UniAGES
Centro Universitário Bacharelado em Direito

ADRIANO SOUZA CALASANS

**CRIMES VIRTUAIS E AS FERRAMENTAS JURÍDICAS NO
DIREITO BRASILEIRO**

Paripiranga
2021

ADRIANO SOUZA CALASANS

**CRIMES VIRTUAIS E AS FERRAMENTAS JURÍDICAS NO
DIREITO BRASILEIRO**

Monografia apresentada no curso de graduação do Centro Universitário AGES como um dos pré-requisitos para obtenção do título de bacharel em Direito.

Orientador: Prof. Dr. José Marcelo Domingos de Oliveira

Paripiranga
2021

ADRIANO SOUZA CALASANS

**CRIMES VIRTUAIS E AS FERRAMENTAS JURÍDICAS NO DIREITO
BRASILEIRO**

Monografia apresentada como exigência parcial
para obtenção do título de bacharel em Direito, à
Comissão Julgadora designada pelo colegiado
do curso de graduação do Centro Universitário
AGES.

Paripiranga, _____ de ----- de 2021.

BANCA EXAMINADORA

Prof. José Marcelo Domingos de Oliveira
UniAGES

Prof.^a Monise Gonçalves de Santana
UniAGES

Ao meu pai José Valter Calasans (*in memoriam*)

AGRADECIMENTOS

A Deus, por minha vida, e por me ajudar a vencer todos os entraves e percalços encontrados ao longo do curso.

À minha mãe, Maristela Bispo de Souza Calasans, por sempre me apoiar em todos os momentos de minha vida e, não diferente, durante meu trajeto como acadêmico em Direito.

À minha esposa, Sirley Silva de Oliveira, aos meus amados filhos, Gabriel Oliveira Calasans Rodrigues e Adrielle Silva de Oliveira Calasans, por permanecerem fieis inseparáveis, os quais me permitiram confiar, com maestria, nesse sonho de conclusão de curso.

Aos meus queridos primos, Ricardo Maia Chaves de Souza e a Arleide Chaves de Souza.

Aos meus professores que dedicaram todo seu tempo com afinco, em especial, aos docentes José Marcelo Domingos de Oliveira, Chisttiane Rabelo Britto, Silvia Manoela Santos de Jesus, Nelson Gonçalves Cardoso Filho, Erlon Leal Martins, Elton Assis, Monise Gonçalves de Santana.

Presenti, logo, a importância extraordinária do conhecimento da psicologia popular como fator das criações literária e empreendi colecionar o nosso folclore, de que dantes não tínhamos quase conhecimento algum.

Sílvio Romero

RESUMO

O presente estudo busca compreender as nuances jurídicas dos crimes virtuais, pontuando a internet como ferramenta propulsora de ações ilícitas e anonimização de infratores, de forma a destacar as carências do ordenamento jurídico quanto à proteção da pessoa que utiliza serviços digitais. O objetivo do trabalho, dessa forma, é o de refletir as deficiências e avanços do Direito Brasileiro no que tange à normatização dos serviços digitais, tratamento de dados e proteção do usuário, bem como a investigação, prevenção e repressão de crimes cibernéticos. A metodologia utilizada é a pesquisa de caráter qualitativo, por meio de revisão bibliográfica, através da ponderação de posicionamentos doutrinários e jurisprudência existente acerca da matéria. As conclusões obtidas vão no sentido de apontar a lacuna normativa presente no ordenamento jurídico brasileiro, vez que a norma ainda não acompanhou o fenômeno da digitalização da vida e o fato de a investigação de crimes virtuais ainda carecer de uma força investigativa que tenha à sua disposição um aparato técnico apropriado para os mais variados tipos de ilícito e formas de ocultação nas redes.

PALAVRAS-CHAVE: Crimes Virtuais. Usuários. Segurança Virtual. Proteção Jurídica.

ABSTRACT

This study seeks to understand the legal cybercrimes nuances, pointing the internet as a tool for promoting illicit actions and offenders' anonymization, in order to highlight the shortcomings of the legal system regarding the digital services users' protection. The work objective, therefore, is to reflect about Brazilian Law deficiencies and advances regarding digital services standardization, data processing and user protection, as well as cybercrimes investigation, prevention and repression. The methodology used is a qualitative bibliographical review research, through the consideration of doctrinal positions and existing jurisprudence about the matter. The conclusions reached point to the normative gap present in Brazilian legal system, since the norm has not yet followed the life digitization phenomenon and the fact that the virtual crimes investigation still lacks an investigative force that has at its disposal an appropriate technical apparatus for the most varied types of illicit and ways of concealment in the networks.

KEYWORDS: Virtual Crimes. Users. Virtual Security. Legal Protection.

SUMÁRIO

1 INTRODUÇÃO	10
2 O CIBER ESPAÇO E O DIREITO: desafios jurídicos nas relações virtuais	15
2.1 A internet, sua história, seus dilemas e desafios jurídicos	15
2.2 As relações virtuais, os protocolos e os riscos	20
3 OS ESTADOS NACIONAIS E OS CRIMES VIRTUAIS: Itinerário de uma resposta jurídica	25
3.1 O Estado-Nação, a globalização e a internet.....	25
3.2 Os crimes virtuais e o Estado-Nação	29
4 OS CRIMES VIRTUAIS E O DIREITO BRASILEIRO	35
4.1 A internet, um território sem lei?.....	35
4.2 Os instrumentos de proteção ao usuário dos serviços de digitais	37
4.3 Vazamento de dados e a proteção do Estado.....	39
5 CONSIDERAÇÕES FINAIS	46
REFERÊNCIAS	51

1 INTRODUÇÃO

A prática delituosa é conceituada como a ação/omissão a um imperativo legal, tutelada de forma mais rígida pelo Direito Criminal de um determinado Estado. No caso do Brasil, as agressões a bens jurídicos relevantes têm sua investigação e punição traçadas pelos Código Penal e Código de Processo Penal, bem como por legislação penal extravagante (Lei de Drogas, Lei dos Crimes Hediondos etc.).

A evolução social, pautada sobretudo na redução de distâncias, fomento tecnológico e meios de comunicação instantâneos, além de ter possibilitada a melhoria da qualidade de vida das pessoas e o incremento de muitas atividades profissionais/econômicas, teve igual progressão percebida no campo das atividades criminosas.

A internet, enquanto uma rede que conecta diversos locais de globo, exerce o papel de poderoso instrumento a agentes criminosos, na medida que demanda uma série de regulamentações estatais e preparo técnico/percepção do usuário dos serviços digitais; diante de uma tela eletrônica, rostos e digitais tem seus rastros facilmente ocultados, atrelado à exposição e localização de alvos mais vulneráveis.

O espaço virtual, também conhecido por ciberespaço, constitui uma comunidade online em que sujeitos de diferentes partes do planeta estabelecem contato, cuja segurança apenas será garantida com a instrução do usuário e a devida instalação do aparato protetor nos instrumentos eletrônicos (aparelhos celulares, computador etc.).

Identificar práticas criminosas, infratores e prevenir os danos se torna ainda mais difícil nesse cenário digital, na medida em que não há elementos físicos a serem extraídos; os dados que se tem são deixados nas redes, mas para isso demandam aparato igualmente robusto por parte dos órgãos investigativos e punitivos.

Assim, fortalecer o ordenamento jurídico e adaptar normativos à realidade virtual se torna o desafio da era, uma vez que o uso da internet se massificou por todos os países do globo e a facilidade de contato/acesso às diferentes localidades demanda esforços, conjuntos das autoridades para tornar o ciberespaço um local seguro a seus usuários.

Legislar, fiscalizar e saber utilizar as ferramentas digitais, assim, é um problema

que ultrapassa as fronteiras, mas cujas discussões só terão êxito quando receberem ao menos um tratamento robusto dos operadores do Direito. O desafio, portanto, é adaptar a permanência de textos legais escritos à dinâmica e velocidade das transformações digitais, uma vez que a cada dia se noticiam novos inventos e se identificam novas ações criminosas.

Sabe-se que estratégias limitadas (regulamentos e marcos legais locais, de âmbito nacional), embora significativos, não abarcam a força normativa necessária para a regulamentação de um fenômeno que abrange todo o mundo e cujas proporções vão além das fronteiras nacionais. O potencial de conexão emanado pela internet, a um só tempo, fortalece a ação criminosa e torna ainda mais vulneráveis as suas vítimas.

O fenômeno da globalização apresenta-se como elemento essencial para a compreensão dos desdobramentos do uso da internet e a regulamentação específica para tornar o ciberespaço um ambiente seguro, independentemente da nacionalidade de seus usuários. Além disso, o fortalecimento de tratados e acordos de cooperação internacional correspondem de igual modo às medidas de rastreamento e identificação de ilícitos, reduzindo o campo de atuação dos infratores e tornando sua ação menos frequente.

Aos Estados-Nação, portanto, cabe a iniciativa do fortalecimento do aparato legal e das políticas de segurança sobre os acontecimentos virtuais, ao passo que à coletividade de países, interessa o compartilhamento de estratégias e cooperação para enfrentar o desafio de regulamentar um instrumento de proporções legais como o é a internet.

Embora se sustente que a rede mundial de computadores se caracterize precipuamente por ser “uma terra sem lei”, é importante pontuar que os serviços digitais devem obediência à legislação de cada país onde sejam ofertados, como também cada habitante goza do direito de segurança no mundo físico e no mundo virtual. Logo, a segurança na navegação é elemento essencial à execução dos serviços online.

O tema do presente trabalho monográfico, assim, consiste numa análise acerca das ferramentas jurídicas presentes no ordenamento nacional frente aos crimes virtuais e à carência de dispositivos e políticas públicas voltadas a tornar a navegação na internet mais segura, com ênfase para a investigação e repressão dos ilícitos envolvendo menores (pornografia infantojuvenil).

O problema de pesquisa é apresentado no seguinte questionamento: quais são as atuais estratégias de enfrentamento à pornografia infantojuvenil no meio virtual e de que modo é possível aprimorar as medidas jurídicas voltadas à repressão de tais crimes, considerando a dinâmica dos atos e elementos que compõe o cenário digital?

O objetivo geral do presente trabalho consiste na compreensão da fragilidade do aparato jurídico proposto ao enfrentamento dos crimes virtuais e a urgente necessidade de tornar a lei efetiva e coadunada à velocidade com que os fenômenos ocorrem na internet. Os objetivos específicos, por outro lado, são esses que se seguem: apontar o escopo mundial da prática de pornografia infantojuvenil no espaço virtual, traçar um comparativo entre a proteção jurídica disposta em âmbito nacional e os protocolos internacionais, descrever a segurança no ciberespaço como um direito básico dos usuários das redes sociais e apontar a legislação de proteção de dados como um passo significativo para tornar a internet um local mais seguro aos seus usuários, independentemente de sua nacionalidade.

A escolha do tema justifica-se ante a contemporaneidade do fenômeno da virtualização da vida e a frequência com que se noticiam crimes cometidos por canais digitais, em especial a pornografia infantojuvenil, uma vez que, a partir do emprego de técnicas de ocultação, criminosos conseguem fazer um maior número de vítimas e frustrar a investigação/punição.

A relevância acadêmica se demonstra pela condução de uma discussão jurídica, pontuada na reflexão da tutela do direito à segurança nas redes desde os bancos universitários, partindo de sujeitos nascidos e que vivem na era digital e, porque não ressaltar, vítimas de alguns crimes cometidos pelos canais virtuais, ou que ao menos tenha conhecimento de pessoas próximas que o foram.

A relevância profissional, por outro lado, revela-se na construção de elemento teórico apto a corroborar as discussões jurídicas acerca dos crimes virtuais e a necessidade de fortalecimento dos institutos normativos das redes sociais e apuradores/responsabilizadores de condutas indesejadas/ilícitas; embora não caiba ao Direito o incremento da tecnologia apropriada para identificação de práticas e seus autores, é necessário que as discussões conduzam a um alerta sobre a distância fática entre os usos corretos da internet e o seu emprego como ferramenta criminosa.

A relevância social, por último, é demonstrada no fato de que tal estudo proporciona uma reflexão acerca dos cuidados preventivos a serem tomados quando do uso da internet e a postura ativa quanto à denúncia de condutas criminosas. A

conscientização popular, assim, é um dos intentos quando se discutem os crimes virtuais, ao passo que a cautela se torna o melhor dos caminhos para a consecução da segurança nas redes.

