CAMPO JURÍDICO
REVISTA DE DIREITO AGROAMBIENTAL E TEORIA DO DIREITO
E-ISSN: 2317-4056

DESAFIOS DO DIREITO NA ERA DA INTERNET: UMA BREVE ANÁLISE SOBRE OS CRIMES CIBERNÉTICOS

[1]**Fabiane Barbosa Marra**

As transformações propiciadas pelos avanços tecnológicos, especialmente pelo aperfeiçoamento da Rede Mundial de Computadores, inovaram e criaram maneiras de se comunicar, informar, negociar, pesquisar, trabalhar e, inclusive, praticar crimes. Nesse cenário, os indivíduos passaram a compartilhar experiências, fatos, notícias, viagens e dados em uma questão de segundos, muito embora se encontrassem em localidades diversas. Além disso, a Internet também se tornou um espaço para a ocorrência de delitos como furtos, estelionatos, racismo, pedofilia etc. No presente artigo, o que se busca é o estudo acerca do desenvolvimento da sociedade sob o viés tecnológico e emparelhado com o Direito, mormente quanto às disposições penais materiais e processuais aplicáveis ou não em casos de crimes praticados atrás das telas dos aparelhos informáticos. Frisa-se que o método a ser utilizado será o crítico-normativo, a fim de que haja maior efetividade das normas jurídicas vigentes.

Palavras-chave: Crimes cibernéticos. Atuação estatal. Marco Civil da Internet. Direito Penal e Direito Processual Penal.

CHALLENGES OF LAW IN THE INTERNET AGE: A BRIEF ANALYSIS ON CYBER CRIMES

The transformations brought about by technological advances, especially the improvement of the World Wide Web, have innovated and created ways of communicating, informing, negotiating, researching, working and even committing crimes. In this scenario, individuals began sharing experiences, facts, news, travel, and data in a matter of seconds, even though they were in different locations. In addition, the Internet has also become a space for crimes such as theft, estelionates, racism, pedophilia, etc. In the present article, what is sought is the study of the development of society under the technological bias and paired with the Law, especially regarding the material and procedural criminal provisions applicable or not in cases of crimes committed behind the screens of computer devices. It is emphasized that the method to be used will be the normative-critical one, so that there is greater effectiveness of the current legal norms.

Keywords: Cybercrime. State action. Civil Framework of the Internet. Criminal Law and Criminal Procedural Law.

Data de submissão: 12/02/2019
Data de aprovação: 05/05/2019
Double Blind Review Process
DOI: https://doi.org/10.37497/revcampojur.v7i2.289

[1] Mestre em Direito pela Universidade Federal de Ouro Preto – UFOP (Brasil). Especialista em Direito Público com ênfase em Direito Penal pela Fundação Escola Superior do Ministério Público de Minas Gerais (2016). Especialista em Direito Público com ênfase em Direito Constitucional pela Universidade Cândido Mendes (2016) Graduada pela Faculdade de Direito Milton Campos. Advogada. Email: fabianemarra@hotmail.com.

INTRODUÇÃO

A sociedade moderna, diante do progresso do conhecimento e da multiplicidade dos percalços que insurgem, inaugura uma nova fase da evolução do homem e das suas respectivas criações. Nesse sentido, este corpo social hodierno caracteriza-se pela dificuldade de se antecipar e de se contrapor adequadamente aos riscos, sejam eles individuais, ecológicos, sociais ou políticos (ROVER, 2004).

As ameaças e os perigos evidenciam-se por meio de uma sociedade transformada e, supostamente emancipada, razão porque o Estado ainda encontra profundos obstáculos para superar apuros e para estabelecer critérios adequados e duradouros de prevenção e atuação. Em outras palavras, inexistem respostas acabadas aptas a conferir uma segurança social e estatal completa frente às inúmeras situações de crises que emergem no tempo e no espaço atualmente.

O desenvolvimento tecnológico, principalmente relacionado à Rede Mundial de Computadores, sem dúvidas, proporcionou avanços significativos para a integração social, ciência, indústria, entre outros. Mas, paralelamente, também concorreu na aparição de novas formas de degradação da coletividade. Se por um lado a Internet perfaz um dos maiores veículos de propagação da informação e do conhecimento, concomitantemente, se tornou um lugar de condutas desagregadoras e criminosas.

Assim, este artigo propõe maneiras de estimular e de incentivar a criação de mecanismos e alternativas a fim de minimizar os riscos decorrentes do uso irresponsável e delituoso da Internet no Brasil. Para tanto, parte-se de conceitos e de classificações correlatos à questão, em especial sobre a configuração da sociedade informacional, a própria Internet e os crimes virtuais. Após, concentra-se nos desafios concernentes ao Direito Penal e Processual Penal vigente em relação aos crimes virtuais. Ao final, apresenta-se parâmetros de atuação do ente estatal, sobretudo apontando os aspectos penais trazidos pelo Marco Civil da Internet.

2 SOCIEDADE INFORMACIONAL E A INTERNET

A expressão "sociedade da informação" (WERTHEIN, 2000), marca o desenvolvimento do corpo social a partir do século XXI não apenas a nível local, mas também mundial. Rotineiramente utilizada nos meios de comunicação, sociedade da informação veio como um substituto da sociedade "pós-industrial". Esta sociedade informacional, como dispõe Castells (2000), encontra-se ligada à expansão e à reestruturação do capitalismo. É uma nova forma de organização econômica e social pautada nas novas tecnologias, especialmente com o desenvolvimento da Internet, o que traduz a ruptura do modelo de contrato social entre capital e trabalho, então característicos do capitalismo industrial. Há, pois, alguns aspectos inerentes: informação como matéria prima; alta penetrabilidade das novas tecnologias; convergência das tecnologias e diferentes áreas do saber; flexibilidade quanto aos processos que são reversíveis; e, ainda, predominância da infraestrutura de Rede.

Nesse contexto, a comunidade atual (OLIVEIRA; SIQUEIRA, 2007a) é notada pelo tratamento da informação. Cada indivíduo e entidade não só possui meios próprios para retenção de dados, mas, de igual forma, tem uma aptidão quase ilimitada para conectar-se às mensagens captadas e, não bastasse, também tem a capacidade para ser um percussor da informação. Logo, a sociedade da informação é arquitetada com base nas tecnologias de comunicação e informação, que abarcam técnicas, adquirição, conservação e propagação de informações por instrumentos eletrônicos, tais como computadores, ipads, celulares, entre outros. Caracteriza-se, ainda, por:

> ser aquela em que o desenvolvimento encontra-se calcado em bens imateriais, como os dados, a informação e o conhecimento. O conceito da sociedade da informação é amplo e não se reduz ao aspecto tecnológico, abrangendo qualquer tratamento e transmissão da informação, que passa a possuir um valor econômico (OLIVEIRA; SIQUEIRA, 2007b, p. 143).

Os membros da sociedade, empresas públicas ou privadas, (OLIVEIRA; SIQUEIRA, 2007c), onde quer que se encontrem e de que forma lhes é mais conveniente, têm a possibilidade de compartilhar e obter notícias instantaneamente valendo-se, em especial, da Rede Mundial de Computadores. Nessa linha, a Internet é

um instrumento inerente às novas práticas da sociedade da informação, mormente porque é o principal veículo para troca de informação à distância.

