UNIVERSIDADE ESTADUAL DA PARAÍBA
CAMPUS I – CAMPINA GRANDE
CENTRO DE CIÊNCIAS JURÍDICAS
CURSO DE DIREITO

ISABELLA MEDEIROS MARTINS SILVA DE OLIVEIRA

TIPIFICANDO OS CRIMES CIBERNÉTICOS:
LACUNA LEGISLATIVA E IMPUNIDADE

CAMPINA GRANDE-PB

2018

ISABELLA MEDEIROS MARTINS SILVA DE OLIVEIRA

TIPIFICANDO OS CRIMES CIBERNÉTICOS: LACUNA LEGISLATIVA E IMPUNIDADE

Trabalho de Conclusão de Curso apresentado ao Centro de Ciências Jurídicas, da Universidade Estadual da Paraíba, como requisito parcial para obtenção do Título de Bacharel em Direito.

Orientadora: Profª Drª Aureci Gonzaga Farias.

Área de concentração: Direito Digital.

CAMPINA GRANDE-PB

2018

O48t Oliveira, Isabella Medeiros Martins Silva de.
Tipificando os crimes cibernéticos [manuscrito] : lacuna legislativa e impunidade / Isabella Medeiros Martins Silva de Oliveira. - 2018.
42 p.
Digitado.
Trabalho de Conclusão de Curso (Graduação em Direito) - Universidade Estadual da Paraíba, Centro de Ciências Jurídicas , 2018.
"Orientação : Profa. Dra. Aureci Gonzaga Farias , Coordenação do Curso de Direito - CCJ."
1. Ambiente Cibernético. 2. Crimes Virtuais. 3. Direito Digital. I. Título
21. ed. CDD 341.757

Elaborada por Fernanda M. de A. Silva - CRB - 15/483 BSCCJ/UEPB

ISABELLA MEDEIROS MARTINS SILVA DE OLIVEIRA

TIPIFICANDO OS CRIMES CIBERNÉTICOS:
LACUNA LEGISLATIVA E IMPUNIDADE

Aprovada em: 07/12/2018.

BANCA EXAMINADORA

Aureci Gonzaga Farias
Profª. Draª. Aureci Gonzaga Farias (Orientadora)
Universidade Estadual da Paraíba (UEPB)

Profª. Draª. Mônica Lúcia Cavalcanti de Albuquerque M. Nóbrega
Universidade Estadual da Paraíba (UEPB)

Maria do Socorro Tomaz Palitó Santos
Profª. Draª. Maria do Socorro Tomaz Palitó Santos
Universidade Estadual da Paraíba (UEPB)

AGRADECIMENTOS

Toda honra, toda a glória e todo o louvor sejam dados Àquele que me deu o dom da vida e me fez perseverar até o fim, agraciando-me com dons, talentos e toda sorte de bênçãos das regiões celestiais. O meu DEUS que criou os céus e a terra, que nunca falha e que jamais se esquece de mim conhece o meu levantar e o meu deitar, muito obrigada.

Ao meu querido e amado esposo **Marcos Oliveira**, por todo o incentivo e compreensão disponibilizados desde o início dessa empreitada, onde contribuiu sempre com seu conhecimento e amor até que o sonho se tornasse realidade.

Aos meus filhos que tanto amo **Matheus** e **Rebecca**, que me apoiaram e ajudaram, com palavras de ânimo e incentivos, bem como, suportando minha ausência em vários momentos de família, simplesmente para facilitar a minha caminhada em sentido ao alvo.

Aos meus pais **Socorro** e **Marcos**, que sempre foram importantes em minha vida, principalmente minha “mãe” que me proporcionou condições para que o conhecimento fosse adquirido, e investindo para que se tornasse concreto.

Aos meus irmãos e amigos que contribuíram direta ou indiretamente para o desfecho deste intento obtivesse sucesso.

A minha orientadora a **Profª Drª Aureci Gonzaga Farias**, pela paciência e empenho dispensados, colaborando para que esse trabalho acadêmico tomasse a forma apropriada, corrigindo e orientando-me durante o período de sua elaboração.

Enfim, a todos os que contribuíram direta e indiretamente, muito obrigado pelo amor e incentivo dispensados com alegria.

RESUMO

O presente Trabalho de Conclusão de Curso, intitulado “Tipificando os Crimes Cibernéticos: Lacuna Legislativa e Impunidade” tem como objetivo central analisar e sugerir a adequação do ordenamento jurídico juntamente com a efetividade da legislação em vigor, referente ao uso da internet e sua segurança, expondo a Lei nº 12.965, de 23 de abril de 2014, que objetiva garantir acesso de qualidade, com privacidade aos seus usuários, sem distinção de classe econômica ou social. Porém, esta lei apresenta alguns dispositivos particulares e devem ser adequadamente considerados. Questiona-se, no entanto, a legislação vigente é capaz de proteger e garantir efetivamente a segurança do uso da *Internet* no Brasil? Ou mesmo, como o Poder Público pode atuar para que a utilização do ambiente virtual seja fiscalizada e organizada a ponto de garantir um uso saudável e seguro aos usuários? Para esclarecer as questões levantadas foram utilizados os métodos observacional e dedutivo. Desse modo, a realização do processo formal e sistemático desses métodos tem por base, neste Trabalho, a taxionomia apresentada por Sylvia Constant Vergara, qualificando a metodologia adotada como procedimento explicativo (quanto aos fins) e a técnica de pesquisa bibliográfica (quanto aos meios), dado que, para a sua fundamentação teórico-metodológica buscaram-se conhecimentos doutrinários e legislações específicas. Enfim, os crimes virtuais se transformaram em uma das piores ameaças aos usuários da rede, pois ainda existe o sentimento de impunidade e a constante garantia de anonimato, que promove a diversificação dos delitos, no ambiente cibernético.

Palavras-chave: Ambiente Cibernético. Crimes Virtuais. Direito Digital.

ABSTRACT

The purpose of this study is to analyze and suggest the adequacy of the legal system, together with the effectiveness of the legislation in force, regarding the use of the Internet and its security, exposing Law No. 12,965, dated April 23, 2014, which aims to guarantee quality access, with privacy to its users, without distinction of economic or social class. However, this law presents some particular devices and must be properly considered. It is questioned, however, the current legislation is able to effectively protect and guarantee the security of Internet use in Brazil? Or, how can the Public Power act so that the use of the virtual environment is monitored and organized to the point of guaranteeing a healthy and safe use to the users? In order to clarify the questions raised, the observational and deductive methods were used. Thus, in the present work, the formal and systematic process of these methods is based on the taxonomy presented by Sylvia Constant Vergara, describing the methodology adopted as an explanatory procedure (for purposes) and the bibliographical research technique (as for the means) , given that, for its theoretical-methodological foundation, doctrinal knowledge and specific legislation were sought. Finally, virtual crimes have become one of the worst threats to network users, because there is still a sense of impunity and the constant guarantee of anonymity, which promotes the diversification of crime in the cyber environment.

Keywords: Cybernetic Environment. Virtual Crimes. Digital Right.

SUMÁRIO

1 INTRODUÇÃO

Em nosso país inexistia lei que regimentasse ou estabelecesse limitações às variadas espécies de acesso e superabundância de dados na rede mundial de computadores. Até esse tempo, as potenciais transgressões de direitos eram protegidas pelo Código Civil, Código de Defesa do Consumidor e leis dispersas.

Assim sendo, surgiu a urgência do estabelecimento de lei que uniformizasse esta utilização. Então, foi aprovada a Lei nº 12.965, de 23 de abril de 2014, conhecida popularmente como o "Marco Civil da Internet" que foi fonte de pesquisa e discussão, no Trabalho de Conclusão de Curso, intitulado "Tipificando os Crimes Cibernéticos: Lacuna Legislativa e Impunidade", tendo como objetivo central, analisar e sugerir a adequação do ordenamento jurídico juntamente com a efetividade da legislação em vigor, referente ao uso da *Internet* e sua segurança.

A Lei nº 12.965, de 23 de abril de 2014, em seu conteúdo evidencia a garantia à defesa dos consumidores que usam a *Internet* para a compra de serviços e produtos; uniformiza a venda de pacote de dados e o fluxo de informações; testifica a liberdade de expressão e orienta os serviços prestados pelos provedores de Internet pactuando o provimento de um serviço com praticidade, sob a responsabilidade das empresas fornecedoras. Portanto, a lei objetiva garantir acesso de qualidade, com privacidade aos seus usuários, sem distinção de classe econômica ou social. Porém, esta lei apresenta alguns dispositivos particulares e devem ser adequadamente considerados. Questiona-se, portanto, se a legislação vigente é capaz de proteger e garantir efetivamente a segurança de uso da *Internet* no Brasil? Ou mesmo, como o Poder Público pode atuar para que a utilização do ambiente virtual seja fiscalizada e organizada a ponto de garantir um uso saudável e seguro aos usuários?

Destaca-se ainda a relevância científica e social do tema objeto de estudo quanto ao acesso à Internet como canal de extensão das fronteiras da comunicação, expondo novas possibilidades criminalísticas, virtual ou digital. Sendo assim, o seu estudo justifica-se em contribuir para o conhecimento e crescimento dos estudiosos e os aplicadores do Direito, público alvo da pesquisa, como também, a sociedade como um todo.

Para esclarecer as questões levantadas neste Trabalho, foram utilizados os métodos, observacional e o dedutivo. A realização do processo formal e sistemático desses métodos tem por base, nesse Trabalho, a taxionomia apresentada por Sylvia

Constant Vergara[1], qualificando a metodologia adotada como procedimento explicativo (quanto aos fins) e a técnica de pesquisa bibliográfica (quanto aos meios), dado que, para a sua fundamentação teórico-metodológica buscaram-se conhecimentos doutrinários e legislações específicas.

Visando atingir os objetivos propostos, o Trabalho de Conclusão de Curso (TCC) estrutura-se em cinco partes, contando como primeira esta Introdução. A segunda parte, intitulada "O Surgimento da Internet", descreve-se acerca do nascimento, crescimento e desenvolvimento da *Internet* como ferramenta dos meios de comunicação.

A terceira, "A Importância do Direito Digital e seus Atributos", investiga-se a necessidade do conjunto de normas, aplicações, conhecimentos e relações jurídicas, oriundas do universo digital; a segurança jurídica mediante o uso da *Internet*, a criação do Comitê Gestor da Internet no Brasil; e ainda a importância da neutralidade de rede.

A quarta parte, "Tipificando os Crimes Cibernéticos", examina-se os crimes cibernéticos e a criação de normas gerais e específicas para a utilização da *Internet* no Brasil. Esmiúça-se o fenômeno das *fake news* e os possíveis prejuízos causados por essa prática, advindos das notícias falsas que, na maioria das vezes, se espalham via *Internet*, e tem sido muito discutido nos ambientes especializados e fora deles.