A metodologia empregada é a pesquisa bibliográfica, de caráter qualitativo, com a referência de posicionamentos doutrinários pacíficos, explanação de termos técnicos específicos do âmbito informático, bem como a menção de institutos normativos voltados à tutela da segurança no ciberespaço e a necessidade de aprimorar os instrumentos jurídicos, no âmbito nacional e internacional.

O trabalho monográfico é estruturado em três capítulos, a saber: (1) o ciberespaço e o direito: desafios jurídicos nas relações virtuais, a internet, sua história, seus dilemas e desafios jurídicos; (2) os estados nacionais e os crimes virtuais: itinerário de uma resposta jurídica; (3) os crimes virtuais e o direito brasileiro. O capítulo inicial traz por subtítulos (1.1) a internet, sua história, seus dilemas e desafios jurídicos e (1.2) as relações virtuais, os protocolos e os riscos. O capítulo seguinte apresenta os subtemas (2.1) o Estado-Nação, a globalização e a internet e (2.2) os crimes virtuais e o Estado-Nação. O capítulo final, (3.1) a internet, um território sem lei?, (3.2) os instrumentos de proteção ao usuário dos serviços digitais e (3.3) vazamento de dados e a proteção do Estado.

O primeiro capítulo trata da história da rede mundial de computadores e menciona os principais desafios propostos a uma conexão de escala global quanto à tutela da segurança no mundo virtual, pontuando os riscos e protocolos ora vigentes e a sua adequação à dinamicidade das relações online; o segundo capítulo, ao seu turno, versa sobre as limitações dos ordenamentos jurídicos nacionais e a demanda por institutos normativos que abarquem a amplitude da atuação criminosa pelas conexões virtuais que não encontram limites nas fronteiras físicas. Frise-se que o fenômeno da globalização é a base para tratativas entre nações e os acordos de cooperação uma chave para o enfrentamento de delitos transnacionais. O terceiro capítulo, por fim, compreende alguns instrumentos de resguardo dos usuários da internet e o modo como o Estado exerce a segurança das informações de seus nacionais frente aos serviços que são oferecidos em sua jurisdição; a proteção jurídica dos dados, aliás, é mencionada como evidência da preocupação quanto à regulamentação dos ambientes virtuais, na medida que normas como GDPL e a LGPD complementam-se e agregam valor às relações no cenário mundial, condicionando transações à sua observância.

Assim, a presente monografia constitui instrumento de leitura relevante para a condução de reflexões quanto à regulamentação dos serviços online, em especial, no que se refere à tutela penal e responsabilidade civil de condutas ilícitas praticadas no ciberespaço e a contenção de danos, dado a amplitude da vulnerabilidade das vítimas dos crimes virtuais. Ao tratar da pornografia infantojuvenil e a crescente identificação de casos semelhantes praticados no mundo virtual, insta perceber que a análise de mídias, programas, estratégias de ocultação de rastros e sítios contidos na *deepweb* são ações para as quais apenas a tutela jurídica é insuficiente, demandando esforço internacional para a vigilância nas redes e rastreamento de práticas criminosas e seus autores.

A questão de proteção dos dados, por último, evidencia um despertar internacional no tocante à promoção da segurança nas relações online, de forma que a restrição de fornecimento de serviços em determinado Estado-Nação conduz (quando não obriga) a formulação de normas relativas à proteção de dados em outros países do mundo, dado à globalização das relações comerciais, econômicas, culturais e sociais.

2 O CIBER ESPAÇO E O DIREITO: DESAFIOS JURÍDICOS NAS RELAÇÕES VIRTUAIS

2.1 A internet, sua história, seus dilemas e desafios jurídicos

O primeiro instrumento popular utilizado para acessar a *internet* fora o computador, posteriormente melhorado drasticamente. O chamado “computador da primeira geração”, construído por J.P. Eckert e John Mauchly, em 1943, era apto a solucionar por volta de cinco mil adições e subtrações, bem como, trezentas e cinquenta multiplicações ou cinquenta divisões por segundo, com o propósito de calcular circuitos táticos que requerem conhecimento expressivo em matemática. Nomeado de ENIAC (*Electrical Numerical Integrator and Computer*) foi o primeiro equipamento digital eletrônico com larga escala sob interesses militares.

Naughton (1999) ilustra a *internet* e o seu desenvolvimento como fatos extraordinários devido à capacidade dos seres humanos de superar metas institucionais e barreiras burocráticas. Dessa forma, a liberdade e a cooperação de informação são pertinentes à inovação. Em 1958, a ARPA foi desenvolvida pelo Departamento de Defesa dos Estados Unidos, objetivando a formação de recursos para pesquisa, com o intuito de avançar e superar a tecnologia militar da União Soviética.

Além disso, criaram a *Arpanet*, oriundo de departamentos da ARPA, o IPTO (*Information Processing Techniques Office*), fundado em 1962. Segundo o Psicólogo e cientista da computação no Massachusetts, Joseph Licklider (1962), tinha como intuito estimular a computação interativa através de pesquisas. Soma-se a isso a criação do *Arpanet* como uma maneira de liberar aos centros de computação e grupos de pesquisa da mesma agência, compartilhar on-line tempo de computação.

Outrossim, para subsidiar a montagem de uma rede interativa de computadores, o IPTO teve uma tecnologia revolucionária de transmissão de telecomunicações, a comutação por pacote que foram criadas por Paul Baran, na *Rand Corporation* e por Donald Davies, no *British National Physical Laboratory*.

O objetivo de Baran era criar um projeto de rede de comunicação descentralizada que a *Rand Corporation* fez ao Departamento de Defesa para

construir um sistema militar de comunicações para sobreviver a um ataque nuclear caso houvesse um. Em 1972, a *Arpanet* teve uma demonstração bem-sucedida e teve lugar numa conferência internacional em Washington.

Outro passo foi tornar a conexão da *Arpanet* com outras redes de computadores como a PRNET e a SATNET. Em 1975, ocorreu a transferência da *Arpanet* para a *Defense Communication Agency* (DCA) com o objetivo de fazer com que a comunicação via computadores fosse disponibilizada às forças armadas.

Nesse sentido, a DCA estabeleceu a chamada *Defense Data Network* para que operasse com protocolos TCP/IP. Em 1983, o Departamento de Defesa criou a MILNET que era uma rede independente para usos militares. Contudo, a *Arpanet* tornou-se a ARPA-INTERNET, e foi dedicada a pesquisa. Em 1984, a *National Science Foundation* montou sua própria rede de comunicações a NSFNET.

Em 1988, usou a ARPA-INTERNET como seu *backbone*. Já em fevereiro de 1990, a *Arpanet* foi removida de operação por ser obsoleta. A partir disso, o Governo dos Estados Unidos colocou a sua administração sob poder da *National Science Foundation*, porém, o controle da NSF sob a NET não durou muito e a NSF privatizou a internet.

Assim, na década de 1980, o Departamento de Defesa comercializou a tecnologia da internet e financiou a fabricação de computadores dos Estados Unidos para incluir o TCP/IP. Em 1995, a NSFNET foi extinta e abriu caminho para a operação privada da internet. Outrossim, a internet expandiu rapidamente como uma rede global, tornando-se possível o projeto original da *Arpanet* que se baseava em uma arquitetura de múltiplas camadas, descentralizada e protocolos abertos de comunicação.

No ano de 1977, dois estudantes de Chicago chamados de Ward Christensen e Randy Suess, criaram um programa conhecido como MODEM que, permitia transferir arquivos de um computador a outro, em 1978, criaram outro programa o *Computer Bulletin Board System* que tinha como objetivo armazenar e transmitir mensagens entre computadores e, liberaram os dois programas para a sociedade.

Em 1983, um programador denominado de *Tom Jennings* que trabalhava na Califórnia, criou um programa de BBS, o FIDO, iniciando a FIDONET.

Hodiernamente, a FIDONET é a rede de comunicações mais barata e acessível do mundo. Em 2000, tinha mais de três milhões de usuários e 40.000 nós. Dessa forma, foram grandes influentes na configuração da internet pelo mundo.

Um estudante de 22 anos da Universidade de Helsinki, Linus Torvalds, desenvolveu um sistema operacional chamando LINUX e distribuiu pela internet de forma gratuita, pedindo para os usuários aperfeiçoarem e que enviasse os resultados para a Net. Foi aperfeiçoado por milhares de *hackers* e usuários, sendo o Linux considerado um dos sistemas mais avançados do mundo.

O que ajudou à internet abarcar no mundo foi o surgimento da sigla “*www*”, que foi desenvolvida por um programador inglês que trabalhava no CERN, Tim Berners-Lee. Em suma, a Microsoft descobriu a internet e juntamente com seu software Windows 95, criou seu próprio navegador, o Internet Explorer. A Sun permitiu o software Java que fosse dado na internet.

A Internet nasceu da interseção da *big science*, da cultura libertária e da pesquisa militar, foram esses importantes centros tecnológicos ligados à defesa que se tornaram essenciais entre essas fontes da Internet. As universidades foram importantes ao manter as redes comunitárias, como por exemplo Boulder no Colorado; Electronic Village em Blacksburg; FreeNet em Cleveland; Chetbuco Suite em Halifax, na Nova Escócia.

A Internet teria sido diferente sem a contribuição tecnológica e cultural das redes pioneiras e muito provável que não teria chegado para todo mundo. Como aconteceu a difusão rápida dos protocolos de comunicação entre os computadores, ocorreu devido à distribuição gratuita e aberta de software que se tornaram código de conduta dos hackers devido ao uso cooperativo de instrumentos.

O desenvolvimento dos serviços comerciais teve como influenciadores os movimentos de base da Internet devido à criação de redes autônomas e sistemas de conferência. Por outro lado, desenvolveram por companhias de telecomunicações e computadores, serviços de e-mail (AT&T, MCI, DEC e outras) e redes montadas para uso interno feita por grandes corporações. As companhias como Comuserve, *America On Line* (AOL) e *Prodigy*, ofereceram serviços on-line. Logo, diversos usos de computadores desenvolveram-se do diversificado alternativo de redes da cultura da liberdade.

A partir das diversas contribuições, a Internet teve como característica a abertura, tanto em sua organização social/institucional como na sua arquitetura técnica. Dessa forma, devido à flexibilidade dos protocolos de comunicação, a *Arpanet* e *Backbones* se conectaram a milhares de redes locais. A Arpanet ajudou a futura Internet a vencer o desafio de difícil concordância quanto a um padrão internacional

comum.

Sistemas de correios e telecomunicações e empresas de telecomunicação (PTTs, sigla de Post, Telegraph and Telephone), defendiam um padrão de comunicação conhecido como o X.25 e, não podia se comunicar com o TCP/IP. Os PTTs organizaram transferência de dados em redes públicas que se conectavam nas fronteiras de suas nações. Ademais, o MINITEL e o PTT, basearam-se no princípio de computadores conectados de forma centralizada que seriam controlados pelo governo.

A arquitetura da Internet e a sua abertura foi a fonte do seu desenvolvimento autônomo, pois os usuários tornavam-se produtores da tecnologia e artífices da rede. Assim, como o acréscimo de nós eram simples, o custo era baixo, a UUCP permitiu a conexão entre a USENET e a ARPANET e o simples conhecimento técnico permitia a conexão com a internet.

Alguns hackers comercializaram as ideias de Tim e ganharam muito dinheiro, e Berners-Lee continuou trabalhando no interesse público por opção dele, como diretor do *World Wide Web Consortium (W3C)*. Logo, comportou-se como um *hacker* e ganhou o respeito da sua comunidade e seu lugar na história, a exemplo do caso de Ted Nelson, Douglas Engelbart, Richard Stallman, Linus Torvalds.

Em concordância com Berners Lee (1999), os usuários são os importantes produtores da tecnologia, pois os novos usos da tecnologia e as suas modificações reais são transmitidas de volta ao globo, simultaneamente. Todavia, o tempo demandado pelo aprendizado e uso é abreviado e o resultado disso é que somos envolvidos no processo de aprendizagem através da produção.

