portal/conteudo/os-novos-crimes-de-inform%C3%A1tica>. Acesso em 27.09.2016.

2.2. Conceito e Abrangência dos Crimes Cibernéticos

Ainda não se chegou a um consenso a respeito do conceito de crime cibernético. São utilizadas expressões como sinônimos, por exemplo, criminalidade mediante computadores, delito informático, criminalidade da informática, delito cibernético, cibercrime, entre outros.

Os primeiros cibercrimes começaram a ocorrer na década de 70, na maioria das vezes eram praticados por especialistas em informática, o qual o objetivo era driblar os sistemas de seguranças das empresas, com um foco principal nas instituições financeiras. Atualmente, o perfil das pessoas que praticam crimes de informática já não é o mesmo daquela época.

Em linhas gerais, entende-se por delito informático, atividade onde um computador ou uma rede de computadores é utilizado como ferramenta ou base de ataque para o cometimento de crime já tipificado ou não. Esta é a definição mais simples que se pode ter dos referidos crimes, haja vista compreender um leque amplo de entendimentos.

Enquanto o Tratado do Conselho Europeu sobre Crime Cibernético usa o termo ‘cibercrime’ para definir delitos que vão de atividades criminosas contra dados até infrações de conteúdo e de copyright, outros autores, no entanto, sugerem definição mais ampla e incluem atividades como fraude, acesso não autorizado, pornografia infantil.

Utilizando a expressão ‘crimes de computador’, Paulo Marco Ferreira Lima os descreve como:

> Sendo qualquer conduta humana (omissiva ou comissiva) típica, antijurídica e culpável, em que a máquina computadorizada tenha sido utilizada e, de alguma forma, facilitado de sobremodo a execução ou a consumação da figura delituosa, ainda que cause um prejuízo a pessoas sem que necessariamente se beneficie o autor ou que, pelo contrário, produza um benefício ilícito a seu autor, embora não prejudique a vítima de forma direta ou indireta[5].

Já para a autora Carla Rodrigues Araújo de Castro, o crime de

[5] LIMA, Paulo Marco Ferreira. **Crimes de computador e segurança computacional**, 2006.

informática:

> É aquele praticado contra o sistema de informática ou através deste, compreendendo os crimes praticados contra o computador e seus acessórios e perpetrados através do computador. Os delitos praticados através da Internet, pois pressuposto para acessar a rede é a utilização de um computador. [6]

O crime cibernético possui algumas características como a transnacionalidade, já que não está restrito apenas a uma região do globo; a universalidade, por se tratar de um fenômeno de massa; e a ubiquidade, pois pode ocorrer em setores privados ou em públicos.

No que diz respeito às consequências da prática do crime para a vítima, o crime digital tem o poder de provocar tanto danos pessoais – como, por exemplo, um e-mail enviado com mensagem racista – quanto materiais, quando o sistema de serviço bancário pela Internet, o Internet Banking, é alvo de pessoas mal intencionadas que furtam as senhas dos clientes.

Cláudio Líbano Manzur, reconhecido pela Chambers Latin America como expert na área de propriedade intelectual e na área de Telecomunicação, Mídia, Tecnologia (TMT), conceitua o Direito Digital como:

> Todas aquellas acciones u omisiones típicas, antijurídicas y dolosas, trátese de hechos aislados o de una serie de ellos, cometidos contra personas naturales o jurídicas, realizadas en uso de um sistema de tratamiento de la información y destinadas a producir un perjuicio en la victima a través de atentados a la sana técnica informática, lo cual, generalmente, producirá de manera colateral lesiones a distintos valores jurídicos, repontándose, muchas veces, un beneficio ilícito en el agente, sea o no se carácter patrimonial, actúe con o sin ánimo de lucro.[7]

Para Richard Spinello, Professor Associado da Prática e Presidente Assistente do Departamento de Gestão e Organização da Escola Carroll of Management do Boston College, a Internet tornou-se um solo fértil para alguns tipos de crimes digitais, uma vez que há vários criminosos espionando no mundo

---

[6] CASTRO, Carla Rodrigues Araújo de. **Crimes de informática e seus aspectos processuais**, 2003.

[7] MANZUR, Claudio Líbano. **Los delitos de hacking en sus diversas manifestaciones**. 2000. Disponível em: <https://pt.scribd.com/doc/308707918/Los-Delitos-de-Hacking-en-Sus-Diversas-Manifestaciones>. Acesso em: 27.09.2016.

digital.

Sendo assim, Spinello acredita que o crime digital ainda é muito obscuro, e esclarece seu significado como: “(...) uma categoria especial de atos criminosos os quais são tipicamente executados através da utilização de tecnologias computacionais e de rede”.

2.3. Dos Delitos Cibernéticos e Sua Classificação

Os crimes digitais são classificados em três categorias: puro, misto e comum.

A primeira classificação abarca qualquer ato ilícito que atente contra o hardware ou software – parte física e tecnológica – do computador. Como exemplo, é possível citar os *crackers*, que nada mais são do que *hackers* que usam seu conhecimento para fins ilegais ou prejudiciais. Estes, são indivíduos que dedicam-se exclusivamente e de forma incomum à área da informática e da tecnologia, elaborando e modificando softwares ou hardwares de forma legal, com intenção de obter melhorias.

Outro exemplo de cibercrime classificado como puro é o vírus Melissa[8], que surgiu em 1999, ocasionando dano de mais de US$ 80.000.000,00 (oitenta milhões de dólares americanos).

São classificados como mistos aqueles que fazem uso da Internet como meio obrigatório para a consumação do delito. Nesta classificação, o objetivo do infrator não é mais atingir o computador da vítima, mas sim quaisquer outros bens jurídicos como, por exemplo, transações bancárias ilícitas via *internet banking*.

Os delitos de informática classificam-se como comuns, quando executados através da Internet, pretendendo cometer o crime fim já tipificado no Código Penal Brasileiro. A pornografia infantil praticada através das redes mundiais de computadores é um exemplo claro do cibercrime comum.

A classificação dos cibercrimes não se esgota em puro, misto e comum. São, ainda, classificados como próprios e impróprios.

---

[8] SCHMIDT, Guilherme. **CRIMES CIBERNÉTICOS Non scholae, sed vitae discimus**. Disponível em: < http://schmidtadvogados.com/v/artigo5>. Acesso em: 09.11.2016.

Serão próprios, quando a execução e a consumação do crime cibernético se concretizar no meio informático. Nesse caso, o bem jurídico tutelado é a própria Internet como, por exemplo, violação de e-mails. Os crimes impróprios, por sua vez, são aqueles já tipificados pelo Código Penal, podendo ser praticados de qualquer forma. A Internet é apenas mais um meio utilizado para violar bens já protegidos pela legislação.

Assim esclarece a autora Rita de Cássia Lopes da Silva que:

> A informação neste caso, por se tratar de patrimônio, refere-se a bem material, apenas grafado por meio de bits, suscetível, portanto, de subtração. Assim, ações como alteração de dados referentes ao patrimônio, como a supressão de quantia de uma conta bancária, pertencem à esfera dos crimes contra o patrimônio[9].

Da mesma forma que as pessoas possuem números que as identificam, como o Cadastro de Pessoa Física (CPF), os computadores e periféricos conectados à Internet também são distinguidos de maneira semelhante, através do endereço IP (*Internet Protocol* ou Protocolo de Internet). Esse número de protocolo é único e permite que as máquinas comuniquem-se na rede.

Desse modo, devido as suas características, o endereço IP é um dos pontos para que o agente do crime seja encontrado. Todavia, as dificuldades iniciam na tentativa de obter este endereço IP, pois apesar de poderem ser descobertos com o provedor de Internet ou com os gerenciadores do site, obter os dados do usuário que estava acessando naquele certo momento é difícil e demorado de se conseguir.

As empresas alegam a inconstitucionalidade de uma suposta quebra de sigilo dos dados de seus clientes. No entanto, o conteúdo das informações continuaria protegido, conforme assegura o art. 5.º, XII, da CF/88, apenas o acesso deixaria de ser confidencial. Além do mais, devido à quantidade de informações que são geradas e armazenadas diariamente nos bancos de dados dos provedores serem incontáveis, é normal que essas empresas não permaneçam com os dados gravados por muito tempo, o que leva à impunidade por ausência de provas devido à morosidade no inquérito policial. Ressaltando ainda que quando o crime envolve

[9] SILVA, Rita de Cássia Lopes da. **Direito penal e sistema informático**, 2003.

pessoas de diferentes países, a identificação torna-se mais complicada.

Ao se obter o endereço IP, deve-se procurar qual é o endereço físico do computador, chamado de endereço MAC. Em seguida, tem que investigar quem realizou o acesso e quem praticou crime. No entanto, essa tarefa torna-se mais embaraçosa quando a rede é aberta ao público, como nos shoppings, universidades, aeroportos e lan houses, pois não é como em uma residência que moram apenas duas ou mais pessoas.

Os criminosos virtuais, na maioria das vezes, utilizam-se da inocência dos usuários para propagar mensagens, coletar informações privilegiadas, ou mesmo prejudicar outrem de alguma forma produzindo grande prejuízo moral ou financeiro para a vítima. Tais criminosos atuam de várias maneiras e cometem crimes como roubo de identidade, pedofilia, calúnia e difamação, ameaça, discriminação, espionagem etc.

Muitos ainda acreditam que as configurações das redes sociais são infalíveis. Ocorre que, na Internet nada é plenamente seguro, de forma que sempre estará presente a possibilidade de invasão permanecendo o indivíduo no anonimato.

> Na Comissão Parlamentar de Inquérito destinada a investigar a prática de crimes cibernéticos e seus efeitos deletérios perante a economia e a sociedade neste país, o Presidente da Associação Brasileira de Criminalística, Dr. Bruno Telles, disse que novos aplicativos e aparelhos protegem cada vez mais o anonimato e dificultam a atuação das autoridades (é possível montar uma rede de pedofilia pelo Whatsapp, onde os dados são criptografados de ponta a ponta)[10].

