UNIVERSIDADE FEDERAL DO CEARÁ

FACULDADE DE DIREITO

MARCOS LEVY GONDIM SALES

A COMPROVAÇÃO DA MATERIALIDADE E DA AUTORIA NOS CRIMES VIRTUAIS

Fortaleza – 2013

MARCOS LEVY GONDIM SALES

A COMPROVAÇÃO DA MATERIALIDADE E DA AUTORIA NOS CRIMES VIRTUAIS

Monografia apresentada ao curso de graduação da Faculdade de Direito da Universidade Federal do Ceará. Área de concentração: Direito Penal.

Orientador: Prof. Michel Mascarenhas

Fortaleza – 2013

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Biblioteca Setorial da Faculdade de Direito

S163c Sales, Marcos Levy Gondim.

A comprovação da materialidade e da autoria nos crimes virtuais / Marcos Levy Gondim Sales. – 2013.

71 f. : enc. ; 30 cm.

Monografia (graduação) – Universidade Federal do Ceará, Faculdade de Direito, Curso de Direito, Fortaleza, 2013.

Área de Concentração: Direito Penal.

Orientação: Prof. Me. Michel Mascarenhas Silva.

1. Crime por computador - Brasil. 2. Autor (Direito penal) - Brasil. 3. Direito penal - Brasil. 4. Sociedade da Informação - Brasil. 5. Fraude na Internet. I. Silva, Michel Mascarenhas (orient.). II. Universidade Federal do Ceará – Graduação em Direito. III. Título.

CDD 343

MARCOS LEVY GONDIM SALES

A COMPROVAÇÃO DA MATERIALIDADE E DA AUTORIA NOS CRIMES VIRTUAIS

Monografia apresentada ao Curso de Direito da Universidade Federal do Ceará como requisito parcial para a obtenção do grau de Bacharel em Direito. Área de Concentração: Direito Penal.

Aprovada em ___/___/___.

BANCA EXAMINADORA

_____

Prof. Ms. Michel Mascarenhas Silva

Universidade Federal do Ceará (UFC)

_____

Prof. Ms. Raul Carneiro Nepomuceno

Universidade Federal do Ceará (UFC)

_____

Thales José Pitombeira Eduardo

Universidade Federal do Ceará (UFC)

Dedico este trabalho a Deus, por ser o guia sublime e razão do meu existir, e à minha família, pelo apoio incondicional ao longo destes anos.

AGRADECIMENTOS

Agradeço especial e inicialmente a Deus, por ter me dado tudo, desde o meu primeiro sopro de vida até a razão da minha existência. Seu sacrifício de amor verdadeiro, com o envio do seu filho unigênito para a morte, coroação e remissão dos pecados dos homens, guia-me em todas as horas, e busco sempre refletir um pouco de Sua luz para o mundo.

Aos anjos da guarda com os quais Ele ocupou a minha vida e resolveu chamá-los de Maria de Lourdes, minha mãe e maior torcedora, cujo carinho, amor e compreensão nunca me faltaram em nenhum segundo; Raimundo Sales, meu pai, por todo o apoio dado para que eu chegasse hoje à minha formatura e por ter me ensinado o valor de ser uma fortaleza familiar; Laíze Aquino e Wilcar Gondim, meus avós, que, desde cedo, instruíram-me com as mais valorosas lições humanas e de Deus com amor irrestrito, missas, lanches e medicina.

Ao meu irmão, cúmplice, herói e inspiração, Paulo Marcelo, ao qual devoto um amor incomensurável, agradeço pelas infinitas horas nas quais compartilhamos nossas visões sobre o mundo, compreendemos nossas existências, brigamos e cuidamos um do outro. Com certeza, trata-se meu irmão de um dos maiores instrumentos que Deus pôs na terra para o meu bem e para o de todos os pacientes que dele precisarem.

À minha companheira, Larissa Ricarte, presente na minha vida, por ter me ensinado o valor de um amor envolto pela mais bela e pura amizade, bem como por me inspirar, todos os dias, a tornar-me um homem melhor. Ao Pedro Junior, Patrícia, Bruno e Lucas Ricarte, por me aceitarem e constituírem a nova família que tanto me faz bem.

Ao meu segundo irmão, Lucas, e, por conseguinte, também minhas mães Luzinete e Norma, pessoas pelas quais tenho um amor fraternal, agradeço pelo constante crescimento que sempre vivemos juntos, o carinho, as brincadeiras infindáveis e as lições divididas.

Ao meu tio Fernando, pelo diagnóstico cardíaco e encaminhamento que renovaram a minha vida por completo, permitindo-me saciar a minha grande paixão pelos esportes, e ao meu primo Fabinho, que me dão demasiada alegria quando estão comigo. Igualmente, ao meu Tio Cid, o mais competente médico de que já ouvi falar, inspirando-me a querer ser um grande profissional, e pai de quatro crianças pelas quais nutro um amor incondicional.

Aos amigos que Deus pôs na terra para serem meus irmãos: Jáder, Leo, Gustavo e Igor, agradeço pelo amadurecimento conjunto, os risos incontroláveis e por todos os momentos que vivemos, ensinando-me a não levar a vida tão a sério desde tão cedo; Fradique, Elano, Brasil, Betão, Caio, Dudu, Fúlvio, Job, Paulo Victor, por toda a diversão, todo o desespero e por todas as emoções que vivemos nestes cinco anos de faculdade. Sinto-me um homem abençoado por ter dividido tantas histórias pitorescas e surpreendentes com todos.