Por conseguinte, a internet evoluiu e continua crescendo no mundo, mas para que continue a acontecer, é necessária a arquitetura de interconexão que deve ser ilimitada, distribuída, descentralizada e multidirecional na sua interatividade, devendo ser aberta, distribuída e suscetível de modificações, segundo os protocolos de comunicação. Deste modo, devem ser montadas em conformidade com os princípios às instituições de governo da rede.

Consequentemente, a cultura da internet é a dos seus criadores, assim, caracteriza-se pela cultura hacker, cultura techno meritocrática, cultura comunitária e virtual e a cultura empresarial. Logo, contribuem para a ideologia da liberdade no mundo da Internet. Dessa maneira, a cultura comunitária virtual acrescenta uma dimensão social, tornando a internet um meio de interação social seletiva.

Já a cultura tecno meritocrática é uma cultura *hacker* que incorpora normas e costumes a redes voltadas para projetos tecnológicos. E a cultura empresarial trabalha atrelada às culturas supracitadas, pois difunde práticas da internet como meio de ganhar dinheiro. A distribuição dos códigos-fonte permitiu a qualquer um modificar o código e desenvolver novos programas, criando um espiral de inovação tecnológica.

Para Tuomi (2002), o tecnolites é a abertura determinada por uma cultura tecnomeritocrática, tratando-se de uma crença no bem inerente ao desenvolvimento científico, assim, está numa relação de continuidade com o Iluminismo e a Modernidade. Nessa cultura, proporciona um bem comum para a comunidade de seus descobridores. As características fundamentais dessa tecno meritocracia são as seguintes:

A descoberta tecnológica é o valor supremo. A relevância e a posição relativa da descoberta dependem da contribuição da comunidade dos cientistas/tecnólogos. A relevância da descoberta é determinada pelo exame dos pares entre os integrantes da comunidade, logo, a definição a quem pertence a comunidade é o desempenho individual de cada um e a reputação é central.

As figuras de autoridade coordenam as tarefas e projetos e ao mesmo tempo, controlam recursos, dessa forma, Kahn e Cerf receberam o controle da Arpanet pelo Departamento de Defesa e, para ser respeitado como membro da comunidade e figura de autoridade, o tecnólogo deve agir conforme as normas informais e formais daquela comunidade e não usar recursos comuns para o seu benefício exclusivo.

A comunicação aberta do *software* é a pedra angular de todo o processo, pois resultam da colaboração concatenada e aperfeiçoamentos e sem essa abertura, pessoas da comunidade agiriam de forma individualista e competitiva e o processo de comunicação ficaria lento. Destarte, a cultura da internet enraíza no exercício acadêmico da ciência e da reputação por excelência.

Segundo Levy (2001), a cultura *hacker* é imprescindível na construção da internet, pois se sustenta no ambiente fomentador de inovações tecnológicas mediante a cooperação e a comunicação livre. Nessa consoante, a cultura *hacker* é o conjunto de crenças e valores que foram emergidos das redes de programadores de computador que interagem *on-line*.

O ciberespaço ultrapassa os limites da compreensão de materiais, seres humanos e informações, constituído e habitado por elementos desconhecidos. Um *software* é um conjunto de instruções codificadas com o objetivo de processar uma

tarefa. Os programas são feitos com códigos especializados, termos técnicos que trabalham juntos para que essa linguagem se aproxime da linguagem natural.

A universalização do ciberespaço é a propagação da copresença dos espaços sociais, físico e informacional. Portanto, a palavra virtual tem três sentidos, o primeiro técnico relacionado à informática, corrente e filosófico. Levy (2001) ensina que o ciberespaço é o terreno onde a sociedade contemporânea está funcionando. Para Tuomi (2002), até pouco tempo, as relações sociais eram de modo presente, e hoje, é um plano virtual de encontros.

Por essa via, é notório a modificação das relações na sociedade devido ao atual cenário do ciberespaço e o modo como a humanidade utiliza os recursos existentes nele. Pois, o ciberespaço permitiu a troca de informações (*e-mail*, *e-books*, entre outros) entretenimento (redes sociais, sites) e serviços *on-line* (bancários, vídeos, filmes), além de consolidar as relações privadas econômicas (bolsa de valores, comércio eletrônico).

Porém, o ciberespaço viabiliza ilícitos, criando conflitos e gerando responsabilidade criminais. Dessa forma, as condutas ilícitas são ilimitadas, destacando-se as ofensas direcionadas a minorias, religião, sexo, etnia, idade, exploração sexual, estelionato digital, golpes e fraudes eletrônicas, invasões hackers, *fake news*, entre outros.

Kunrath (2002) leciona que os crimes contra a honra denominados de calúnia, injúria e difamação ocorrem mais por meios virtuais e saem do controle devido à facilidade de disseminação daquilo que foi dito. Outro crime grave é o *bullying*, assédio sexual, assédio moral, ameaça, pedofilia, é bastante visível em redes como *Facebook*, *Instagram*, *Twitter* etc. Deste modo, os delitos digitais são pertinentes ligados ao ciberespaço e as condutas contrárias ao ordenamento jurídico.

2.2 As relações virtuais, os protocolos e os riscos

Os primeiros usuários de computadores criaram relações e comunidades virtuais que moldaram o comportamento e a organização social. Programadores das redes *Usenet News*, *FIDONET* E *BBS*, desenvolveram o envio de mensagens, salas de *chat*, jogos para múltiplos usuários. A *Arpanet* tinha usuários envolvidos nessa

interação social devido à criação das primeiras listas de correspondência a *SF-Lovers*.

Na década de 1980, a maioria dos usuários do UUCP eram membros da cultura *hacker*. Em 1990, quando a *web* virou um sucesso, milhões de usuários levaram para a Net as inovações sociais. No entanto, a contribuição na evolução da internet foi decisiva, como a BBSs foi um sistema orientado para o sexo que liderou por anos uma forma de prática *online*, comercial e privada.

Já por outro lado, o *Institute for Global Communication* (IGC), promoveu causas sociais relevantes como a preservação do meio ambiente e a paz mundial. Dessarte, as comunidades *on-line* originaram-se devido aos movimentos contraculturas e dos modos de vida alternativos. Em 1985, o WELL que foi um dos primeiros sistemas de conferência, iniciou-se na área da Baía de São Francisco por Stewart Brand, biólogo, que criou o Whole Earth Catalog.

À medida que as relações virtuais se expandiam, suas conexões originais com a contracultura enfraqueciam. A maioria dos observadores de Howard Rheingold a Steve Jones, reconhecia a diversidade dos grupos virtuais. Assim, para deleite dos pós-modernos, os MUDs eram o domínio privilegiado para a representação de identidades falsas.

A maioria desses jogadores de MUDs eram adolescentes e estudantes, logo, os usuários se adaptavam às tecnologias para satisfazer seus desejos e interesses. Na França, o Minitel que era burocrático, popularizou-se devido a um de seus sistemas chamado de *Messengeries Roses*, orientadas para o sexo, porém, grupos extremistas de direita como o nazismo e racismo se aproveitaram da flexibilidade da Net e divulgaram suas ideias racistas e nazistas para articularem como o país.

Entretanto, a cacofonia das comunidades virtuais não representa um sistema coerente de normas sociais e valores, como a cultura *hacker*. A primeira característica fundamental dessas comunidades é o valor da comunidade livre. A prática das comunidades virtuais condensa a prática da livre expressão global. Para John Gilmore, essa liberdade expressão foi compartilhada por muitos usuários da Net desde a comunicação on-line.

O segundo valor é a formação autônoma de redes, sendo a possibilidade dada a qualquer indivíduo de encontrar a sua destinação na Net, caso não encontre, poderá criar e divulgar sua própria destinação. A publicação autônoma, auto publicação e auto-organização, e a formação de redes autônomas constituem um padrão de comportamento que circula na internet e chega à sociedade.

O ciberespaço materializado como ferramenta comunicativa/informativa, tornou-se um suporte indispensável da globalização, economia capitalista e um dos vetores de disseminação da democracia, liberdade de expressão e dos valores. Porém, os riscos do ciberespaço estão em alguns indivíduos que criam um espaço de conflitos desenvolvendo a criminalidade virtual, o terrorismo.

Apesar das vantagens, essa tecnologia pode deixar os Estados e a sociedade vulneráveis a ataques. Dessa forma, o ciberespaço apresenta recursos infinitos, porém, permite também a exposição da privacidade das pessoas, ofensas, ataques e agressões. Por exemplo, o *cyberbullying*, uma espécie de violência psicológica e simbólica praticada na internet que tem como intuito difamar, humilhar, agredir verbalmente, denegrindo a imagem da vítima.

No ordenamento jurídico brasileiro, a Lei nº 13.185/2015 foi criada para reprimir atos de intimidação sistemática todo ato de violência física ou psicológica, intencional e repetitivo que ocorre sem motivação evidente, praticado por indivíduo ou grupo, contra uma ou mais pessoas, com o objetivo de intimidá-la ou agredi-la, causando dor e angústia à vítima, em uma relação de desequilíbrio de poder entre as partes envolvidas.

Outro exemplo é a pornografia de vingança conhecida como *revenge porn*, que ocorre quando as fotos digitais, vídeos amadores, ou qualquer material de incitação sexual, de natureza íntima e privada é divulgada no ciberespaço sem o consentimento da vítima. Ocorre sempre ao fim de relacionamentos, pois o ex-parceiro busca vingança pelo término e divulga a vítima nas redes.

Assim, a violação da privacidade, intimidade e da individualidade configura-se a infração dos direitos da personalidade e dos direitos fundamentais definidos pela Constituição. O *revenge porn*, produz resultados desastrosos e está ligada à violência de gênero contra a mulher. O direito à liberdade de expressão está consolidado nos direitos fundamentais.

Contudo, a internet incrementa violações dos direitos infantojuvenis, a partir do aliciamento on-line, onde o pedófilo usa webcams e bate papo para convencer a criança por meio da chantagem a produzir e mandar fotos eróticas de si ou vídeos pornográficos. No caso do abuso, mesmo sendo on-line, o adulto força a criança a participar de jogos sexuais com ele.

Há também a simulação de pornografia com imagens reais, o qual o sujeito pega uma foto comum da vítima e faz uma montagem em situação de abuso, essa

prática ocorre devido ao abusador fantasiar a criança numa situação de sexo ou porque quer usar a imagem como forma de aliciamento, apresentando a fotografia para chantageá-la, ameaça-la e divulgá-la como se fosse verdadeira.

As crianças e os adolescentes não veem os riscos de se expor na internet devido a questão sociocultural, pois, vivemos na época da supervalorização da imagem do corpo e erotização precoce. Mesmo havendo o tabu de não falar sobre a sexualidade infantojuvenil, é notório que a sociedade e a internet introduzem comportamentos sexualizados nelas, antecipando as fases da criança.

Esse fato aumenta a vulnerabilidade das crianças e dos adolescentes devido ao reflexo da sociedade que valoriza o sexo, o corpo, a competição e o individualismo; em suma, as vítimas têm sua exposição ampliada como nunca registrado, dado o fato de que, uma vez compartilhada, determinada mídia (vídeo, imagem), não há como mensurar sua propagação pelo ciberespaço e tampouco conta-se com uma ferramenta eficaz para sua exclusão/remoção das redes sociais. O perigo, portanto, mora justamente no convencimento e estímulo de exposição da vítima que, por se tratar de um ser ainda em formação, atende às vontades/sugestões do interlocutor, concedendo ao criminoso as informações que este almeja.

Verifica-se, assim, que os crimes cibernéticos têm grandes impactos na sociedade, pois o número de pessoas conectadas à rede só aumenta, o que não vem acompanhado da obtenção de informações e práticas de procedimentos seguros na internet e quanto mais indivíduos expostos, mais chances de virem a ser vítimas de cibercriminosos (SILVEIRA, 2015, p. 20).

Para entender o ciberespaço brasileiro, é preciso analisar a infraestrutura necessária, ou seja, a consolidação física da rede. Conforme Stanton e Filippo, foram estruturadas duas grandes fases do ciberespaço brasileiro, o acadêmico e o comercial.

Assim, a iniciativa para criar a rede e a infraestrutura do ciberespaço foi empreendida por instituições públicas não comerciais, sendo elas o Laboratório Nacional de Computação Científica (LNCC) no Rio de Janeiro, a Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP) e o da Universidade Federal do Rio de Janeiro (UFRJ).