Surgida na Guerra Fria[2], a Internet foi amplamente desenvolvida pelos Estados Unidos da América com o fito militar, apesar de já existissem estudos anteriores acerca da Rede. Almejava-se uma tecnologia que interligasse computadores situados em localidades diferentes, permitindo um maior controle sobre a então União Soviética. Com o passar do tempo, a informática e a Internet perderam o cunho de Guerra, ganhando espaço nas mais variadas relações humanas. Nos últimos anos, constata-se uma verdadeira revolução nos hábitos de comunicação, trabalho e entretenimento das pessoas, com o aumento excessivo de acesso às redes sociais, em virtude do barateamento destas vias de comunicação.

Conforme dispõe Robert Spadinger:

> A Internet é onipresente, seja na vida individual, como entretenimento ou forma de comunicação, seja nas corporações ou até nos serviços públicos governamentais. Nos próximos anos, se assistirá à continuada escala da Internet e de todos os serviços conjugados em todos os setores. O mundo se transforma a cada dia mais em uma grande Rede, cada vez maior, mas conectada, disponível em qualquer lugar e em qualquer aparelho com o qual se realiza uma infinidade de atividades pessoais e profissionais (SPADINGER, 2012, p. 65).

A Internet reduziu as distâncias e permitiu a troca de mensagens instantâneas entre os indivíduos que se encontram em localidades diversas. Existe um intercâmbio social de experiências, modos de viver e pensar, representando, assim, uma face da globalização. Além do mais, a interligação dos computadores trouxe à tona um conceito novo de espaço, o ciberespaço. A utilização desta nova infraestrutura para práticas grupais influenciaram na autuação do Direito, o qual precisa ser rediscutido. No que tange a definição da Internet, Ticiane Morais Franco (2014, p. 19) .ressalta:

> A internet como um sistema de rede aberta, expressa na liberdade do fluxo de informação, a partir de uma rede internacional de computadores conectados entre si, que possibilita o intercâmbio de informações e a transferência de arquivos de toda a natureza, entre máquinas que estejam conectadas a uma rede, por meio do protocolo de rede TCR-IP (*Transmission Control Protocol/Internet Protocol).*

[2] A Internet foi amplamente desenvolvida no auge da Guerra Fria. Esta foi instaurada entre os dois pólos mais influentes e antagônicos no mundo à época: União Soviética e Estados Unidos, em meados da década de 1960.

O desenvolvimento das novas tecnologias refletiu consideravelmente na forma de se conectar na Rede. O Wi-Fi - "Wireless Fidelity" (ROHRMAM, 2005a) - representa uma inovação no meio de se comunicar, eis que é uma rede local de fácil instalação e mobilidade e que se vale de sinais de rádio, viabilizando ao acesso sem imposição de fronteiras entre os usuários. Aos computadores interligados na Rede, é atribuído um endereço singular, que representa um numerário de identidade, de localização, denominado TCP-IP (ROHRMAM, 2005b).

As Redes conectadas valem-se do TCP-IP, que significa "Internet Protocol", perfazendo um protocolo constituído por quatro bytes. Cada um destes é composto por outros oito bytes. O primeiro aglomerado de quatro algarismos pode variar de zero a duzentos e cinquenta e cinco e, em regra, cada número encontra-se separado por ponto. Em relação ao dever de localização na Rede sobre determinada página, os computadores interligados memorizam o endereço de IP e seus respectivos designativos, propiciando detectar de onde partiram mensagens, arquivos, comandos, entre outros. E, segundo Rorhrmam (2005c, p. 1), mencionado protocolo "não é uma linguagem de programação propriamente dita, mas um padrão de comunicação utilizado pelos computadores para troca de dados".

O provedor de acesso (DOMINGUES; FINKELTEIN, 2003), programa que viabiliza a conexão com à Internet, pode ser público ou comercial, havendo neste último a cobrança de tarifas ou assinaturas para o acesso às informações na Rede. Quando os clientes conectam-se à Internet, recebem uma localização conforme o endereço IP de seu respectivo provedor. Há, pois, um armazenamento e consulta de dados que permitem identificar o real endereço da página e o vestígio digital do usuário. Com efeito, a segurança na Internet enseja o aprimoramento de mecanismos tecnológicos. Nesse diapasão, destaca-se a possibilidade de criptografia que, segundo Shoueri (2001, p. 21/22), consiste em

> assegurar a privacidade, a identidade da autoria, a inalterabilidade de conteúdo, enfim, a segurança na celebração dos contratos virtuais é que surgiu a criptografia, espécie de assinatura codificada, regulada pela criptologia, representativa da codificação de informações de forma apta a impedir a interceptação não desejada, por meio de convenções secretas às partes contratantes e às testemunhas.

Em outras palavras, a criptografia pode ser realizada pela linguagem assimétrica ou simétrica. Na primeira, a mensagem é criptada por uma chave pública e desvendada por uma privada. Já na simétrica, tanto na origem quanto no destinatário há uma chave secreta de descodificação. O espaço de acesso também é um elemento a ser considerado quando se trata da Internet. Apesar da conexão com a Rede ocorrer principalmente em casa e no trabalho, cada vez mais os internautas têm uma maior flexibilidade geográfica de acesso. Nas ruas, parques, praças e, também, aeroportos, é possível o acesso à Internet por meio das redes sem cabos de Wi-Fi, as quais podem ou não serem gratuitas e administradas por empresas de telefonia ou pelo governo.

Por fim, ao mesmo tempo em que se tem uma popularização dos meios de se interligar, há de se observar que os espaços públicos de acesso são cada vez mais vulneráveis no que concerne à interceptação de dados, senhas e outras informações privativas do usuário. Há, portanto, o lançando de novos desafios quanto à segurança da Rede.

3 RELAÇÃO ENTRE O DIREITO E A INTERNET

No Brasil, o Marco Civil da Internet encontrou entraves desde o projeto até a efetiva promulgação. Tais dificuldades não minimizaram a sua importância, ao contrário. Além do surgimento de uma nova fase da sociedade a partir no século XXI, o Direito certamente não acompanhou toda essa evolução tecnológica, principalmente quanto à prática de crimes virtuais. Assim, o Marco Civil trouxe diretrizes relevantes para a utilização da Rede Mundial de Computadores. Acerca da criação da Internet e da emergência da Constituição Federal de 1988, vale ressaltar que:

> Essa Constituição chega em um momento de grande maturidade para a democracia brasileira, em que o país, havendo repelido uma lei de imprensa das mais sombrias origens, encontra-se a trilhar caminhos mais balanceados na ponderação entre a liberdade de expressão e outros direitos e garantias fundamentais. A questão que se apresenta agora é como fazê-lo no ambiente da Internet. Como estruturar os compromissos normativos e tecnológicos que compõe a Internet no Brasil para que ela seja, ainda que um instrumento de destruição criativa, também um espaço para preservação de certos valores essenciais não somente à sua natureza, como meio, mas à nossa dignidade como fim (THOMPSON, 2012, p. 3).

A ausência de regulamentação propicia condutas abusivas de alguns usuários, dada a sensação de liberdade irrestrita e impunidade. A criação do Marco Civil direcionou a forma de realização de negócios na Internet e também de diversas formas de entretenimento. O Marco Civil da Internet não estabelece sanções penais e, sim, orientações acerca das condutas praticadas no âmbito digital. Ressalta-se, por exemplo, que serviços prestados por empresas deverão apresentar-se com maior clareza aos usuários da Rede Mundial de Computadores, sendo, ainda, necessária a proteção de dados cadastrais dos clientes, não devendo divulgá-los sem a respectiva outorga.