Na conclusão, procura-se expor a importância da utilização dos meios virtuais de forma consciente, com apontamentos quanto à eficácia ou ineficácia da legislação vigente, bem como propor, de forma sucinta, sugestões que sejam úteis no sentido de motivar a criação de legislação específica, relativa aos crimes cometidos no ambiente cibernético.

A estruturação deste Trabalho – referências, numeração progressiva das páginas, resumo, sumário, citações e trabalhos acadêmicos – obedecem às normas oficiais da Associação Brasileira de Normas Técnicas (ABNT).

---

[1] VERGARA, Sylvia Constant. **Métodos de pesquisa em administração.** 16. ed., São Paulo: Atlas, 2016, p.41.

2 O SURGIMENTO DA INTERNET

A Internet se tornou uma grande maravilha tecnológica na segunda metade do século XX, surgindo no ano de 1969, nos Estados Unidos da América (EUA), com o estabelecimento do chamado *Advanced Research Projects Agency Network* (ARPANET).[2] Esta agência foi primeiramente composta pelo Departamento de Defesa Americana e por quatro universidades daquele país, com o intuito da criação de um método que comportasse a transmissão rápida de dados para que assim, diante da guerra ou fatalidade, os registros de uma instituição pudessem ser preservados, mediante sua transferência para outros computadores conectados ao sistema. Depois, uniram-se a este sistema outras universidades, laboratórios, centros de pesquisas e, mais adiante, empresas, a partir de vantagens tecnológicas, sendo continuadamente conquistados, sobretudo os computadores, permitindo assim o uso dos equipamentos para fins pessoais e comerciais.

Assim, por diversos anos, o sistema *ARPANET* supriu às carências de órgãos governamentais e de entidades privadas, auxiliando como forma de acesso a banco de dados e também como correio eletrônico. Inicialmente, desenvolveram redes locais pequenas, intituladas de *Local Area Network* (*LAN*)[3], situadas em locais hábeis nos EUA e interligadas através da telecomunicação geográfica. No entanto, no ano de 1973, houve um acontecimento importante, onde o autor da *ARPANET*, Vinton Gray Cerf[4], do Departamento de Pesquisa Avançada da Universidade da Califórnia, consignou o Projeto de Controle de Transmissão, juntamente ao lançamento dos protocolos *Transmission Control Protocol/Internet Protocol* [5] (TCP/IP), servindo as-

---

[2] Pode-se dizer ser a "mãe" da *Internet*, desenvolvida pela agência Americana - *Advanced Research and Projects Agency* (ARPA), Agência de Pesquisas em Projetos Avançados em 1969, que tinha o objetivo de interligar as bases militares e os departamentos de pesquisa do governo americano.

[3] Rede de área local de dispositivos que estão interligados entre si através de um meio físico (*ethernet*). É um conjunto de *hardware* e *software* que permite a computadores individuais estabelecerem comunicação entre si, trocando e compartilhando informações e recursos. Tais redes são denominadas locais por cobrirem apenas uma área limitada (1 km no máximo, além disso, passam a ser denominadas *MANs*). Redes em áreas maiores necessitam de tecnologias mais sofisticadas, visto que, fisicamente, quanto maior a distância de um nó da rede ao outro, maior a taxa de erros que ocorrerão devido à degradação do sinal.

[4] Matemático e informático estadunidense. Referenciado como um dos fundadores da *Internet* foi em 2005, vice-presidente e "*Chief Internet-Evangelist*" da *Google*.

[5] Também chamado de pilha de protocolos *TCP/IP* é um conjunto de protocolos de comunicação entre computadores em rede.

sim de instrumento para a ordenação de normas técnicas adequadas para a transmissão de informações, através da rede de computadores, fazendo com que os usuários sejam identificados com endereços e nomes de domínio. Os modelos criados admitiram a interligação entre diferentes redes, surgindo, portanto, a Internet como um sistema mundial de comunicação.

No ano de 1981, a empresa *Xerox* lançou o primeiro computador com *mouse* e interface gráfica. Posteriormente, o físico inglês Tim Berners-Lee [6] inventa a linguagem *Hyper Text Markup Language* (HTML)[7]. Já no ano de 1989, foi criada a *World Wide Web* (WWW)[8], emanada num Laboratório Europeu de Física, em Genebra, ferramenta tecnológica importante para o tráfego de documentos, imagem e sons pela rede, transformando a Internet num fenômeno de comunicação de massa e indispensável ao movimento de integração que predomina em todo o mundo.

O crescimento desta nova tecnologia deslanchou, a partir do ano de 1990, devido à parceria entre o governo norte-americano e entidades privadas. A Internet se ampliou além do local de seu nascedouro nos EUA e ganhou espaço mundialmente, sem limitações de fronteiras físicas, assim, uma revolução tecnológica e comportamental nasceu. Numa inaudita rapidez, novos hábitos tecnológicos se inserem ao dia a dia das pessoas e das organizações, como, por exemplo, as transações financeiras, atualmente simplificadas pelo *Internet Banking e Mobile Banking* [9], sem citar os bancos exclusivamente digitais, onde todos os contatos com clientes são totalmente *on-line*, podendo, até mesmo, abrir contas através de telefones celulares, bem como outras facilidades.

Contemporaneamente, os robôs não se limitam apenas aos equipamentos industriais ou aparelhos humanoides que tanto fascinam, abrangem a várias estrutu-

---

[6] Físico britânico, cientista da computação e professor do Instituto de Tecnologia de Massachusetts (MIT). É o criador da *World Wide Web*, tendo feito a primeira proposta para sua criação a 25 de março de 1989.

[7] Termo técnico que foi traduzido para a língua portuguesa como "linguagem de marcação de hipertexto", é uma técnica de linguagem de programação *web*. A tecnologia é fruto da junção entre os padrões *HyTime* e *SGML*, que não são mais utilizados.

[8] Significa em português, rede de alcance mundial, também conhecida como *web* ou *WWW*. *World Wide Web* é um sistema de documentos em hipermídia que são interligados e executados na *Internet*.

[9] Banco internético, *e-banking*, banco *on-line*, *on-line banking*, às vezes também banco virtual, banco eletrônico ou banco doméstico, são termos utilizados para caracterizar transações, pagamentos e outras operações financeiras e de dados pela Internet por meio de uma página segura de banco.

ras automatizadas criados por um *software*, que são possuidores de inteligência artificial e também aptidão para solucionar, conforme o ambiente, um segmento pré-programado automático, como se as máquinas possuíssem vida e capacidade próprias, inclusive, de efetuar buscas, analisar arquivos e fazer pesquisas em geral numa velocidade muito alta.

A Revista Tribuna do Advogado apresentou, em um artigo publicado com o título de "Advocacia Artificial", um debate sobre a utilização progressiva de robôs no âmbito jurídico, onde difundiu informações verdadeiramente inauditas, como *in verbis*:

> Agora, imagine um robô como seu colega de escritório. Não se trata de ficção científica: em maio, foi divulgada a notícia de que o primeiro 'robô-advogado' do mundo acabara de ser 'contratado' por uma grande banca de advocacia americana. Trata-se da inteligência artificial 'Ross', que usa o supercomputador Watson, da IBM, para operar como fonte inesgotável de informações para os cinquenta advogados da divisão de falências da banca. (KERCKHOVE, 2016).

No entanto, ainda estamos nos habituando ao novo mundo de transformações rápidas, pois temos visto o rompimento de regras da Sociedade Industrial e a fusão da Sociedade da Informação, onde as mutações sociais e econômicas percebidas cotidianamente nos indivíduos são determinadas pela tecnologia intitulada de disruptiva[10], quando surgem novas conjunturas, novos modelos na divulgação de conhecimentos, nos acordos comerciais, nas tipologias de diversão e lazer, e, também em outras formas de comportamento anteriormente não imaginados, brotando protótipos temporais e espaciais, gerando um mundo cibernético *borderlessness*[11], ou seja, sem fronteiras e com contingência na transmissibilidade e acolhimento de comunicações em qualquer local do planeta.

As empresas virtuais atualmente desfrutam da possibilidade de possuir consumidores em qualquer parte do mundo, diante da multiplicação das comunidades virtuais estenderem-se além das fronteiras físicas, unificadas, buscando objetivos e

---

[10] Termo que descreve a inovação tecnológica, produto, ou serviço, com características "disruptivas", que provocam uma ruptura com os padrões, modelos ou tecnologias já estabelecidas no mercado.

[11] A ausência de fronteiras pode se referir a País sem fronteiras, um território insular sobre o qual um Estado-nação mantém a soberania sob o direito internacional, que não compartilha o território terrestre de nenhuma de suas ilhas; venda sem fronteiras, o processo de venda de serviços para clientes fora do país de origem dos serviços, eliminando as ações destinadas especificamente a impedir o comércio internacional.

interesses comuns, sendo de natureza econômica, cultural ou de qualquer outra espécie.

A significação técnica acerca da *Internet* é bem delimitada por Pinheiro (2009, p. 14):

> A Internet consiste na interligação de milhares de dispositivos do mundo inteiro, interconectados mediante protocolos (IP, abreviação de *Internet Protocol*). Ou seja, essa interligação é possível porque utiliza um mesmo padrão de transmissão de dados. A ligação é feita por meio de linhas telefônicas, fibra óptica, satélite, ondas de rádio ou infravermelho. A conexão do computador com a rede pode ser direta ou através de outro computador conhecido como servidor. Este servidor pode ser próprio ou, no caso dos provedores de acesso, de terceiros. O usuário navega na Internet por meio de um browser, programa usado para visualizar páginas disponíveis na rede, que interpreta as informações do website indicado, exibindo na tela dos usuários textos, sons e imagens. São browsers o MS Internet Explorer, da Microsoft, o Netscape Navigator, da Netscape, e o Mozilla, da The Mozilla Organization com cooperação da Netscape, entre outros.

Na atualidade, é corriqueiro comparar a Revolução Digital com as grandes conquistas antigas da humanidade. Ao lembrar-se do período das primeiras navegações às terras chamadas de Novo Mundo, percebe-se que foi estabelecida uma das fases da globalização, aproximando povos e incrementando o comércio, fazendo surgir um novo estágio de evolução, principalmente no referente ao desenvolvimento dos meios de transporte marítimo. A era virtual compara-se à Revolução Industrial, que ocasionou resultado crucial nas tecnologias desenvolvidas nos séculos XIX e XX, diante de novas descobertas e maneiras de trabalho, enquanto a Revolução Digital associa importância ao indivíduo e às empresas, graças à quantidade de informação e ao conhecimento transmitido em velocidade imediata.