Em última análise, têm-se de um lado defensores da vedação ao anonimato para preservar liberdades e, de outro, patronos do combate ao anonimato, quando se trata de crimes. Ou seja, é possível visualizar certa relativização da vedação disposta no artigo 5º, inciso IV da República Federativa do Brasil, conforme veremos adiante com mais destaque.

3. OS ASPECTOS LEGISLATIVOS DO CRIME CIBERNÉTICO E A QUESTÃO

[10] Informação fornecida pelo Presidente da Associação Brasileira de Criminalística, Dr. Bruno Telles, na Comissão Parlamentar de Inquérito destinada a investigar a prática de crimes cibernéticos, realizada em Brasília, em setembro de 2015.

DO ANONIMATO

O capítulo em voga trata dos aspectos legislativos do crime cibernético, isto é, da ausência de legislação específica para incidir diretamente nos delitos de informática.

Embora a Convenção de Budapeste tenha sido criada no ano de 2001, o Brasil foi um dos poucos países que não assinou, ratificou, tampouco aderiu à Convenção de Budapeste – conforme será demonstrado no decorrer do presente trabalho, a lista dos membros adeptos ao Tratado, em anexo (Anexo. 01).

No entanto, foi criado Projeto de Lei do Senado nº 76/2000 que sequer foi votado, tendo sido arquivado. Como será visto adiante, o que temos hoje, é apenas a Lei nº 12.737/12, conhecida como Carolina Dieckmann.

Ademais, será abordada a questão do anonimato: seu conceito e a sua ambiguidade no mundo virtual.

3.1. Convenção de Budapeste e seu Protocolo Adicional

Foram poucos os países que disciplinaram o combate aos crimes cibernéticos. Dado preocupante, em vista de uma modalidade de crime com uma abrangência internacional.

Diante de tal quadro, em 21 de setembro de 2001, foi criada a Convenção de Budapeste – uma espécie de Tratado Internacional de direito penal e direito processual penal – firmado no âmbito do Conselho da Europa para definir de forma harmônica os crimes praticados por meio da Internet e as formas de persecução.

A referida Convenção ficou disponível para assinatura em Budapeste em novembro de 2001 e entrou em vigor no mês de julho de 2004. Até 02 de setembro de 2006, somente 15 Estados haviam assinado, ratificado ou aderido à Convenção, enquanto mais 28 Estados a assinaram, mas não a ratificaram. O Brasil, porém, até a presente data, não assinou, sequer ratificou, tampouco aderiu à Convenção de Budapeste – conforme se demonstra na lista dos membros adeptos ao Tratado, em anexo (Anexo. 01).

O Projeto de Lei do Senado nº 76/2000, de autoria do Senador Renan Calheiros, que visava a definição e tipificação dos delitos informáticos, aguardava

votação no Congresso Nacional. Contudo, tal projeto, está atualmente arquivado.

Resta clara, portanto, a necessidade de uma legislação específica para combater os crimes cibernéticos. Outros países já editaram suas leis sobre o assunto e está em andamento a Convenção de Budapeste, que visa regular o combate a esses crimes no âmbito mundial, incentivando uma política de cooperação recíproca entre as polícias, a qual o Brasil ainda não ratificou.

3.2. Conceito e Ambiguidade do Anonimato no Ambiente Virtual

Preliminarmente, faz-se necessário o esclarecimento do que vem a ser o anonimato, também entendido como um hábito praticado entre aqueles que não querem ser identificados. Ocorre quando não possui nome, nem assinatura, ocultando quem transmite a informação.

Convém ressaltar, no entanto, que a Constituição Federal de 1988 em seu artigo 5º, IV[11] veda expressamente o anonimato.

Além da Constituição, o anonimato é vedado através de diversas outras normas, como aquelas contidas nos artigos 144 da Lei 8.112/90; 14 da Lei 8.429/92 e 6° da Lei 9.784/99, as quais determinam qualificação no processo.

Ainda em análise da norma constitucional, assinala-se que numa sociedade democrática de direito, a liberdade de expressão gera também um dever de responsabilidade com relação à manifestação emitida, na medida em que esta fere os direitos fundamentais de terceiros.

Por outro lado, tal vedação constitucional não implica dizer que a Carta Magna considere a ideia do anonimato negativa. Há situações em que o anonimato é fundamental para a preservação da ordem democrática, como no caso de sigilo da fonte jornalística ou mesmo em mecanismos de denúncias anônimas com o objetivo de combate ao crime e garantia de direitos. Vai além, o anonimato é forma legítima do exercício da liberdade de expressão e comunicação. Questiona-se, porém, a legitimidade da relativização da prática do hábito de não se identificar.

Neste sentido, em 28/05/2015, o relator especial da ONU para Liberdade

---

[11] Art. 5º da **Constituição Federal de 1988**: Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
IV - é livre a manifestação do pensamento, sendo vedado o anonimato.

de Expressão, David Kaye, publicou seu primeiro Relatório Anual em que analisa a relação entre o direito de expressão e de opinião e direito à privacidade, com o uso de criptografia e do anonimato na era digital[12]. O documento avalia, ainda, os cenários em que governos podem impor restrições a essas práticas.

O artigo, entre outros pontos, defende que qualquer um que queira expressar opiniões on-line deve poder fazê-lo anonimamente para se prevenir de assédio ou represálias. O anonimato é uma condição essencial para que jornalistas protejam suas fontes, como dito anteriormente, e também para que delatores de ilegalidades não sejam perseguidos.

Outra perspectiva, não muito distinta, mas analisada por outro ponto é de que a vedação do anonimato é um direito a ser defendido, visto que aquele que tem algo a esconder não é obrigado a produzir provas contra si mesmo, pois a vedação ao anonimato é um direito fundamental a ser defendido.

As iniciativas anônimas, quando não são contaminadas em seu objetivo, o são em seus meios, e todo o trabalho para neutralizá-las é digno. Quem tem algo a esconder não é obrigado a produzir prova contra si mesmo, e tem seus segredos constitucionalmente guardados pelo direito à privacidade. É de se perceber, portanto, que a facilidade ao anonimato na Internet, tem facilitado a criminalidade de maneira exorbitante.

Há quem defenda, ainda, a criação de ferramentas de identificação daqueles que habitualmente assinam sem nome, considerados anônimos, fundamentando na linha clássica em que o direito de um termina onde começa o do outro.

Frente ao quadro exposto – no qual foi criada uma Convenção Internacional para definir os crimes praticados por meio da rede mundial de computadores e suas formas de persecução, optando o Brasil por não adotá-la; paralelamente, o anonimato enraíza-se por entre o cometimento dos crimes cibernéticos – faz-se indispensável à análise da edição da Lei Carolina Dieckmann.

3.3. A Experiência Brasileira: A Edição da Lei Carolina Dieckmann

[12] CANABARRO, Diego R. **Uma breve análise do Primeiro Relatório do Professor David Kaye ao Conselho de Direitos Humanos da ONU**. 2015. Disponível em: <http://observatoriodainternet.br/post/uma-breve-analise-do-primeiro-relatorio-do-professor-david-kaye-ao-conselho-de-direitos-humanos-da-onu>. Acesso em: 25.09.2016.

Inicialmente, é necessária uma análise sobre a Lei nº 12.737/12 (Anexo 02), conhecida extra oficialmente como Lei Carolina Dieckmann, que veio acrescentar ao Código Penal, dispositivos legais que tipificam os delitos cibernéticos, bem como modificar o texto legal já existente. É indiscutível que a lei em voga representa um avanço considerável na garantia da segurança de dados, no entanto, a forma como ela originou provoca consequências sérias na investigação dos crimes eletrônicos, tendo em vista sua imperfeição.

Embora a nossa legislação penal seja defasada quanto aos crimes cibernéticos, conforme demonstrado no capítulo anterior, em maio de 2011, Carolina Dieckmann, famosa atriz brasileira, foi vítima do cometimento de mais um crime por meio da Internet: supostamente foram copiadas do seu computador pessoal, 36 (trinta e seis) fotos em situação íntima, que acabaram divulgadas na Internet[13].

Por conseguinte, o crime ganhou proporção, tendo em vista a fama da atriz, que, veio dar nome ao Projeto de Lei nº 2.793/2011 que resultou na 'Lei Carolina Dieckmann'. A mais recente em nosso ordenamento referente a crimes cibernéticos.

A lei foi sancionada em 02 de dezembro de 2012 pela ex Presidente Dilma Rousseff, gerando alterações no Código Penal Brasileiro, tipificando os chamados delitos informáticos.

O legislador teve como intenção, atualizar e incluir algumas situações no nosso ordenamento jurídico. Através da Lei foram acrescentados os artigos 154-A e 154-B, bem como modificados o texto legal já existente dos artigos 266 e 298 do Código Penal.

O objeto jurídico tutelado pelo artigo 154-A é a proteção do direito constitucional à intimidade. O ilícito consiste em invadir um sistema pessoal, particular da vítima e obter, alterar ou danificar, informações contidas ali. O legislador foi perspicaz ao utilizar a expressão 'dispositivo informático', assim não se limitando aos computadores, mas abarcando igualmente os aparelhos celulares ou smartphones, tablets etc.

Em suma, o primeiro artigo acrescentado pela Lei em voga, tem como fim proteger dados pessoais conectados ou não a Internet de agentes que tenham

---

[13] **Lei Carolina Dieckmann**. 2016. Disponível em: <https://pt.wikipedia.org/wiki/Lei_Carolina_Dieckmann> Acesso em: 29 set. 2016.

intenções inidôneas. E punir não somente quem de fato cometeu a invasão, mas também quem facilitou o delito, através da criação de programas ou dispositivos informáticos e ainda um agente que difunda as informações particulares.