De outra banda, a privacidade, a intimidade e outros direitos constitucionalmente previstos também estão inseridos na Lei 12.965/14. Em relação à liberdade de expressão, garantia fundamental, destaca-se sua readequação na realidade da Internet. A incerteza quanto a aplicação do ordenamento jurídico, mormente pela ausência de fronteiras que a Internet, ao mesmo tempo em que permitiu o intercâmbio cultural, também despertou uma liberdade ilusória sem limite e, por vezes, um sentimento de impunidade. Ao encontro a estes problemas, o Marco Civil veio estabelecer previsões legais aos usuários da Rede. Assim, a retirada de determinados conteúdos do ar, por exemplo, se faz por meio de ordem judicial em consonância às previsões presentes na nova Lei.

Frisa-se que o uso da Rede Mundial de Computadores não se manteve voltado apenas para o bem da sociedade, pois nem todos os indivíduos valeram-se ou valem-se do ambiente virtual de maneira razoável e adequado. Existem, de fato, pessoas que acreditam que a Rede é um lugar sem lei, onde a qualquer tempo tudo se pode, criando outras formas para a prática delituosa ou mesmo aprimorando os delitos já viventes. Ante a tal conjuntura, a Internet deve ser entendida pelo Direito como "uma mídia eletrônica, na qual não há fronteira, não há limite territorial e as comunicações ocorrem ora com lapso de tempo, ora em tempo real" (DOMINGUES; FINKELTEIN, 2003, p. 130).

Forçoso reconhecer que, para o Direito Pátrio, muito embora não existam dois mundos diversos, um virtual e outro real, as necessidades demandadas no ambiente

informático, em que vigora a Rede, são consideravelmente diferentes. Além do mais, mencionada evolução nas novas formas de se comunicar exigem do Direito, especialmente do Direito Penal e Processual Penal, uma nova dinâmica perante as ameaças oriundas do uso inadvertido da Internet. Antes, porém, urge destrinchar os principais crimes virtuais praticados por detrás dos aparelhos informáticos.

4 CRIMES VIRTUAIS

Cumpre destacar, inicialmente, que os crimes virtuais não abrangem apenas práticas no âmbito da Rede Mundial de Computadores, mas também quaisquer ação ou omissão que guarde ligação com sistemas informáticos. Isso porque, o computador pode ser apenas um instrumento, ou meio, tal como ocorre em uma fraude fora da Internet. Assim, é necessário compreender que a Rede é prescindível para configuração de crimes virtuais. Neste viés, Araújo Lima (1995, p. 127 e 133) consigna que:

> No atual estágio de desenvolvimento científico, o conceito de criminalidade informática deverá girar em torno da idéia de direito de informação e de direito de informática, nos quais a informação, o ambiente e a relevância econômica serão fatores fundamentais. A informação há de ser considerada como um bem de valor econômico, cultural, e político, além de se haver transformado num potencial de risco específico. O ambiente há de ser tratado como um elemento gerador da confiabilidade e *segurança da informação*, a despeito de sua vulnerabilidade. Esse novo modo de ver as coisas, torna evidente que os bens intangíveis devem ser tratados de forma inteiramente diferente daquela pela qual são tratados os crimes tradicionais, de caráter material.

Em relação ao conceito dos "crimes cibernéticos", o secretário executivo da Associação de Direito e Informática do Chile, define:

> Todas aquelas ações ou omissões típicas, antijurídicas e dolosas, trate-se de fatos isolados ou de um série deles, cometidos contra pessoas naturais ou jurídicas, realizadas em uso de um sistema de tratamento da informação e destinadas a produzir um prejuízo na vítima através de atentados à sã técnica informática, o qual, geralmente, produzirá de maneira colateral lesões a distintos valores jurídicos, reportando-se, muitas vezes, um benefício ilícito no agente, seja ou não seja de caráter patrimonial, atue com ou sem ânimo de lucro (MANZUR; PINHEIRO, 2000, p. 18/19).

Mais a mais, Reginaldo César Pinheiro propõe o conceito para crimes informáticos como sendo "toda conduta positiva ou negativa (ação ou omissão),

praticada total ou parcialmente no ambiente informático e que venha causar algum prejuízo à vítima, seja ele patrimonial ou não" (ROSSINI, 2002a, p. 140). Ainda, quanto à definição de crimes virtuais, a Organização para a Cooperação Econômica e Desenvolvimento da ONU, dispõe: "o crime de informática é qualquer conduta ilegal não ética, ou não autorizada, que envolva processamento automático e dados e/ou transmissão de dados" (ROSSINI, 2002b, p. 110).

Conclui-se, portanto, que crime virtual é a conduta típica, ilícita e culpável que preenche os pressupostos de crime ou de contravenção penal, ocorrida com dolo ou culpa, perpetrada por pessoa física ou jurídica por meio da informática, seja na Rede Mundial de Computadores ou não, e que vai de encontro à segurança do sistema informático, o qual deve observar a integridade, desimpedimento e a privacidade de indivíduos e entidades.

4.1 CLASSIFICAÇÕES

Existem diversas classificações para crimes virtuais, entre as quais destaca-se a oferecida por Marco Aurélio Rodrigues da Costa (1995). Ele divide os crimes de informática entre puros, mistos e comuns.

O crime informático puro é o que se encontra relacionado ao sistema de informática, isto é, o sujeito ativo pretende apenas corromper os dados do computador do sujeito passivo, tais como o "software" e o "hardware" e, assim, é percebido nos vírus que contaminam um computador, por exemplo. Já o crime de informática misto, diz respeito à violação do bem jurídico diferente do sistema, porém este é instrumento inerente à consumação do delito, como ocorre no caso do furto eletrônico a contas bancárias online. E, por último, o crime informático comum é aquele que está previstos na lei penal e pode ou não ocorrer com o uso do computador, a exemplo da pedofilia, do racismo e do cyberbullying[3].

[3] O termo caracteriza-se por um ou mais atos hostis repetidos e deliberados de ameaças e ofensas praticados por meio de aparelhos informáticos com acesso à Internet, em regra. No Brasil, diversos casos envolvendo pessoas famosas ganharam notoriedade, o que denota que ninguém está isento dessa prática grave e criminosa.

Sergio Marcos Roque (2000), por sua vez, consigna duas categorias de crimes de informática: os praticados por meio do uso do computador e os efetuados contra os sistemas em si. Naquele, o computador é um instrumento para consecução do crime, que será um delito comum. Já nos crimes perpetrados contra os dados informáticos, a ação dos criminosos é voltada especificamente contra o sistema, configurando um delito autêntico, em que o uso do computador é essencial para a existência do fato típico, ilícito e culpável.