No entanto, os novos fenômenos econômicos e sociológicos proveem da comunicação massificada favorecida pela Internet, de modo que o Direito é presumido também diante das alterações de conceitos, comportamentos e atitudes, ocasionando o chamado de reengenharia jurídica, em que se resume a função isolada de um operador de Direito na interpretação da norma jurídica, para assim beneficiar resolução de planejamento e estratégia criada por equipes e pelo pensamento coletivo.

Então, formando-se, o denominado Direito Digital, onde foi registrado o primeiro marco no Brasil, a partir da Portaria Interministerial nº 147, de 31 de maio de 1995, editada pelos Ministérios da Comunicação e da Ciência e Tecnologia, regulando assim a utilização dos meios da rede pública de telecomunicações para o pro-

vimento e a utilização de serviços de conexão da *Internet.* A partir dessa determinação foi permitido o desenvolvimento comercial da comunicação eletrônica no Brasil e o consequente incremento das normas jurídicas pertinentes.

3 A IMPORTÂNCIA DO DIREITO DIGITAL E SEUS ATRIBUTOS

Nos últimos vinte anos o Direito Digital vem num desenvolvimento abundante, ampliando assim uma nova doutrina jurídica que se baseia na aplicação de normas jurídicas adequadas ao ciberespaço, num reconhecimento de que a legislação e a doutrina jurídica tradicional são insuficientes para regular as relações no mundo virtual, as quais desafiam novos questionamentos e novas soluções, num ambiente carente do que se chama de fronteiras espaço-tempo. Como nova disciplina, vem representando uma reestruturação na forma de entender o próprio Direito, partindo do princípio de novos modelos e padrões fundamentados na esfera filosófica, científica, social e cultural.

O Direito Digital conduz a uma interpretação atípica, lembrando que a Lei nº 12.965, de 23 de abril de 2014, intitulada como o "Marco Civil da Internet" (MCI), também conhecida como a "Constituição da Internet Brasileira", aponta em seu artigo 6º, que, "na interpretação desta lei, serão levados em conta, além dos fundamentos, princípios e objetivos previstos, a natureza da Internet, seus usos e costumes particulares e sua importância para a promoção do desenvolvimento humano, econômico, social e cultural". Todavia, percebe-se que o Direito Digital é uma linha de entendimento jurídico do qual se chama "Sociedade da Informação", cujo estudo auxilia a raciocinar juridicamente enquanto atravessam-se barreiras geográficas e temporais, num tempo em que as decisões das pessoas físicas e jurídicas são ocasionadas na velocidade do mundo virtual.

A ampliação das formas de comunicação em massa, antes mesmo do invento da *Web* no século XX, como o rádio, a televisão e o cinema, já inspirava e aproximava pessoas, projetando o que se convencionou chamar de Aldeia Global[12], ilustração figurativa da nova interligação da humanidade. Assim, a *Internet* dinamizou o resultado incorporativo, fabricando uma infinidade de nações virtuais, unificadas diante dos mais variados interesses.

---

[12] Termo criado pelo filósofo canadense Herbert Marshall McLuhan. Ele tinha o objetivo de indicar que as novas tecnologias eletrônicas tendem a encurtar distâncias e o progresso tecnológico tende a reduzir todo o planeta à mesma situação que ocorre em uma aldeia: um mundo em que todos estariam de certa forma, interligados. A expressão foi popularizada em sua obras "A Galáxia de Gutenberg" (1962) e, posteriormente, em "Os Meios de Comunicação como Extensão do Homem" (1964). McLuhan foi o primeiro filósofo a tratar das transformações sociais provocadas pela revolução tecnológica do computador e das telecomunicações.

Contudo, a informação é um requisito básico do Direito Digital ou da Internet e tem ganhado importância diante das consequências nos acordos comerciais, na responsabilidade civil e nas limitações referentes à liberdade de expressão e para que se torne praticável deverá se adaptar a alguns fundamentos e atributos da avocada Revolução Digital, cuja ferramenta mais importante deste novo tempo é a capacidade característica quanto à circulação das informações, que resulta as transformações em hábitos e relações sociais, através dos avanços tecnológicos rapidamente.

A utilização dos meios virtuais presume clareza, contribuição, distribuição de informação e aptidão de movimentação da rede, conjecturando-se semelhantemente novos posicionamentos e condutas nas mídias sociais, a evolução progressiva de uma cidadania digital, com apontamentos de mobilização política e maior conversação entre pessoas, governo e empresas.

Por conseguinte, os operadores jurídicos serão requisitados ao manuseio das novas significações referentes à liberdade de expressão e suas limitações, averiguação de autenticidade da prova eletrônica, interpretação adequada ao Direito do Consumidor, proteção de dados pessoais e da propriedade intelectual, tipificação de crimes eletrônicos, intimação das partes em processo judicial por meio virtual, tributação de operações comerciais e inúmeros exemplos que desafiam o Poder Judiciário, necessitando assim, possuir, competência que encubra as omissões que não conseguem ser acatadas apenas pelo empenho da hermenêutica eficaz concebida pelos Tribunais, mas igualmente pela sucessiva atualização das leis.

Com efeito, é característico que o Poder Judiciário considere o passado, isto é, os enfrentamentos anteriores, com os recursos interpretativos aprofundados que o Direito possui disponibilidade no momento em que se decide um problema já existente na realidade, pois, em que pese a solidificação da jurisprudência daquele Poder, sempre, caberá, ao Poder Legislativo aprofundar a criação de novos preceitos legais, direcionando-se ao futuro, partindo de experiências vivenciadas, compensando a ausência da ordem jurídica atual, corrigindo e precavendo polêmicas que provavelmente permanecerão na sociedade futura.

Assim sendo, verifica-se que nas novas legislações que virão tornam-se previsíveis a proximidade do tempo em que conjunturas modernistas se converterão em realidade, como os *chips* usados em aparelhos domésticos, fornos de microondas, máquinas de lavar roupas, aparelhos de som e outros equipamentos, que conseguí-

rão se comunicar entre si e serão reconhecidos pelo seu endereço *IP*, isto é, endereço de protocolo da *Internet*, com a finalidade da comunicação digital. Pode-se exemplificar o assunto em comento com uma geladeira porta-refrigerantes, que possuirá um *chip* ligado a um determinado estabelecimento comercial, que acionado, exigirá a reposição de novo estoque das bebidas que chegarem ao fim. Esse novo comportamento é chamado Internet das Coisas[13], onde assuntos como responsabilidade civil e insolvência terão que ser regimentadas e sancionadas legalmente, haja vista que nesse caso, a geladeira sempre será inimputável.

Por conseguinte, *Internet of Things ou IoT,* originada do inglês, é uma rede de objetos físicos (veículos, prédios etc.) que possuem tecnologia embarcada, sensores e conexão com a rede e é capaz de coletar e transmitir dados, que emergiu dos avanços de várias áreas, como sistemas embarcados, microeletrônica, comunicação e sensoriamento. De fato, a *IoT* tem recebido bastante atenção, tanto da academia quanto da indústria, devido ao seu potencial de uso nas mais diversas áreas das atividades humanas.

Existem atualmente pessoas que levam em seus próprios corpos *chips* com diversificadas funções, tanto para verificar a saúde, medindo a glicemia, como atender funcionalidades da vida, como exemplo, abrir um portão com sinais eletromagnéticos, sem a necessidade de uso da chave, assim se estimula ao que existe atualmente, a possibilidade de viver simultaneamente *on-line e off-line*, onde dispositivos de inteligência artificial incorporam e acrescentam a inteligência real.

Entretanto, percebe-se a defasagem do Direito convencional em relação ao mundo digital, que se manifesta através do fenômeno em que a norma sempre estará acelerando atrás do fato, sendo um desafio da sociedade digital, que carece ocupar, para sua conservação, a paz social que, segundo a afirmação de Rudolf Von Ihering (2011), é o fim do Direito, enquanto que o meio de que se serve para consegui-lo é a luta. Contudo, a luta pelo Direito, na esfera digital, é na verdade a luta contra a inutilidade da lei antiga, devendo à sociedade requisitar interpretações atuali-

---

[13] É uma extensão da Internet atual, que proporciona aos objetos do dia-a-dia (quaisquer que sejam), mas com capacidade computacional e de comunicação, se conectarem a *Internet*. A conexão com a rede mundial de computadores viabilizará, primeiro, controlar remotamente os objetos e, segundo, permitir que os próprios objetos sejam acessados como provedores de serviços. Estas novas habilidades, dos objetos comuns, geram um grande número de oportunidades tanto no âmbito acadêmico quanto no industrial. Todavia, estas possibilidades apresentam riscos e acarretam amplos desafios técnicos e sociais. Disponível em: <https://pt.wikipedia.org/wiki/Internet_das_coisas>. Acesso em: 03 de out. de 2018.

zadas e novas leis, apropriadas às relações sociais existentes na Internet e através de equipamentos digitais. Então, a luta pelo Direito é concreta, que recepciona vida e energia do Direito reflexivo, mas também devolve.

Ponderando sobre o avanço tecnológico, que fatalmente superará o desenvolvimento legislativo, não existe sobra de tempo para criação de jurisprudência na forma tradicional dos Tribunais, visto que, por conta da rapidez e a vitalidade do Direito Digital ocasionam diversas vezes, com a finalidade de resolução de conflitos, a interpretação por comparação, a utilização da arbitragem e do Direito usual, considerando os usos e costumes adotados nas redes digitais. Ante a ausência de normas capazes de acompanhar a evolução tecnológica. Por outro lado, uma norma legal ou mesmo contratual que trate de institutos jurídicos adaptados às práticas digitais deve ter sempre um caráter comum, para que subsista no tempo e seja maleável para acolher a várias realidades da Sociedade da Informação, em especial, às variações cibernéticas.

Os apontamentos feitos por Pinheiro (2009) merecem ser aclamados, quando reporta que, além dos elementos que concebem a fórmula tridimensional do Direito (fato, valor e norma), ainda existe no Direito Digital, o elemento “tempo”. No entanto, sabe-se, que Miguel Reale criou esta fórmula, juntando o valor da Justiça, a realidade social e histórica de um lugar ou época e o ordenamento, destacando os três pilares do Direito que não podem ser separados um do outro. Entretanto, o “tempo” apontado como quarto elemento, não resulta do intervalo de validade de uma norma, mas sim de que a união fato-valor-norma necessita ter certa velocidade de resposta para que tenha certa validade dentro da sociedade digital, pois, caso não haja resposta rápida, pode logo acontecer o esgotamento do direito subjetivo.