Por conseguinte, o segundo artigo acrescentado, qual seja, 154-B, tem o objetivo de definir que os delitos do art.154-A estão condicionados à ação penal pública mediante representação, salvo nos casos em que o sujeito passivo é a Administração Pública. Neste caso, a ação penal será pública incondicionada.

Além das inclusões mencionadas, a Lei também modificou a redação de dispositivo 266 do Código Penal. Foi ampliado o alcance deste artigo passando a tutelar a interrupção dos serviços telemáticos ou informação de utilidade pública.

O último dispositivo que teve seu texto alterado pelo legislador foi o 298. Finda uma discussão que existia na doutrina e na jurisprudência sobre a natureza do cartão bancário com a inclusão do parágrafo único, afirmando que o cartão bancário de crédito ou débito é documento particular. A alteração é mais sentida no âmbito dos crimes monetários, porém se estende aos crimes cibernéticos, no tocante ao roubo de dados de cartões bancários na rede mundial de computadores e sua utilização indevida.

Embora vigente a Lei Carolina Dieckmann, percebe-se que existe uma lacuna na legislação penal brasileira, tendo em vista o alcance do anonimato frente ao cometimento dos crimes cibernéticos em questão.

Levando-se em consideração que os crimes de informática evoluem conforme ocorrem os avanços tecnológicos, existe uma grande necessidade de progresso do Direito e das autoridades policiais, bem como das ferramentas utilizadas por estes, para que os criminosos possam ser adequadamente punidos.

No entanto, antes de redigir uma lei, é preciso pensar na sua criação. Jean-Daniel Delley - professor aposentado da Faculdade de Direito da Universidade de Genebra, e especialista em democracia direta e método legislativo – apresentou um procedimento metódico de elaboração das leis, dividido em fases interdependentes.

Para que se legisle com qualidade, no modelo mencionado pelo jurista, o procedimento legislativo deve ser dividido em algumas etapas: (i) definição do problema; (ii) determinação dos objetivos; (iii) estabelecimento de cenários alternativos; (iv) escolha das soluções; (v) avaliação prospectiva; (vi) execução e (vii)

avaliação retrospectiva[14].

Ocorre que muitas vezes, o modelo apresentado, que parece ser ideal, não é seguido com fidelidade pela pessoa do legislador brasileiro. É o que se verifica quando da criação da Lei em questão – Carolina Dieckmann – oriunda do Projeto de Lei nº 2.793/2011, apresentado ao Congresso Nacional pelo Deputado Paulo Teixeira (PT/SP) em 29 de novembro de 2011, que tramitou em regime de urgência e em tempo recorde comparado a outros Projetos de Lei.

Embora a norma seja de grande relevância para o ordenamento jurídico, abordando condutas ilícitas que violam diversos bens jurídicos, na prática deixam a desejar pela qualidade da redação.

Constata-se, portanto, que a norma criada foi instituída às pressas. Em sua essência, a norma penal contém tão somente o tipo penal, restando ausente a forma como devem ser disciplinados os meios processuais, através dos quais se garantem a eficácia da norma.

Não é diferente o entendimento do advogado Dr. Carlo Frederico Müller, quando analisa a celeridade da criação da norma em face do interesse público por se tratar de um caso em que a vítima era famosa. “Deveria ter sido elaborada com maior cautela, de forma a atender efetivamente às necessidades que a tecnologia vem trazendo para os cidadãos”, critica[15].

Ademais, é claro e evidente o papel preponderante da mídia como formadora de opinião. Sua inegável força dentro das instituições e o seu poderio econômico e ideológico transformaram-na em uma espécie de condutora das massas e ditadora de regras.

Preocupação reside no fato de que a mídia, no afã do sensacionalismo e do glamour, transformou-se numa espécie de “legisladora” penal, tendo em vista que casos criminais célebres são espetacularizados pelos meios de comunicação e acabam provocando imediatas alterações na lei penal, na imensa maioria das vezes precipitadas e desastrosas. A sua influência sobre o Poder Legislativo brasileiro na elaboração das leis penais se tornou inegável.

O Jurista Juan L. Fuentes Osório ao comentar sobre a percepção da

---

[14] DELLEY, Jean-Daniel. **Pensar as leis. Introdução a um procedimento metódico. Cadernos da Escola do Legislativo**. Belo Horizonte: 2004.

[15] MÜLLER, Carlo Frederico. **Texto ruim inviabiliza Lei Carolina Dieckmann, afirmam advogados**. 2013. Disponível em: <http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&infoid=33404>. Acesso em: 17.11.2016.

realidade criminal pelos veículos de comunicação aduz que o trabalho de comunicação da mídia resume-se em três fases: (i) eleição dos acontecimentos que serão notícia; (ii) hierarquização das notícias segundo sua importância; por fim, (iii) a tematização ou conversão de uma notícia em tema de debate social[16].

Pode-se dizer, portanto, que a informação não é inocente. Os próprios meios de comunicação acabam exigindo do Poder Legislativo uma repressão penal bastante severa, sugerindo muitas vezes, sem nenhum tipo de respaldo técnico, a correta forma de se legislar na seara penal.

É diante deste quadro que o legislador acaba cedendo aos chamamentos e apelos da mídia e acaba se deixando levar pelo "clamor público" na elaboração das leis penais.

A Mídia acaba sendo legitimada pela sociedade e ainda continua sendo considerada fidedigna, imparcial e transparente. Assim o seu poder aflora e se sobrepõe sobre os poderes constituídos.

Isto posto, a primeira crítica feita à nova legislação diz respeito à condicionante de violação indevida de mecanismo de proteção do equipamento. Explica a advogada especialista em direito digital, Sandra Tomazi, que "se o computador não tem mecanismos de segurança, como antivírus ou senha, não há como demonstrar essa violação" [17], sendo impossível a tipificação do crime, tendo em vista que no direito penal não se permite a analogia.

Wanderson Castilho, especialista em crimes eletrônicos, aponta que quem produz ou difunde dispositivo ou programa de computador, como vírus, também é enquadrado pela nova lei. Porém, a clonagem de redes, por exemplo, não está definida na norma.

Além disso, pode-se verificar tomando como exemplo o novo artigo 154-A do Código Penal – que prevê a invasão de dispositivo informático – a ausência de suporte técnico-jurídico dos legisladores na redação do texto legal. Por consequência, percebe-se que grande parcela daqueles que se enquadram no artigo mencionado deixa de ser punida, em face da má redação da legislação.

---

[16] OSORIO, Juan. L. Fuentes. **A influência da mídia na produção legislativa penal brasileira**. Disponível em: <http://www.ambito-juridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=8727&revista_caderno=3#_ftn15 >. Acesso em: 17.11.2016.

[17] TOMAZI, Sandra. **Uma lei, muitas dúvidas**. 2013. Disponível em: <http://www.gazetadopovo.com.br/vida-publica/justica-direito/uma-lei-muitas-duvidas-0amq7lj8b0skxnonfd5qh1glq>. Acesso em: 17.11.2016.

O advogado criminalista Dr. Ney de Moura Teles, em manifestação sobre a Lei dos Crimes Hediondos relata que:

> O legislador brasileiro, ao cumprir o mandamento constitucional, talvez pela pressa diante de fortes pressões – encontrava-se o Congresso Nacional sobre forte pressão da Mídia eletrônica, na ânsia de atender aos reclamos da camada mais rica da população, que assistia ao seqüestro para fins de extorsão, de alguns de seus mais importantes representantes, preferiu selecionar alguns tipos já definidos em lei vigente e rotulá-los como hediondos, em vez de apresentar uma noção explícita do que seria a hediondez que caracteriza tais crimes[18].

Não foi diferente o que aconteceu com a Lei nº 12.737/2012, quando na ânsia de atender ao clamor da camada mais favorecida da sociedade, o legislador, em tempo recorde, acrescentou apenas dois artigos tipificando o crime cibernético e modificou o texto legal de outros dois dispositivos já existentes no Código Penal. Sem estabelecer qual seria o procedimento para o os casos em que os delitos eletrônicos restassem configurados. Em vista disso, é evidente a falha da pessoa do legislador frente à criação da lei nº 12.737/2012.

Ademais, é de se verificar que o anonimato apresenta-se de forma ambivalente quando, por um lado, é vedado constitucionalmente, conforme disposto no artigo 5º, inciso IV da Carta Magna. E, por outro lado, é compreendido como um direito a ser defendido, garantindo a liberdade de expressão daqueles que não querem se expor, como, por exemplo, nos casos de “denúncia anônima”.

Diante desta garantia mitigada do anonimato no mundo virtual, vê-se que a Lei Carolina Dieckmann, embora específica, não é suficiente para capturar os sujeitos ativos do crime cibernético.

Não obstante o anonimato ser vedado constitucionalmente, no mundo virtual há certa garantia, tendo em vista a dificuldade de se descobrir o autor do delito. À vista disso, acredita-se que há influência direta na prática dos crimes cibernéticos. O que leva a inúmeras discussões em Comissões Parlamentares de Inquérito, objetivando encontrar mecanismos que impeçam a prática dos crimes virtuais, contudo, assegurando o anonimato à liberdade de expressão.

Assim, em maio do corrente ano, a Câmara dos Deputados, em Comissão Parlamentar de Inquérito dos Crimes Cibernéticos, prosseguiu com o

---

[18] TELES, Ney de Moura. **A influência da mídia na produção legislativa penal brasileira**. Disponível em: <http://www.ambito-juridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=8727&revista_caderno=3#_ftn46>. Acesso em: 17.11.2016.

relatório final no qual está contido o projeto de lei que permite aos juízes a determinação do bloqueio de sites e aplicativos voltados à prática de crimes.

A ampliação fornecida pelo projeto de lei é tamanha, que os juízes poderão determinar o bloqueio do acesso a sites e aplicativos abrigados fora do país ou que não possuam representação no Brasil e que sejam essencialmente dedicados à prática de crimes puníveis com pena mínima de dois anos de reclusão, excetuando-se os crimes contra a honra.