Noutro aspecto, Túlio Lima Vianna considera que os delitos virtuais subdividem-se em quatro grupos, quais sejam:

> 1) Delitos informáticos impróprios: são aqueles nos quais o computador é usado como instrumento para a execução do crime, mas não há ofensa ao bem jurídico inviolabilidade da informação automatizada (dados).
> 2) Delitos informáticos próprios: são aqueles em que o bem jurídico protegido pela norma penal é a inviolabilidade das informações automatizadas (dados).
> 3) Delitos informáticos mistos: são aqueles complexos em que, além da proteção da inviolabilidade dos dados, a norma visa a tutelar bem jurídico de natureza diversa. São os delitos derivados do acesso não autorizados a sistemas computacionais que ganharam "status" de delitos "sui generis" dada a importância do bem jurídico protegido diverso da inviolabilidade dos dados informáticos.
> 4) Delito informático mediato ou indireto: é o delito-fim não informático que herdou esta característica do delito-meio informático realizado para possibilitar a sua consumação (apud, ROSSINI, 2004, p. 121).

Após a exposição de algumas classificações doutrinárias para os crimes virtuais, não se pode olvidar do Décimo Congresso sobre Prevenção de Delito e Tratamento do Delinquente, celebrado em Viena (FURLANETO NETO e GUIMARÃES, 2003). Na ocasião, a ONU também relacionou tipos de delitos informáticos mais específicos, quais sejam: espionagem industrial (espionagem avançada feita em proveito de empresas ou próprio); sabotagem de sistemas (envio de mensagens que obsta aos verdadeiros usuários terem acesso a um determinado *site);* sabotagem e vandalismo de dados (apagar ou alterar base da dados); pesca ou averiguação de senhas secretas (programas de identificação de senhas dos usuários e cometer delitos contra a honra, financeiros, entre outros); estratagemas (técnicas para violar segredos de segurança); pornografia infantil (armazenamento e compartilhamento de fotos de crianças); jogos de azar (pautado na falsa percepção da realidade e nos países onde é tido como delito); fraude (ofertas mentirosas no

comércio eletrônico); e lavagem de dinheiro (utilizar de vendas pelo computador para ocultar transações).

Diante deste novo cenário e a par das principais definições e classificações dos crimes virtuais, é de suma importância tratar, neste artigo, no tópico seguinte, acerca da aplicação ou não das legislações vigentes no ordenamento jurídico aos fatos e agentes responsáveis pela prática de delitos cibernéticos.

6 DESAFIOS INICIAIS DO DIREITO PENAL E DO PROCESSO PENAL NOS CRIMES VIRTUAIS

O Direito, ao aspirar a tutela do bem jurídico do cidadão, precisa impreterivelmente acompanhar a evolução dos costumes, hábitos e formas de se relacionar da sociedade, sendo, então, dessa forma, possível garantir uma proteção efetiva. Hoje em dia, indivíduos que, a princípio, não demonstram nenhuma vocação para práticas criminosas, valem-se do suposto anonimato da Rede Mundial de Computadores para aferir vantagens ilícitas de diversas naturezas, ou mesmo para propagar frustrações pessoais e ódio.

Dessa maneira, a mesma Internet que representa avanços tecnológicos na comunicação, na informação, na ciência, no comércio, é também aquela que difunde uma noção equivocada de impunidade, seja pelo referido anonimato, seja pela dificuldade no rastreamento do autor, ou ainda, seja pela dificuldade de aplicação da legislação em vigor. É de se destacar já que existem alguns mecanismos tecnológicos que podem auxiliar na proteção dos bens jurídicos no que tange à Rede Mundial de Computadores, tais como: o controle de acesso subdividido em autorização e autenticação; dispositivos de defesa composto por um sistema ou um corpo de sistemas, que reforça o cumprimento de políticas de controle de acesso; "Virtual Private Network", que permite a troca de informações seguras por meio da utilização de redes públicas; monitoramento de arquivos de registros gerados pelos serviços de rede; sistemas compostos de harware e software capazes de capturar informações; e a Criptografia e assinatura digital (DOMINGUES; FINKELTEIN, 2003).

Todavia, a ausência de incentivos eficazes ao desenvolvimento de programas mais sofisticados, bem como a desvalorização de profissionais da área tecnológica, são desafios que precisam ser superados para que a Internet seja de fato uma rede de progresso em prol da coletividade. Além do mais, reconhecer que o Direito tradicional não acompanhou em igual medida as novas tecnologias, também demonstra que a legislação aplicável em toda a persecução penal no caso de crimes virtuais precisa de aperfeiçoamentos, pois, caso contrário, o processo estará fadado ao fracasso, em virtude da ausência de provas de materialidade ou autoria, ou pelo instituto da prescrição, por exemplo.

Por fim, conscientizar a população sobre o uso moderado e razoável, da Internet, nos limites constitucionais e em respeito aos direitos de si próprio e dos outros, é um importante começo para prevenção e controle das práticas criminosas no âmbito virtual.

7 COMPETÊNCIA PENAL E CRIMES VIRTUAIS

A Internet perfaz uma teia de cobertura mundial, em que diversos computadores se encontram interligados. Os limites de aplicação do ordenamento jurídico de um determinado Estado, não obstante a inexistência de fronteiras que delineiam a soberania de um pais, têm sido superado com o apoio mútuo, uns países com os outros. E isso é de extrema importância para a discussão acerca da competência dos crimes informáticos. Uma, porque não há um tratamento universal para aplicação de normas quando se diz delitos virtuais. Duas, porque ainda que existam tratados que dispõe sobre os crimes virtuais, muitas vezes não há a reciprocidade, ou seja, nem todos os Estados aderiram determinado tratado, dificultando a repressão dos delitos informáticos numa relação mundial.

Além do mais, a partir do momento em que ocorrem mudanças nos hábitos e propostas, os fundamentos normativos também devem passar por um aperfeiçoamento, interpretativo ou literal, de modo a acompanhar as transformações em voga, o que abrange preceitos de territorialidade, jurisdição, local do delito, etc. Quanto à competência para apurar a prática dos crimes virtuais, existem peculiaridades que

devem ser observadas dada a infinidade de crimes os quais se diversificam pelas formas de consumação e resultado.

Primeiramente, insta frisar que nem todos os crimes praticados na Internet são de competência da Justiça Federal. Para que haja a competência da União, é mister a adequação formal em alguma das hipóteses previstas no artigo 109, incisos IV e V, da Constituição Federal de 1988. Veja-se:

> Art. 109. Aos juízes federais compete processar e julgar:
> IV - os crimes políticos e as infrações penais praticadas em detrimento de bens, serviços ou interesse da União ou de suas entidades autárquicas ou empresas públicas, excluídas as contravenções e ressalvada a competência da Justiça Militar e da Justiça Eleitoral;
> V - os crimes previstos em tratado ou convenção internacional, quando, iniciada a execução no País, o resultado tenha ou devesse ter ocorrido no estrangeiro, ou reciprocamente (BRASIL, Constituição da República Federativa do Brasil, de 5 de outubro de 1988).

Desta feita, o tão somente fato da conduta ter se concretizado pela Rede Mundial de Computadores não determina a competência Federal. É necessário que o delito tenha sido cometido no território nacional para a aplicação da legislação brasileira, bem como a adesão pelo Brasil a um tratado ou convenção internacional de combate à conduta então praticada e, ainda, uma relação de internacionalidade (iniciada a execução no Brasil, o resultado ocorre no estrangeiro; ou iniciada a execução no estrangeiro, o resultado ocorre no Brasil).