Existe ainda a conceitualização de territorialidade que também passa a ter estruturas, que são diferentes numa sociedade globalizada e convergente. Diante disso, não é possível a consolidação do território em que ocorreu a relação jurídica e seus efeitos, pois no mundo virtual são construídos territórios de difícil demarcação, onde diferentes culturas se comunicam o tempo todo.

A noção do Direito Digital, como globalizado e convergente, atrai também uma nova adjetivação, por se tratar de um Direito Comunitário. Por meio do ambiente virtual o indivíduo possui muito mais acesso ao conhecimento e informação, repartindo preocupações de cunho universal, vinculando-se a outros indivíduos, além das fronteiras nacionais. Assim, “fato, valor, norma e tempo” superam as limitações

territoriais de um Estado, requerendo procedimentos comuns e certificações normativas supranacionais, como ocorre relacionado em algumas documentações e leis derivadas da Comunidade Europeia que discutem sobre o *e-commerce* [14] e crimes eletrônicos.

Na realidade, esta relevante comunidade de países e pessoas que formam o universo digital onde questionam assuntos que atraem a todos, principalmente certas discussões como direito à privacidade e segurança, liberdade de expressão e direito à defesa da honra e da intimidade, proteção de dados e acesso à informação e tantas problemáticas ainda não solucionadas diante da comunicação em massa, mundialmente. Por conseguinte, perspectivas conflitivas complicadas de solucionar, através da lei ou da judicialização, incentivam a prática da autorregulamentação como desfecho de contestação, corrigindo-se omissões existentes no Direito, podendo-se exemplificar com os provedores de acesso à Internet que estabelecem normas-padrão, especialmente no que tange a questões de privacidade e prática de ilícitos.

Ressalta-se, contudo, que isentos preceitos que lhe são particulares, o Direito Digital, pontualmente, não se classifica como uma área específica do Direito, isso ocorre devido a ele não possuir objeto próprio como outros ramos possuem, distinguindo-se exclusivamente pelo modo como trafega, isto é, pelas vias virtuais. Sendo assim, um Direito com um *modus operandi* distinto, existindo, na verdade, a dimensão de várias áreas da ciência jurídica, que desenvolvem novas ferramentas para suprir as expectativas e ao aprimoramento dos institutos jurídicos em vigência.

3.1 A INTERNET E A NECESSIDADE DE SEGURANÇA JURÍDICA

A população sempre pensou que a rede/*Internet* não pertencia a ninguém, seria uma “terra sem dono”, não conseguindo ser compreendida, incorporando conceitos de posse e propriedade, sendo somente uma ferramenta de comunicação em equivalência mundial que precisa ser aberta e colaborativa. Entretanto, a Internet iniciou criando, em algumas pessoas, a imaginação de que nela se possuía uma autonomia irrestrita, gerando atualmente a necessidade de regras, disciplina legal e de segurança jurídica.

---

[14] Comércio eletrônico ou *e-commerce*, comércio virtual ou venda não presencial, é um tipo de transação comercial feita especialmente através de um equipamento eletrônico, como, por exemplo, computadores*, tablets* e *smartphones*.

A Lei nº 12.965, de 23 de abril de 2014, veio ocupar esta função, instituindo princípios, garantias, deveres e direitos para o uso da rede mundial de computadores no Brasil, constituindo assim, as regras que deverão ser amparadas pelo Poder Público acerca do assunto, principalmente para assegurar o direito de acesso da rede mundial de computadores a todas as pessoas físicas e jurídicas (que consta em seu artigo 4º, inciso I).

A Lei nº 12.965, de 23 de abril de 2014, não surgiu por uma proposta do governo, mas sim da sociedade. Sua conceituação surgiu muitos anos antes dos escândalos causados por roubo de informações sigilosas dos governos em diversos Países, onde se discutia no ambiente público como seria feito a normatização da *Internet* no Brasil, mais precisamente à chamada Lei Azeredo, cujo projeto de lei foi batizado assim devido seu relator e mais assíduo defensor ser o deputado Eduardo Azeredo, que apresentava o estabelecimento de uma extensa lei criminal voltada para a *Internet*. A ideia de uma ampla visão da população brasileira era que a Lei Azeredo, caso decretada, acarretaria um imenso regresso no ambiente regulatório da *Internet* no País.

Com um texto imenso, a Lei Azeredo, transformava em delitos atitudes usuais na rede, realizadas por milhões de usuários, como exemplo, criminalizava práticas como transferir as músicas de um *iPod*[15] de volta para o computador; ou, ainda, incriminava condutas como desbloquear um celular para ser usado por operadoras diferentes, ambas penalizadas com até quatro anos de reclusão. Esses são apenas dois exemplos pontuais, pois caso viesse a ser aprovada, a legislação representaria uma imobilização de oportunidade de modernização no País, causando prejuízos eternos como consumidores de produtos tecnológicos, incriminando várias fases indispensáveis para a pesquisa, inovação e produção de novos serviços tecnológicos.

A Lei nº 12.965, de 23 de abril de 2014, alterou a legislação do País para determinar aos cidadãos, ao governo e às organizações direitos e responsabilidades em relação à *Internet*, sendo guiada por um grupo de dez princípios, entre eles, neutralidade da rede, privacidade, liberdade de expressão, segurança e universalidade. Esses princípios são utilizados como marco para avaliar o estado da governança da

---

[15] Marca registada da *Apple Inc*. refere-se a uma série de media *players* portáteis projetados e vendidos pela *Apple*. Desde 2008, a linha de *iPods* inclui o *iPod classic, o iPod shuffle, o iPodnano e o iPod touch*.

Internet no Brasil e também verificar a efetivação dessa lei, projetos de lei e leis, relacionados a esses princípios e à governança da *Internet* mundial. Ademais, avalia o estado do uso e da infraestrutura da *Internet* no Brasil, pois o País é um dos pilares do ecossistema da *Internet* mundial e um exemplo de visão alternativa na esfera da política internacional relativa à governança de redes *online*.

A princípio, a Lei nº 12.965, de 23 de abril de 2014, versa sobre as bases para a utilização da Internet, salientando, primordialmente, a liberdade de expressão. Em seu artigo 2º, são relacionados pontos importantes como: o reconhecimento da escala mundial da rede, os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais, a pluralidade e a diversidade, a abertura e a colaboração, a livre iniciativa, a livre concorrência e a defesa do consumidor e, por fim, a finalidade social da rede.

Já o seu artigo 3º, aponta preceitos que a orientam quanto: a garantia da liberdade de expressão, a comunicação e manifestação de pensamento, nos termos da Constituição da República Federativa do Brasil, de 1988; a proteção da privacidade e dos dados pessoais; a preservação e garantia da neutralidade da rede; a preservação da estabilidade, a segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas; a responsabilização dos agentes, de acordo com suas atividades; resguardar a natureza participativa da rede; a liberdade dos modelos de negócios promovidos na Internet, desde que não conflitem com os demais princípios estabelecidos. Reiterando, no parágrafo único, que os princípios apresentados não descartam outros previstos no ordenamento jurídico pátrio relacionado à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte.

No entanto, essa lei deixou expressos quais os intuitos que pretende, uma vez que se dedica a favorecer o que estabelece seu artigo 4º, onde aborda alguns temas como: o direito de acesso à *Internet* a todos; o acesso à informação, ao conhecimento e à participação na vida cultural e na condução dos assuntos públicos; a inovação e o fomento à ampla difusão de novas tecnologias e modelos de uso e acesso; a adesão a padrões tecnológicos abertos que permitam a comunicação, a acessibilidade e a interoperabilidade entre aplicações e bases de dados.

Entretanto, existe uma ampla lista de direitos dos usuários da *Internet*, assegurados pelo artigo 7º, a saber: a inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação; a

inviolabilidade e sigilo do fluxo de suas comunicações via *web*, como também suas comunicações armazenadas; a não suspensão da conexão à *Internet*, salvo por débito diretamente decorrente de sua utilização; a manutenção da qualidade contratada da conexão à *Internet*; as informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de *Internet*, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade; o não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações na *Internet*, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei.

Além do mais, devem fornecer informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que justifiquem sua coleta; não sejam vedadas pela legislação e estejam especificadas nos contratos de prestação de serviço ou em termos de uso de aplicações de *Internet*; consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais; exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de *Internet*, a seu requerimento, ao término da relação entre as partes, ressalvada as hipóteses de guarda obrigatória de registros previstos em lei; publicidade e clareza de eventuais políticas de uso dos provedores de conexão e de aplicações de *Internet*; acessibilidade, consideradas as características físico-motores, perceptivas, sensoriais, intelectuais e mentais do usuário; aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na *Internet*.

3.2 O QUE É COMITÊ GESTOR DA INTERNET NO BRASIL?

De fato, a *Internet* surgiu, no Brasil quando a Fundação de Pesquisas do Estado de São Paulo (FAPESP) e o Laboratório Nacional de Computação Científica, que é uma Unidade de Pesquisa do Ministério da Ciência, Tecnologia e Inovação, localizada no Rio de Janeiro, e que se ligaram às instituições de pesquisa nos Estados Unidos da América (EUA). Em seguida, ocorreu a criação da Rede Nacional de Pesquisa (RNP), unida ao Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq), com a missão de dissipar o uso da *Internet* para fins educacionais e sociais.

Através da Portaria Interministerial n° 147, de 31 de maio de 1995, os Ministérios das Comunicações e da Ciência e Tecnologia, criou o Comitê Gestor da Internet no Brasil (CGI.br), órgão responsável, dentre outras coisas, em atribuir a faixa de números *IP´s* que o Brasil irá utilizar. Esse Comitê passou a abarcar-se verdadeiramente nas resoluções relacionadas ao estabelecimento, à administração e ao uso da Internet no País.

A atual composição do CGI.br foi estabelecida pelo Decreto nº 4.829, de 3 de setembro de 2003, que é integrado por, nove representantes do setor governamental, quatro do setor empresarial, quatro do terceiro setor, três da comunidade científica e tecnológica e um representante de evidente conhecimento em assuntos de *Internet*.

O CGI.br é composto por nove membros representantes do setor governamental: o Ministério da Ciência Tecnologia e Inovação; Ministério das Comunicações; Ministério da Defesa; Ministério do Desenvolvimento, Indústria e Comércio Exterior; Ministério do Planejamento, Desenvolvimento e Gestão; Agência Nacional de Telecomunicações; Conselho Nacional de Desenvolvimento Científico e Tecnológico; Conselho Nacional de Secretários para Assuntos de Ciência, Tecnologia e Inovação; Casa Civil da Presidência da República.