Ao Sandoval e ao Paulo Henrique, que, em 2009, materializaram a vontade de Deus em minha vida e fizeram-me conhecer a Obra Lumen de Evangelização, comunidade católica com a qual já muito aprendi e que foi responsável por uma verdadeira renovação do meu espírito, fazendo-me ser um homem infinitamente melhor.

A todos os meus ex-colegas da AJURE-CE do Banco do Brasil, em especial Gelter, Antônio Carlos (AC BIKE), Walmar, Milene e Maria do Carmo, sou infinitamente grato pelas inúmeras lições e por todo o amadurecimento a mim proporcionados durante a nossa calorosa convivência diária naquele velho prédio no centro de Fortaleza.

Por fim, agradeço aos meus incríveis amigos e mentores Camilla Teófilo e Rodrigo Leitão, pessoas as quais Deus pôs em meu caminho para me fazer enxergar o meu futuro profissional e existencial, ajudando-me, ainda, na construção de valores éticos e inspirando-me grandiosas ideias.

RESUMO

A presente obra tem como escopo o estudo da comprovação da materialidade e da autoria nos crimes cibernéticos, ou seja, aqueles praticados pelo intermédio do uso de dispositivos tecnológicos. Aborda-se, inicialmente, as razões de a prática de atos ilícitos, no âmbito virtual, ter se tornado cada vez mais comum, a ponto de ser necessária a intervenção direta do Direito Penal na espécie para resguardar os interesses da população brasileira, a qual gradativamente se torna mais conectada à rede mundial de computadores. Analisa-se a legislação atinente à temática, em especial as leis federais n. 12.735/12 (Lei Azeredo) e n. 12.737/12 (Lei Carolina Dieckmann), que configuram as mais modernas armas de combate aos crimes informáticos no estado brasileiro. De igual modo, são discorridos os aspectos doutrinários de classificação e de terminologia relativos aos delitos informáticos, bem como se aborda a metodologia utilizada especialmente por *hackers* e *crackers* para a realização de seus ataques. Por fim, serão estudados os principais meios utilizados pelos órgãos de investigação criminal em nosso país em busca de uma eficaz produção de provas nessa seara, com vistas a possibilitar a condenação em juízo dos criminosos que aterrorizam o ordenamento por intermédio de sistemas informáticos.

Palavras-chave: Crimes Virtuais. Autoria e Materialidade. Investigação. Direito Penal Informático.

ABSTRACT

This work seeks to study the evidence of materiality and authorship in cybercrimes, in other words those practiced with the use of technological devices. Initially, discusses the reasons why illicit acts have become so increasingly common, in the cyber world, that it became necessary the direct intervention of the criminal law in order to protect the interests of the Brazilian population, which gradually becomes more connected to the World Wide Web. Analyzes the relevant legislation to the theme, in particular federal laws n. 12.735/12 (Azeredo Bill) and n. 12.737/12 (Law Carolina Dieckmann), which constitute which constitute the most modern weapons to combat computer crimes in the Brazilian state. It also discusses the doctrinal aspects of classification and terminology related to computer crimes, as well as discusses the methodology used especially by hackers and crackers to conduct their attacks. Finally, it studies the main means used by the criminal investigators in our country for an efficient production of evidence in order to allow the condemnation in court of criminals that terrorize through computer systems.

Keywords: Virtual Crimes. Authorship and materiality. Investigation. Computer Criminal Law.

SUMÁRIO

1. INTRODUÇÃO

A revolução tecnológica, vivida por nossa sociedade, desde meados do século XX, tem oferecido à população global, dentre outros aspectos, cada vez mais novos meios de promover a interatividade pessoal, facilitar a execução de tarefas diárias e outros meios que proporcionam demasiado conforto aos que aderem à utilização dessas novidades.

Com efeito, em relação a outros períodos históricos, denota-se atualmente um verdadeiro "boom" tecnológico, a exemplos da massificação do acesso à internet de banda larga e da queda vertiginosa dos preços ofertados ao consumidor para adquirir seu computador, laptop ou *smartphone* e ter acesso ao mundo cibernético.

Contudo, salta aos olhos que essas e outras inovações tecnológicas trouxeram à tona um número cada vez maior de invasões à privacidade das pessoas, furtos de informações pessoais, estelionatos e outros crimes praticados pelo âmbito informático, que "surfaram" a onda do incremento tecnológico para também desenvolverem-se.

De igual modo, verifica-se existir de uma verdadeira carência de informações e de meios de defesa disponibilizados para a população em geral contra essas novéis práticas delitivas. De fato, o estado brasileiro mostrou-se tão sonolento quanto à questão dos crimes informáticos que, não obstante a exploração comercial da internet ter sido iniciada em 1990, somente em 2012, ou seja, 22 anos depois, foi sancionada no Brasil uma lei que tratasse especificamente do enquadramento penal de diversas condutas ilícitas costumeiramente perpetradas no âmbito virtual.

Contudo, a efetiva aplicação do Direito Penal na responsabilização dos infratores virtuais esbarra, dentre outros aspectos, na incerta localização do autor, que busca, com a utilização do extenso espaço cibernético, livrar-se impunimente dos atos ilícitos que venha a cometer, recorrendo inclusive ao uso de diversas técnicas para camuflar-se ou para potencializar o alcance de suas empreitadas delituosas.

Nesse diapasão é que se almeja precipuamente, na presente obra, estudar-se a configuração material do crime informático e em que medida a computação forense e os demais elementos de investigação usualmente aplicados se amoldam às regras penais do nosso ordenamento, com vistas à comprovação da autoria infracional e a consequente condenação dos criminosos virtuais.