Contrário à proposta, o relator do Marco Civil na Câmara, Deputado Alessandro Molon (Rede-RJ), considera que bloquear sites e aplicativos não é uma medida eficaz para coibir a prática dos crimes eletrônicos, tendo em vista que os sites ilícitos mudam rapidamente de endereço.

Para Molon, é preciso identificar a autoria do delito, para poder restringir a liberdade do indivíduo, através de uma pena restritiva de direito. Pois, acredita que o bloqueio de um endereço não contém a execução de criminoso.

Resta claro, que, de um lado, estão entidades vinculadas à defesa dos direitos autorais e da propriedade intelectual. Que enxergam a proposta como uma maneira de coibir os crimes cibernéticos. Por outro lado, reúnem-se ativistas que incitam a censura à liberdade de expressão dos usuários. Mais uma vez, uma face do anonimato sendo esmagada pelo cometimento dos delitos virtuais.

Uma das sugestões do projeto de lei é a remoção de conteúdos idênticos que já tiveram sua retirada determinada pela Justiça, mas sem que haja necessidade de uma nova decisão judicial. O prazo fixado para que isso aconteça é de 48 (quarenta e oito) horas.

Atualmente, o Código Penal Brasileiro em seu artigo 154-A, considera crime invadir dispositivo informático, tão somente se os requisitos do artigo forem preenchidos. Quais sejam, o objetivo de obter, adulterar ou destruir o dado sem a autorização do proprietário do dispositivo. Com o projeto de lei, a possibilidade de punir o infrator pela invasão de dispositivo é ampliada, tendo em vista que será considerado crime a invasão com ou sem vantagem pessoal.

Frente à necessidade que o Direito e as autoridades policiais têm de tomar providências e medidas de urgência para que os criminosos possam se adequadamente punidos, desafio é combater a impunidade na rede se afetar os princípios básicos da liberdade e da privacidade.

A Câmara propõe, ainda, as possíveis sanções que o infrator deverá receber, caso não siga as regras delimitadas como, por exemplo, prestação de serviço comunitário ou pagamento de cesta básica. A depender do grau do delito cometido, poderá ser detido por até 04 (quatro) anos.

A Internet "necessita de uma cobertura legal. Ao não ter uma legislação eficaz, o crime se beneficia, e o Judiciário age na desproporcionalidade, como aconteceu nas vezes em que houve o bloqueio do Whatsapp" [19].

O Diretor executivo do Instituto de Tecnologia e Sociedade do Rio de Janeiro, Fabro Steibel, faz crítica às propostas feitas pela CPI sobre os crimes de informática, haja vista violarem o princípio da liberdade. Princípio que, para ele, comanda a Internet e uma vez violado, censura a liberdade de expressão do usuário.

Destarte, Fabro defende que:

> A internet tem de ser aberta. Você pode criminalizar práticas, conteúdos e autores, mas não a internet. Não há sentido, em uma metáfora, bloquear todos os caminhões dos Correios porque ali no meio há uma carta que tem um crime. A internet é apenas um meio. É desproporcional, do ponto de vista do Marco Civil, comprometer o conjunto de pessoas que fazem o uso de um aplicativo de maneira legal só porque alguns não fazem. [20]

Demi Getschko, Membro do Comitê Gestor da Internet no Brasil, partilha do mesmo entendimento supramencionado. Ao contrário do objetivo final que o projeto de lei tem, qual seja retirar o site do ar por consequência de um delito eletrônico – poderá prejudicar a investigação da autoria do crime quando se exclui o meio através do qual é possível identificar o infrator.

Assim expõe seu entendimento:

> Crimes são crimes, não importa onde ocorram. Meu medo em relação a essa discussão é de que ela seja pretexto para garantir caminhos curtos para se tirar do ar tudo aquilo o que se considerar violação de propriedade intelectual, o que pode dar margem para muitas interpretações. Não está

---

[19] SANDRO, Alex. **Como os projetos e propostas da CPI dos Crimes Cibernéticos podem mudar o uso da internet**. 2016. Disponível em: <http://zh.clicrbs.com.br/rs/vida-e-estilo/noticia/2016/05/como-os-projetos-e-propostas-da-cpi-dos-crimes-ciberneticos-podem-mudar-o-uso-da-internet-5807438.html>. Acesso em: 29.09.2016

[20] STEIBEL, Fabro. Ibid.

> claramente dito, mas é uma hipótese sobre o que está por trás de todo este processo.[21]

São 06 (seis) as propostas de lei pelos Deputados. Faz-se necessário o destaque de mais duas: a primeira inclui a definição da competência para investigar suspeita de crimes eletrônicos praticados sobre a esfera de atuação da Polícia Federal.

A segunda proposta alude que os indivíduos que forem condenados pela prática do crime cibernético, deverão ser punidos com penas restritivas de direito, de igual modo, com o confisco de bens e valores.

[21] GETSCHKO, Demi. Ibid.

4. APLICAÇÃO JURISPRUDENCIAL E A POSSIBILIDADE DE RELATIVIZAÇÃO DO ANONIMATO

A partir do artigo 5º, inciso IV da Constituição Federal, é possível identificar certa relativização do anonimato, quando limita a manifestação do pensamento e no mesmo dispositivo, exige um dever: “é vedado o anonimato”. Ou, ainda, quando este anonimato é garantido pelo mundo virtual, para o alastramento dos crimes cibernéticos.

Por conseguinte, os delitos de informática, deparam-se, ainda, com grandes dificuldades de configurar a justa causa, por seus elementos principais, quais sejam autoria e prova da materialidade do crime. Sendo o endereço IP, elemento fundamental para o auxílio da busca pelos infratores dos referidos crimes.

No presente capítulo, será apresentada a aplicação jurisprudencial para demonstrar a configuração das dificuldades mencionadas acima.

4.1. Casos Práticos e a Dificuldade de Localizar a Autoria do Delito Cibernético

É de se verificar que um dos principais desafios dos crimes cibernéticos é identificar a prova da sua autoria. Especialistas na área explicam que a maior objeção é a ausência de obrigação dos servidores de gravar os dados de seus usuários.

Posta assim a questão, o entendimento do Tribunal Regional Federal da 5ª Região em sede de julgamento de Habeas Corpus impetrado, demonstra a total complexidade das investigações para que se chegue a razoável indício de autoria do crime eletrônico.

> Ementa: PENAL. PROCESSUAL PENAL. ORGANIZAÇÃO CRIMINOSA. CRIMES CIBERNÉTICOS. COMPLEXIDADE DAS INVESTIGAÇÕES. INDÍCIOS DE MATERIALIDADE E AUTORIA. PERICULOSIDADE DOS AGENTES E GRAU INTENSO DE CULPABILIDADE DAS CONDUTAS. NECESSIDADE DE GARANTIA DA ORDEM PÚBLICA, CONVENIÊNCIA DA INSTRUÇÃO PROBATÓRIA E DA GARANTIA DA APLICAÇÃO DA LEI PENAL QUE AUTORIZAM A MANTENÇA DAS PRISÕES CAUTELARES. DENEGAÇÃO DA ORDEM. - Trata-se de investigação complexa sobre organização criminosa voltada à prática de crimes cibernéticos, tendo por vítimas instituições financeiras de renome, além dos particulares correntistas, formada por vários componentes, cuja atuação fez-se em vários estados da federação. - Após a realização de escutas telefônicas,

> quebras de sigilo bancário e fiscal, apreensão de diversos bens e prisão de vários investigados, dentre estes os pacientes, chegou-se a indícios razoáveis de materialidade e autoria delitiva, aptos a fundamentarem as prisões cautelares, diante da necessidade de garantia da ordem pública, da aplicação da lei penal e por conveniência da instrução probatória. - Ademais, não se verifica no caso em tela excesso de prazo, tampouco ausência de fundamentação da decisão que cuidou de decretar as prisões preventivas, mas, ao contrário, acumulam-se nos autos os requisitos para suas manutenções. - Denegação da ordem liberatória.
> (TRF-5 – Primeira Turma - Habeas Corpus HC 2376 PB 0008133-45.2006.4.05.0000)

A partir deste julgado, resta clara a dificuldade de se chegar a indícios razoáveis da prova da autoria, isto é, identificar o autor do delito cibernético, cujo elemento é determinante para a configuração da justa causa. Foi precisa a realização de escutas telefônicas, quebras de sigilo bancário e fiscal, apreensão de diversos bens e prisão de vários investigados.

Apesar da vedação expressa do anonimato pela Constituição da República Federativa do Brasil, inexiste lei que determine alguma identidade digital obrigatória.

Sabe-se, porém, que o acesso à Internet é feito através de um número de protocolo IP único. No entanto, não é incomum, não conseguir identificar o usuário que estava na máquina naquele momento, pelo fato de ser o IP um acesso/número e não uma pessoa. Situações dessa espécie acontecem em grande escala nos crimes cometidos por meio de computadores públicos, *lan houses* e *cybercafés*.

O Governador do Estado de São Paulo, Geraldo Alckmin, instituiu no ano de 2006 a Lei nº 12.228, que disciplina a obrigatoriedade dos estabelecimentos comerciais da região – que ofertam a locação de computadores e máquinas para acesso à Internet, utilização de programas e jogos eletrônicos, designados como *lan houses*, *cybercafés* ou *cyber offices* – a criar e manter cadastro atualizado de seus usuários, contendo nome e endereço completos; data de nascimento; telefone e número de documento de identidade, conforme dispõem os artigos 1º e 2º da referida Lei[22].

---

[22] **Art. 1º da Lei 12.228/06:** - São regidos por esta lei os estabelecimentos comerciais instalados no Estado de São Paulo que ofertam a locação de computadores e máquinas para acesso à internet, utilização de programas e de jogos eletrônicos, abrangendo os designados como “lan houses”, cibercafés e “cyber offices”, entre outros.
Art. 2º - Os estabelecimentos de que trata esta lei ficam obrigados a criar e manter cadastro atualizado de seus usuários, contendo:
I - nome completo;
II - data de nascimento;
III - endereço completo;

O parágrafo 4º[23] do artigo 2º da Lei nº 12.228/06 apresenta um limite temporal mínimo de 60 (sessenta) meses para que as informações e os registros previstos no dispositivo mencionado sejam mantidos.