Todavia, não é exclusivo para o setor público participar do CGI.br, pois é constituído também por quatro representantes do setor empresarial, cuja indicação será efetivada por meio da constituição de um colégio eleitoral, que elegerá, por votação não secreta, os representantes dos seguintes segmentos: provedores de acesso e conteúdo da *Internet*; provedores de infraestrutura de telecomunicações; indústria de bens de informática, de bens de telecomunicações e de *software*; e, se-

tor empresarial usuário. Participam, ainda, quatro representantes do terceiro setor[16], cuja indicação será efetivada por meio da constituição de um colégio eleitoral[17], composto por entidades de representação apropriadas ao terceiro setor, que elegerá, por votação não secreta, os respectivos representantes; e, por fim, três representantes da comunidade científica e tecnológica[18], cuja indicação será efetivada por meio da constituição de um colégio eleitoral formado por entidades de representação pertinentes à comunidade científica e tecnológica, que elegerá, por votação não secreta, os respectivos representantes.

3.3 A IMPORTÂNCIA DA NEUTRALIDADE DA REDE

O princípio da neutralidade de rede era absolutamente recepcionado pela sociedade jurídica internacional, positivada atualmente pela Lei nº 12.965, de 23 de abril de 2014, em seu artigo 9º. Acredita-se que esse princípio brotou de um acontecimento sucedido nos primórdios do serviço de telefonia, quando as ligações telefônicas precisavam da intermediação de uma central de telefonistas. Nesse tempo, existia uma telefonista que, ao receber o pedido de um cliente interessado em estabelecer contato telefônico com uma determinada empresa, redirecionava astuciosamente a ligação para a empresa concorrente, que geralmente pertencia a um parente. Por isso, despontou a ideia de que a telefonista, que era a conexão obrigatória do sucesso da ligação telefônica, necessitaria ser uma pessoa isenta e imparcial, que de modo algum viesse a encaminhar capciosamente as ligações para destinos de sua conveniência pessoal.

De modo genérico, os provedores de conexão são as empresas que possibilitam o acesso dos internautas à *Internet*. Em uma sinonímia medíocre, porém provei-

---

[16] É o conjunto de entidades da sociedade civil com fins públicos e não lucrativos conservados pela ênfase na participação voluntária em âmbito não governamental.

[17] É um órgão formado por um conjunto de eleitores com o poder de um corpo deliberativo para eleger alguém a um posto particular. De maneira geral, esses eleitores representam diferentes organizações, regiões ou entidades, com cada organização, região ou entidade representada por um número determinado de eleitores ou com votos ponderados de uma maneira particular. Algumas vezes, no entanto, os eleitores são simplesmente pessoas importantes cuja sabedoria, espera-se, resultará em uma escolha melhor do que a de um corpo eleitoral mais largo.

[18] É a comunidade de pessoas e organizações que geram as ideias científicas, que testam essas ideias, que publicam em revistas científicas, que organizam conferências, que formam os cientistas, que atribuem fundos de pesquisa etc.

toso à compreensão dos menos familiarizados com as terminologias técnicas. No ambiente virtual, os provedores de conexão fazem o papel dessa telefonista, resguardando as chaves da porta de acesso à *Internet*, passando-se por elo que interliga o mundo físico ao espaço cibernético. Consequentemente, é intolerável que desamparem a neutralidade e passem a incentivar o acesso dos internautas a determinadas aplicações ou a deteriorar o tráfego de serviços prestados por empresas concorrentes.

Nessa perspectiva, não seria permitido que os provedores de conexão instituíssem escalas de valores de seus pacotes de acesso à *Internet* de acordo com o conteúdo dos *sites* visitados pelos internautas. Assim, não poderia precisar que o valor do pacote fosse de trinta reais para ter acesso apenas ao *Facebook*; de quarenta reais para acessar também o *Twitter*; ou de setenta reais para acessar qualquer *site*. Isso é proibido, por postergar o princípio da neutralidade de rede.

Acredita-se que apesar de já ter apontamentos de posicionamentos contrários, que posterga a neutralidade de rede mediante oferta privilegiada a determinadas aplicações como, por exemplo, o *Facebook*, que através de uma velocidade de conexão mais veloz, ainda que sob o pretexto da gratuidade, porém, ofertas gratuitas de acesso à determinada aplicação é uma estratégia de *marketing*, pois obviamente tanto o provedor de conexão, que expande sua base de clientes e a capacidade de tráfego através de suas redes, quanto o provedor de aplicações, que promove a potencialidade publicitária de seu serviço, possuem vantagens econômicas indiretas por essa oferta.

Verifica-se que, com o incentivo ao acesso a determinada aplicação o provedor de conexão desrespeita o princípio da neutralidade de rede, dessa maneira protege o conteúdo de uma aplicação em desvantagem de outro, desviando ou incentivando o redirecionamento do internauta a determinada aplicação.

A propósito, isso descumpre inclusive a natureza diversificada e soberana da *Internet*, que, por sua extraordinária eficácia de multiplicação de informações, conduz aceleradamente, em ídolos e em celebridades, vários anônimos de renda baixa que postam seus talentos em redes sociais ou em outra aplicação. Caso os provedores de conexão venham a poder exercer manipulação ao acesso dos internautas a determinados *sites*, a natureza diversa da *Internet* será lesada.

A Lei nº 12.965, de 23 de abril de 2014, ordena que a neutralidade de rede reconheça somente, como exceções, conjecturas específicas pertencentes a ques-

tões técnicas que prejudique a qualidade do serviço e serviços de emergência. Existem, a título de exemplo, procedimentos médicos que são realizados *on-line*, os quais nunca poderiam aceitar demora no trânsito de dados, podendo assim ocasionar a frustração do resultado. Em circunstâncias como essas, que compreendem serviços de emergência, o provedor de conexão poderá prestigiar o fluxo dos dados, assim, por meio da referia lei, ficou especificado os casos que acolherão o princípio da neutralidade de rede.

Por fim, atente-se que nada há de ilícito na comercialização de pacotes de conexão à *Internet* que ordenam os preços conforme a velocidade de acesso ou o volume de dados trafegados. Desse modo, não ofende o princípio da neutralidade de rede, pois não confunde privilégio de acesso a determinadas aplicações ou *sites*.

4 TIPIFICANDO OS CRIMES CIBERNÉTICOS

A legislação brasileira tipificou os crimes cibernéticos antes de instituir as normas gerais para a utilização da Internet no Brasil, que foi iniciada pela Lei nº 9.296, de 24 de julho de 1996, onde regulamentou norma constitucional pressentida no artigo 5º, inciso XII, da Constituição da República Federativa do Brasil, de 1988, no que se refere ao sigilo das conversas telefônicas e de dados, amparo constitucional da pessoa, sendo somente excepcionada por ordem judicial.

Então, foi disciplinada a eventualidade de resolução do Poder Judiciário como possibilidade de violação do sigilo das conversas telefônicas e de dados, desde que existam requisitos legais, principalmente os vestígios de autoria ou participação em delitos, contudo também discorreu de matéria penal, enquadrando-se o autor do crime de obtenção ilegal de comunicações telefônicas, informática ou telemática mediante prisão de dois a quatro anos e multa.

O Código Penal foi alterado quatro anos depois, por determinação da Lei nº 9.983, de 14 de julho de 2000, onde houve a introdução do delito de inclusão de dados enganosos nos sistemas informatizados ou bancos de dados da Administração Pública (artigo 313-A) e também o crime tipificado como modificação ou alteração não autorizada daqueles sistemas (artigo 313-B). No entanto, a Lei nº 11.829, de 25 de novembro de 2008, estabeleceu novo tipo penal no Estatuto da Criança e do Adolescente, penalizando aquele que, de algum modo, publique, através de maneira cibernética, telemática, por vídeo ou outra forma que contenha material pornográfico contendo crianças e adolescentes. (ECA, artigo 241-A).

As formas criminosas na esfera eletrônica ou cibernética são imensuráveis, como por exemplo, a contaminação de mensagem por vírus através do correio eletrônico, pela utilização indevida ou não autorizada de senhas ou numeração do cartão de crédito, falsidade ideológica, insultos nos ambientes digitais, confisco de domínio empresarial, reproduzir *sites* com o intuito de subtrair informações dos usuários, como número dos documentos pessoais, telefone, informações bancárias etc., facilitando negociações comerciais posteriores à utilização de cartão de crédito clonado.

Geralmente os crimes não são tipificados por leis específicas, mas sim articulados dentro das espécies penais costumeiramente expressos no Código Penal brasileiro, como furto, falsa identidade, estelionato, calúnia, difamação e outros.

As ações fraudulentas eletronicamente estão contidas no estudo dos crimes informáticos, por meio das quais se procuram informações diversificadas, como levantamento de bancos de dados, funcionamento de *softwares*, senhas de terceiros e outros, baseando-se, conforme aponta o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (Cert.br)[19]:

> (...) numa mensagem não solicitada que se passa por comunicação de uma instituição conhecida, como um banco, empresa ou site popular e procura induzir usuários ao fornecimento de dados pessoais e financeiros. Inicialmente, este tipo de mensagem induzia o usuário ao acesso a páginas fraudulentas na Internet. Atualmente, o termo também se refere à mensagem que induz o usuário à instalação de códigos maliciosos, além da mensagem que, no próprio conteúdo, apresenta formulários para o preenchimento e envio de dados pessoais e financeiros.

No início dos anos 90 disseminaram-se os atos criminosos através da Internet, originando em longo prazo, reclamações aos órgãos públicos e privados, manifestando a necessidade de uma política de Segurança da Informação. Então, empresas começaram a nortear os usuários dos dispositivos eletrônicos, informando sobre os perigos existentes na sociedade digital que se iniciava, assim houve investimento na formação e promoção de recursos humanos e tecnológicos em políticas corporativas de prevenção de fraudes, determinando aos poucos um aliciamento de que as autoridades policiais e judiciais necessitavam de mais domínio e técnica para evitar o uso impróprio dos instrumentos digitais, pretendendo classificar as ações de investigação, imprescindíveis para o confisco de materiais ilegais que circulam na rede e para o reconhecimento dos infratores virtuais.

O Congresso Nacional aprovou a diligência legislativa onde a punição dos crimes eletrônicos no Brasil foi objetivada pela publicação da Lei nº 12.737, de 30 de novembro de 2012, que se tornou popularmente conhecida como “Lei Carolina Dieckmann”[20], que promoveu alterações no Código Penal brasileiro, tipificando os chamados delitos ou crimes informáticos. A aludida lei incorporou um dispositivo criminal, que assim determina:

---

[19] É responsável por tratar incidentes de segurança em computadores que envolvam redes conectadas à *Internet* no Brasil.

[20] Foi proposta em referência e diante de situação específica experimentada pela atriz Carolina Dieckmann, em maio de 2012, que supostamente foram copiadas de seu computador pessoal, 36 (trinta e seis) fotos em situação íntima e conversas, que acabaram divulgadas na Internet sem autorização.