Em setembro de 1988, o Laboratório Nacional de Computação Científica no Rio de Janeiro, pertencente ao Conselho Nacional de Desenvolvimento Científico e Tecnológico- CNPq e atualmente subordinado ao Ministério da Ciência e Tecnologia,

foi responsável pelo estabelecimento da primeira conexão das instituições científicas brasileiras à rede BITNET.

Em novembro de 1988, ocorreu uma segunda conexão às redes BITNET e HEPNET pela Fundação de Amparo à Pesquisa do Estado de São Paulo- FAPESP, que foi ligada ao Fermi National Laboratory em Chicago. A UFRJ em maio de 1989 empreendeu a terceira conexão de acesso à rede Bitnet através da UCLA em Los Angeles.

O Ministério de Ciência e Tecnologia MCT, criou um Grupo e Trabalho que tinha como intuito formular um plano de criação de uma rede acadêmica nacional que ficaria encarregada de planejar o ciberespaço brasileiro. Em 1989, foi formulado pelo MCT (SEI), CNPq e a FINEP, o projeto de constituição da Rede Nacional de Pesquisa (RNP), que teve o apoio das instituições estaduais- FAPERJ – Fundação de Amparo à Pesquisa do Estado do Rio de Janeiro; a FAPESP Fundação de Amparo à Pesquisa do Estado de São Paulo; e a FAPERGS – Fundação de Amparo à Pesquisa do Estado do Rio Grande do Sul. Mas, só em 1990 foi efetuado o lançamento formal da RNP.

3 OS ESTADOS NACIONAIS E OS CRIMES VIRTUAIS: Itinerário de uma resposta jurídica

3.1 O Estado-Nação, a globalização e a internet

O ciberespaço não envolve somente materiais, informações e seres humanos, também é constituído e alimentado por corpos estranhos, meio máquinas, meio textos, meio cenários, meio atores: os aplicativos. Um aplicativo, ou *software*, é uma relação ponderadamente organizada de instruções codificadas, com o objetivo de tornar mais fácil para você ou mais processadores executar uma incumbência. Por meio de dois perímetros que dominam, interpretam programas, agem sobre informações, transformam outros programas, fazem redes e computadores funcionarem, operam máquinas físicas, viajam, se reproduzem etc.

Os aplicativos são escritos como um auxílio às linguagens técnicas, combinações personalizadas para escrever instruções para processadores de computador. Existe um vultoso número de dialetos através das quais a programação se processa, com maior ou menor grau de especialização em determinadas tarefas.

Os reiterados programas permitem que o computador forneça serviços específicos a seus usuários. Observa-se algumas espécies tradicionais, isto é, alguns aplicativos calculam ou pagam automaticamente dois funcionários de uma empresa, outros emitem mensagens para seus respectivos consumidores, permitem ou administram estoques, enquanto outros ainda são capazes de controlar máquinas em tempo real conforme informações dispostas por sensores.

Existem sistemas especializados que permitem detectar a origem do pão ou dar conselhos financeiros. Como eu próprio, um editor de texto permite a redação, modificação e organização dos textos. Um gráfico mostra uma tabela com números, me mantém responsável, ajuda a tomar decisões financeiras ou monetárias. Um gerente de bancos de dados permite a formação de mais ou mais bancos de dados, uma localização rápida de informações pertinentes de acordo com várias chaves de pesquisa, bem como uma apresentação de informações de vários ângulos, a partir das necessidades. Um programa gráfico permite que gráficos impecáveis sejam produzidos de forma simples.

Importa ressaltar que *apps*, *softwares* ou programas sofrem mudanças e atualizações contínuas, de forma que um mesmo programa, ontem, possui dados e configurações diversas nos dias de hoje; tais atualizações se dão como um reflexo da própria evolução dos mecanismos, mas também como uma maneira de reforçar sua segurança, considerando que a atividade cibernética de codificação e decodificação está sujeita a invasões, ocultação, sequestro de informações, alterações desautorizadas etc.

Logo, seria forçoso compreender que o fenômeno da atualização também não se refletiria em programas espíões, invasores, *crackers*, *hackers*, *phishing*, dentre outros; as ferramentas para ocultação de IP, perfis falsos, navegação anônima, disponibilização de serviços/produtos ilegais/ilícitos ganham força com um mercado consumidor numeroso que, infelizmente, recebe pouca atenção das autoridades, já que ultrapassam fronteiras e permite que uma determinada ação, num local, gere efeitos em outro local completamente diferente.

O principal acontecimento cultural anunciado para o surgimento do ciberespaço é a desconexão de dois operadores sociais ou máquinas abstratas (muito mais que vaidades) que são universais e totalizadas pelas razões simples: ou o ciberespaço dissolve a pragmática da comunicação que, desde a invenção da escrita, reuniu ou universal e totalidade. Isso remete, de fato, à situação existente antes de ser escrito - mais em outra escala e em outra órbita - acompanhando a interconexão e dinamismo em tempo real das memórias online que se tornam novamente possíveis, para os parceiros de comunicação, compartilhando ou o mesmo contexto, ou hipertexto vivo muito imenso.

Novas tecnologias impactam a vida das pessoas das maneiras mais variadas possíveis: a primeira observação se expressa pela facilitação da vida cotidiana (diminuição da necessidade e da frequência de locomoção, comodidade, lazer, mecanismos de busca, extração de dados e informações, ampliação de serviços e produtos), enquanto que outros aspectos mais específicos são a agilidade comunicativa, armazenamento de dados, promoção de criação, modificação e envio de arquivos, filtragem e tratamento de informações, etc.

O domínio das informações e técnicas de utilização/emprego de programas conduz a uma popularização do saber e das habilidades informáticas, tendo em vista que os instrumentos tecnológicos se encontram à disposição de parcela considerável da população mundial.

Compreende-se, assim, a figura do ciberespaço como uma comunidade virtual que une indivíduos e entidades de diferentes partes do globo, bem como as mais diferentes comunidades do mundo real, aproximando-os e permitindo o diálogo, troca de saberes, informações, dados, fornecimento de serviços, compartilhamento de fatos, opinativos, formando, assim, um espaço *online* de dimensões incalculáveis.

Importa destacar que o ciberespaço, a partir do momento que propicia a formação de uma cibercultura (hábitos e crenças da comunidade virtual), também reflete as relações de violência de domínio do mundo físico, a saber, conflitos advindos da exclusão e manutenção da diversidade cultural diante dos imperialismos político, econômico e midiático. Assim, é possível entender que as normas de controle e de bom convívio nas redes se torna vital para a liberdade e respeito também nas relações *online*.

Gangues políticas inescrupulosas conseguiram arrastar as massas, justificaram (muitas vezes até aos próprios olhos) suas repressões, suas exações, suas loucuras destrutivas por meio de teorias nacionalistas, racistas, imperialistas, religiosas, socialistas, marxistas ou outras mais.

Sem dúvida, essas teorias, religiões, grandes imagens fabricantes de identidades possuem sua importância, mas, de tanto examinar em nome de que os crimes “totalitários” foram cometidos, parecemos esquecer de quais crimes se trata, e de como foram perpetrados (LÉVY, 1999, p. 80).

Mencione-se aqui as técnicas de divulgação e cooptação de apoiadores para ideias, projetos sociais, utopias, interesses econômicos, estratégias de poder, como também sua banalização, despeito e até perseguição, promovida pelos canais digitais, com emprego de sua dinamicidade e de sua capacidade de chegar aos mais variados lugares do mundo. Portanto, verifica-se o perigo oculto na atribuição de um sentido único a técnicas presentes no ciberespaço; programas, ferramentas e instrumentos não guardam, por si só, as mesmas características da pessoa/grupo/entidade que deles faz uso.

Por outro lado, há que se considerar que, para a manutenção de supremacia militar e/ou preservação de poderio informacional/econômico/bélico, vê-se que o desenvolvimento de tecnologias cibernéticas é, em muitas ocasiões, incentivado pelo próprio Estado. A competição econômica, ademais, envolve também interesse de grandes corporações e grupos geopolíticos, de forma que os instrumentos virtuais

respondem a propósitos de seus desenvolvedores, mantendo a autonomia dos usuários em segundo plano.

A internet se torna uma ferramenta valiosa não apenas para interesses de pessoas comuns, mas também de grupos econômicos, corporações, entes públicos e Estados como um todo. Como revela Lévy (2007), é impossível pensar numa realidade de século XXI em que um determinado prestador de serviços ou fornecedor de produtos não tenha, pelo menos, um perfil em rede social para alavancar os rendimentos e notoriedade de seu empreendimento; os órgãos públicos expressam uso voltando à propagandear projetos, políticas e ações, enquanto que representantes e agentes políticos tentam atrair os olhares dos pretensos eleitores acerca de seu perfil e de sua atividade, ações e iniciativas. Os Estados, por fim, utilizam a internet como instrumento fortalecedor de sua autonomia e substrato da segurança de seus interesses e relações no cenário global.

Logo, as oportunidades oferecidas pelo ciberespaço multiplicam-se ante à diversidade de seus usuários, interesses, necessidades e aplicações; cada utilização irá demandar um programa ou *software* distinto, individualmente ou em conjunto com outras ferramentas, o que conduz a uma complexificação dos procedimentos virtuais e a demanda com profissionais que dominem as técnicas de trato do aparato físico e virtual.

Estabeleça-se um comparativo das técnicas informáticas para com outras, igualmente postas como sinais da evolução humana, por exemplo, a agricultura irrigada; esta favoreceu o desenvolvimento das civilizações orientais, acarretando transformações sociopolíticas. De igual forma, o aparato tecnológico revolucionou a relação entre nações e a vivência em sociedade.

O cenário, dado a dimensão que se extrai do ciberespaço, exige ao menos a disposição para coadunar competências, partilhar recursos e construir projetos, uma vez que a manutenção da dinâmica do processo evolutivo das tecnologias trará melhores resultados, ante uma cooperação flexível e transversal; não há espaço para divisões e muros, quando a internet transcende fronteiras.

A apropriação dos canais virtuais guarda em si também uma evolução da humanidade, considerando que tais processos *online* corroboram com a construção de uma inteligência coletiva (domínio de técnicas, aparato ferramental, partilha de dados, informações e seu correspondente tratamento). Há aqui também uma preocupação para com os questionamentos que se surgem relativos às relações de

poder e domínio no ciberespaço; a aceleração do movimento tecnossocial toma a internet como instrumento privilegiado de inteligência coletiva que demanda normatização, consciência, cautela e vigilância.

O compartilhamento de informações e a formação da rede de inteligência coletiva é ilustrada pelo fato de que pesquisadores e estudantes do mundo inteiro se comunicarem, trocaram artigos, arquivos, dados, experiências e observações, promoverem conferências virtuais em atendimento a interesses específicos, dentre outros. A resolução de problemas alavanca o desenvolvimento científico e a colaboração de sujeitos, a partir das técnicas de programação, independentemente de tratar-se o usuário de um especialista em tecnologia ou alguém sem instrução, uma vez que a formação numa área específica não proporciona, por si só, o conhecimento básico para lidar com o ciberespaço.

Verifica-se, assim, a globalização como um fenômeno que une, em seus efeitos, comunidades inteiras, indivíduos, corporações, entidades, grupos econômicos e nações, situando-os num cenário virtual em que passam a compor, observadas suas especificidades, uma comunidade virtual sem limites e sem fronteiras. Na medida que esse fenômeno permitiu o encurtamento de distância e a economia de tempo, é importante observar que o desenvolvimento tecnológico demanda cautela, normatização, cooperação internacional e atualização de instrumentos, para que a navegação se dê num território seguro em que os dados e perfis dos usuários sejam preservados, mantidos a salvo de todo e qualquer ataque ou invasão de mecanismos maliciosos.

3.2 Os crimes virtuais e o Estado-Nação

Atualmente o ordenamento jurídico brasileiro passou por algumas significativas mudanças recentes em função da jurisprudência relacionada ao julgamento de crimes cibernéticos, e aqui especialmente se destaca a aprovação do novo Marco Civil da Internet (MCI) brasileira, sancionado em 23/04/2014, pela Lei nº 12.965/2014. Anunciado por alguns como tendo criado um grande avanço na área de neutralidade da rede, que exige tratamento igualitário a todo conteúdo que trafega na internet, admitidas algumas exceções, o MCI de fato apresentou alguns avanços, diversos dos

quais ainda pendem de devida regulamentação. Contudo, foi duramente criticado por peritos em informática e advogados especialistas em direito digital, em diversos aspectos tais como a guarda de registros (logs) de acesso e privacidade de usuários e liberdade de expressão.