Na consecução do nosso objetivo, preliminarmente se abordarão as razões da necessidade de o Direito Penal intervir diretamente na matéria e como isto é feito, em nosso ordenamento, levando-se em consideração não só a natureza do Direito Penal, mas, também, tendo em vista as regras basilarmente estatuídas por nossa Constituição Federal.

Isso porque gradualmente se percebeu que as regras esparsamente previstas no ordenamento jurídico brasileiro não logravam êxito na tutela dos direitos dos usuários das redes mundial de computadores e locais privadas. Revelou-se, portanto, necessária a atuação do Direito Penal, com vistas à identificação das condutas humanas lesivas praticadas no universo digital cuja grave repercussão atenta não só contra os direitos individuais da vítima, mas acaba também por oferecer um alto risco à ordem como um todo, para consequentemente serem cominadas as respectivas penas em busca da proteção dos bens jurídicos mais relevantes.

Uma vez discorrida a importância da problemática na nossa atual era e sua relação com o Direito Penal, ser-nos-á mister verificar a resposta do estado brasileiro ante os delitos virtuais, tratando-se das leis promulgadas voltadas ao combate contra esses, nos moldes estabelecidos pela nossa Carta Magna.

De igual modo, cumpre-nos abordar quais as principais espécies de condutas delituosas perpetradas pela rede em nosso país, sem se olvidar do estudo da classificação dos crimes informáticos e da terminologia relacionada à temática de modo a facilitar a compreensão da matéria. Empós, serão analisados os usuais métodos utilizados pelos infratores para a consumação de seus delitos nesse âmbito.

No âmago do presente trabalho, por fim, entrar-se-á no incurso dos meios empregados pelos órgãos responsáveis pela persecução criminal em nosso país, tratando-se dos meios de provas mais eficazes e da medida a ser utilizada para o obtenção destas, para, então, finalizarmos com a análise da configuração e comprovação material do crime cibernético e da autoria por parte do agente executor, pretendendo-se viabilizar a justa condenação dos criminosos virtuais no ordenamento pátrio.

2. O DIREITO PENAL E A SOCIEDADE DA INFORMAÇÃO

A existência do Direito Penal é vital para possibilitar a existência do pacífico convívio dentro de uma comunidade social, independentemente do tamanho ou estado em que atualmente aquela se encontre.

Isso porque o homem, conforme saber rasteiro, trata-se de um ser social em amplos aspectos de sua própria existência, desde a necessidade basilar dele por um indivíduo do sexto oposto para que seja possível a perpetuação de sua espécie.

Por ser dotado de anseios, em diferentes níveis de intensidade, ocasiões há em que o homem atua externamente à esfera de domínio próprio para entrar na esfera de domínio comum de outro(s) indivíduo(s), ocasião em que se chocarão as vontades inerentes a cada um desses.

A ciência do Direito, por excelência, nasceu justamente para regular a medida da proporcionalidade das obrigações e dos direitos de cada um dos indivíduos, delimitando a tênue linha de possibilidade da atuação de um corpo sem que essa venha a causar injustos prejuízos a outrem.

O Direito Penal, em especial, recai na efetiva proteção dos bens inerentes à subsistência humana, aplicando uma sanção mais gravosa ao indivíduo que, por suas condutas, demonstrar demasiada periculosidade ao pacífico convívio social. Nesse sentido, a valiosa lição de Rogério Greco[1]:

> A finalidade do Direito Penal é proteger os bens mais importantes e necessários para a própria sobrevivência da sociedade, ou, nas precisas palavras de Luiz Regis Prado, "o pensamento jurídico moderno reconhece que o escopo imediato e primordial do Direito Penal radica na proteção de bens jurídicos - essenciais ao indivíduo e à comunidade". Nilo Batista também aduz que "a missão do direito penal é a proteção de bens jurídicos, através da cominação, aplicação e execução da pena". A pena, portanto, é simplesmente o instrumento de coerção de que se vale o Direito Penal para a proteção dos bens, valores e interesses mais significativos da sociedade.
>
> Com o Direito Penal objetiva-se tutelar os bens que, por serem extremamente valiosos, não do ponto de vista econômico, mas sim político, não podem ser suficientemente protegidos pelos demais ramos do Direito.

De fato, o significado dos bens, valores e interesses da sociedade como um todo flutua dinamicamente na medida em que a sua cultura se desenvolve.

[1] GRECO, Rogério. Curso de Direito Penal, vol. I. 13. Ed., Rio de Janeiro: Impetus, 2011, p. 2.

Especialmente, nota-se uma aceleração do processo evolutivo das sociedades contemporâneas, e por conseguinte da dinâmica do significado dos bens, valores e interesses daquelas, na medida em que são criados novos meios de tecnologia que permitem a existência de formas inéditas de as sociedades se relacionarem diretamente umas com as outras, bem como internamente.

O início da exploração comercial da internet na década de 90, graças à criação da rede mundial de computadores (*World Wide Web*), vertiginosamente incrementou a forma de as pessoas se comunicarem e compartilharem suas ideias. Com a criação de diversas páginas na *web* e de softwares de *Messenger* (tais como os mais famosos pioneiros ICQ e MSN Messenger), permitiu-se às pessoas terem rápido acesso a informações do mundo inteiro, compartilharem textos e mídias digitais, realizarem compras sem saírem de casa, efetuarem transações bancárias *online* pelo internet *banking* de sua instituição financeira etc.