Nota-se de proêmio, que a lei em voga é direcionada aos proprietários de estabelecimentos comerciais que oferecem locação de computadores com acesso à Internet. Assim, a inobservância do disposto em lei, sujeitará o infrator às penalidades de multas e, em caso de reincidência, cumulativamente com a multa, suspensão das atividades ou fechamento definitivo do estabelecimento[24].

Embora a lei, de natureza administrativa, tenha sido instituída para os proprietários de *cybercafés*, *offices* e outros, por óbvio, o cadastramento obrigatório dos usuários também é medida essencial para restringir o alastramento dos crimes cibernéticos.

Neste viés, no que tange aos desafios do cibercrime, para fins de punição do infrator, além da identificação da autoria, outra dificuldade encontrada pelos profissionais da área é o conflito de competência: territorial e jurisdicional. Tendo em vista o caráter universal do crime, poderá ser praticado em um lugar e consumado em outro. Dificultando assim, o trabalho do julgador.

4.1.1. Conflito de Competência

O crime executado através da Internet é considerado interfronteiro, isto é, sem fronteiras, tendo em vista a possibilidade de acontecer em toda rede e em qualquer parte do mundo. É possível a proibição de crimes já tipificados no Código Penal Brasileiro como, por exemplo, pornografia infantil na Internet, todavia, a referida proibição só poderá ser desempenhada no território brasileiro.

Para Marco Antônio de Barros:

> Se um crime contra a honra de uma pessoa foi perpetrado em um estado da federação ou em outro país, sua transmissão virtual propagará efeitos para

---

IV - telefone;
V - número de documento de identidade.

[23] **§ 4º -** As informações e o registro previstos neste artigo deverão ser mantidos por, no mínimo, 60 (sessenta) meses.

[24] **Art. 6º -** A inobservância do disposto nesta lei sujeitará o infrator às seguintes penalidades:
I - multa, no valor de R$ 3.000,00 (três mil reais) a R$ 10.000,00 (dez mil reais), de acordo com a gravidade da infração, conforme critérios a serem definidos em regulamento;
II - em caso de reincidência, cumulativamente com a multa, suspensão das atividades ou fechamento definitivo do estabelecimento, conforme a gravidade da infração.

> todo o mundo. Pode ser que a vítima se encontre em outra unidade da federação ou país, e ali venha a tomar conhecimento do crime [25].

Fixar a competência territorial do crime eletrônico pode ser um dos maiores problemas em seu procedimento, tendo em vista que a execução do delito pode ocorrer em lugares distintos.

De início, faz-se necessária a distinção dos conceitos de crimes à distância e crimes plurilocais. Aqueles ocorrem quando a execução e o resultado se desvinculam por meio do espaço nacional e estrangeiro. Ou seja, a conduta e o resultado da ação consumam-se em países distintos. Fala-se em crimes plurilocais quando, dentro de um mesmo país a conduta é praticada em um local e o resultado se produz em outro.

É pacífico o entendimento de que no caso dos crimes à distância – isto é, quando a conduta ou o resultado do delito ocorre em país estrangeiro – aplica-se a teoria da ubiquidade ou também chamada teoria mista, concretizada no artigo 6º do Código Penal Brasileiro[26].

É o que explica Dr. Eudes Quintino de Oliveira Júnior, promotor de justiça aposentado do Estado de São Paulo:

> (...) essa teoria, trazida pelo Código Penal, somente se aplica aos chamados crimes à distância, isto é, aqueles em que a conduta criminosa é praticada em um país, e o resultado vêm a ser produzido em outro. Crimes à distancia não são os delitos que ocorrem em diversas comarcas. Exige-se, necessariamente, pluralidade de países.[27]

Solução outra, encontra-se no artigo 7º da mesma legislação, para os crimes plurilocais, cuja ação se inicia em país estrangeiro, mas o dano do crime ocorre no território nacional.

Ademais, ainda sobre os crimes plurilocais, por força do artigo 70 do Código de Processo Penal, a regra é de que a competência será determinada pelo lugar em que a infração se consumar ou, no caso de tentativa, pelo lugar em que for praticado o último ato de execução.

---

[25] PAESANI, Liliana Minardi, coordenadora. **O Direito na Sociedade da Informação**. 2006

[26] **Art. 6º do Código Penal Brasileiro** - Considera-se praticado o crime no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado.

[27] JUNIOR, Eudes Quintino de Oliveira. **Lugar do crime: teoria da ubiquidade (cp) ou do resultado (cpp)?**. 2011. Disponível em: < https://eudesquintino.jusbrasil.com.br/artigos/121823112/lugar-do-crime-teoria-da-ubiquidade-cp-ou-do-resultado-cpp>. Acesso em: 24.11.2016.

Via de regra, os cibercrimes serão julgados pela Justiça Comum do Estado. Por outro lado, serão de competência da Justiça Federal, quando, nos termos do artigo 109, inciso IV da Carta Magna, os crimes eletrônicos violarem bens, serviços ou interesses da União, suas entidades autárquicas ou empresas públicas.

Ademais, conforme prevê o Manual Prático de Investigação do Ministério Público Federal de São Paulo:

> É competência da Justiça Federal julgar os crimes eletrônicos praticados contra os entes da Administração Federal indicados nesse inciso. Podemos citar, a título exemplificativo, o estelionato eletrônico, o dano ou a falsificação de dados constantes em sistemas informatizados mantidos por órgão ou entes da administração pública federal[28].

O Superior Tribunal de Justiça consolidou entendimento no mesmo sentido, como se pode demonstrar no julgado abaixo:

> CONFLITO NEGATIVO DE COMPETÊNCIA. CRIME DE INJÚRIA PRATICADO POR MEIO DA INTERNET, NAS REDES SOCIAIS DENOMINADAS ORKUT E TWITTER. AUSÊNCIA DAS HIPÓTESES DO ART. 109, INCISOS IV E V, DA CF. OFENSAS DE CARÁTER EXCLUSIVAMENTE PESSOAL. COMPETÊNCIA DA JUSTIÇA ESTADUAL.
> 1 - O simples fato de o suposto delito ter sido cometido por meio da rede mundial de computadores, ainda que em páginas eletrônicas internacionais, tais como as redes sociais"Orkut"e"Twitter", não atrai, por si só, a competência da Justiça Federal.
> 2 - É preciso que o crime ofenda a bens, serviços ou interesses da União ou esteja previsto em tratado ou convenção internacional em que o Brasil se comprometeu a combater, como por exemplo, mensagens que veiculassem pornografia infantil, racismo, xenofobia, dentre outros, conforme preceitua o art. 109 , incisos IV e V , da Constituição Federal .
> 3 - Verificando-se que as ofensas possuem caráter exclusivamente pessoal, as quais foram praticadas pela ex-namorada da vítima, não se subsumindo, portanto, a ação delituosa a nenhuma das hipóteses do dispositivo constitucional, a competência para processar e julgar o feito será da Justiça Estadual"(CC 121/431/SE Rel. Min. MARCO AURÉLIO BELLIZZE, Terceira Seção, DJe 07/05/2012). (STJ – Terceira Seção – AGRAVO REGIMENTAL NOS EMBARGOS DE DECLARAÇÃO NO CONFLITO DE COMPETÊNCIA AgRg nos EDcl no CC 120559 DF 2011/0310940-9).

À Justiça Federal também compete julgar e processar as hipóteses previstas no inciso V do artigo 109 do mesmo dispositivo de lei[29], o delito tipificado

---

[28] FEDERAL, Ministério Público. **Crimes Cibernéticos. Manual Prático de Investigação**. São Paulo: 2006.

[29] **Art. 109 da Constituição Federal**. Aos juízes federais compete processar e julgar:

no dispositivo 241 do ECA (Estatuto da Criança e do Adolescente) e o crime do racismo – disposto na Lei nº 7.716/89. Tendo em vista o caráter intefronteiro da consumação dos crimes executados por meio da rede mundial de computadores.

Conforme demonstrado, é nítida a dificuldade da identificação na autoria dos cibercrimes. Tão difícil quanto, é provar a materialidade do crime para que seja possível – juntamente à identificação do autor do crime – a soma dos elementos da justa causa.

É indispensável a autorização judicial para a identificação do IP de onde pode ter partido a ação delituosa e, quando identificado, necessária comprovação de quem, efetivamente, utilizou aquele PC para a prática do crime. Este ponto, numa análise mediatista, pode parecer mero detalhe, mas, em sede de Direito e Processual Penal, a determinação da prova da materialidade e autoria do crime para formação da justa causa, são fatores indispensáveis.

4.1.2. Dificuldade de Provar Configuração dos Elementos da Justa Causa

Toda e qualquer infração penal, para produzir efeitos processuais penais, deve ter a sua existência demonstrada. A materialidade do crime – um dos elementos necessários para configurar a justa causa – trata da prova de existência do crime.

O indivíduo que pretende cometer algum dos delitos tipificados na Lei nº 12.737/12, dificilmente, utilizará sua identificação pessoal real, mas sim através da garantia relativizada do anonimato frente aos cibercrimes, passará por outra pessoa.

Nas redes de computadores mundiais, existe uma razoável possibilidade de encontrar o indivíduo que comete delitos de informática, qual seja através do IP da máquina utilizada pelo usuário.

Internet Protocol, significado da sigla IP em inglês é uma sequência de números capaz de identificar um dispositivo de rede. Assemelha-se ao número de Telefone de um indivíduo, cujo número identifica a pessoa e permite que haja

---

V - os crimes previstos em tratado ou convenção internacional, quando, iniciada a execução no País, o resultado tenha ou devesse ter ocorrido no estrangeiro, ou reciprocamente;
V- A as causas relativas a direitos humanos a que se refere o § 5º deste artigo; (Incluído pela Emenda Constitucional nº 45, de 2004).

comunicação. De igual modo, o nº do CPF, código capaz de identificar a pessoa física.