Aqui vale destacar que ainda não está pacificado ou o que deve ocorrer para caracterizar uma violação indeterminada do mecanismo de segurança, conforme definido por nenhum dispositivo legal, visto que é sempre ou o usuário que possui um determinado nível de segurança implementada ou que talvez seja inviável verificar tal violação. Outro acontecimento bastante significativo foi o relatório da CPI dos Crimes Cibernéticos (2016), ou que ratificou a necessidade urgente de investimento na área perimetral com a apresentação de vários projetos de lei, visto que gostaria de encontrar habilitação para alguns crimes, para além de Auxiliar tanto na investigação desses crimes quanto na melhor qualidade de dois entes públicos para tratar desse problema. O investimento nesta capacidade será auxiliado com recursos da Fistel.

Observa-se também que na velocidade da experiência na mudança de dois hábitos da população, em função de dois usos de novas tecnologias, tem trazido um enorme desafio na adaptação e definição de regras de condutas, tantas vezes são usados e explorados por mentes criminosas. De modo diverso, a internet permite novas formas de interação social, além de facilitar a aplicação de golpes e a prática de crimes. Quanto ao resto, Eleutério e Machado (2011) ratificou ou entendeu que, apesar do emprego de computadores não ser novidade, até a data da legislação brasileira não está elaborado e precisa ser revisto, a fim de possibilitar a classificação adequada dos diversos tipos de crimes cibernéticos

Tradicionalmente, as pessoas são forçadas a instalar programas de pesquisa em servidores que monitoram e relatam os momentos em que o arquivo é suspenso, emoldurado ou baixado. Esses programas são baseados em coleções de hash (hashes são pressupostos de um documento que ou deixam se distingue de qualquer outro na internet) e, como tal, são sempre eficazes, dependendo da catalogação prévia de uma imagem de pornografia infantojuvenil.

Isto é ineficaz ou relacionado a situações em que novas imagens não são identificadas pelo programa, devido à ausência do respectivo *hash* catalogado na biblioteca. É imprescindível, portanto, que as forças de justiça busquem alternativas viáveis e que possam ser implementadas rapidamente, tanto em termos de legislação nacional quanto em termos de cooperação internacional efetiva.

Nem o Brasil, nem o problema da pornografia infantojuvenil é muito sério e precisa ser tratado de forma adequada. Embora seja difícil definir ou identificar o problema, é certo que este infortúnio aumentou significativamente com a implantação da Internet, visto que, não em 2009, foi designada como um dos dois crimes mais comuns cometidos na Internet (PINHEIRO, 2009). No entanto, deve-se destacar que a termo pedofilia representa uma doença (OMS, 1993), transtorno mental ou desvio sexual caracterizado pela atração por crianças ou adolescentes, não devendo, portanto, ser confundida com pornografia infantojuvenil.

Enquanto nova demanda, na atualidade, o suspense da pornografia infantojuvenil é identificado de várias maneiras, para além da rapidez na identificação, pode-se mencionar contato com criminosos feito por investigadores. Assim que uma falha for determinada, um pedido obtido por dispositivos eletrônicos para serem apurados.

Um estudo de caso evidencia a existência de mídias de crianças em arquivos pornográficos (PI), ao passo que em relação a adolescentes tal intento é mais complexo, dada a aceleração do seu desenvolvimento. Frequentemente isso é observado em adolescentes do sexo feminino, por vezes, confundidas com adultos.

A técnica MMFF utilizada combina métodos de detecção de pele ou palavras visuais e conceito SentiBank, o qual associa imagens de pele, comparando-as ao vocabulário empregado no PI e rotula alguns sentimentos relativos à exploração das vítimas que aparecem na imagem.

Os sentimentos mais detectados são o medo e a raiva, tendo em contraposição a raridade destes serem identificados em outros tipos de pornografia. Dessa forma, pode-se salvar apenas os arquivos PI existentes e os inéditos. O combate ou o abuso sexual de crianças e adolescentes não se questiona para elencar um dado arquivo como PI, como também para buscar nos locais nos quais são potencialmente tributados.

Em 2013, um estudo analisou o tráfego IP em conexões P2P identificou 1.8 milhões de nós de eMule (no caso do programa de comunicação) que continuam a ter PI, sendo vários arquivos como mídias de PI já identificadas e têm seu *hash* definido por agências de força (HURLEY *et al.*, 2013). Nesse método, pode-se localizar arquivos de *hash* de cabelo PI e cabelo com arquivos relevantes, vez que funcionam somente em material outrora identificado.

Se um arquivo for alterado, não será possível identificá-lo na biblioteca de

hashes. De igual modo, não é possível afirmar que todos os arquivos IP foram catalogados.

Logo, assim como empregando métodos anteriores que vários arquivos PI foram revelados, ainda há carência por novos instrumentos de busca automatizada para continuar com a criação incessante de PI. Assim, como este novo método, os novos arquivos igualmente serão analisados, pois vários deles apresentam PI não catalogado. Ao contrário da velocidade de análise mecânica de cada dois arquivos, esse novo processo resultará em investigações e diminuirá consideravelmente a demora na resolução de casos.

Na necessidade de combater os crimes cibernéticos, principalmente *ransomware*, transita invariavelmente cabelos sujeitos à territorialidade / extraterritorialidade. Apesar de existirem diversos mecanismos de investigação, incluindo colaborações em tempo real, a exemplo do caso do *World Information System (I-24/7)* 18 da Interpol, ou que funciona 24 horas por dia, 7 dias por semana, sabe-se que os cibercriminosos utilizam *hardware* que camufla sua identidade, dificultando a análise de seus vestígios, conforme tópicos anteriores.

Um exemplo importante de toda essa complexidade é que um criminoso em um determinado país pode infectar uma máquina em outro, usando um servidor que está em um terceiro país. Em outra forma de ataque, os criminosos também podem infectar uma determinada máquina.

Percebe-se, dessa forma, que a prática delituosa e a consecução dos efeitos em sua vítima extravasam as fronteiras nacionais, o que desafia a aplicação de normas restritas a um determinado território. A forma como enfrentar crimes praticados num local e vítimas afetadas em outro exige do Direito um esforço transnacional para a identificação de criminosos, repressão de delitos e proteção dos usuários nas redes.

Ressalte-se que, dependendo do caso concreto, tal conduta poderá ultrapassar 2 anos, não mais classificada como de menor potencial ofensivo, submetendo-se à Vara Criminal. O significado da competência será determinado pelo local onde a infração foi consumida, como fulcro e não o art. 70 do Código de Processo Penal, consagrando a teoria do resultado. Ponto importante é a análise da redação contida no art. 5º Código Penal que deve se aplicar ao direito brasileiro, com prejuízo das convenções, tratados e normas da Diretoria Internacional ao crime praticado em território nacional, aderindo também à teoria da territorialidade temperada, em que o

Brasil abre uma lacuna a sua exclusividade em prol da cooperação internacional.

Antes de nos aproximarmos, quantos anos de crimes à distância que começaram em um país e terminaram em outro, tentando-se dá aplicação da norma penal sem espaço, à aplicabilidade do art. 6º Código Penal assoma de forma mais adequada. É considerada praticada ou crime não onde ocorre ou omissão, não total ou parcial, como ocorre ou deveria ser produzida ou resultar, também aderindo à teoria da ubiquidade.

Sabe-se que existem várias possibilidades de invadir e infectar uma máquina, a título de exemplo, mas o usuário executará um *malware* "camuflado" anexado ou seu e-mail (prática descrita como *phishing*) ainda estará configurado ou crime, ante a presença de um vírus de vontade (fraude) que pode enganar criminoso ou usuário, o *malware* instalado vai até burlar os mecanismos de proteção da máquina.

Outro ponto é a finalidade especial do ato descrito não de tipo criminoso: "com o objetivo de obter, adulterar ou destruir dados ou informações com a autorização expressa ou tácita do proprietário do dispositivo". Perceba que não há crime em comentar ao conduzir dois criminosos subsumidos ao tipo criminoso, considerando *ransomware* em sua operação silenciosa, criptografar os arquivos, alterar os dados, empacotar as informações, obtendo em seus servidores de controle e comando, podendo também os destruir, assimilar procurados ou criminosos.

Essa evolução das ameaças gera novos desafios para a segurança de computadores, que pode ser vista como um processo cíclico, o qual começa com a descoberta de novas ameaças. A partir daí, elas são estudadas e, por fim, são desenvolvidas medidas para prevenção. Porém, é um ciclo desbalanceado, pois apenas uma parte das novas ameaças são descobertas e apenas uma parte das ameaças descobertas recebem tratamento a tempo (KAWAKANI, 2014, p. 15).

Percebe-se, assim, que a própria tecnologia coloca à disposição um instrumental de busca e identificação de autores e das práticas delituosas, já que o registro das movimentações no ciberespaço é armazenado num lugar comum. Contudo, é importante destacar que tal intento somente se dá por aprimoramentos constantes na base de conhecimentos técnicos e programas investigativos/detectores, associado à autorização judicial de quebra de sigilo de dados e informações telemáticas, uma vez que a autoridade policial, por si só, não tem a prerrogativa de atentar contra a privacidade alheia, quando os elementos estão resguardados por ato volitivo do seu proprietário.

No final da infração penal, “ou instalar vulnerabilidades para obter vantagem ilícita” é um mero esgotamento, mas também constitui uma finalidade específica de um ataque de *ransomware*. Uma das etapas e a instalação do programa ou que irá modificar e explorar as vulnerabilidades do sistema para a etapa final, obrigam a vítima a pagar um valor, visando a obter um novo ou controlar o seu sistema.

O elemento central não estuda dois crimes ou a teoria do crime e da conduta, para os quais pode ser comissivo ou omissivo, intencional ou culposos. Nenhum campo de conduta, ou Direito Penal pátrio adotou a teoria da ação finalista, elaborada por Welzel. Para esta teoria, uma conduta é um comportamento humano intencional dirigido a um fim. A conduta deve ser definida em lei como crime anterior à sua prática para que possa ser punida pelo Estado, atendendo ao princípio da legalidade inescrutável não inciso XXXIX, do art. 5º, da Constituição Federal, crime segundo ou qualificativo sem lei anterior que o defina ou defina sem pena com prévia cominação legal. Tal princípio também está presente no art. 1º do Código Penal Brasileiro.

Portanto, os crimes cibernéticos são as condutas praticadas através de dispositivos conectados à internet. Não em nível nacional existem dispositivos legais especialmente concebidos para a segurança de dados de computador, como no caso do art. 154-A do Código Penal, acatado pela Lei nº 12.737, de 30 de novembro de 2012 (Lei Carolina Dieckmann) ou que tipifique a conduta de invasão de dispositivo de computador alheio, conectado ou não a rede de computadores, através de violação indecifrável do mecanismo de segurança.

4 OS CRIME VIRTUAIS E O DIREITO BRASILEIRO

4.1 A internet, um território sem lei?

Outrora, na informática, os softwares foram criados e vendidos com códigos fontes, pois não existia muitos computadores o que levava o *hardware* a ter valor agregado, dessa forma, o *software* era livre, havendo a liberdade de uso, disponibilizando os códigos fontes. Além disso, que se adquira o equipamento que possui um determinado *software* tem total liberdade para fazer alterações em seu próprio benefício, sendo ainda possível estudar ou código-fonte para desenvolver um novo *software* compatível.

Não terminou dois anos 70, com o crescimento das indústrias de *hardware* e *software*, o surgimento de um conceito de “*software* proprietário”, modalidade de *marketing* a qual o comprador do *software* não tinha acesso direto aos códigos-fonte. O destino que ou aumento dá a concorrência fez como o setor em busca de mecanismos de proteção de propriedade intelectual, tais como autores diretos e patentes de proteção ou código-fonte.