> Art. 154-A do Código Penal – CP 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 três meses a um ano e multa.

Porém, essa lei avança instituindo que incide na mesma pena quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no artigo 154-A do Código Penal brasileiro. Caso, através de invasão, venha adquirir conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim determinadas por lei, ou controlar remotamente sem autorização o dispositivo invadido, a penalidade será agravada, podendo variar de seis meses a dois anos e multa, caso a conduta não constitua delito mais grave. No entanto, a pena pode ser aumentada de um terço à metade, caso o delito seja praticado contra presidente da República, governadores e prefeitos, presidente do Supremo Tribunal Federal, presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal e dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.

Todavia, a Lei nº 12.737, de 30 de novembro de 2012, concebeu mais uma ampliação ao artigo 266 do Código Penal, quando qualificou o crime de interrupção de serviço telemático ou de informação de utilidade pública, ou dificultar o restabelecimento, inserindo, também, ao artigo 298, parágrafo único, da mesma lei, o crime de falsificação de cartão de crédito ou cartão de débito. A interrupção citada pode ser feita de várias maneiras, como, a destruição física de uma rede ou um ataque virtual às funcionalidades da rede cibernética, sendo crime, portanto, a conduta nomeada como ataque de denegação de serviço. Os delitos virtuais podem ser a oportunidade para a facilitação de outras condutas criminosas mais graves, com objetivos definidos pela norma legal. Nesta situação, o crime virtual não é reputado para fins penais, considerando-se somente para o delito cometido, cuja penalidade é mais grave.

Logo, se o responsável, invadir o dispositivo informático, cometer extorsão contra a vítima, será penalizado pelo último delito, que absorverá o crime eletrônico, julgando não somente o alvo almejado pelo infrator, que é defraudar e também a

penalidade sobreposta a esta atitude, com reclusão, de quatro a dez anos e multa, artigo 158, que é maior do que o delito do artigo 154-A, ambos do Código Penal brasileiro, podendo ser penalizado com detenção de três meses a um ano e multa.

No entanto, futuramente se tornará trivial que sejam publicadas novas leis penais para coibir delitos eletrônicos, diante da grande imaginativa e incessantes transformações que acontecem no universo da tecnologia da informação, cuja aplicabilidade e segurança necessitam estar infindavelmente asseguradas. Possivelmente isto aconteça rapidamente, já que é possível ver insuficiências na norma atual, diante da omissão em determinar penalidades para ataques de sistemas eletrônicos localizados nas nuvens[21], ou seja, no *clouding computing* [22], que não consegue ser qualificada como ataque ao dispositivo informático apontado pelo artigo 154-A do Código Penal, diante da ausência de um *hardware* ou outro meio físico de transferência de dados.

As violações virtuais criam novos métodos e uma enorme evolução da ciência criminalística, para que assim, sejam investigados e penalizados. Esta ciência circunda distintos aspectos do conhecimento técnico-científico, todos destinados para as funções policiais e judiciais na área criminal, procurando evidências materiais do crime, para fins de constituição de prova das infrações penais. A obtenção destas evidências, através dos meios oficiais, pretende alcançar conclusões acerca da prática de uma violação eletrônica, e, se faz pela chamada computação forense, que pode se definir como o uso de métodos científicos na preservação, coleta, validação, identificação, análise, interpretação, documentação e apresentação de evidências digitais. Por sua vez, evidência digital pode ser definida concisamente como qualquer informação que possa ser extraída de um computador ou dispositivo eletrônico.

No Brasil, a previsão é que exista por volta de oito milhões de internautas, e esta quantidade não para de aumentar a cada dia. Conforme um estudo executado pelo *site* alemão *Alldas.de*, o Brasil possui o maior grupo de *hackers* do mundo, e,

---

[21] O armazenamento de dados é feito em serviços que poderão ser acessados de qualquer lugar do mundo, a qualquer hora, não havendo necessidade de instalação de programas ou de armazenar dados. O acesso a programas, serviços e arquivos é remoto, através da *Internet* - daí a alusão à nuvem.

[22] O conceito de “computação em nuvem” refere-se à utilização da memória e da capacidade de armazenamento e cálculo de computadores e servidores compartilhados e interligados por meio da *Internet*, seguindo o princípio da computação em grade.

entre os atos cometidos por eles, são apontados invasões contra o Pentágono, a *Microsoft* e a *International Business Machines (IBM)* americana.

O ambiente virtual proporciona sensação de liberdade plena, facilitando o anonimato, cuja prática é proibida no Brasil, devido ao apontamento que a Constituição da República Federativa do Brasil, de 1988, possui em seu artigo 5º, inciso IV, e assim, proporcionando um mundo onde não existem fronteiras, facilitando a prática de crimes complexos, que demandam uma conclusão vertiginosa e exclusiva, pois o aumento de tais crimes é exatamente relativo aos progressos da tecnologia.

Apesar das ações serem intituladas como crimes virtuais, não existe legislação própria para tipificar tal delito, pois se depara caracterizada em textos legislativos atuais, como o Código Penal e legislação isolada e, diferentemente da afirmação de alguns autores, a utilização das leis que existem direcionadas a essas condutas não é caso de analogia, pois são novas formas delituosas, e novos bens jurídicos carecendo de amparo penal. No entanto, a diferenciação apresenta-se no *modus operandi*, de forma que a utilização das novas tecnologias pelo criminoso reflete precisamente na *Internet*, e gera a necessidade de que os estudiosos e os aplicadores do Direito precisem atualizar suas ideias.

Nesse contexto, os tipos de crimes mais comuns, cometidos através do ambiente virtual, são crimes contra a honra; pornografia infantil; violação dos direitos autorais; perfis falsos; crimes contra a liberdade individual e contra o patrimônio; *fake news*, entre outros.

No ambiente virtual, tornou-se trivial, particularmente em páginas de entretenimento, deparar-se com as *fake news* (notícias falsas) sobre pessoas, seja por preconceito a orientação sexual, raça, religião, etnia etc., ou simplesmente por crueldade. Podem ocorrer também por envio de *e-mail,* especificamente, à pessoa contendo conteúdo caracterizador da injúria, sendo assim consumada a violação. Diante de vários crimes cibernéticos, é muito comum os de calúnia, difamação e injúria, previstos no Código Penal brasileiro como crimes contra a honra, em seus artigos 138 a 145.

Já a caracterização do tipo de crime de pornografia infantil acontece quando o criminoso divulga fotos ou vídeos obscenos de crianças na *Internet*. Essa conduta está contida no Estatuto da Criança e do Adolescente a partir do artigo 240, onde aponta que, ao divulgar conteúdo pornográfico expondo crianças e adolescentes, se configura crime.

Mas, devido à facilidade de acesso que a *Internet* oferece, fica disponível uma infinidade de arquivos e informações que podem ser facilmente copiadas, ainda que, a cópia possa ser feita de forma lícita onde aponta o autor da citação mencionando-o, ou seja, expondo a autoria originária do conteúdo do texto. Acontece que com a *Internet* e a ferramenta copiar e colar, essa prática se tornou muito mais fácil e muitas vezes o indivíduo não tem a intenção de incorrer o plágio, mas pratica devido à falta de conhecimento em determinados assuntos, cometendo assim o crime de violação dos direitos autorais, que se encontra apontado pela Lei nº 9.610, de 19 de fevereiro de 1998.

É muito comum encontrar nas redes sociais perfis falsos, também conhecidos por *fake*, onde pessoas criam identidades falsas, usando fotos de outras pessoas, seja por divertimento ou com o intuito de prejudicar alguém, configurando assim os crimes por falsidade ideológica, bem como existem delitos que são praticados contra a liberdade individual[23], caracterizado pela ameaça, inviolabilidade de correspondência, divulgação de segredos, divulgação de segredos contidos ou não em sistemas de informação ou bancos de dados da Administração Pública. Ainda ocorrem também, o furto, extorsão, dano e estelionato, caracterizando os crimes contra o patrimônio.

Com efeito, a propagação das *fake news* aproveita-se do poder da *Internet* em disseminar informações pelo mundo todo, com o intuito de prejudicar ou beneficiar alguém, as quais podem ser criadas com a finalidade de receberem concordância, através de curtidas ou apenas visualizações das páginas dos *sites*.

Não obstante, o estabelecimento de direitos e deveres cibernéticos, ainda que tardio, é de extrema importância para o combate dos crimes virtuais, especificamente das *fake news*, uma vez que através dessas normas poderá ser vislumbrada, com mais facilidade, o que está sendo violado, estabelecendo, assim, as condutas ilícitas.

---

23 Código Penal brasileiro abrange os artigos 146 a 149 e engloba aqueles crimes que ferem a liberdade legalmente garantida das pessoas em território brasileiro. O atentado à liberdade individual é caracterizado pela perda, ocasionada pela ação de terceiro, do direito de autodeterminação, consubstanciado na máxima "ninguém é obrigado a fazer ou deixar de fazer algo, senão em virtude de lei".

Na verdade, as *fake news* assemelham-se a uma categoria de "imprensa marrom"[24], veiculando intencionalmente conteúdos falsos, com o objetivo de auferir algum tipo de vantagem permanentemente, seja financeira ou não, mediante rendimentos provenientes de anúncios, política ou eleitoral. O Dicionário de Cambridge conceitua as *fake news* como indicação de histórias falsas que, ao preservarem o aspecto de divulgações jornalísticas, são semeadas através da *Internet* ou por outras mídias, sendo naturalmente geradas para induzir opinião política ou para ridicularizar.

A propagação de forma vertiginosa e excessiva das *fake news* estabelece um fenômeno na atualidade, que o Brasil vem procurando criminalizar. Há poucos anos, pessoas físicas e jurídicas recorriam a estratégias de comunicação para suprimir as notícias falsas, através de notas de esclarecimento e contestações. Atualmente, modificaram a estratégia e estão demandando os Tribunais, buscando punição para os responsáveis e restabelecimento dos prejuízos ocasionados à sua imagem.

As *fake news* estão compostas para alcançar alguns propósitos essenciais como: defraudar o leitor, abastecer rumores, distorcer informações verídicas, agredir a honra de personalidades públicas e auferindo, com isso, os resultados desejados. Os prejuízos que estão causando a instituições e direitos ainda não foram equacionados, mas estabelecem fragilidade a diversos preceitos do povo brasileiro, sendo capaz de influenciar resultados de eleições gerais – como ocorreu no pleito norte-americano de 2017 e no Brasil em 2018 – a despeito de o Tribunal Superior Eleitoral prometer um combate sem descanso. Ainda assim, a jurisprudência brasileira, sobre crimes virtuais contra a honra, vem se robustecendo, particularmente no Superior Tribunal de Justiça (STJ).