O endereço IP, é composto por um código sequencial de até 04 números, com no máximo 03 dígitos cada e separados por um ponto. Os números variam de 0 a 255, por exemplo, endereço de IP 193.172.55.254.

Ocorre que, os serviços que fornecem conexão à rede, em sua maioria, adotam o sistema de IP dinâmico e não estático. Ou seja, a cada conexão o provedor recebe um IP diferente. Em vista desse sistema, faz-se necessária a obtenção de outros dados como data, hora exata da conexão ou comunicação e o fuso horário do sistema, para que exista a possibilidade de configurar a materialidade do crime, através da qual será encontrado o autor do delito e, por conseguinte, restar configurado os elementos da justa causa.

Existem endereços eletrônicos com o fim de identificar qual o fornecedor de acesso à conexão responsável por cada *Internet Protocol*. Tendo em vista a necessidade de comprovar a materialidade do crime e localizar sua autoria, quando se identifica o provedor, faz-se necessário solicitar os dados de conexão do usuário que utilizou aquele endereço de IP durante o período específico. É o que diz o Ministério Público em seu Manual de Investigação:

> Nos pedidos feitos aos provedores de acesso e às companhias telefônicas, é imprescindível que haja, no mínimo, a menção a esses três indicadores: a) o número IP; b) a data da comunicação; e c) o horário indicando o fuso horário utilizado – GMT ou UTC. Sem eles, não será possível fazer a quebra do sigilo de dados telemáticos[30].

A partir da citação feita pelo Ministério Público Federal, faz-se necessário explanar os conceitos de interceptação de dados telemáticos e o que seria a quebra de sigilo dos dados de conexão e de usuário.

A autora Carla Rodrigues explica que interceptar os dados telemáticos é:

> Interromper o curso originário, impedir a passagem, sendo que na lei tem o sentido de captar a comunicação, conhecer seu conteúdo. Interceptar é ter contato com teor da comunicação, não impedindo que ela chegue ao seu destinatário. A telemática é uma ciência que trata da manipulação de dados

[30] FEDERAL, Ministério Público. **Crimes Cibernéticos. Manual Prático de Investigação.** São Paulo: 2006.

> e informações, conjugando o computador, sistemas de informática, com os meios de comunicação, telefônicas ou não. Assim, qualquer comunicação feita através de sistema de informática é protegida pela lei; a título de exemplo, citamos as comunicações feitas na Internet[31].

Através da interceptação de dados telemáticos, portanto, é possível as autoridades acessarem informações a respeito de todas as conexões executadas pelo infrator no ambiente virtual. Como a interceptação não impede que os dados cheguem ao seu destinatário, ocorrerá tão somente a coleta das informações ou a observação por terceiro.

O procedimento a ser seguido na interceptação dos dados é aquele previsto na Lei nº 9.296/96, qual seja a Lei de Interceptações Telefônicas. Tendo em vista equipararem-se, em todas as questões legais.

A quebra do sigilo dos dados de conexão do usuário, por sua vez, ocorre quando é necessária a disponibilização dos dados da conexão do usuário, ou seja, quando as informações de data, hora exata da conexão ou da execução do crime deverão ser fornecidas. De igual modo, quando os dados do usuário também são apresentados como, por exemplo, o endereço físico em que o computador estava instalado quando ocorreu o delito.

A identificação da autoria e consequente responsabilização dos infratores de delitos eletrônicos no mundo virtual são possíveis através da análise de *logs*. Entende-se por *log*, o registro de todo o histórico dos usuários pelo sistema informático. No entanto, é imperioso destacar que não se sabe por quanto tempo os sistemas devem armazenar tais registros. Obstruindo, mais uma vez, o trabalho da perícia quanto à identificação da autoria do crime.

Em face da ausência de uma legislação que prevê por quanto tempo os *logs* devem permanecer armazenados, em Julho de 2008, a Google – empresa multinacional de serviços online e software dos Estados Unidos – assinou Termo de Ajustamento de Conduta com o MPF (Ministério Público Federal).

O Termo em questão visa estabelecer período mínimo de arquivo dos *logs* para auxiliar a investigação dos crimes. Desse modo, o período fixado foi de, no mínimo, 06 (seis) meses. Ocorre que, embora seja um prazo mínimo, vai de

---

[31] CASTRO. Carla Rodrigues Araújo de. **Crimes de Informática e seus aspectos processuais**. Rio de Janeiro: 2001.

encontro com o andamento das perícias e dos inquéritos policiais, sendo a investigação bloqueada com a perda das informações.

Não obstante o Termo assinado pela Google, Marco Aurelio Greco questiona como é possível identificar o agente frente aos serviços complexos existentes na Internet que dificultam o trabalho do perito. É o chamado 'serviço de máscara'[32]

Os chamados 'serviços de máscara' citados por Marco Aurélio seriam os denominados *proxys* – em português, procurador. *Proxys* nada mais é que um servidor intermediário que atende a requisições repassando os dados do cliente para outro servidor, oferecendo, por sua vez, o serviço de anonimato.

Recebe o nome de 'serviço de máscara' pela característica de promoção do anonimato aos seus clientes. Tornando, por sua vez, a identificação da máquina de origem das ações virtualmente impossível de rastrear.

Resta prejudicada a comprovação da materialidade do delito, tendo em vista o caráter volátil dos crimes cibernéticos. Uma vez que as provas podem ser deletadas logo após a execução do crime, ou facilmente perdidas. Ainda, as provas de um delito informático caracterizam-se pela sua complexidade, considerando que podem estar embaralhadas no meio de dados legítimos e lícitos. Exigindo, assim, análise apurada dos técnicos.

Como se percebe, para a materialidade do delito eletrônico configurar-se, é necessária a prova pericial. De igual modo, é indispensável a interceptação do fluxo de comunicações desempenhadas através do computador. No entanto, conforme demonstrado acima, a interceptação em questão, somente poderá ser feita através de autorização judicial.

Destarte, em face de tantas problemáticas para a identificação da prova da materialidade e da autoria dos delitos informáticos, torna-se evidente que a forma como o anonimato é garantido no mundo virtual em nada colabora para convergir com a localização da autoria e a prova de existência do crime.

---

[32] GRECO, Marco Aurelio apud INELAS, Gabriel Cesar Zaccarias de. **Crimes na Internet**. 2009.

4.2. A Relativização do Anonimato

O ambiente virtual em que a Internet se encontra, significa que as ações praticadas por meio dela irão representar as ações que os indivíduos poderiam realizar no mundo real. Por exemplo, a expressão do pensamento irá se materializar através de textos, imagens divulgados e transmitidos pela Internet, os quais são dados suscetíveis de serem processados apenas por computadores, mas é, paralelamente, dirigido às relações sociais.

A vedação constitucional disposta no artigo 5º, IV, destaca-se quando é aplicado aos meios de comunicação, tendo em vista que tais meios envolvem a liberdade de expressão e a garantia da privacidade, do sigilo, os quais também são direitos previstos pela Constituição.

À análise do tema, o Min. Celso de Mello da Suprema Corte Constitucional fez apreciação cristalina, observando que esse veto tem objetivo de acautelar as consequências do exercício do direito de livre expressão, nos seguintes termos:

> 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[33].

Convém delimitar, portanto, o âmbito de incidência da referida proibição. Somente quando ocorrer a livre manifestação do pensamento é que estará vedado o anonimato, pois, é a partir do momento em que tal expressão humana ingressa no mundo social, quando fica conhecida por pelo menos outra pessoa através de processo comunicativo, que poderá influir na esfera jurídica alheia ou chegar a violá-la – ensejando a busca pela reparação.

---

[33] 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**. Disponível em <http://www.ambitojuridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=9964>. Acesso em: 13.11.2016.

O âmbito sobre onde vai recair a vedação constitucional será assim delimitado, em face das outras garantias constitucionais que asseguram a inviolabilidade do sigilo da comunicação de dados, da intimidade, da vida privada da honra e da imagem das pessoas (mesmo sendo estas violadoras da lei). Ou seja, asseguram os direitos da personalidade do indivíduo.

Frise-se, contudo, que a vedação do anonimato em si, não é vista com maus olhos pela Constituição Federal. Em diversas situações, ele é fundamental para a preservação da ordem democrática, como no caso de sigilo da fonte jornalística ou mesmo em mecanismos de denúncias anônimas com o objetivo de combate ao crime e garantia de direitos.

Em geral, a violação aos direitos da personalidade é efetuada através da atividade jornalística. Solução para o problema, então, é a ponderação de direitos, uma vez que a liberdade à informação também é um direito constitucionalmente tutelado, englobando liberdade de expressão e liberdade de imprensa.

Na necessária ponderação de princípios, a dignidade da pessoa humana, enquanto fundamento da República, assume papel relevante. Além disso, há de prevalecer o interesse coletivo sobre o particular.

No Brasil, o anonimato é tratado como mecanismo auxiliar às condutas criminosas. Assim, a pretexto de proteger ameaças de ofensa aos direitos de personalidade e assegurar que o ofensor possa ser responsabilizado, a Constituição Federal proíbe o anonimato, desconsiderando-o como meio necessário e garantidor da plena liberdade de expressão.

Ao passo em que defende a plenitude do pensamento e suas múltiplas formas de expressão, a Constituição Federal também proíbe o direito ao anonimato alegando que todo o individuo deve ser responsabilizado pelas suas opiniões e publicações.

Nesse contexto, a vedação ao anonimato consignada na Constituição Federal se apresenta como uma limitação à plena manifestação de pensamento, impedindo que o anonimato seja enxergado em seu outro sentido, isto é, como pressuposto lógico da liberdade de expressão. Por outro lado, e este, de forma a relativizar a figura do anonimato, ele é visto como incentivo à clandestinidade, o que, em meios eletrônicos, contribui para prática de ofensas aos direitos da personalidade.