Assim, ao adquirir um “*software* proprietário”, o usuário recebe uma licença de uso, uma permissão para uso, não exclusivamente. Dessa forma, mesmo ao adquirir uma cópia original, o usuário não se torna um doador de software, portanto, acessa o código-fonte para desenvolver melhorias em seu próprio benefício, muito menos para criar um *software* compatível.

De igual modo ou adquirente, não é possível ou direcionada a realização de exploração econômica do software (cópia e revenda, aluguel etc.), salvo autorização expressa do titular da obra prevista ou do contrato de licença de uso. Além disso, é ilegal à reprodução não autorizada de *software*, inclusive deixando-o para uso interno de empresas, não está sujeito à respectiva licença de uso.

Apesar disso, é corriqueira no Brasil, a pirataria corporativa. Nesses casos, pode-se buscar e apreender softwares irregulares, flagrantes prisões e abertura de processos cíveis e criminais, por uso indevido de propriedade intelectual e sonegação fiscal.

Existem duas dimensões da liberdade de expressão, como reverbera Denny

(2016), relativo à condição direta do município, de não estar protegida pelo estado de atuação, de ser vedada por censura, por não poder analisar previamente dois conteúdos disponibilizados na Internet. Nenhum meio digital pode assumir a função de censor ou código de programa de computador, podendo bloquear conteúdo, condicionar o acesso, tanto em pequena como em grande escala, ao exemplo do conteúdo erótico que costuma ser bloqueado nos países islâmicos.

Em concordância com Dinamarco (2006), a jurisdição é a função do Estado para que aplique a Lei e administre a Justiça, logo, a internet não possui fronteiras. Para La Chapelle e Fehlinger (2016), devem-se seguir esses critérios sob a lei aplicável na obtenção de informações digitais, a lei do local onde estão os servidores que armazenam os dados; a lei do local de incorporação da empresa que presta o serviço; a lei do local dos registradores de onde o domínio foi registrado.

Logo, as empresas de internet deverão respeitar os parâmetros legais ao fornecerem os dados digitais solicitados. O Processo Produtivo Básico (PPB) foi definido pela Lei nº 8.387, de 30 de dezembro de 1991, como “ou conjunto mínimo de operações, não estabelecimento fabril, que caracteriza a efetiva industrialização de determinado produto”. O PPB consiste em etapas mínimas de fabricação necessárias para que as empresas cumpram para fabricar determinado produto, a título de compensação por benefícios fiscais.

O PPB é adequado para um produto específico e não para empresas. Os PPBs são constituídos através de Portais Interministeriais, assimilados pelos Ministros do Desenvolvimento, Indústria e Comércio Exterior (MDIC) e da Ciência, Tecnologia e Inovação (MCTI). Não discriminação no tráfego de pacote de dados A neutralidade da rede fundamenta esse ponto. O artigo 9º da Lei 12.965/14 (Marco Civil) exige tratamento isonômico para preservar o caráter público e irrestrito do acesso à internet e os fundamentos, princípios e objetivos do uso da internet no país.

Em outras palavras, nenhum provedor de aplicação ou de conexão poderá favorecer algum tipo de serviço para algumas pessoas em detrimento do acesso de internet de outras. O tráfego de dados poderá ganhar discriminação, ou seja, maior atenção, de forma excepcional em casos indispensáveis ou para priorização de serviços de emergência.

A publicização da pornografia infantojuvenil se dá frequentemente através de e-mails e conexões que utilizam compartilhamento P2P, como eMule, Gnutella e *Ares Galaxy* (LIBERATORE; LEVINE; SHIELDS, 2010). Neste caso, estas ferramentas de

partilha eliminarão a obrigatoriedade de servidores, fazendo com que os computadores realizem ligações interligadas, vez que a conexão entre duas máquinas é direta a todos nós, atribuindo-nos responsabilidades equivalentes. Assim, o método de conferir arquivos armazenados em um servidor tornou-se ineficaz.

4.2 Os instrumentos de proteção ao usuário dos serviços de digitais

Dessa forma, o governo disponibilizava informações de caráter não sigiloso online, pois os cidadãos eram livres para expressar opiniões e até mesmo ficar atentos e vigiar, o governo devido ao povo que é soberano. Todos os governos do mundo utilizam a internet. No ano de 2000, os cidadãos britânicos poderiam escrever via website para parlamentares.

Conforme Coleman, Taylor, e Van den Donk, (1999) e Docter, Dutton e Elberse (1999), elaboraram um estudo sobre o uso da internet da OECD devido à política tradicional e estudaram também, a DNET. Em 1998, na Califórnia, houve a eleição para governador e o *Public Policy Institute of California*, elaborou uma pesquisa de opinião dos cidadãos e 54% desses eleitores afirmaram que os governantes não se importavam com o que as pessoas pensavam a respeito deles.

Logo, os indivíduos não querem mais gastar energia fazendo indagações aos políticos pois, acreditam que eles só se importam caso haja interesse pessoal ou quando está em época de eleição. Porém, segundo Castells, (1997) a internet é importante para a nova dinâmica política chamada de política informacional. A influência do comportamento eleitoral é devido a política da mídia e ao acesso do governo perante a sociedade.

Para Rose-Ackerman (1999) e Thompson (2000), os indivíduos não confiam em programas, mas sim em pessoas e a política de mídia foi criada para personalizar e organizar a imagem do candidato, dessa forma, pode ocorrer também o vazamento de informações para prejudicar o adversário e prejudicar a imagem para que não seja eleito.

Ademais, a internet é um canal de comunicação para ativistas políticos, jornalistas e cidadãos com o intuito de espalhar informações e rumores políticos, mas para não correr riscos na internet, deve-se saber que, tudo que ocorre nela não é

apenas virtual e sim real pois, as pessoas que interagem são reais. Dessa forma, o risco que passa no dia a dia, poderá ficar exposto na internet já que poderá também sofrer golpes, portanto, para se prevenir, não passe informações pessoais para estranhos, utilizando sempre a criptografia, privacidade e segurança na internet.

Devendo analisar os mecanismos de segurança como a identificação que permite ao usuário que se identifique; autenticação para verificar se aquela pessoa é o que realmente diz ser; integridade para que proteja as informações; confidencialidade que protege o acesso não autorizado. Contudo, a política de segurança é o direito e responsabilidade de cada ser relacionado à segurança dos recursos computacionais, considerado um importante mecanismo de segurança para as empresas e usuários.

Logo, não é admissível divulgações de informações confidenciais; compartilhamento de senhas; mensagens contendo spam; calúnia, difamação ou ameaça; cópia de materiais que contém direitos autorais e; ataque a outros computadores.

A Internet não requer apenas novas soluções jurídicas para novos problemas; também afeta a forma como os problemas e as soluções jurídicas devem ser analisados. Ao romper com os paradigmas jurídicos tradicionais e desafiar os mecanismos convencionais de tutela, a Rede representa dois grandes objetos de estudo, dois professores preocupados com esta nova realidade social. A principal dificuldade, portanto, é apresentar propostas de soluções eficientes para os problemas práticos que surgem, reconhecendo as limitações do ordenamento jurídico.

Uma proposta a ser mencionada, oportunamente, é a elaboração de instrumentos jurídicos de caráter internacional e acordos de cooperação para normatizar a conexão virtual entre países, a fiscalização, vigilância e apuração de práticas delituosas que superam os limites entre nações. Sem dúvida, normas de caráter global propiciam a unificação da tutela jurídica dos usuários das redes e conferem menos riscos de os criminosos escaparem à responsabilização, dado a redução de atos burocráticos e do tempo de investigação.

Para isso, devem ser criadas formulações jurídicas, devem ser encontrados outros equilíbrios, não dois contratos, a família, a empresa e o próprio Estado, para que ou não tenha diretamente uma espécie de camisola da força que requeira o emprego de dádiva. Novas técnicas e que prevaleça um clima de cooperação dominado pela ética.

Por ser tema de interesse global, o funcionamento da internet demanda preparo técnico dos seus usuários, mudança comportamental quanto à exposição de dados e à utilização de instrumentos que possam assegurar a integridade dos aparelhos/máquinas, uma vez que grande parte dos ilícitos identificados são concluídos graças à imperícia e vulnerabilidade de suas vítimas (ausência de instrução mínima, cautela, uso de antivírus etc.).

É claro que tentar aplicar as regras formais existentes para novas tecnologias pode funcionar ocasionalmente, mas não há razão para provar que funcionará sistematicamente. Além disso, dois problemas traçados pelas novas tecnologias requerem a aplicação de princípios gerais em vez de regras específicas. Apresentar propostas de soluções eficientes para a proteção da privacidade na área da Internet e, sem dúvida, tarefa desafiadora, dada uma tarefa qualificada intérprete do Direito não pode ser evitado, sob pena de perpetuar situações injustas. Isso ou não.

Para tanto, entende-se que não basta uma simples análise do material direto e do processo direto, mas também da jurisprudência brasileira e estrangeira. Ou abordagem meramente enciclopédica inútil. Estamos principalmente interessados em oferecer propostas para problemas específicos, chamando a atenção para a necessidade urgente de compreensão de dois novos fenômenos, fugindo do lugar comum que entende nada existir de novo sobre o sol. Percebe-se, nesta obra, um grande número de referências à doutrina.

4.3 Vazamento de dados e a proteção do Estado

Contudo, no mundo virtual ocorre muito o vazamento de dados e, os golpistas se aproveitam e roubam a identidade do usuário para aplicar golpes que poderá ser considerado como crime contra a fé pública. Com essa tecnologia, pode-se violar a privacidade devido à possibilidade de relacionar indivíduos com processos específicos de comunicação em contextos institucionais específicos.

Para Lawrence Lessig, a transformação da liberdade e da privacidade na internet é um resultado de sua comercialização direta. O desenvolvimento de novas arquiteturas de *software* foi devido à necessária confirmação de comunicação na internet para ganhar dinheiro e permitir o controle da comunicação por computador.

A felicidade com a liberdade trazida pela internet foi grande que esqueceram a persistência de vigilância no ambiente como o local de trabalho. À medida que os trabalhadores se tornam dependentes da interconexão por computador em sua atividade, a maioria das empresas decidiram que têm o direito de monitorar os seus funcionários.

Programas como *Gatekeeper* exibem no servidor toda a atividade de internet que tem em qualquer organização filiada a ele. Nos Estados Unidos, 92% dos websites coletam dados pessoais dos seus usuários e os processam segundo interesses comerciais. Porém, as companhias alegam que usam os dados de forma agregada para perfis de *marketing*.

Na União Europeia, ocorreu uma ação governamental em favor da defesa do consumidor e levou à elaboração de uma lei de privacidade sob a qual as companhias não podem usar os dados de seus compradores sem o consentimento deles.

Por fim, o problema passa a ser a troca de dados pelo acesso a *websites*, pois a maioria dos consumidores renunciam a seus direitos à privacidade para usar a internet. Os códigos maliciosos conhecido como *malware*, são programas com a finalidade de desenvolver ações e atividades maliciosas para comprometer e vaziar informações do computador da vítima.

A exploração de grupos são vulneráveis, execução de mídia infectadas, web maliciosas. O Estado criou o Marco Civil da Internet para punir os usuários que utilizam de má-fé os provedores, Lei Nº 12.965/2014. Logo, a privacidade é protegida pela Constituição e Marco Civil com a finalidade de proteger os usuários, pois a identidade e individualidade são desenvolvidas pelas informações pessoais.

Celant e Meneghetti (2014) tratam do impacto do Marco Civil da Internet como um avanço normativo no Brasil, demonstrando que a inovação legislativa pôs fim a uma lacuna que expunha a segurança dos usuários da internet. Nascia, naquele momento histórico, o marco inicial do direito digital no ordenamento jurídico nacional, ocasião seguida pela elaboração de artigos e estudos quanto ao impacto da legislação, os avanços trazidos e se, de fato, o texto normativo alcançou a garantia de segurança que dele se esperava.

O Marco Civil da Internet não resolve todo a complexa problemática envolvendo os direitos na internet, mas é um primeiro passo da legislação brasileira, o início de uma busca de regularização do uso dessa ferramenta revolucionária com o objetivo de se proteger os direitos e garantias de todos os indivíduos dentro do eterno conflito ente liberdade e controle (CELANT e

MENEGHETTI, 2014, p. 14).