Contudo, diversas pessoas perceberam que poderiam se utilizar do universo virtual para invadir dispositivos de seu interesse, mesmo estando eles localizados a milhares de quilômetros de distância, para obter informações pessoais do usuário e se beneficiarem com essas em detrimento da vítima. Algumas dessas formas de locupletação ilícita, por exemplo, tratam-se da realização de transações financeiras indevidas e a contratação de empréstimos utilizando-se os dados da vítima, porém em benefício do agressor.

De igual modo, a violação de direitos autorais e a propagação de conteúdo pornográfico, inclusive envolvendo crianças e adolescentes, encontrou fecundo campo no âmbito cibernético.

Adriane Ianzen (2013) explica que a distribuição de conteúdos digitais "(...) está cada vez mais facilitada devido ao avanço das tecnologias móveis e ao fácil acesso a qualquer comunidade. Ao mesmo tempo em que ocorre esse avanço, crescem a pirataria e a distribuição ilegal desses conteúdos".[2]

Nessa toada, é de todo importante que o Direito Penal se atualize igualmente ao surgimento de novas modalidades criminosas que possam ser perpetradas por meio da utilização de redes sem fios e da internet, sob pena de ser abalada a paz social que permite o convívio dentro do ordenamento jurídico.

[2] IANZEN, Adriane. PINTO, José Simão De Paula. CORREIO, Egon Walter Wildauer. Os sistemas de proteção de direito digital (DRM): Tecnologias e tendências para *e-books*. Encontros Bibli: Revista Eletrônica de Biblioteconomia e Ciência da Informação, 2013, Vol.18 (36), p.203.

Para tanto, dentre outras medidas, são necessárias não só a criação de novos tipos penais, mas também de leis que regulamentem a responsabilidade dos usuários da internet e, de igual modo, das empresas provedoras de acesso à rede mundial de computadores e provedoras de sítios eletrônicos, independentemente da natureza desses, para, conforme se verá, facilitar a tarefa processualística na correta e eficaz aplicação do Direito Penal na espécie.

Iniciando-se nossos estudos acerca das infrações penais cibernéticas, bem como as formas utilizadas atualmente pelos órgãos de persecução criminal para comprovar a autoria e a materialidade daqueles crimes, importa planear preliminarmente a concepção do Direito Penal. Desta forma, poderemos compreender o modo como são eleitos os bens jurídicos tutelados no ordenamento jurídico e a sua relação com o desenvolvimento da tecnologia e das relações sociais, que, transpondo fronteiras todos os dias, culminam no surgimento de novas formas de agressão, as quais devem ser albergadas pelo Direito.

2.1. Do Direito Penal e da seleção dos bens penalmente relevantes

A natureza do Direito Penal está intrinsecamente ligada à existência de violência e de excessos que gravemente ofendem o convívio em sociedade. Consoante se extrai do escólio do ilustre doutrinador Cezar Roberto Bittencourt[3], entende-se modernamente que a criminalidade é um fenômeno social normal, que não ocorre somente na maioria das sociedades de uma ou outra espécie, mas, sim, em todas aquelas constituídas por seres humanos. Utilizando-se dos ensinamentos de Durkheim, considerado um dos pais da Sociologia, o autor explica que:

> (...) o delito não só é um fenômeno social normal, como também cumpre outra função importante, qual seja, a de manter aberto o canal de transformações de que a sociedade precisa. Sob um outro prisma, pode-se concordar, pelo menos em parte, com Durkheim: as relações humanas são contaminadas pela violência, necessitando de normas que as regulem. E o fato social que contrariar o ordenamento jurídico constitui ilícito jurídico,

[3] BITTENCOURT, Cezar. Roberto. Tratado de Direito Penal: Parte Geral, 1. São Paulo: Saraiva, 2011, p. 46.

> cuja modalidade mais grave é o ilícito penal, que lesa os bens mais importantes dos membros da sociedade.

Nesse diapasão, tem-se que o Direito Penal é o responsável por identificar as condutas humanas cuja gravidade atente contra a ordem como um todo, cominando, em seu corpo, as sanções correspondentes à execução do ato criminoso. De tal modo, busca-se a prevenção da ocorrência de novos delitos e a repressão direta contra o infrator, confluindo ao anseio da sociedade de ver o transgressor da lei respondendo devidamente pela prática de atos, cuja ilicitude recai sobre os bens tidos como os mais valorosos para o ordenamento jurídico.

Com efeito, Deocleciano Torrieri Guimarães, define o Direito Penal como "parte do direito público com as penas cominadas para fatos que atentem contra a ordem, infrações e as sanções punitivas que lhes correspondem; direito criminal"[4].

Para Cezar Roberto Bittencourt[5] o Direito Penal pode ser concebido:

> (...) por um lado, como *um conjunto de normas jurídicas que tem por objeto a determinação de* infrações *de natureza penal e suas sanções correspondentes — penas e medidas de segurança.* Por outro lado, apresenta-se como um conjunto de valorações e princípios que orientam a própria aplicação e interpretação das normas penais. Esse conjunto de normas, valorações e princípios, devidamente sistematizados, tem a finalidade de tornar possível a convivência humana, ganhando aplicação prática nos casos ocorrentes, observando rigorosos princípios de justiça. Com esse sentido, recebe também a denominação de *Ciência Penal,* desempenhando igualmente uma função criadora, liberando-se das amarras do texto legal ou da dita *vontade estática do legislador,* assumindo seu verdadeiro papel, reconhecidamente valorativo e essencialmente crítico, no contexto da modernidade jurídica.