CONSIDERAÇÕES FINAIS

Através do presente estudo, foi visto que por volta de 1760 o mundo experimentou a mudança de paradigma do avanço da tecnologia, a partir do momento em que as máquinas industriais substituíram o lugar do trabalhador operário. Dando espaço para, na década de 60, surgir a Internet.

Pouco tempo depois, surgem os primeiros delitos cometidos na rede mundial de computadores. Fazendo com que os estudiosos da área procurassem definir o conceito do que seria um cibercrime. Ocorre que, conforme demonstrado no trabalho em questão, ainda não se chegou a um consenso a respeito da definição do crime cibernético.

Restou demonstrada, que com o surgimento de tais crimes, se fez necessária a criação de um tratado internacional – o qual não foi ratificado pelo Brasil. Porém, este editou a Lei nº 12.737, popularmente conhecida como Carolina Dieckmann, através da qual é possível avaliar até onde o anonimato pode alcançar, tendo em vista seu caráter ambíguo e sua vedação constitucional.

Feitas essas considerações, ressalte-se que o problema traz em seu bojo um conflito entre a garantia constitucional e civil da privacidade e a tutela do bem jurídico penal. A partir disso, buscou-se, então, investigar a possibilidade de criar mecanismos para coibir a propagação dos crimes cibernéticos.

Ocorre que, quando a garantia mitigada do anonimato frente aos crimes eletrônicos une-se à carência de suporte técnico jurídico do Poder Legislativo na redação dos dispositivos que deram origem à Lei nº 12.737/2012, o trabalho compreendido pelo Poder Judiciário é quase que impossível. Por consequência, grande parcela dos que invadem dispositivo de informática, enquadrando-se no artigo 154-A do Código Penal, deixará de ser punida.

Pela primeira vez no Brasil, uma legislação tipifica como crime a invasão de dispositivos informáticos, incluindo também o delito a interrupção de serviços informáticos de utilidade pública. É de salientar, no entanto, que a norma penal criada para tratar dos crimes cibernéticos é falha, conforme demonstrado no presente estudo. Embora a sua origem tenha sido um grande avanço no combate ao cibercrime.

Embora a Câmara dos Deputados esteja investigando, em incansáveis Comissões Parlamentares de Inquérito, a melhor forma de restringir o alastramento dos cibercrimes, a criação de mais uma norma penal no ordenamento jurídico brasileiro, certamente, não é a melhor medida, tampouco medida eficaz para ir de encontro aos delitos em voga.

Tal posicionamento é defendido, tendo em vista o ordenamento jurídico inflado e ineficaz que temos. Visto que, para todo problema surgido, o ser humano quer solucionar com a criação de uma norma. Ademais, já existe lei que tipifica o crime como sendo de informática, qual seja, Lei nº 12.737/12, penalizando o infrator na medida da sua proporção.

Conforme apresentado ao longo do estudo, o Governador de São Paulo, Geraldo Alckmin, instituiu a Lei nº 12.228/2006 que disciplina a obrigatoriedade dos estabelecimentos comerciais da região que oferecem acesso à Internet, a criar e manter cadastro atualizado de seus usuários.

Verifica-se, portanto, que a Lei Estadual tem caráter administrativo, ou seja, a sanção contida na norma é de natureza administrativa e não punitiva, como na norma penal. Cujo instrumento é a *ultima ratio*, o último recurso, recorrendo em situações de punição por condutas intoleráveis.

Paralela a esta lei, incide a norma penal pura. A ex Presidente Dilma Rousseff, sancionou em 2012 a Lei nº 12.737, popularmente conhecida como Carolina Dieckmann. O legislador brasileiro deu origem à norma de natureza penal, com sanções punitivas, restritivas de direito, punindo o sujeito ativo daquele que invade dispositivo informático, enquadrando-se no tipo penal do crime cibernético.

É de se verificar, portanto, que o problema não está na norma, até porque ela foi criada, mas sim na complexidade do crime e na velocidade com que ele se perpetua. Velocidade esta, que o direito, definitivamente, não acompanha. Desconfigurando, assim, a criação de uma possível legislação específica – ou norma penal.

À vista disso, entende-se que o caso excepcional de legislar administrativamente para auxiliar a aplicação da lei penal, é uma possibilidade crível e concreta de restringir os cibercrimes.

Ou seja, quando uma lei de âmbito estadual – direcionada aos

proprietários de estabelecimento comercial que disponibilizam o acesso à Internet – e outra de âmbito nacional – dirigida aos infratores do cibercrime – se juntam, podem com maior eficácia coibir os delitos de informática, quando obrigam o cadastramento dos seus usuários, identificando-os. Limitando, por sua vez, o cometimento das infrações em ambientes públicos.

Ocorre que, uma destas leis envolve tão somente o Estado onde foi criada. Ademais, é notório que a norma de âmbito nacional não é suficiente para auxiliar na identificação dos autores do delito em questão, tampouco para restringi-lo. Com o quadro em cena, inicialmente, deve-se fazer uma pesquisa para saber em quais Estados do Brasil os crimes cibernéticos têm maior incidência. Por conseguinte, a lei estadual deverá ser criada.

Mas não uma norma de natureza penal, de âmbito nacional. Tendo em vista que a soma das normas administrativa e penal, conforme demonstrado acima é suficiente para se chegar ao infrator.

Isto posto, a prova da materialidade do crime e da autoria torna-se mais fácil de serem localizados. De igual modo, o anonimato, com toda sua característica relativizada, também reduz, restringindo cada vez mais o ambiente dos criminosos virtuais.

REFERÊNCIAS

CANABARRO, Diego R. **Uma breve análise do Primeiro Relatório do Professor David Kaye ao Conselho de Direitos Humanos da ONU**. 2015. Disponível em: <http://observatoriodainternet.br/post/uma-breve-analise-do-primeiro-relatorio-do-professor-david-kaye-ao-conselho-de-direitos-humanos-da-onu>. Acesso em: 25.09.2016.

CASTRO, Carla Rodrigues Araújo de. **Crimes de informática e seus aspectos processuais**. Rio de Janeiro: 2003. Ed. Lúmen Juris. Ed 2ª. p. 9.

CASTRO, Carla Rodrigues Araújo de. **Crimes de Informática e seus aspectos processuais**. Rio de Janeiro, 2001. Ed. Lúmen Juris. pp.111-112

CPI - CRIMES CIBERNÉTICOS - Reunião Audiência Pública Ordinária (Parte 1 de 2). 2015. Disponível em: <https://www.youtube.com/watch?v=quFi6vCfvRE> Acesso em: 29 out. 2015.

CPI - CRIMES CIBERNÉTICOS - Reunião Audiência Pública Ordinária (Parte 2 de 2). 2015. Disponível em: <https://www.youtube.com/watch?v=w0swUAjYjgU> Acesso em 30 out. 2015.

DAOUN, Alexandre Jean. **Os novos crimes de informática**. 2016. Disponível em: <http://www.egov.ufsc.br/portal/conteudo/os-novos-crimes-de-inform%C3%A1tica>. Acesso em 27.09.2016.

DELLEY, Jean-Daniel. **Pensar as leis. Introdução a um procedimento metódico. Cadernos da Escola do Legislativo**. Belo Horizonte, 2004. p. 103.

Ministério Público Federal. **Crimes Cibernéticos. Manual Prático de Investigação**. 2006. pp. 15, 41.

GETSCHKO, Demi. **Como os projetos e propostas da CPI dos Crimes Cibernéticos podem mudar o uso da internet**. 2016. Disponível em <http://zh.clicrbs.com.br/rs/vida-e-estilo/noticia/2016/05/como-os-projetos-e-propostas-da-cpi-dos-crimes-ciberneticos-podem-mudar-o-uso-da-internet-5807438.html> Acesso em: 29 set. 2016.

GRECO, Marco Aurelio apud INELAS, Gabriel Cesar Zaccarias de. **Crimes na Internet**. 2009. Ed: 2ª. p. 117.

JUNIOR, Eudes Quintino de Oliveira. **Lugar do crime: teoria da ubiquidade (cp) ou do resultado (cpp)?**. 2011. Disponível em: <https://eudesquintino.jusbrasil.com.br/artigos/121823112/lugar-do-crime-teoria-da-ubiquidade-cp-ou-do-resultado-cpp>. Acesso em: 24.11.2016.

Lei Carolina Dieckmann. 2016. Disponível em: <https://pt.wikipedia.org/wiki/Lei_Carolina_Dieckmann> Acesso em: 29.09.2016.

LEMOS, André. LÉVY, Pierre. **O futuro da Internet: em direção a uma**

ciberdemocracia. São Paulo: 2010, Ed. Paulus. p.10.

LIMA, Paulo Marco Ferreira. **Crimes de computador e segurança computacional**. Ed: Atlas. Ed 2º, p. 31.

MANZUR, Claudio Líbano. **Los delitos de hacking en sus diversas manifestaciones**. 2016. Disponível em: <https://pt.scribd.com/doc/308707918/Los-Delitos-de-Hacking-en-Sus-Diversas-Manifestaciones>. Acesso em: 27.09.2016.

MORAES, Geórgia. **Peritos pedem colaboração de provedores para combater crimes cibernéticos**. 2015. Disponível em <http://www2.camara.leg.br/camaranoticias/noticias/SEGURANCA/496136-PERITOS-PEDEM-COLABORACAO-DE-PROVEDORES-PARA-COMBATER-CRIMES-CIBERNETICOS.html>. Acesso em: 08.11.2015.

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**. Disponível em <http://www.ambitojuridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=9964>. Acesso em: 13.11.2016.

MÜLLER, Carlo Frederico. **Texto ruim inviabiliza Lei Carolina Dieckmann, afirmam advogados**. 2013. Disponível em <http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&infoid=33404>. Acesso em: 17.11.2016.