Diante o artigo 4º, inciso IV da Lei de Acesso à Informação, relaciona a pessoa natural identificável, além disso, pequenas informações aparentemente irrelevantes podem formar um mosaico da personalidade da pessoa, comprometendo inclusive a segurança da informação, facilitando a descoberta de senhas. A coleta de dados pessoais passou a ser rotineira e virou forma de remunerar o emprego de programas ditos gratuitos que são, na verdade, pagos via cessão de dados pessoais.

Enquanto nova demanda, na atualidade, o suspense da pornografia infantojuvenil é identificado de várias maneiras, para além da rapidez na identificação, pode-se mencionar contato com criminosos feito por investigadores. Assim que uma falha for determinada, um pedido obtido por dispositivos eletrônicos para serem apurados.

Um estudo de caso evidencia a existência de mídias de crianças em arquivos pornográficos (PI), ao passo que em relação a adolescentes, tal intento é mais complexo, dada a aceleração do seu desenvolvimento. Frequentemente isso é observado em adolescentes do sexo feminino, por vezes, confundidas com adultos. O combate ou o abuso sexual de crianças e adolescentes não se questiona para elencar um dado arquivo como PI, como também para buscar nos locais nos quais são potencialmente tributados. Um estudo de 2013 que analisa o tráfego IP em conexões P2P (HURLEY et al., 2013) identificou 1.8 milhões de nós de eMule (no caso do programa de comunicação) que continuam a ter PI, sendo vários arquivos como mídias de PI já identificadas e têm seu *hash* definido por agências de força.

Uma soberania é possível como característica ou ser una (inadmissível à coexistência com o mesmo Estado de duas soberanias), indivisível (aplica-se à universalidade de dois átomos ou nenhum Estado, sendo inadmissível a existência de partes separadas da mesma soberania), inalienável (seu titular desaparece quando ficando se ela) e imprescritível (impossível por um certo tempo, aspira à existência permanente). Em qualquer caso, levando-se em conta as características de soberania, e inadmissível que empresa estrangeira que tenha subsidiária, ou venha a prestar serviços no Brasil, submeta apenas parte da soberania nacional: concorda com a submissão de legislação comercial ou brasileira fiscal, portanto, favor não atender às decisões do Poder Judiciário brasileiro para a prestação de informações telemáticas.

A internet não tem fronteiras e, de igual modo, foi arquitetada para que seja, a princípio, acessada de qualquer parte do mundo. Isso significa a formação de uma realidade virtual nas barreiras físicas de delimitação territorial de dois Estados. À medida que as relações humanas se multiplicam, esta ferramenta, que, criada para ser global, esbarra as diferenças culturais refletidas em diferentes legislações. Ou o mesmo conteúdo pode ser tratado de maneira diferente em diferentes países e ser tratado como legal ou ilegal. Não que se trate de crimes reais ou virtuosos que expõem evidências digitais, a investigação torna-se mais complexa, já que se torna mais difícil especificar o local onde provavelmente serão coletadas.

Embora a internet pareça ser uma rede etérea, seu funcionamento depende de uma infraestrutura real. Além disso, para acessar essa comunidade virtual, são necessários provedores de conexão de rede que atribuem ao usuário um número IP (Internet Protocol) por meio do qual passa a navegar fora do ciberespaço. Ou conteúdos a serem acessados ou para as plataformas que permitem a produção de conteúdo próprio do usuário, inclusive mensagens de e-mail ou outros meios de comunicação pela internet, dependendo da estrutura disponibilizada pelos provedores de aplicativos da internet.

O correto funcionamento da rede obedece a critérios matemáticos de organização que permitem a fluência da estrutura. Isso significa que as empresas provedoras de internet determinam as informações a respeito dos passes que os usuários podem usar para acessar a rede: acessos, postagens e comunicações. São essas informações que geralmente permitem, de forma precisa, desvendar um crime cibernético ou obter uma prova digital para elucidar um crime real. Ou que você esteja atordoado ou o mundo jurídico obtendo tais informações, dadas que consubstanciam a prova digital.

A Convenção de Budapeste é o tratado internacional sobre crimes cibernéticos, assinado no Conselho Europeu que visa harmonizar a legislação penal e processual penal, a fim de permitir a cooperação para a obtenção de dados digitais. Foi assinado em 23 de novembro de 2001 e aberto à aceitação e ratificação de outros dois países, tendo sido aprovado por 52 signatários.

O Brasil não é signatário da Convenção de Budapeste, mas por ser o único tratado existente sobre crimes cibernéticos, é modelo e parâmetro para as demais legislações. Não que se trate da preservação e captação de provas virtuais, a Convenção de Budapeste determina que haja preservação de dados, quando

necessária, com prazo de 90 (noventa) dias, prorrogado por igual período.

Fato preocupante é a ausência do Estado Brasileiro na aludida convenção, considerando o grau de participação do país do cenário mundial e o quantitativo populacional que utiliza a internet, seja para interesses pessoais ou profissionais. Logo, percebe-se que a mera existência de uma norma não supre a tutela internacional da segurança do usuário na internet, pois a questão da soberania das nações exige a concordância do Estado em recepcionar em seu ordenamento interno a norma de caráter internacional. O Brasil, assim, apresenta mais uma fragilidade no que se refere à segurança no ciberespaço.

Alcançar a efetividade jurídica e a proteção das garantias às quais se propõe a tutelar, demanda do Estado um posicionamento proativo na discussão de projetos voltados à evolução da tecnologia da comunicação em face da virtualização do direito, que não deve ser unicamente observado pelos tribunais, mas como por todo conjunto estatal tendo em vista a preservação do cidadão brasileiro frente à questões de risco no ciberespaço (ROCHA, 2017, p. 29).

Para a aplicação do Direito Penal, ou seja, o Estado brasileiro que possuir o *jus puniendi* adotou, como regra ou princípio da territorialidade, nos termos do referido art. 5º do Código Penal, sem prejuízo da incidência de outros princípios nos casos, o disposto no art. 7º, inciso II, do mesmo diploma legal. E, para a definição do lugar do crime, opta o criminal legislador pela Adoção do Princípio da Ubiquidade (art. 6º do CP), afirmando que se considera prática ou crime “nenhum local onde ocorra ou omissão, não todos ou em Parte, bem como onde produz ou deve produzir ou resultar”.

Dá uma análise dos dois artigos acima citados, inferindo que, na prática de crimes pela internet, ou crime em território nacional, torna-se totalmente irrelevante para a aplicação do direito penal ou local em que se baseia a sede da empresa prestadora do serviço de Internet ou onde se baseia a informação telemática. Portanto, se trata de crime cibernético ou brasileiro, ficará sujeito à jurisdição brasileira, cabendo ao Estado investigar e reprimir a conduta criminosa praticada e fazer cumprir as decisões proferidas pelo tribunal brasileiro para efetiva celeridade do crime, em necessidade de cooperação internacional ou cumprimento da decisão.

Os serviços prestados pela web são considerados relações de consumo, bem como o utilizador de dois serviços de Internet que cumpram a definição de “consumidor” e os prestadores de serviços e ligação à Internet, não o significado de

“fornecedor”. art. 2º e 3º, do Código de Defesa do Consumidor. Caso contrário, nas relações de consumo derivadas de serviços de internet prestados por empresas nacionais ou estrangeiras no Brasil, há uma responsabilidade subsidiária entre as sociedades controladoras e controladas, com o objetivo de resguardar os direitos diretos do consumidor, usuário da internet (art. 28, § 2º, CDC).

Os tribunais que você tem aplicado ou entendendo que há uma responsabilidade subsidiária, e da mesma solidária, entre as empresas controladoras e controladas, em situações que envolvem responsabilidade civil de empresas prestadoras de serviços de Internet, quando houver dano causado por mais prestação de serviço ou dano causado à Outrem através da Internet.

Segundo Bruno Pinto Coratto:

[...] em tese, a empresa não pode ser responsabilizada objetivamente por danos – morais ou materiais-, causados pela má utilização das ferramentas que disponibiliza. Isso porque os provedores não exercem um controle prévio às publicações de seus usuários, sob pena de inviabilizarem a postagem de informações em tempo real, um dos maiores atrativos da internet. Além disso, não parece aplicável a teoria do risco, uma vez que a prática de ilícitos por parte dos usuários de redes sociais é situação imprevisível, e não constitui risco inerente à atividade dos provedores (CORATTO, 2013, p.10).

A imprevisibilidade das práticas delituosas nas redes origina-se da forma instantânea com que se dá os fatos virtuais; sem dúvida, por ser este o ponto de maior fidelidade dos usuários da internet, é ela ao mesmo tempo, o fato que mais expõe as vítimas. Compreende-se, dessa forma, que é necessária a formulação de ferramentas que possam acompanhar a agilidade dessas ações.

Doutrina e jurisprudência reconhecem a necessária proteção ou jurisdição contra práticas comerciais abusivas, exercidas em economias globalizadas, conforme demonstrado por diversas legislações. Ou, ao mesmo tempo, poderá ser informado de determinadas decisões judiciais norte-americanas, pois se preocupará em analisar e compreender a transformação das instituições jurídicas diante de dois avanços tecnológicos, ponto fundamental para se chegar a soluções adequadas aos problemas delineados pela Internet.

A inovação apresentada no campo da jurisprudência, todavia, não é suficiente para a garantia da segurança aos usuários da rede mundial de computadores; é necessário um esforço de demais esferas do poder político, a saber, as entidades legislativas e executivas. Portanto, a elaboração de leis modernas e contemporâneas

à evolução dos mecanismos digitais e o aparato tecnológico à disposição das políticas públicas de segurança são cruciais para o enfrentamento dos crimes virtuais. De nada adianta, por exemplo, uma legislação atualizada, sem que a polícia tenha suporte técnico para a busca de informações ocultas na rede.

Essa grande experiência jurídica para lidar com problemas relacionados à Internet tem sido explicada, em parte, em razão de que tanto a Rede quanto suas principais inovações foram - e ainda são - concebidas, desenvolvidas e utilizadas nos Estados Unidos, fazendo como seu sistema. Análise certos problemas antes que eles ocorram em outras nações. Daí não decorre, porém, o fato de todas as soluções pelos abastados são recomendadas para o ordenamento jurídico brasileiro.

5 CONSIDERAÇÕES FINAIS

O presente trabalho monográfico versou sobre a tutela jurídica conferida à segurança do usuário na internet e a dimensão dos instrumentos normativos ante à prática de crimes no cenário virtual, considerando as proporções de fatos, a vulnerabilidade das vítimas e a diversidade de estratégias e programas de ocultação de rastros e anonimização dos criminosos.

O intuito do estudo é situar a internet enquanto uma ferramenta que revolucionou as relações pessoais e institucionais numa escala global; nunca antes havia sido tão rápido e fácil contatar simultaneamente pessoas de diferentes partes do globo, trocar informações e controlar em tempo real aparelhos, desconsiderando fronteiras e limitações físicas.

Há que se pontuar que a mesma proporção de comodidades trazidas pela rede mundial de computadores também brindou uma nova preocupação, uma vez que a atividade delituosa também arvoreceu com a infinidade de estratégias e caminhos oferecidos pelas redes sociais; algoritmos, programas, sítios, canais de busca e aplicativos de comunicação aproximam cada vez mais vítimas, dos mais diversos tipos (menores, idosos, hipossuficientes, técnicos e não técnicos, pessoas físicas ou jurídicas), a pretensos criminosos, hábeis ou não no manuseio de instrumentos de conexão, sequestro de dados e exposição de afetados.

Ao reduzir o escopo da análise ao âmbito nacional, é possível identificar as fragilidades presentes no ordenamento jurídico brasileiro frente à atividade delituosa no cenário digital, na medida que a legislação não acompanha a rapidez e dinamicidade do desenvolvimento tecnológico e o surgimento de aparelhos e canais de comunicação/conexão nacional e internacional. Outra fragilidade, sem dúvida, é o fraco aparato de recursos à disposição das autoridades responsáveis pela fiscalização de condutas nas redes e investigação de crimes virtuais (a polícia, infelizmente, mal conta com programas de rastreamento e identificação de IPs, o que torna uma corrida injusta entre agentes da lei e criminosos).