De fato, conforme visto, a convivência humana é capaz de moldar os seus valores a depender do contexto vivido pela sociedade. Desse modo, no âmbito penalista do Direito, tem-se a necessidade de se demarcar as fronteiras entre os fatos sociais que constituem ilícitos jurídicos penalmente relevantes e aqueles que não o são, levando-se em consideração as constantes mudanças ocorridas na sociedade, seja no que atine aos seus valores, seja em relação às novas modalidades de condutas lesivas que passem a

[4] GUIMARÃES, Deocleciano Torrieri. Dicionário Técnico Jurídico. 10ª ed., São Paulo: Rideel, 2008, p. 265.
[5] BITTENCOURT, Cezar Roberto. Tratado de Direito Penal: Parte Geral, 1. São Paulo: Saraiva, 2011, p. 48.

merecer guarida penal, advindas da constante invenção e modernização de tecnologias por parte do homem.

Isso porque, naquela seara, são previstas como sanções contra o infrator desde a aplicação de simples multas, penas restritivas de direito, penas privativas de liberdade ou, até mesmo, a máxime em represália humana: a pena de morte, o que, em regra, desestimula a realização da conduta infracional e, de igual modo, garante à vítima e à própria sociedade que o infrator venha a ser responsabilizado pelo seu ato tido como criminoso.

Veja-se que o Estado é o ente responsável pela promoção da heterotutela dos direitos subjetivos e pela pacificação entre os corpos sociais, em razão de um comum entendimento por parte dos seus tutelados de que a terceirização de tamanho poder corresponde à melhor opção civilizatória.

Ante o elevado alcance das medidas repressivas penalistas, deve ele, em cumprimento do seu dever constitucional, dispor de meios suficientes para que não incorra no subjetivismo de seus julgadores e, consequentemente, na promoção de verdadeira injustiça em seu ordenamento. Para tanto, é salutar a existência de uma sistemática baseada em critérios objetivos para a aplicação das normas de Direito Penal.

Nessa toada é que o Estado, em qualquer das manifestações de seu poder tripartido relacionadas ao Direito Penal, deverá ater-se imediatamente à letra da lei, tendo como norte as regras basilares estatuídas pela Constituição da República Federativa do Brasil de 1988, que asseguram aos cidadãos uma série de direitos e garantias fundamentais e visam à consecução dos objetivos fundamentais assumidos pelo estado brasileiro.

2.2. Princípios Penais Limitadores

Em decorrência da opção do legislador Constituinte de 1988 pela composição de um Estado Democrático de Direito pautado no respeito à dignidade da pessoa humana, uma série de princípios são observados em vigor na seara penal pátria, explícita ou implicitamente.

Sem a pretensão de se exaurir o tema, sob pena de bastante nos desviarmos da missão pretendida pelo presente trabalho, veremos especialmente dois desses

princípios, quais sejam o Princípio da Legalidade Penal e o Princípio da Intervenção Mínima, em razão de sua notória importância I) para resguardar o direito fundamental do homem de ser julgado apenas pela infração objetiva dos critérios legais, prevenindo-o contra a possível aplicação de arbítrios subjetivos por parte do Estado, e; II) para amoldar as condutas que merecem adequar-se penalmente, tudo com vistas à adequação típica das novas modalidades criminosas virtuais.

2.2.1. Princípio da Legalidade Penal

O princípio da legalidade, ou princípio da reserva legal, é amplamente albergado no ordenamento brasileiro, em especial na Constituição Federal de 1988, que em seu art. 5º, II, assevera que ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei.

Reverbera o princípio em comento precisamente a natureza do Estado Democrático de Direito, uma vez que, neste, a criticada concentração de poder absoluto nas mãos de um ente soberano dá lugar à preponderância das leis previstas no ordenamento, desde as resoluções e leis delegadas ali vigentes aos altivos preceitos da Constituição Federal.

Paulo Bonavides, citado por Rogério Greco[6], de forma elucidante ensina que:

> O princípio da legalidade nasceu do anseio de estabelecer na sociedade humana regras permanentes e válidas, que fossem obras da razão, e pudessem abrigar os indivíduos de uma conduta arbitrária e imprevisível da parte dos governantes. Tinha-se em vista alcançar um estado geral de confiança e certeza na ação dos titulares do poder, evitando-se assim a dúvida, a intranquilidade, a desconfiança e a suspeição, tão usuais onde o poder é absoluto, onde o governo se acha dotado de uma vontade pessoal soberana ou se reputa *legibus solutus* e onde, enfim, as regras de convivência não foram previamente elaboradas nem reconhecidas.

[6] GRECO, Rogério. Curso de Direito Penal, vol. I. 13. Ed., Rio de Janeiro: Impetus, 2011, p. 93.

Dessa forma, vislumbra-se que, no Brasil, o Estado não é uma figura cuja finalidade se encerra em si mesmo, porém é ele mais um meio de a própria população atingir sua finalidade de existência harmônica, amparada legalmente, com o fito de coibir a prática de atos ilícitos que desestruturem o equilíbrio do ordenamento.

No que atine ao Princípio da Legalidade Penal, tem-se que este se encontra expressamente previsto tanto no art. 5º, XXXIX, da CF/88, como também no art. 1º do Código Penal Brasileiro, cujas redações pouco diferem entre si, estabelecendo este último dispositivo que: "*Não há crime sem lei anterior que o defina. Não há pena sem prévia cominação legal*".

Daquele dispositivo, considerando-se ainda os corolários do Princípio da Dignidade Humana, referidas premissas sobressaem: I) necessário é que uma lei crie a figura do crime, ficando vedado no ordenamento o estabelecimento de crimes por costumes; II) de igual modo, como requisito para a punição de determinada conduta, esta tem que se amoldar à figura típica prevista em lei (tipicidade fechada), sendo proibida a aplicação da analogia *in malam partem* contra o agente.