OSORIO, Juan. L. Fuentes. **A influência da mídia na produção legislativa penal brasileira**. Disponível em <http://www.ambito-juridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=8727&revista_caderno=3#_ftn15 >. Acesso em: 17.11.2016.

PAESANI, Liliana Minardi (coord.). **O Direito na Sociedade da Informação**, p. 292.

Projeto de Lei do Senado nº 76, de 2000. 2016. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/43555> Acesso em: 29.09.2016.

SANDRO, Alex. **Como os projetos e propostas da CPI dos Crimes Cibernéticos podem mudar o uso da internet**. 2016. Disponível em: <http://zh.clicrbs.com.br/rs/vida-e-estilo/noticia/2016/05/como-os-projetos-e-propostas-da-cpi-dos-crimes-ciberneticos-podem-mudar-o-uso-da-internet-5807438.html>. Acesso em: 29.09.2016.

SCHMIDT, Guilherme. **CRIMES CIBERNÉTICOS Non scholae, sed vitae discimus**. Disponível em: <http://schmidtadvogados.com/v/artigo5>. Acesso em: 09.11.2016.

SCIREA, Bruna, JUSTINO, Guilherme. **Como os projetos e propostas da CPI dos Crimes Cibernéticos podem mudar o uso da internet**. 2016. Disponível em <http://zh.clicrbs.com.br/rs/vida-e-estilo/noticia/2016/05/como-os-projetos-e-

propostas-da-cpi-dos-crimes-ciberneticos-podem-mudar-o-uso-da-internet-5807438.html> Acesso em: 29 set. 2016.

SILVA, Rita de Cássia Lopes da. **Direito penal e sistema informático**. 2003. p. 97.

STEIBEL, Fabro. **Como os projetos e propostas da CPI dos Crimes Cibernéticos podem mudar o uso da internet**. 2016. Disponível em <http://zh.clicrbs.com.br/rs/vida-e-estilo/noticia/2016/05/como-os-projetos-e-propostas-da-cpi-dos-crimes-ciberneticos-podem-mudar-o-uso-da-internet-5807438.html> Acesso em: 29.09.2016.

SYDOW, Spencer Toth. **Crimes Informáticos e Suas Vítimas.** São Paulo: Saraiva, 2015.

Ministério da Ciência e Tecnologia. **Sociedade da informação no Brasil Livro Verde**. p.171.

TELES, Ney de Moura. **A influência da mídia na produção legislativa penal brasileira**. Disponível em: <http://www.ambito-juridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=8727&revista_caderno=3#_ftn46>. Acesso em: 17.11.2016.

TOMAZI, Sandra. **Uma lei, muitas dúvidas**. 2013. Disponível em: <http://www.gazetadopovo.com.br/vida-publica/justica-direito/uma-lei-muitas-duvidas-0amq7lj8b0skxnonfd5qh1glq>. Acesso em: 17.11.2016.

ZANELLATO, Marco Antonio. **Condutas Ilícitas na Sociedade Digital**. São Paulo, 2002. pp. 169-171.

ANEXOS

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE
Avenue de l'Europe
F-67075 Strasbourg Cedex
Tel. +33 (0)3 88 41 20 00
www.coe.int

Treaty Office

Full list

Chart of signatures and ratifications of Treaty 185

Convention on Cybercrime

Status as of 29/09/2016

Title	Convention on Cybercrime
Reference	ETS No.185
Opening of the treaty	Budapest, 23/11/2001 - Treaty open for signature by the member States and the non-member States which have participated in its elaboration and for accession by other non-member States
Entry into Force	01/07/2004 - 5 Ratifications including at least 3 member States of the Council of Europe

State who signed State who ratified State who neither signed nor ratified State who suspended State who denounced

	Signature	Ratification	Entry into Force	Notes	R.	D.	A.	T.	C.	O.
Members of Council of Europe										
Albania	23/11/2001	20/06/2002	01/07/2004				A.			
Andorra	23/04/2013									
Armenia	23/11/2001	12/10/2006	01/02/2007				A.			
Austria	23/11/2001	13/06/2012	01/10/2012		R.	D.	A.			
Azerbaijan	30/06/2008	15/03/2010	01/07/2010		R.	D.	A.	T.		
Belgium	23/11/2001	20/08/2012	01/12/2012		R.	D.	A.			
Bosnia and Herzegovina	09/02/2005	19/05/2006	01/09/2006				A.			
Bulgaria	23/11/2001	07/04/2005	01/08/2005		R.	D.	A.			
Croatia	23/11/2001	17/10/2002	01/07/2004				A.			
Cyprus	23/11/2001	19/01/2005	01/05/2005				A.			
Czech Republic	09/02/2005	22/08/2013	01/12/2013		R.	D.	A.			
Denmark	22/04/2003	21/06/2005	01/10/2005		R.		A.	T.		
Estonia	23/11/2001	12/05/2003	01/07/2004				A.			
Finland	23/11/2001	24/05/2007	01/09/2007		R.	D.	A.			
France	23/11/2001	10/01/2006	01/05/2006		R.	D.	A.			
Georgia	01/04/2008	06/06/2012	01/10/2012			D.				
Germany	23/11/2001	09/03/2009	01/07/2009		R.	D.	A.			
Greece	23/11/2001									
Hungary	23/11/2001	04/12/2003	01/07/2004		R.	D.	A.			
Iceland	30/11/2001	29/01/2007	01/05/2007		R.		A.			
Ireland	28/02/2002									
Italy	23/11/2001	05/06/2008	01/10/2008				A.			
Latvia	05/05/2004	14/02/2007	01/06/2007		R.		A.			
Liechtenstein	17/11/2008	27/01/2016	01/05/2016		R.	D.	A.			
Lithuania	23/06/2003	18/03/2004	01/07/2004		R.	D.	A.			
Luxembourg	28/01/2003	16/10/2014	01/02/2015				A.			
Malta	17/01/2002	12/04/2012	01/08/2012			D.				
Moldova	23/11/2001	12/05/2009	01/09/2009			D.	A.	T.		
Monaco	02/05/2013									
Montenegro	07/04/2005	03/03/2010	01/07/2010	55	R.		A.			
Netherlands	23/11/2001	16/11/2006	01/03/2007				A.	T.		

	Signature	Ratification	Entry into Force	Notes	R.	D.	A.	T.	C.	O.
Norway	23/11/2001	30/06/2006	01/10/2006		R.	D.	A.			
Poland	23/11/2001	20/02/2015	01/06/2015		R.		A.			
Portugal	23/11/2001	24/03/2010	01/07/2010			D.	A.			
Romania	23/11/2001	12/05/2004	01/09/2004				A.			
Russia										
San Marino										
Serbia	07/04/2005	14/04/2009	01/08/2009	55			A.			
Slovakia	04/02/2005	08/01/2008	01/05/2008		R.	D.	A.			
Slovenia	24/07/2002	08/09/2004	01/01/2005				A.			
Spain	23/11/2001	03/06/2010	01/10/2010			D.	A.			
Sweden	23/11/2001									
Switzerland	23/11/2001	21/09/2011	01/01/2012		R.	D.	A.			
The former Yugoslav Republic of Macedonia	23/11/2001	15/09/2004	01/01/2005				A.			
Turkey	10/11/2010	29/09/2014	01/01/2015							
Ukraine	23/11/2001	10/03/2006	01/07/2006		R.	D.	A.			
United Kingdom	23/11/2001	25/05/2011	01/09/2011		R.		A.			

Non-Members of Council of Europe

	Signature	Ratification	Entry into Force	Notes	R.	D.	A.	T.	C.	O.
Argentina										
Australia		30/11/2012 a	01/03/2013		R.		A.			
Canada	23/11/2001	08/07/2015	01/11/2015		R.	D.	A.			
Chile										
Colombia										
Costa Rica										
Dominican Republic		07/02/2013 a	01/06/2013			D.	A.			
Ghana										
Israel		09/05/2016 a	01/09/2016		R.		A.			
Japan	23/11/2001	03/07/2012	01/11/2012		R.	D.	A.			
Mauritius		15/11/2013 a	01/03/2014				A.			
Mexico										
Morocco										
Panama		05/03/2014 a	01/07/2014				A.			
Paraguay										
Peru										
Philippines										
Senegal										
South Africa	23/11/2001									
Sri Lanka		29/05/2015 a	01/09/2015		R.	D.	A.			
Tonga										
United States of America	23/11/2001	29/09/2006	01/01/2007		R.	D.	A.			

Total number of signatures not followed by ratifications	6
Total number of ratifications/accessions	49

Notes

- (55) Date of signature by the state union of Serbia and Montenegro.

a: Accession s: Signature without reservation as to ratification su: Succession r: Signature "ad referendum".
R.: Reservations D.: Declarations A.: Authorities T.: Territorial Application C.: Communication O.: Objection.
Source : Treaty Office on http://conventions.coe.int - * Disclaimer.

LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012.

Vigência

Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências.

A PRESIDENTA DA REPÚBLICA Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

Art. 1º Esta Lei dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências.

Art. 2º O Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, fica acrescido dos seguintes arts. 154-A e 154-B:

"Invasão de dispositivo informático

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

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

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

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

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

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

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

§ 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:

I - Presidente da República, governadores e prefeitos;

II - Presidente do Supremo Tribunal Federal;

III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou

IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal."

"Ação penal

Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos."

Art. 3º Os arts. 266 e 298 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, passam a vigorar com a seguinte redação:

"Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública

Art. 266. .....

§ 1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.

§ 2º Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública." (NR)

"Falsificação de documento particular

Art. 298. .....

Falsificação de cartão

Parágrafo único. Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito." (NR)

Art. 4º Esta Lei entra em vigor após decorridos 120 (cento e vinte) dias de sua publicação oficial.

Brasília, 30 de novembro de 2012; 191º da Independência e 124º da República.

DILMA ROUSSEFF
José Eduardo Cardozo