Se, de um lado, há um esforço global pela universalização do acesso à internet e facilitação do uso de redes sociais, é notório que há pouca preocupação voltada à instrução dos usuários, sobretudo quanto ao compartilhamento de dados e adoção de condutas preventivas, vez que a tela de um aparelho eletrônico (celular, computador,

etc.) esconde quem de fato se encontra do outro lado; nesse cenário, nota-se que crianças e adolescentes tornam-se as vítimas mais frequentes, somado à vulnerabilidade de autodeterminação e instrução, também identifica-se a ausência de zelo/vigilância por parte da família/responsáveis legais.

Assim, a internet se torna uma poderosa ferramenta aliada a infratores, pois permite o acesso a um número ilimitado de potenciais vítimas, a informações/dados divulgados sem filtro (seja por invasão de aparelhos ou falha humana), bem como sua anonimização e ocultação de atividades online, a partir do emprego de programas e técnicas desenvolvidas com esse propósito. O simples fato de entrar num sítio eletrônico, aliás, é algo a ser monitorado, pois é frequente a duplicação quase idêntica de páginas e perfis sociais, o que induz o indivíduo a erro e facilita o acesso a informações privadas de cunho pessoal/profissional.

A própria dificuldade de firmação de acordos de cooperação internacional e as diferenças entre ordenamentos jurídicos internos faz com que boa parte da legislação de proteção cibernética restrinja-se a alguns Estados ou mesmo torne morosa a aceitação de convenções e sua alocação no Direito nacional, com desdobramentos negativos à tutela do direito a uma navegação online segura.

Contudo, é importante se atentar para a demonização da rede mundial de computadores, na medida que o serviço de conexão não apresenta, por si só, um propósito benigno ou maligno, dependendo este das intenções das pessoas fazem uso e da omissão das autoridades que deveriam regulamentar o serviço. Assim, é salutar observar a revolução mundial propiciada pelo avanço digital, acrescentando-se a carência pela atualização constante do aparato normativo e a regulamentação da sua disponibilização e uso ideal, com a finalidade de resguardar a privacidade e demais direitos daqueles que, de alguma forma, encontram-se inseridos no ciberespaço.

Protocolos internacionais, assim, revelam-se medidas de extrema necessidade, uma vez que nem todas as nações do mundo são signatárias de convenções e acordos internacionais de tutela de bens jurídicos expostos pela internet, bem como a instrumentalização de políticas públicas locais e internacionais de alcance/identificação/punição de infratores que utilizam os serviços digitais para intentos ilícitos. A resposta estatal deve primar pela regulamentação da conexão virtual e proteção dos sujeitos expostos pelo uso pessoal ou de terceiros, uma vez que o compartilhamento de dados alcançou proporções jamais registradas na história da humanidade.

É importante também mencionar a relevância do tema tratado no estudo, sobretudo no aspecto pessoal do pesquisador, para a ciência jurídica e para a sociedade como um todo; sob o ponto de vista pessoal, registre-se que é um assunto de interesse do graduando, na medida que a tutela jurídica dos crimes cibernéticos é um tema atual e que exige maior atenção dos estudiosos da área, especialmente no que concerne ao fenômeno da globalização e seus desdobramentos no campo do Direito.

A relevância do estudo para a ciência jurídica, por outro lado, é de incremento do arcabouço teórico acerca das ferramentas jurídicas voltadas a resguardar a segurança do usuário na internet, bem com a garantia de qualidade do serviço colocado à disposição da população brasileira e do restante do mundo; contribui-se, assim, com a democratização do conhecimento e incentivo de mudança de postura e comportamento quando se está no cenário virtual.

A relevância social, conforme mencionado na introdução do presente trabalho monográfico, segue a perspectiva de reflexão sobre a importância da cautela quanto ao uso da internet e o acesso a locais virtuais seguros, bem como a compreensão de que se deve investir em programas e instrumentos de segurança para os aparelhos que viabilizam o acesso à rede, evitando-se interferências, invasões e tentativa de comandos externos.

Os objetivos foram alcançados, uma vez que restou demonstrada a fragilidade do aparato jurídico proposto ao enfrentamento dos crimes virtuais, bem como necessidade de efetividade normativa que acompanhe a velocidade dos fenômenos virtuais; registre-se também que foram apontados o escopo mundial da prática de pornografia infantojuvenil no espaço virtual, traçou-se um comparativo entre a proteção jurídica disposta em âmbito nacional e os protocolos internacionais. Descreveu-se a segurança no ciberespaço como um direito básico dos usuários das redes sociais e apontou-se a legislação de proteção de dados como um passo significativo na busca por tornar a internet um local mais seguro aos seus usuários, sejam eles nacionais ou estrangeiros.

Os resultados obtidos com o estudo do tema foram a demonstração de que necessária se faz uma atuação conjunta dos atores internacionais, proporcionando segurança jurídica aos usuários da rede mundial de computadores sem distinção de nacionalidade, elaboração de institutos coesos e aplicáveis em situações variáveis, igualdade de tratamento e protocolo de fiscalização de ilícitos no ciberespaço e

identificação/investigação de seus autores, investimento e descentralização de aparatos disponibilizados às forças de segurança, desenvolvimento de políticas públicas voltadas à proteção digital e educação de base/instrução técnica para que os usuários da internet conheçam minimamente os riscos e os perigos escondidos através de *links* e de programas desconhecidos/sem certificação da autoridade competente.

As ações de combate à pornografia infantojuvenil, por exemplo, se dá através da identificação de atividades suspeitas, captação e compartilhamento de mídias sensíveis, a partir da disponibilização de dados de vítimas, obtidos de forma direta/presencial ou por indução do menor, que acessa as redes sociais sem a devida vigilância de seus responsáveis. Assim, verifica-se que há uma fragilidade por parte do responsável legal da vítima e uma amplificação de sua vulnerabilidade ocasionada pelo estímulo social à exposição exagerada em redes sociais, principais canais de captação de mídias e de contato direto entre criminosos e suas vítimas.

Embora conste a evolução tecnológica relacionada aos instrumentos de busca, identificação e localização de criminosos nos terrenos virtuais e físicos, é necessário acrescentar que as consequências da violação de bens jurídicos ganham proporções incalculáveis quando esta se dá na internet, considerando que a exposição ocorre perante todo o planeta, em diferentes idiomas, bem como a dificuldade de exclusão do material ilícito de sítios, blogs, redes sociais e outros meios de armazenamento virtual. Dessa forma, a prevenção é o melhor dos caminhos, algo que somente se obtém com conscientização, educação, disciplina das redes e fortalecimento dos órgãos de investigação/punição.

Há que se pensar também numa releitura do uso das redes sociais, pautando o comedimento e a limitação de acesso de terceiros a dados pessoais, sobretudo vídeos e imagens de menores, além de se atentar para o fato de que muitas redes sociais adultas estão povoadas por menores que informam idades elevadas, num sinal de fragilidade do próprio aplicativo de comunicação.

Outra situação relatada ainda mais grave é identificada nos casos em que são os próprios pais, os responsáveis pela exposição exagerada da criança e do adolescente; almejando a popularidade, influência e recebimento de elogios, frequentemente agem em prol da fragilização da privacidade dos menores, revelando detalhes preciosos de sua vida, seus dados, atraindo indivíduos mal-intencionados e dispostos a usarem da inocência de suas vítimas para proveitos escusos.

Por fim, é imperioso destacar que este estudo se debruça apenas sobre uma

das vertentes da tutela estatal da segurança virtual, limitando seu escopo à legislação, doutrina e jurisprudência vigentes até então, o que conduz a compreensão de que o presente tema deverá continuar sendo debatido, agregado e pontuado por estudiosos não apenas do Direito, como também de outras áreas do conhecimento humano.

Assim, é possível obter segurança na navegação *online*, desde que respeitados os limites legais e éticos de conduta no ciberespaço e considerando a vastidão de instrumentos dispostos à facilitação da vida, como também de armadilhas preparadas para indivíduos imperitos ou que não deveriam fazer uso de canais virtuais sem o acompanhamento de um responsável.

REFERÊNCIAS

BERNERS-LEE, Tim. **Weaving the Web**: the original design and ultimate destiny of the world wide web. São Francisco: Harper Collins, 1999. Disponível em: <https://www.worldcat.org/title/weaving-the-web-the-original-design-and-ultimate-destiny-of-the-world-wide-web-by-its-inventor/oclc/729965164?referer=di&ht=edition>. Acesso em: 23 mai. 2021.

CELANT, João Henrique Pickcius; MENEGHETTI, Tarcísio. **Liberdade e controle no ciberespaço**: uma análise do marco civil da internet e do governo eletrônico. Disponível na internet via: <<http://www.publicadireito.com.br/artigos/?cod=1f9caf93105becc0>>. Acesso em: 26 mai. 2021.

CERT.BR. **Cartilha de Segurança para Internet**: versão 4.0. São Paulo: Comitê Gestor da Internet no Brasil, 2012. Disponível em: https://www.academia.edu/37235044/Cartilha_de_Seguran%C3%A7a_na_Internet. Acesso em: 24 mai. 2021.

CORATTO, Bruno Pinto. **A responsabilidade civil dos provedores de informação na internet**: a figura das redes sociais como fornecedores segundo o CDC. Disponível na internet via: <<https://ambitojuridico.com.br/edicoes/revista-119/a-responsabilidade-civil-dos-provedores-de-informacao-na-internet-a-figura-das-redes-sociais-como-fornecedores-segundo-o-cdc/>>. Acesso em: 26 mai. 2021.

DENNY, Danielle M. T. **Internet Legal**. Piracicaba: Imagens DD, 2016. Disponível em: DD: Direito da Informática (danielledenny.blogspot.com). Acesso em: 27 mai. 2021.

KAWAKANI, C. T. **Segurança de computadores e aprendizado de máquina**. 64 p. Trabalho de Conclusão de Curso (Bacharelado em Ciência da Computação) – Universidade Estadual de Londrina, Londrina-PR, 2014. Disponível em: <http://www.uel.br/cce/dc/wp-content/uploads/TCC-ClaudioKawakani-BCC-UEL-2014.pdf>. Acesso em: 25 mai. 2021.

LÉVY, Pierre. **A inteligência coletiva**: por uma antropologia do ciberespaço (Traduzido por Luiz Paulo Rouanet). 5ª ed. São Paulo: Loyola, 2007.

_____. **Cibercultura**. Tradução de Carlos Irineu da Costa. 3ª ed. São Paulo: Editora 34, 1999.

MINISTÉRIO PÚBLICO FEDERAL. 2ª Câmara de Coordenação e Revisão. **Crimes cibernéticos**. Brasília: MPF, 2018. Disponível em: <https://memorial.mpf.mp.br/ce/vitrine-virtual/publicacoes/crimes-ciberneticos-coletanea-de-artigos>. Acesso em: 25 mai. 2021.

ROCHA, Mariana Thamiris Silva. **Direito digital e o Marco Civil da internet**: o posicionamento da Lei 12.965/14 diante dos tratados internacionais no combate aos conflitos virtuais. 2017. Trabalho de Conclusão de Curso (Bacharelado em Direito) –

ASCES/ UNITA, Caruaru, Pernambuco, 2017. Disponível em: <http://repositorio.asc.es.edu.br/bitstream/123456789/1195/1/Artigo%20Cient%20C3%a0dfico%20-%20MARIANA%20THAMIRIS%20SILVA%20ROCHA.pdf>. Acesso em: 25 mai. 2021.

SANTOS, José Wilson dos; BARROSO, Rusel Marcos Batista. **Manual de Monografia da AGES: Graduação e pós-graduação**. Paripiranga: AGES, 2019.

SILVEIRA, Beatriz de Oliveira da. **A Violência na Prática de Crimes no Ciberespaço**. 2015. Dissertação (Mestrado em Segurança Pública) – Instituto de Filosofia e Ciências Humanas, Universidade Federal do Pará, Belém, 2015. Disponível em: https://www.ppgsp.propesp.ufpa.br/ARQUIVOS/teses_e_dissertacoes/dissertacoes/0SILVEIRA.pdf. Acesso em: 25 mai. 2021.

TUOMI, Ilkka. **Participatory Innovation: Change and Meaning in the Age of the Internet** (no prelo), 2002. Disponível em: <http://www.meaningprocessing.com/personalPages/tuomi/articles/NOIStart.pdf>. Acesso em: 23 mai. 2021.