Com efeito, no exercício do seu poder, o Estado esbarra em limites à excessiva intervenção penal formalmente, quando da elaboração de leis, e materialmente, quando da aplicação destas pelos julgadores, de modo a respeitar as garantias à liberdade individual da população e a segurança jurídica do ordenamento.

Sobre o tema, ensina o Juiz de Direito Alberto Jorge C. de Barros Lima[7]

> O princípio da legalidade opera como uma imposição restritiva ao legislador, atuando formalmente quando fixa regulações estruturais para o fabrico das normas penais, obrigando-o, via reserva legal, a valer-se do **processo legislativo** para criminalizar comportamentos. Somente a **lei**, portanto, em sua acepção mais estrita, pode criminalizar. Decretos, portarias, decretos-legislativos, medidas provisórias, estas últimas dotadas de força de lei, não podem, em razão de tal imposição, ter essa serventia. (p. 191)

Salta aos olhos, desse modo, a necessidade da tipificação legal das condutas perpetradas no mundo virtual que sejam configuradoras de lesividade ao direito alheio e apresentem riscos à ordem geral, para que o Estado possa intervir ativamente, com a movimentação do seu aparato administrativo, na aplicação das regras previstas no seu direito repressivo.

[7] LIMA, Alberto Jorge C. de Barros. Direito Penal Constitucional: A imposição de Princípios Constitucionais Penais, São Paulo: Saraiva, 2012, p. 191.

De fato, a vigilância tem de ocorrer tanto no sentido da prevenção à impunidade, com a adequação típica das condutas lesivas, como também no sentido de prevenir a aplicação de sanções penais desnecessárias em face de condutas que não apresentem gravidade ao ordenamento.

Com efeito, no mundo virtual, existem diversas categorias de atos invasivos à privacidade e lesivos aos direitos dos usuários da rede mundial de computadores, que podem ser perfeitos tanto com ou sem a anuência daquele, sendo essencial para o governo mapear quais condutas merecem a repressão estatal no âmbito do Direito Penal, quais àquelas que são usuais nas relações cibernéticas e que não apresentem lesividade e, por fim, quais as condutas que, não obstante se enquadrarem como atos ilícitos, não são de tal relevância a ponto de ser necessária a intervenção penal estatal.

2.2.2. Princípio da Intervenção Mínima

Como dito anteriormente, dos diversos fatos sociais que diuturnamente ocorrem no ordenamento, incumbe ao Direito Penal tutelar apenas aqueles de maior relevância à proteção e à garantia da ordem como um todo, necessários para uma pacífica convivência em sociedade.

Excluem-se, assim, os atos imorais ou outros ilícitos, cuja repercussão mais limitada não poderia dar ensejo ao acionamento da máquina estatal penalmente em busca de severamente reprimir o agente, incumbindo aos demais ramos do Direito coibir outras pessoas a absterem-se de praticá-los.

Sobre o tema, oportunamente leciona Rogério Greco[8], *in verbis*:

> O legislador, por meio de um critério político, que varia de acordo com o momento em que vive a sociedade, sempre que entender que os outros ramos do direito se revelem incapazes de proteger devidamente aqueles bens mais importantes para a sociedade, seleciona, escolhe as condutas, positivas ou negativas, que deverão merecer a atenção do Direito Penal. Percebe-se, assim, um princípio limitador do poder punitivo do Estado (...).

Não se pode olvidar que a seara penalista compõe um sistema jurídico macro que prevê sanções diversas em face de condutas que, de algum modo, lesem o direito de outrem, de modo que, na existência de um recurso menos gravoso a ser

[8] GRECO, Rogério. Curso de Direito Penal, vol. I. 13. Ed., Rio de Janeiro: Impetus, 2011, p. 46.

aplicado contra o autor do ato ilícito e que seja capaz de efetivamente solucionar o conflito, é preferível que este seja aplicado em detrimento das medidas coercitivas previstas no âmbito do Direito Penal.

Nessa linha, a precisa doutrina de Fernando Capez[9], que aduz:

> Da intervenção mínima decorre, como corolário indestacável, a característica de subsidiariedade. Com efeito, o ramo penal só deve atuar quando os demais campos do Direito, os controles formais e sociais tenham perdido a eficácia e não sejam capazes de exercer essa tutela. Sua intervenção só deve operar quando fracassam as demais barreiras protetoras do bem jurídico predispostas por outros ramos do Direito. Pressupõe, portanto, que a intervenção repressiva no círculo jurídico dos cidadãos só tenha sentido como imperativo de necessidade, isto é, quando a pena se mostrar como único e último recurso para a proteção do bem jurídico, cedendo a ciência criminal a tutela imediata dos valores primordiais da convivência humana a outros campos do Direito, e atuando somente em último caso (*ultima ratio*).

De igual modo, em reforço ao caráter subsidiário do Direito Penal, Roxin, citado por Rogério Greco[10], aduz, *ipsis litteris:*

> "A proteção de bens jurídicos não se realiza só mediante o Direito Penal, senão que nessa missão cooperam todo o instrumental do ordenamento jurídico. O Direito penal é, inclusive, a última dentre todas as medidas protetoras que devem ser consideradas, quer dizer que somente se pode intervir quando falhem outros meios de solução social do problema - como a ação civil, os regulamentos de polícia, as sanções não penais etc. Por isso se denomina a pena como a *'ultima ratio* da política social' e se define sua missão como proteção *subsidiária* de bens jurídicos."[4]

De fato, o Princípio da Intervenção Mínima não só indica quais os bens possuem maior importância para serem tutelados pelo Direito Penal, como também direciona o legislador no sentido da descriminalização daquelas condutas que, de acordo com o atual contexto social de um ordenamento, passaram a não mais apresentar-se como risco à harmonia dela em decorrência das mutações culturais ocorridas, desmerecendo a especial atenção da seara criminal.