Na atualidade, resta a consignação do STJ, com base no artigo 70, do Código de Processo Penal brasileiro, que aponta o local a ser considerado da infração como sendo o que foi publicado em conteúdo, independente do local onde fica o provedor. Ainda está em debate a modificação de trecho da Lei nº 12.965, de 23 de abril de 2014, com intuito de que as providências judiciais para remoção de conteúdo sejam

---

[24] É uma expressão de cunho pejorativo, utilizada para se referir a veículos de comunicação (principalmente jornais, mas também revistas e emissoras de rádio e TV) considerados sensacionalistas, ou seja, que buscam elevadas audiências e vendagem através da divulgação exagerada de fatos e acontecimentos, sem compromisso com a autenticidade. Disponível em: < https://pt.wikipedia.org/wiki/Imprensa_marrom>. Acesso em: 10 de nov. de 2018.

concedidas, independentemente da indicação da *URL*[25] que é o endereço de um recurso disponível em uma rede, seja a rede *Internet* ou *Intranet*, e significa em inglês *Uniform Resource Locator*, e em português é conhecido por Localizador Padrão de Recursos.

O Tribunal Regional Federal da 3ª Região, recentemente, penalizou um *blog* por publicar assunto que imputava ao juiz federal Sérgio Moro associação a um partido político e envolvimento no desvio de meio milhão de reais por corrupção ativa, em uma prefeitura do Estado do Paraná. A Justiça identificou que o *blog* – havia replicado reportagem divulgada por outro propagador, substituindo o título – imputando ao magistrado crimes caluniosos, com evidente ultraje à honra.

Entretanto, uma vez que o jornalismo foi capaz de expandir sua tiragem com a edição de notícias sensacionalistas ainda no século dezenove, que não ocorriam divulgações falsas, mas obtinham "cores exageradas", que desvirtuavam a transparência dos acontecimentos; atualmente temos como condutores das notícias falsas o acesso democratizado às redes sociais, a desconcentração na produção de conteúdo e o compartilhamento desengajado, composto por uma multidão de usuários que não levam em conta se a fonte é confiável.

As *fake news* alcançaram ao estágio presente de dispersão com o amparo da tecnologia das plataformas sociais. O algoritmo definido pode constituir o papel do responsável acerca de quais postagens os usuários verão primeiro, essa é uma maneira de acrescer a interatividade dos usuários e oferecer assuntos que possam gerar mais interesse. Existem robôs que são programados para atuarem a partir de determinada palavra-chave e rejeitar as *fake news*. Por conseguinte, as redes sociais promovem a construção da visão de mundo dos usuários, dominando os meios tradicionais de comunicação.

No ano de 2017, pesquisadores da Universidade de São Paulo (USP) produziram um estudo sobre as *fake news,* devido terem sido vítimas delas. Foi realizado pelo grupo de pesquisa Monitor do Debate Político no Meio Digital da USP, onde elaborou um *ranking* falso dos maiores *sites* de *fake news* do Brasil, que obteve mais de duzentos mil compartilhamentos e ainda encontra-se no ar. Esse "viral" em

---

[25] *URL* é um endereço virtual com um caminho que indica onde está o que o usuário procura, e pode ser tanto um arquivo, como uma máquina, uma página, um *site*, uma pasta etc. Também pode ser o *link* ou endereço de um *site*. Um *URL* é composto de um protocolo, que pode ser tanto *HTTP*, que é um protocolo de comunicação, *FTP* que é uma forma rápida de transferir arquivos na *Internet* etc.

inúmeras plataformas acabou por validar a aparência de verdadeira a uma notícia falsa, composta no formato de matéria jornalística, que acabou sendo publicada pela própria comunidade acadêmica como sendo verdadeira.

A consequência deixada pelas *fake news* é a desinformação da população, que acaba rodeada numa desordem acerca do que é falso ou verdadeiro, contribuindo para arruinar a cidadania e o direito de acesso à informação, garantido pela Constituição da República Federativa do Brasil, de 1988, concebendo todo tipo de abusos e inseguranças, com impactos negativos para a vida das pessoas e das instituições.

Portanto, é indispensável que os Órgãos Públicos transmitam uma advertência eficaz contra a sensação de impunidade e anonimato que ainda persiste no ambiente virtual, compreendida equivocadamente por muitos usuários como uma terra sem lei, que a justiça não alcança. Haja vista que, o poder persuasivo das *fake news* é inumerável. Diante disto, se houver demora na retirada do conteúdo falso da *Internet*, poderá trazer graves consequências sociais nos mais variados segmentos. Nem sempre é possível aguardar o trâmite de ação judicial que, geralmente, é lento e insuficiente para alcançar o objetivo pleiteado, quando existe necessidade de retirada imediata de notícia falsa.

Verifica-se, assim, que o elemento “tempo” é de grande importância neste tipo de crime, pois, quanto maior o tempo para a exclusão de uma notícia falsa na *Internet*, maiores serão as consequências para as vítimas, podendo, inclusive, ocasionar danos irreversíveis. Com o estabelecimento da Lei nº 12.965, de 23 de abril de 2014, a responsabilização dos provedores passou a ser norteada por novas regras. O *caput* do artigo 19 está referenciado que o provedor de aplicações de *Internet* só seria responsabilizado civilmente por danos procedentes de conteúdo criado por terceiros após descumprir ordem judicial específica determinando sua retirada

No Brasil ainda não existem projetos de lei realmente efetivos ao combate das *fake news*. É relevante que o norteie-se por países que têm editado legislações com a finalidade de combater as notícias falsas, seguindo os bons exemplos vindos do exterior e estabeleça proposta com multas significativas às redes sociais por falhas na remoção de notícias falsas e determinando outros meios de coerção com a finalidade de combatê-las, visto que a Lei nº 12.965 de 23 de abril de 2014, é insuficiente para tal, conforme ficou evidenciado nas eleições de 2018.

Registre-se, por oportuno, que no ano de 2018, o Congresso Nacional apresentou quatorze projetos de lei, sobre o tema das *fake news*, todos com o intuito de encontrar novos recursos para o problema, através de modernizações legislativas e a acolhimento de práticas saudáveis que venham a contribuir com o aperfeiçoamento do ambiente digital, porém a barreira da morosidade e burocratização nos trâmites, ainda retarda e repele soluções céleres que venham a trazer a segurança necessária ao assunto em debate.

Dentre os projetos em questão, treze tramitam na Câmara dos Deputados, de autoria dos seguintes deputados: Luiz Carlos Hauly, Jorge Côrte Real, Francisco Floriano, Pompeo de Mattos, Carlos Sampaio, Heuler Cruvinel, Celso Rossomanno, Arthur Oliveira Maia, Fábio Trad[26] e um no Senado Federal[27], de autoria do Senador Ciro Nogueira, do Estado do Piauí.

---

[26] Podem-se citar como exemplo os Projetos de Lei nº 6.812/2017; nº 7.604/2017; nº 8.592/2017; nº 9.532/2018; nº 9.533/2018; nº 9.554/2018; nº 9.626/2018; nº 9.647/2018; nº 9.761/2018; nº 9.838/2018; nº 9.884/2018; nº 9.931/2018; nº 9.973/2018.

[27] Projeto de Lei do Senado nº 473/2017, que altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal, para tipificar o crime de divulgação de notícia falsa.

5 CONCLUSÃO

Diante da pesquisa apresentada, reafirmamos que os crimes virtuais se transformaram em uma das piores ameaças aos usuários da rede, pois ainda existe o sentimento de impunidade e a constante garantia de anonimato, que promove a diversificação dos delitos, no ambiente cibernético, não sendo possível contrariar que o universo virtual se tornou em um abrangente espaço para a prática de delitos e assim a presente perspectiva da informatização, é assustadora a quantidade de prejuízos acarretados à intimidade, à honra e à segurança, emanados do descomedido uso incorreto da *Internet*.

Mostramos que a legislação brasileira, como também os meios de proteção atinentes ao direito digital ainda são recentes e pouco eficientes. Não se deve discorrer fantasiosamente como se tudo fosse diversão, pois embora esta tipologia criminosa não motive normalmente acidentes corpóreos, ainda podem ocasionar incidentes de descomunal proporção. Sendo assim, é primordial um diálogo entre os diferentes polos intrinsecamente empenhados na coibição de delitos semelhantes e no resguardo dos direitos historicamente assegurados, fazendo predominar os fundamentos da democracia e do Estado Democrático de Direito.

É indiscutível que as *fake news* necessitam de cuidados por parte da sociedade contemporânea, sobretudo quando abarca disputas eleitorais, devido ao poder persuasivo no pleito e delimitador das eleições. Assim sendo, a legislação e a jurisprudência não podem omitir-se para tais ocorrências, devendo beneficiar o método que melhor se ajuste a elas, procurando decrescer ao máximo os efeitos negativos característicos às *fake news*, uma vez que a Lei nº 12.965, de 23 de abril de 2014, se revela ineficaz para combatê-las com a exatidão que merecem, pois os preceitos consolidados do “mundo virtual” ultrapassaram as fronteiras do Direito trivial, para alçá-lo a rapidez do “tempo”, quanto às inovações tecnológicas, que os fatos sociais e virtuais não conseguem acompanhar, de modo que as leis, regras e normas, ao que parecem, sempre estão aquém do avanço tecnológico.

Por fim, faz-se necessário apontar sugestões que possam ser úteis a ensejar novas linhas de pesquisa acerca do assunto, que são qualificar os profissionais atuantes nas áreas diretamente ligadas aos delitos cibernéticos, equipando-os com instrumentos equivalentes à vertiginosa renovação tecnológica; reconsiderar a Lei nº 12.965, de 23 de abril de 2014 – o Marco Civil da Internet, reconduzindo efetiva-

mente, expandindo seu panorama, alcançando outros delitos virtuais; buscando regimentar a maneira de quebra de sigilo para obtenção da autoria central do delito cibernético sem eclodir a liberdade de expressão e a intimidade pessoal; investir em cursos de segurança digital e/ou estruturas adequadas que beneficiem o Poder Judiciário e os Órgãos de Segurança Pública com conhecimentos técnicos e sistemas tecnológicos de investigação satisfatórios.

REFERÊNCIAS

ABRUSIO, Juliana Canha; BLUM, Renato Ópice. **Crimes eletrônicos**. Disponível em: <http://buscalegis.ufsc.br/arquivos/crimes_eletronicos.htm>. Acesso em: 20 jul. 2018.

AFONSO, Carlos A. Governança da Internet: uma análise no contexto da CMSI. In: AFONSO, Carlos A. (Org). **Governança da Internet:** contexto, impasses e caminhos. Rio de Janeiro: Rits, 2005. Disponível em: <http://www.nupef.org.br/downloads/Livro_Governaca_Internet.pdf>. Acesso em: 30 de maio 2018.