Destaca-se, a título de exemplos, os crimes de tráfico internacional de drogas, arma de fogo, pessoas para exploração sexual, envio ilegal de crianças ou adolescentes para o exterior e racismo, como modalidades em que a competência é da Justiça Federal, já que previstos em tratados internacionais e legislações pátrias. Em relação ao crime de racismo, especificamente, o Superior Tribunal de Justiça definiu que a competência territorial será determinada conforme o local de onde partiram as ofensas tidas como racistas, confira-se:

> PENAL. CONFLITO DE COMPETÊNCIA. CRIME DE RACISMO PRATICADO POR INTERMÉDIO DE MENSAGENS TROCADAS EM REDE SOCIAL DA INTERNET. USUÁRIOS DOMICILIADOS EM LOCALIDADES DISTINTAS. INVESTIGAÇÃO DESMEMBRADA. CONEXÃO INSTRUMENTAL. EXISTÊNCIA. COMPETÊNCIA FIRMADA PELA PREVENÇÃO EM FAVOR DO JUÍZO ONDE AS INVESTIGAÇÕES TIVERAM INÍCIO.

> 1. A competência para processar e julgar o crime de racismo praticado na rede mundial de computadores estabelece-se pelo local de onde partiram as manifestações tidas por racistas. Precedente da Terceira Seção.
> 2. No caso, o procedimento criminal (quebra de sigilo telemático) teve início na Seção Judiciária de São Paulo e culminou na identificação de alguns usuários que, embora domiciliados em localidades distintas, trocavam mensagens em comunidades virtuais específicas, supostamente racistas. O feito foi desmembrado em outros treze procedimentos, distribuídos a outras seções judiciárias, sob o fundamento de que cada manifestação constituía crime autônomo.
> 3. Não obstante cada mensagem em si configure crime único, há conexão probatória entre as condutas sob apuração, pois a circunstância em que os crimes foram praticados - troca de mensagens em comunidade virtual - implica o estabelecimento de uma relação de confiança, mesmo que precária, cujo viés pode facilitar a identificação da autoria.
> 4. Caracterizada a conexão instrumental, firma-se a competência pela prevenção, no caso, em favor do Juízo Federal de São Paulo - SJ/SP, onde as investigações tiveram início. Cabendo a este comunicar o resultado do julgamento aos demais juízes federais para onde os feitos desmembrados foram remetidos, a fim de que restituam os autos, ressalvada a existência de eventual sentença proferida (art. 82 do CPP).
> 5. Conflito conhecido para declarar a competência do Juízo Federal da 9ª Vara Criminal da Seção Judiciária de São Paulo, o suscitante. (São Paulo. Superior Tribunal de Justiça. Conflito de Competência. CC 116.926/SP, Rel. Ministro Sebastião Reis Júnior, Terceira Seção, julgado em 04/02/2013, DJe 15/02/2013) .

De igual forma, e sob um aspecto mais aprofundado, a divulgação de imagens pornográficas de crianças e adolescentes em página da Internet também é delito de competência da Justiça Federal. Isso porque, além de estar previsto no artigo 241-A do Estatuto da Criança e do Adolescente, o Brasil comprometeu-se, por meio da Convenção sobre Direitos da Criança, adotada pela Assembleia Geral das Nações Unidas, a combater a violência de cunho sexual contra crianças e adolescentes. Verifica-se, ainda, a transnacionalidade do delito, já que as imagens podem ser visualizadas em qualquer computador. Ademais, a competência territorial será da Seção Judiciária do local onde o réu publicou as fotos ou, quando a publicação ocorrer no exterior, deverá ser observado o artigo 7°, §2°, do Código Penal. É o que se extrai da jurisprudência do Tribunal Federal da 4ª Região:

> DIREITO PENAL. APELAÇÃO CRIMINAL. ART. 241 DO ESTATUTO DA CRIANÇA E DO ADOLESCENTE. PUBLICAÇÃO E DISPONIBILIZAÇÃO, EM AMBIENTE VIRTUAL, DE FOTOS E VÍDEOS PORNOGRÁFICOS ENVOLVENDO CRIANÇAS E ADOLESCENTES. INTERNACIONALIDADE DEMONSTRADA. COMPETÊNCIA DA JUSTIÇA FEDERAL. MATERIALIDADE, AUTORIA E DOLO EVIDENCIADOS. CRIME DE QUADRILHA OU BANDO. ART. 288, DO CP. NÃO CONFIGURAÇÃO. DOSIMETRIA DA PENA. UTILIZAÇÃO DA INTERNET COMO INSTRUMENTO PARA A EXECUÇÃO DO CRIME. CIRCUNSTÂNCIA INERENTE À TIPIFICAÇÃO CONSOLIDADA PELA LEI 10.764/2003. CONCURSO MATERIAL. SOMA DAS PENAS PRIVATIVAS DE LIBERDADE SUPERIOR A QUATRO ANOS. SUBSTITUIÇÃO POR RESTRITIVAS DE

> DIREITOS. IMPOSSIBILIDADE. 1. Tratando-se da potencial prática de crime cuja previsão resulta de orientações traçadas em acordos e tratados internacionais - dos quais o Brasil é signatário - visando combater a pedofilia via internet, deflagrada a operação policial em território pátrio a partir de investigações realizadas no exterior, tem-se por caracterizada a internacionalidade necessária a vis atractiva da Justiça Federal (art. 109, inciso V, da CF/88). 2. Evidenciado, pela prova produzida, que o acusado, conscientemente, publicou e forneceu material pedófilo por meio da rede mundial de computadores, resta configurada a prática das condutas descritas no art. 241 do Estatuto da Criança e do Adolescente, tanto na redação original, quanto na anterior à Lei 11.829, de 2008. 3. O crime de quadrilha ou bando visa punir a associação de no mínimo quatro pessoas, que assim se reúnem de forma estável ou permanente com a finalidade precípua de cometer uma série de crimes. Nessa perspectiva, ainda que presentes os requisitos numérico e temporal (permanência das comunidades virtuais pedófilas por vários meses), não se tem por caracterizado o delito previsto no art. 288, do CP, quando a prova produzida evidenciar que a associação dos integrantes dessas comunidades virtuais não se dava de forma estável, mas, senão, ocasionalmente. 4. A alteração legislativa promovida pela Lei 10.764, de 12.11.2003 integrou ao caput do artigo 241, do ECA, a utilização da "rede mundial de computadores ou internet" como meio de comunicação apto a apresentar, produzir, vender, fornecer, divulgar ou publicar fotografias ou imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente. Portanto, sendo o uso da internet inerente ao tipo, descabe a negativação da circunstância judicial culpabilidade sob esse fundamento. 5. Reconhecido o concurso material de crimes, as penas privativas de liberdade aplicam-se cumulativamente, consoante o disposto no artigo 69, caput, do CP. Assim, sendo a soma das penas superior a 4 anos, inviável sejam elas consideradas isoladamente para fins de substituição por restritivas de direito (art. 44, inciso I, do CP). (Santa Catarina. Tribunal Regional Federal da 4ª Região. Apelação Criminal. ACR 200572040079800, TADAAQUI HIROSE, TRF4 - SÉTIMA TURMA, D.E. 25/11/2010).