Veja-se, por exemplo, que durante muito tempo se debateu entre os operadores de Direito a repercussão ofensiva da simples prática do consumo de drogas.

---

[9] CAPEZ, Fernando. Curso de Direito Penal, Parte Geral: (arts. 1º a 120). 15 ed., São Paulo: Saraiva, 2011, pgs. 38/39.

[10] GRECO, Rogério. Curso de Direito Penal, vol. I. 13. Ed., Rio de Janeiro: Impetus, 2011, p. 49.

Anteriormente à vigência da Lei n. 11.343/2006 (nova Lei de Drogas), o agente que fosse pego adquirindo, guardando ou trazendo consigo, *para uso próprio*, substância entorpecente sem autorização poderia ser condenado ao cumprimento de pena de detenção de seis meses a dois anos, além do pagamento de multa, segundo a redação do art. 16 da Lei Federal n. 6.368, que foi editada em 1976.

Atualmente, após a queda de diversos valores conservadores com o atual contexto cultural em que vivemos, bem como graças à percepção do legislador em relação a essas novidades, a novel Lei de Drogas, promulgada em 23 de agosto de 2006, passou a tratar de forma vertiginosamente diversa daquela acima vista o agente que porta drogas para o consumo próprio. Com efeito, não existe mais previsão de aplicação de pena restritiva de liberdade para o usuário, mas, tão somente, são aplicáveis a ele penas de advertência, prestação de serviços à comunidade e medida educativa de comparecimento a programa ou curso educativo, conforme o disposto no art. 28 do referido diploma legal[11].

Em caminho diametralmente oposto ao percorrido pelo legislador em relação ao porte de drogas para o consumo pessoal, segue o trato estatal em face da perpetração de atos ilícitos pelo mundo cibernético.

Notou-se uma profunda necessidade de atualização legal no decorrer dos últimos anos em relação à responsabilidade na utilização da rede mundial de computadores e de redes locais privadas, exsurgida da difusão bem mais acentuada dos meios de tecnologia à população brasileira e do acesso amplo à internet por parte desses.

Viu-se, com efeito, que os demais ramos do Direito não estavam sendo suficientemente efetivos na contenção de atos lesivos que vinham ocorrendo diuturnamente a partir do uso de dispositivos informáticos, sendo notória a necessidade de uma intervenção penal nesse âmbito virtual do nosso ordenamento.

Nesse diapasão, é que novos dispositivos legais passaram a ser criados para a criminalização dos atos mais perversos à incolumidade de nossa ordem, tais como os previstos na recente Lei Federal n. 12.737 de 2012, também conhecida como Lei Carolina Dieckmann, que trouxe em seu bojo novas modalidades delitivas de plena – e

[11] Art. 28 da Lei n. 11.343/2006: "Quem adquirir, guardar, tiver em depósito, transportar ou trouxer consigo, para consumo pessoal, drogas sem autorização ou em desacordo com determinação legal ou regulamentar será submetido às seguintes penas: I — advertência sobre os efeitos das drogas; II — prestação de serviços à comunidade; III — medida educativa de comparecimento a programa ou curso educativo".

justa - aplicação dentro do nosso ordenamento, conforme será melhor visto no tópico 3.1.

2.3. A Era da Tecnologia e o Direito Penal no Estado Democrático de Direito brasileiro

A Constituição Federal de 1988 marcou um importante período de transição entre o fim dos governos militares e a redemocratização do nosso país.

Em seu corpo, a Carta Política bem reflete os anseios da população por um Estado mais transparente, atento à voz de sua população e das necessidades desta. Com vistas à preponderância da dignidade da pessoa humana, nota-se que a Constituição implementou verdadeiramente um caráter de Estado Democrático de Direito em nosso país, estatuindo uma série de obrigações a serem prestadas pelo governo, possibilitando a cobrança do cumprimento daquelas por parte da população, elevando a um novo patamar crimes como o de racismo e outros especialmente degradantes, dentre outras importantes medidas, ampliando sobremaneira o leque de direitos fundamentais e garantias em nosso ordenamento.

Como consectário do implemento de um novo paradigma constitucional, todas as demais normas do ordenamento jurídico preexistentes tem de estar de acordo com os preceitos materiais ali estatuídos, sob pena de não serem recepcionadas completa ou parcialmente.

Nessa senda, em que pese o caráter repressivo e limitador de direitos inerente ao Direito Penal, tem-se que este teve também de acompanhar o regramento constitucionalmente previsto.

Tendo em vista a natureza socialdemocrata da nossa Carta Magna, a aplicação de diversas normas de ordem material e processual do Direito Penal sofreu alterações, seja por meio da reinterpretação dada pelos tribunais pátrios à luz da nova Constituição, seja pela sua não recepção no ordenamento (por exemplo, a Lei Federal n. 5.250/97, conhecida como Lei de Imprensa), ou, ainda, pela entrada de lei posterior que refletisse o atual contexto em que se insere o fato social anteriormente tido como criminoso, ab-rogando ou derrogando o regramento anterior.