BRASIL. Decreto n.º 4.829, de 03 de setembro de 2003.
Dispõe sobre a criação do Comitê Gestor da Internet no Brasil (CGI.br), sobre o modelo de governança da Internet no Brasil, e dá outras providências. Brasília, 2003. **Presidência da República.** Disponível em: < http://www.planalto.gov.br/ccivil_03/decreto/2003/d4829.htm>. Acesso em: 01 jul. 2018.

_____. Decreto-Lei nº 2.848, de 07 de dezembro de 1940. Código Penal. **Presidência da República**. Disponível em: < http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm>. Acesso em: 03 de maio 2018.

_____. Decreto-Lei nº 3.689, de outubro de 1941. Código de Processo Penal. **Presidência da República**. Disponível em: < http://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del3689.htm>. Acesso em: 03 de maio 2018.

_____. Lei nº 11.829, de 25 de novembro de 2008. Altera a Lei nº 8.069, de 13 de julho de 1990 - Estatuto da Criança e do Adolescente, para aprimorar o combate à produção, venda e distribuição de pornografia infantil, bem como criminalizar a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na internet. Brasília, 2008. **Presidência da República.** Disponível em: < http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2008/Lei/L11829.htm>. Acesso em: 10 de maio 2018.

_____. Lei nº 12.737, de 30 de novembro de 2012. Lei Carolina Dieckmann. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Brasília, 2012. **Presidência da República.** Disponível em: < http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12737.htm>. Acesso em: 25 abr. 2018.

_____. Lei nº 12.965, de 23 de abril de 2014. Marco Civil da Internet. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, 2014. **Presidência da República.** Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 03 abr. 2018.

_____. Lei nº 8.069, de 13 de julho de 1990. Estatuto da Criança e do Adolescente. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Brasília, 1990. **Presidência da República.** Disponível em: < http://www.planalto.gov.br/ccivil_03/LEIS/L8069.htm>. Acesso em: 02 jun. 2018.

_____. Lei nº 9.296, de 24 de julho de 1996. Regulamenta o inciso XII, Parte Final, do artigo 5º da Constituição Federal. Brasília, 1996. **Presidência da República.** Disponível em: < http://www.planalto.gov.br/ccivil_03/LEIS/L9296.htm>. Acesso em: 02 jun. 2018.

_____. Lei nº 9.610, de 19 de fevereiro de 1998. Altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências. Brasília, 1998. **Presidência da República.** Disponível em: < http://www.planalto.gov.br/ccivil_03/LEIS/L9610.htm>. Acesso em: 02 jun. 2018.

_____. Lei nº 9.983, de 14 de julho de 2000. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal e dá outras providências. Brasília, 2000. **Presidência da República.** Disponível em: < http://www.planalto.gov.br/ccivil_03/LEIS/L9983.htm>. Acesso em: 04 de maio 2018.

_____. Tribunal Regional Federal da 3ª Região. **Trf3 condena blogueiro por calúnia e difamação contra Juiz Federal Sérgio Moro.** Disponível em: < http://web.trf3.jus.br/noticias/Noticias/Noticia/Exibir/366648>. Acesso em: 28 de maio 2018.

_____. Decreto Nº 4.829, de 3 de setembro de 2003. Dispõe sobre a criação do Comitê Gestor da Internet no Brasil - CGI.br, sobre o modelo de governança da Internet no Brasil, e dá outras providências. Brasília, 2003. **Presidência da República.** Disponível em: < http://www.planalto.gov.br/Ccivil_03/decreto/2003/D4829.htm>. Acesso em: 25 de maio 2018.

CASTRO, Catarina Sarmento e. **Direito da informática, privacidade e dados pessoais.** Coimbra: Edições Almedina, 2005.

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br). **Cartilha de Segurança para Internet**. 2. ed., São Paulo: Comitê Gestor da Internet no Brasil, 2012.

Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação. CETIC.BR. Indicadores e Estatísticas Tic para o Desenvolvimento. São Paulo, 2013. Disponível em:<https://www.cetic.br/media/docs/publicacoes/2/NICbr_PORTUGUES-web.pdf>. Acesso em: 08 ago. 2018.

Comitê Gestor da Internet no Brasil (CGI.br). *TIC Domicílios 2014*: **Pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros.** Disponível em: <http://www.cgi.br/media/docs/publicacoes/2/TIC_Domicilios_2014_livro_eletronico.pdf>. Acesso em: 05 jul. 2018.

_____. Portaria Interministerial N° 147, de 31 de maio de 1995. Brasília, 1995. **Ministérios da Comunicação e Ciência e Tecnologia.** Disponível em: <https://cgi.br/portarias/numero/147>. Acesso em: 05 jun. 2018.

_____. O CGI.br e o Marco Civil da Internet. [S.l.]: CGI.br, 2013. **Comitê Gestor da Internet no Brasil.** Disponível em: <http://www.cgi.br/publicacao/o-cgi-br-e-o-marco-civil-da-internet/91>. Acesso em: 15 de maio 2018.

_____. Resolução CGI.br/RES/2009/003/P. Princípios para a governança e uso da internet no Brasil, 2009. **Comitê Gestor da Internet no Brasil.** Disponível em: <http://www.cgi.br/resolucoes/documento/2009/003>. Acesso em: 01 jun. 2018.

_____. Resolução CGI.br/RES/2012/005/P. Posicionamento do CGI.br em relação ao Marco Civil da Internet no Brasil, 2012. **Comitê Gestor da Internet no Brasil.** Disponível em: <http://www.cgi.br/resolucoes/documento/2012/005>. Acesso em: 01 ago. 2018.

_____. Resolução CGI.br/RES/2012/010/P. Posicionamento do CGI.br em relação ao parecer final do Deputado Alessandro Molon ao Marco Civil da Internet no Brasil, 2012. **Comitê Gestor da Internet no Brasil.** Disponível em: <http://www.cgi.br/resolucoes/documento/2012/010>. Acesso em: 05 ago. 2018.

_____. **Revista.br.** Ano 04. ed. 5 [S.l.]: CGI.br, 2013c. Disponível em: <https://www.cgi.br/media/docs/publicacoes/3/cgibr-revistabr-ed5.pdf>. Acesso em: 01 jul. 2018.

COPETTI NETO, Alfredo; FISCHER, Ricardo Santi. A natureza dos direitos e das garantias dos usuários de internet: uma abordagem a partir do modelo jurídico garantista. In: LEMOS, Ronaldo; LEITE, George Salomão (Coord.). **Marco Civil da Internet**. São Paulo: Atlas, 2014.

FLORÊNCIO FILHO, Marco Aurélio. *et al*. **Marco civil da internet:** Lei nº 12.965/2014. São Paulo: Revista dos Tribunais, 2014.

FURLANETO NETO, Mário; GUIMARÃES, José Augusto Chaves. Crimes na internet: elementos para uma reflexão sobre a ética informacional. **Revista CEJ.** Ano VII, nº 20, Brasília, 2003.

GETSCHKO, Demi. As origens do Marco Civil da Internet. In: LEMOS, Ronaldo; LEITE, George Salomão (Org.). **Marco Civil da Internet.** São Paulo: Atlas, 2014.

_____. Internet, Mudança ou Transformação? In: **Comitê Gestor da Internet no Brasil.** Pesquisa sobre o Uso das Tecnologias da Informação e da Comunicação. São Paulo: 2009.

GUERRA, Gustavo Rabay. Direito à inviolabilidade e ao sigilo de comunicações privadas armazenadas: um grande salto rumo à proteção judicial da privacidade na rede. In: LEMOS, Ronaldo; LEITE, George Salomão (Coord.). **Marco Civil da Internet.** São Paulo: Atlas, 2014.

HOESCHL, Hugo C.; BARCELLOS, Vânia. **O ciberespaço e o direito.** Disponível em: <www.iadis.net/dl/final_uploads/200405L021.pdf>. Acesso em: 10 set. 2018.

IHERING, Rudolf Von. **A luta pelo direito.** Rio de Janeiro: Forense, 2011.

JESUS, Damásio Evangelista de. **Crimes na Internet.** Disponível em: <http://www.cepad.com.br>. Acesso em: 13 jul. 2018.

JESUS, Damásio Evangelista de; MILAGRE, José Antonio. **Marco Civil da Internet:** Comentários à Lei 12.965/14. São Paulo: Saraiva, 2014.

KERCKHOVE, Rita de Cassia Bittar Van. Advocacia Artificial. In: **Revista Tribuna do Advogado**. Rio de Janeiro: Ordem dos Advogados do Brasil (OAB), 2016. Disponível em: < http://www.oabrj.org.br/materia-tribuna-do-advogado/19303-advocacia-artificial>. Acesso em: 29 out. 2018.

LEONARDI, Marcel. **Responsabilidade civil dos provedores de serviço de internet.** São Paulo: Juarez de Oliveira, 2005. Disponível em: <http://www.fdvdigital.org/rede/index.php/item/responsabilidade-civil-dos-provedores-deservicos-de-internet>. Acesso em: 02 set. 2018.

MAGRANI, Bruno. Novos Desenvolvimentos sobre a regulação da neutralidade de rede. In: **Observatório Brasileiro de Políticas Digitais.** Disponível em: <https://observatoriodainternet.br/post/novos-desenvolvimentos-sobre-a-regulacao-da-neutralidade-de-rede>. Acesso em: 02 out. 2018.

MARTINS. Elaine. **O que é TCP/IP?.** (2012). Disponível em: <http://www.tecmundo.com.br/o-que-e/780-o-que-e-tcp-ip-.htm>. Acesso em: 11 jun. 2018.

MATOS, Miguel. (Coord.). **Relatório sobre os projetos de lei em tramitação no Congresso Nacional.** Brasília: Congresso Nacional. Conselho de Comunicação Social (CCS), 04 de maio de 2018.

MIRANDA, Napoleão. Globalização, soberania nacional e direito internacional. **Revista CEJ,** Brasília, n. 27, p. 86-94, out/dez. 2004. Disponível em: <http://www2.cjf.jus.br/ojs2/index.php/cej/article/viewFile/638/818>. Acesso em: 05 out. 2018.

PINHEIRO, Patrícia Peck. **Direito digital**. 5. ed., São Paulo: Saraiva, 2014.

REALE, Miguel. **Teoria tridimensional do direito.** 5. ed., São Paulo: Saraiva, 1994.

SILVA, Michéle Cândido da. **A territorialidade do ciberespaço.** Disponível em: <http://www.tamandare.g12.br/ciber/territoriovirtual.PDF>. Acesso em: 01 set. 2018.