Diferentemente ocorre nos crimes praticados contra a honra por meio da utilização das redes sociais, já que terão a competência da Justiça Estadual, determinada pelo local do domicílio do acusado. Os delitos de calúnia, injúria ou difamação, ainda que praticados em páginas de acesso internacionais, ultrapassando os limites das fronteiras, em regra, são de competência do ente da Federação, pois normalmente não preenchem os requisitos para configuração da competência Federal. Veja-se:

> CONFLITO NEGATIVO DE COMPETÊNCIA. CRIME DE INJÚRIA PRATICADO POR MEIO DA INTERNET, NAS REDES SOCIAIS DENOMINADAS ORKUT E TWITTER. AUSÊNCIA DAS HIPÓTESES DO ART. 109, INCISOS IV E V, DA CF. OFENSAS DE CARÁTER EXCLUSIVAMENTE PESSOAL. COMPETÊNCIA DA JUSTIÇA ESTADUAL.
> 1 - O simples fato de o suposto delito ter sido cometido por meio da rede mundial de computadores, ainda que em páginas eletrônicas internacionais, tais como as redes sociais "Orkut" e "Twitter", não atrai, por si só, a competência da Justiça Federal.
> 2 - É preciso que o crime ofenda a bens, serviços ou interesses da União ou esteja previsto em tratado ou convenção internacional em que o Brasil se comprometeu a combater, como por exemplo, mensagens que veiculassem pornografia infantil,

> racismo, xenofobia, dentre outros, conforme preceitua o art. 109, incisos IV e V, da Constituição Federal.
> 3 - Verificando-se que as ofensas possuem caráter exclusivamente pessoal, as quais foram praticadas pela ex-namorada da vítima, não se subsumindo, portanto, a ação delituosa a nenhuma das hipóteses do dispositivo constitucional, a competência para processar e julgar o feito será da Justiça Estadual.
> 4 - Conflito conhecido para declarar a competência do Juízo de Direito do Juizado Especial Cível e Criminal de São Cristóvão/SE, o suscitado. (São Paulo. Superior Tribunal de Justiça. Conflito de Competência. CC 116.926/SP, Rel. ministro Sebastião Reis Júnior, Terceira Seção, julgado em 04/02/2013, DJe 15/02/2013).

No mesmo sentido, é o caso da troca de e-mails com conteúdo pornográfico de crianças e adolescentes entre duas pessoas residentes no Brasil. A competência será Estadual, haja vista que o fato permaneceu restrito entre duas pessoas, não subsistindo a internacionalidade. Confira-se o precedente do STJ, CC 121215 / PR, de 12/12/2012:

> CONFLITO DE COMPETÊNCIA. CRIMES RELACIONADOS À DIVULGAÇÃO DE MATERIAL PORNOGRÁFICO ENVOLVENDO CRIANÇAS E ADOLESCENTES POR MEIO DA INTERNET. INEXISTÊNCIA DE ELEMENTOS DE INTERNACIONALIDADE. COMPETÊNCIA DA JUSTIÇA ESTADUAL. PRECEDENTES DO STJ. 1. O fato de o suposto crime praticado contra menores ter sido cometido por meio da rede mundial de computadores (internet), não atrai, necessariamente, a competência da Justiça Federal para o processamento do feito. 2. Para se firmar a competência da Justiça Federal, além de o País ser signatário de acordos e tratados internacionais, deve-se demonstrar que a divulgação das cenas pornográficas envolvendo crianças e adolescentes efetivamente ultrapassou as fronteiras do Estado Brasileiro. 3. A hipótese dos autos demonstra ser apenas a troca de mensagens eletrônicas entre pessoas residentes no Brasil, por meio de correio eletrônico e de comunidades virtuais de relacionamento como MSN, sem transpor a fronteiras do Estado Brasileiro, ausente o requisito da transnacionalidade, motivo pelo qual deve ser apurada pela Justiça estadual. 4. Conflito conhecido para declarar competente o Juízo de Direito da Vara Criminal de Rolândia/PR, o suscitado. (Paraná. Superior Tribunal de Justiça. Conflito de Competência. CC 121215/PR. Relatora Min. Laurita Vaz. Terceira Seção. Julgado em 12/12/2012).

Em relação ao estelionato praticado pela Internet com a vítima residente no exterior, por exemplo, a competência é da Justiça Estadual, porque além do artigo 69 do Código de Processo Penal dispor que o local de residência da vítima não é determinante para competência jurisdicional, por outro lado, o local de execução, consumação e obtenção da vantagem pelo beneficiário da fraude é o que de fato definem o local de processamento e julgamento da ação penal. Logo, na hipótese de uma compra pela Internet e o pagamento efetuado por transação eletrônica em território nacional, a competência será definida conforme a cidade onde ocorreram os fatos, sendo, portanto, de Competência Estadual.

Lado outro, no que concerne ao furto mediante fraude, perpetrado por meio do sistema informático, a competência será Federal, nos termos do julgado que segue:

> EMENDA: CONFLITO NEGATIVO DE COMPETÊNCIA. PENAL E PROCESSO PENAL. FRAUDE ELETRÔNICA NA INTERNET. TRANSFERÊNCIA DE NUMERÁRIO DE CONTA DA CAIXA ECONÔMICA FEDERAL. FURTO MEDIANTE FRAUDE QUE NÃO SE CONFUNDE COM ESTELIONATO. CONSUMAÇÃO. SUBTRAÇÃO DO BEM. APLICAÇÃO DO ART. 70 DO CPP. COMPETÊNCIA DA JUSTIÇA FEDERAL PARANAENSE. 1. O furto mediante fraude não se confunde com o estelionato. A distinção se faz primordialmente com a análise do elemento comum da fraude que, no furto, é utilizada pelo agente com o fim de burlar a vigilância da vítima que, desatenta, tem seu bem subtraído, sem que se aperceba; no estelionato, a fraude é usada como meio de obter o consentimento da vítima que, iludida, entrega voluntariamente o bem ao agente. 2. Hipótese em que o agente se valeu de fraude eletrônica para a retirada de mais de dois mil e quinhentos reais de conta bancária, por meio da "Internet Banking" da Caixa Econômica Federal, o que ocorreu, por certo, sem qualquer tipo de consentimento da vítima, o Banco. A fraude, de fato, foi usada para burlar o sistema de proteção e de vigilância do Banco sobre os valores mantidos sob sua guarda. Configuração do crime de furto qualificado por fraude, e não estelionato. 3. O dinheiro, bem de expressão máxima da idéia de valor econômico, hodiernamente, como se sabe, circula em boa parte no chamado "mundo virtual" da informática. Esses valores recebidos e transferidos por meio da manipulação de dados digitais não são tangíveis, mas nem por isso deixaram de ser dinheiro. O bem, ainda que de forma virtual, circula como qualquer outra coisa, com valor econômico evidente. De fato, a informação digital e o bem material correspondente estão intrínseca e inseparavelmente ligados, se confundem. Esses registros contidos em banco de dados não possuem existência autônoma, desvinculada do bem que representam, por isso são passíveis de movimentação, com a troca de titularidade. Assim, em consonância com a melhor doutrina, é possível o crime de furto por meio do sistema informático. 4. A consumação do crime de furto ocorre no momento em que o bem é subtraído da vítima, saindo de sua esfera de disponibilidade. No caso em apreço, o desapossamento que gerou o prejuízo, embora tenha se efetivado em sistema digital de dados, ocorreu em conta-corrente da Agência Campo Mourão/PR, que se localiza na cidade de mesmo nome. Aplicação do art. 70 do Código de Processo Penal. 5. Conflito conhecido para declarar competente o Juízo Federal de Campo Mourão - SJ/PR. (Paraná. Superior Tribunal de Justiça. Conflito de Competência. CC 200601661530, Rel. Ministra Laurita Vaz. Terceira Seção, julgado em 11/12/2007).

Por fim, a Lei 12.737/2012[4] tipificou a invasão dos dispositivos informáticos ocorridas no Brasil, atribuindo pena, consoante ao artigo 154-A do Código Penal, para as situações de violação de mecanismo de segurança que vislumbram a obter, destruir ou adulterar dados ou informações sem autorização do titular do respectivo dispositivo. A finalidade é de proteção à privacidade e, consequentemente, à intimidade e à vida privada do indivíduo. É, pois, de competência Estadual o crime em análise, que será processado mediante a representação do ofendido no local onde ocorreu a invasão (por ser um delito formal, não se exige o resultado), o que será excepcionado na hipótese de cometimento contra algum ente da União.

[4] Esta Lei, que dispõe sobre a tipificação criminal de delitos informáticos, foi uma tentativa do legislador de criminalizar condutas praticadas por meio de recursos de tecnologia e intoleráveis pela sociedade.

6 MEIOS DE PROVA E CRIMES VIRTUAIS

Com base nos ensinamentos de Fernando Tourinho Filho, destaca-se que provar é

> antes de mais nada, estabelecer a existência da verdade; e as provas são os meios pelos quais se procura estabelecê-la. É demonstrar a veracidade do que se afirma, do que se alega. Entendem-se, também, por prova, de ordinário, os elementos produzidos pelas partes ou pelo próprio Juiz visando a estabelecer, dentro do processo, a existência de certos fatos. É o instrumento de verificação do *thema probandum* (TOURINHO, 2009, P. 522).

Nesse contexto, a responsabilidade penal somente poderá ser configurada quando houver um conjunto comprobatório robusto apto a determinar a autoria e a prática ilícita. Para tanto, os meios de prova sinalizam o atalho que o magistrado deve traçar para fundamentar a sua decisão sobre os fatos controvertidos. Nas palavras de Paulo Rangel "meios de prova são todos aqueles que o juiz, direta ou indiretamente, utiliza para conhecer a verdade dos fatos, estejam eles previstos em Lei ou não". (RANGEL, 2014, p. 463). Nesse diapasão, tem-se a inspeção judicial, indícios, confissão, depoimentos, testemunhas, documentos, perícias, que podem compor o processo e, como se vê, perfazem um rol de meios de prova.

As infrações perpetradas no âmbito informático, de um modo geral, não deixam rastros e, em função das incertezas que a Rede Mundial de Computadores ainda perpetua, muitos casos carecem da identificação do autor do fato. Esclarece-se que, da mesma forma como se observa nas investigações com quebra de sigilo telefônico, é necessária prévia autorização judicial para ter acesso a determinadas informações nas redes virtuais[5]. Ou seja, muito embora as práticas criminosas estejam cada vez mais sofisticadas, a utilização de determinada prova deve obedecer o mesmo trâmite previsto na legislação aplicada em infrações penais comuns, haja vista que, por vezes, ainda não foram readequadas ou atualizadas.

[5] Recentemente o Superior Tribunal de Justiça, 5ª Turma, RHC 67.379-RN, decidiu que conversas arquivadas no WhatsApp estão protegidas pelo sigilo telefônico, de sorte que é necessária autorização judicial para que os agentes policiais tenham acesso ao conteúdo das referidas conversas de agente preso em flagrante delito, sob pena de invalidação da prova.

E, não fosse suficiente, as provas no ambiente informático encontram-se mais vulneráveis ao perecimento, pois são preservadas apenas quando têm alguma relevância para o provedor de acesso ou nas hipóteses em que o Judiciário - quando acionado a tempo - assim determina. Em tal conjuntura, ressalta-se que o armazenamento de dados efetuado pelo provedor de acesso é de suma importância para o arcabouço probatório nos crimes virtuais. As informações guardadas pelos provedores permitem identificar o IP e, consequentemente, a localização do criminoso. Portanto, referida prova material é vista como um grande passo para se localizar o autor de um delito informático.

Soma-se a isso a prova pericial, que também é um meio de prova importante nos delitos informáticos. Nos casos de pedofilia e racismo perpetrados na Rede, por exemplo, a perícia é a prova que permite a configuração da materialidade e a indicação da autoria delitiva, então necessárias para lastrear a condenação criminal.

Conclui-se, aqui, que há muito o que evoluir quanto aos meios de prova no âmbito informático, uma vez que estes ainda são muito superficiais e restritos frente as necessidades hodiernas. Em suma, os crimes virtuais ou são novas modalidades de delitos ou são infrações que se aprimoraram com o uso da Internet, o que demanda, por óbvio, técnicas mais aperfeiçoadas e modernas de apuração, estando sempre observados os princípios constitucionais e garantias fundamentais correlatos.

9 CONSIDERAÇÕES FINAIS

A Internet ultrapassou os limites impostos pelas fronteiras tornando-se, na atualidade, o principal veículo de divulgação da informação, comunicação, comercialização e, inclusive, de práticas delituosas. Nesta alçada tecnológica, vislumbra-se a ausência de mecanismos completos de proteção e sanção oriundos do Direito Penal e Processual Penal. Há uma grande restrição para a aplicação efetiva da norma, produção probatória e, até mesmo, de adoção de medidas de urgência no que diz respeito ao ambiente informático.

O auxílio mútuo dos países para reprimir transgressões à norma (cooperação internacional), bem como a extensão das leis preexistentes e aplicáveis a certas

condutas criminosas perpetradas na seara virtual, configuram alternativas importantes para os desafios impostos à incidência do Direito vigente na conjuntura atual. Além do mais, o aprimoramento da legislação não se confunde com a criação de inúmeras leis para a repressão de crimes cibernéticos. A eficácia da lei pertinente aos crimes virtuais depende muito mais de um desenvolvimento tecnológico de adequação da regra à conduta praticada, do que propriamente à produção de novas leis.

Ademais, a Rede Mundial de Computadores e os avanços tecnológicos como um todo demandam também uma maior conscientização, prevenção e, quando necessário, repressão estatal às ações criminalmente proibidas. É preciso incutir nos indivíduos a importância do uso consciente da Internet, isto é, fomentar o respeito recíproco. Esta mudança na forma de agir dos usuários da Internet somada à melhor atuação do Estado na persecução penal, afastará a intensa impunidade dos infratores virtuais e tornará o meio informático mais seguro para todos.

REFERÊNCIAS

ARAÚJO JÚNIOR, *João Marcelo de. Dos Crimes contra a ordem econômica*. São Paulo: RT, 1995, p. 127 e 133.

BRASIL. *Constituição da República Federativa do Brasil de 1988*. Disponível em <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm> Acesso em 19 de março de 2019.

CASTELLS, Manuel. *A era da informação: economia, sociedade e cultura*. In: A sociedade em Rede. São Paulo: Pa e Terra, 2000. v. 1.

DA COSTA, Marco Aurélio Rodrigues. *Crimes de Informática*. 1995. 22 f. Monografia [Graduação em Direito] - Pontifícia Universidade Católica do Rio Grande do Sul. Disponível em:<http://www.jus.com.br/doutrina/crinfo.html>.Acesso em 16/06/2000. Crimes de Informática e investigação policial. In: PENTEADO, Jacques de Camargo (Coord.) et al. *Justiça Penal, 7: críticas e sugestões: justiça criminal moderna: proteção à vítima e à testemunha....* São Paulo: Revista dos Tribunais, 2000. (Centro de Extensão Universitária, v. 7), p. 317/318.

DOMINGUES, Alessandra de Azevedo e FINKELTEIN, Maria Eugênia (Organização). *DIREITO & INTERNET - Aspectos jurídicos relevantes.* São Paulo, 2003: Quarter Latin, volume III, pgs. 421/422.

DOMINGUES, Alessandra de Azevedo e FINKELTEIN, Maria Eugênia (Organização). *DIREITO & INTERNET - Aspectos jurídicos relevantes.* São Paulo, 2003: Quarter Latin, pgs. 378/379.

FILHO TOURINHO, Fernando da Costa. *Manual de Processo Penal.* São Paulo: Saraiva, 2009, p.522.

MANZUR, Cláudio Líbano. Chile: *Los delictos de hacing em sus diversas manifestaciones*. In: Revista Eletrònica de Derecho Informático, n. 21, abr. 2000. Disponível em: <http:// publicaciones.derecho.org/redi>, apud Reginaldo César Pinheiro. Os crimes virtuais na esfera jurídica brasileira. Boletim IBCCRIM - Publicação Oficial da Instituto Brasileiro de Ciência Criminais. São Paulo, ano 8, n. 101, p. 18/19.

MORAIS, Ticiane Franco. *Marco Civil da Internet: A neutralidade da Rede na Perspectiva das Telecomunicações*. Nova Lima, 2014, p. 19.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. Décimo Congresso sobre Prevenção de Delito e Tratamento do Delinquente. Disponível em: <http://www.onu.org/>. Acesso 17 out 2002. E, NETO, Mário Furlaneto e GUIMARÃES, José Augusto Chaves. *Revista do IBCCRIM - Direito da Informática - Crimes na Internet: elementos para uma reflexão sobre a ética informacional* - - R. CEJ, Brasiliam n. 20, p. 67-73, jan./mar 2003, p. 71.

PARANÁ. Superior Tribunal de Justiça. Conflito Negativo de Competência. CC 200601661530, LAURITA VAZ, TERCEIRA SEÇÃO, DJ DATA: 11/12/2007 PG:00170 ..DTPB. Disponível em: < https://www2.jf.jus.br/juris/unificada/Resposta>. Acesso em 20 jun. 2018.

PARANÁ. Superior Tribunal de Justiça. Conflito de Competência. CC 121215/PR. Relator Min. LAURITA VAZ, TERCEIRA SEÇÃO, Julgado em 12/12/2012. Disponível em: <http://www.lexml.gov.br/urn/urn:lex:br:superior.tribunal.justica;secao.3:acordao;cc:2012-12-12;121215-1243005>. Acesso em 01 jun. 2018.

RANGEL, Paulo. *Direito Processual Penal.* São Paulo; Atlas, 2014, Ed. 22ª, p. 463.

ROHRMAM, Carlos Alberto. *Curso de Direito Virtual.* Belo Horizonte: Del Rey, 2005, p. 1.

ROSSINI, Augusto Eduardo de Souza. *Brevíssimas considerações sobre delitos informáticos*. São Paulo: ESMP, jul. 2002. p. 140 (Caderno Jurídico, ano 02, n. 04).

ROSSINI, Augusto Eduardo de Souza. Informática, Telemática e Direito Penal. São Paulo: Memória Jurídica, ano 2004, p. 121.

ROVER, Aires José. *Livro Direito e Informática*. Artigo Heline Sivini Ferreira: Sociedade, Risco e Direito. Barueri, SP: Manole, 2004, página 01.

SHOUERI, Luis Eduardo (organizador). *Internet - O Direito na Era Virtual*. Rio de Janeiro: Forense, 2001, Ed. 2ª, pgs. 21/22.

SIQUEIRA JR, Paulo Hamilton e OLIVEIRA, Miguel Augusto Machado de. *Livro Direitos Humanos e Cidadania*. São Paulo: Revista dos Tribunais, 2007, p. 144 - Telefônica. A sociedade da informação: presente e perspectivas, p. 16 - disponível em <www.telefonica.com.br/sociedadedainformacao/informes_home.htm)>. Acesso em 20 jun. 2018.

SIQUEIRA JR, Paulo Hamilton e OLIVEIRA, Miguel Augusto Machado de. *Livro Direitos Humanos e Cidadania*. São Paulo: Revista dos Tribunais, 2007, p. 143. In: JR, Paulo Hamilton Siqueira e OLIVEIRA, Miguel Augusto Machado de. *Livro Direitos Humanos e Cidadania*. São Paulo: Revista dos Tribunais, 2007, p. 144 - Telefônica. A sociedade da informação: presente e perspectivas, p. 16 - disponível em <www.telefonica.com.br/sociedadedainformacao/informes_home.htm)>. Acesso em 17 de março de 2018.

SPADINGER, Robert. *O futuro das telecomunicações e uma análise dos desafios para a inserção do Brasil numa cadeia global*. In: KUBOTA, Luis Claudio *et al. Tecnologias da Informação e comunicação:* competência, políticas e tendências. Brasília: Ipea, 2018, p. 65.

SANTA CATARINA. Tribunal Federal da 4ª Região. Apelação Criminal. ACR 200572040079800, TADAAQUI HIROSE, TRF4 - SÉTIMA TURMA, D.E. 25/11/2010.). Disponível em: < http://jurisprudencia.trf4.jus.br/pesquisa/inteiro_teor.php?orgao=1&documento=2956916>. Acesso em 20 jun. 2018.

SÃO PAULO. Superior Tribunal de Justiça. Conflito de Competência. CC 116.926/SP, Rel. Ministro SEBASTIÃO REIS JÚNIOR, TERCEIRA SEÇÃO, julgado em 04/02/2013, DJe 15/02/2013. Disponível em: <https://www2.jf.jus.br/juris/unificada/Resposta>. Acesso em 20 jun. 2018.

SERGIPE. Tribunal Regional Federal. Conflito de Competência. CC 121.431/SE, Rel. Ministro MARCO AURÉLIO BELLIZZE, TERCEIRA SEÇÃO, julgado em 11/04/2012, DJe 07/05/2012. Disponível em: <http://www.stj.jus.br/SCON/jurisprudencia/toc.jsp#DOC2>. Acesso em: 20 jun. 2018.

THOMPSON, Marcelo. Revista de Direito Administrativo. Marco Civil ou Demarcação de Direitos? Democracia, razoabilidade e as fendas na internet do Brasil,

set./ago, 2012. Disponível em: < http://bibliotecadigital.fgv.br/ojs/index.php/rda/article/view/8856/7678 >. Acesso em 20 jun. 2018.

WERTHEIN, Jorge. Publicação de Artigos Científicos. A sociedade da Informação e seus Desafios, maio/ago. 2000. Disponível em: < www.scielo.br/pdf/%0D/ci/v29n2/a09v29n2.pdf >. Acesso em 20 jun. 2018.