Em solar elucidação do acima aduzido, veja-se o exemplo da Lei Federal n. 11.106/05. Dentre outras medidas, a referida lei revogou os arts. 217 e 219 do Código Penal, que dessoavam da atual conjuntura social do século XXI, na medida em que tipificavam a conjunção carnal e o rapto perpetrados contra mulheres, porém sob a condição de essas serem "honestas", ou seja possuírem bons costumes e decência, em desarrazoada discriminação contra todas as outras mulheres que não se encaixassem nesses subjetivos e questionáveis moldes.

Ainda, é digno de menção que o título o qual trata dos crimes sexuais passou por novas alterações para, finalmente, possibilitar também que pessoas do sexo masculino pudessem ser tidas como vítimas de crimes sexuais, como o estupro, em ressonância com o art. 5º, I, da CF/88, que aduz serem homens e mulheres iguais em direitos e obrigações, e com o princípio da dignidade da pessoa humana, fortemente presente naquela Carta Política.

Forçoso nos é reconhecer que a dignidade humana passou a ser o norte na formação de todo o Direito Penal em nosso ordenamento jurídico, de modo que cabe aos operadores de Direito aferirem a medida da adequação típica e da constitucionalidade dos fatos sociais elevados à categoria abstrata de conduta configuradora da norma penal incriminadora.

Ademais, digno mencionar-se a precisa lição do magistério de Fernando Capez[12], que disserta acerca da verificação, no caso concreto, da constitucionalidade do enquadramento típico, aduzindo *ipsis litteris:*

> Em outras situações, o tipo, abstratamente, pode não ser contrário à Constituição, mas, em determinado caso específico, o enquadramento de uma conduta em sua definição pode revelar-se atentatório ao mandamento constitucional (por exemplo, enquadrar no tipo do furto a subtração de uma tampinha de refrigerante). A dignidade humana, assim, orienta o legislador no momento de criar um novo delito e o operador no instante em que vai realizar a atividade de adequação típica.

Em que pesem os avanços em determinadas áreas da legislação penal, vislumbra-se que, atualmente, vigora um verdadeiro descompasso entre a velocidade com a qual diversos meios criminosos evoluem e o engessado processo por meio do qual o Poder Legislativo trata dessas inovações; especialmente, esse quadro emoldura o que ocorre com os crimes cibernéticos.

[12] CAPEZ, Fernando. **Curso de Direito Penal, Parte Geral : (arts. 1º a 120)**. 15. São Paulo: Saraiva, 2011, p. 25.

Com efeito, o século XXI, com seguidas revoluções tecnológicas, notoriamente apresentou inúmeras novas formas de as pessoas relacionarem entre si, reduzindo a fronteira de contato entre elas. Ora, era inimaginável na década de 1990 que qualquer pessoa poderia possuir um aparelho telefone móvel, conectar-se a uma rede de internet globalmente provisionada e se comunicar, em tempo real com áudio e imagem, com uma pessoa em qualquer lugar do planeta.

Contudo, empresas como a *Microsoft* (esta, por intermédio do seu software chamado *Skype*), vão além dessa experiência: proporcionam ao usuário a possibilidade de realizar uma videoconferência em que até 10 pessoas se comunicam simultaneamente em vídeo e áudio, bem como possibilitam que estes enviem arquivos entre si, e, em questão de frações de segundos, arquivos contendo milhares de informações são disponibilizados e compartilhados.

Esse é apenas um dos milhares de exemplos de novas tecnologias as quais estão ao alcance dos mais de setenta e cinco milhões de brasileiros usuários da internet[13] e que, contudo, podem ser utilizada para obliterar a imagem e a vida de uma pessoa, em fração de segundos, sem que ela sequer imagine.

Em uma visão maquiavélica e utilitarista, poder-se-ia chegar à seguinte equação lógica: milhares de pessoas tem acesso ao compartilhamento desenfreado de informações por meio da rede, assim como tem acesso a dados privados cujo compartilhamento não é desejado por seu possuidor; tais informações podem ser degradantes à imagem de uma pessoa, empresa ou até mesmo de um ente governamental; ante a impossibilidade atual de controlar o conteúdo que é transmitido por meio da rede, a solução mais eficaz seria cortar o meio de as pessoas se conectarem.

Contudo, a ordem mundial se insere em um contexto de exauriente globalização das relações culturais e comerciais, impulsionadas pelo incremento dos meios de comunicação, de modo que o livre acesso à internet mostra demasiados pontos positivos à coletividade para que seja barrado.

Com efeito, o direito à internet, em nosso ordenamento, se amolda aos preceitos da nossa "Constituição Cidadã" sob muitos aspectos, tais como a promoção dos meios de trabalho, pesquisa e ensino, manifestações culturais e de opinião, lazer etc., que podem efetivamente fazer parte de uma harmoniosa convivência em nossa

[13] De acordo com o apontamento do *World Factbook* (livro mundial dos fatos), disponibilizado e atualizado pela agência de inteligência americana (CIA) e que pode ser acessado no *link*: <https://www.cia.gov/news-information/featured-story-archive/2012-featured-story-archive/mobile-phone-and-internet-usage.html>. Acesso em 10.10.13, às 21:46.

sociedade, desde que utilizada a internet com responsabilidade, o que requer a atuação direta do Estado para tanto.

Por essas razões, não pode o nosso governo se abster de tratar o Direito da Informática do modo coerente com a atual magnitude que os novos meios de tecnologias se apresentam.

Fabrízio Rosa[14] assevera que, junto ao Direito Civil da Informática, o Direito Penal da Informática compõe os dois ramos do Direito da Informática, que assim se diferenciam, *ipsis litteris*:

> (...) pode-se definir o chamado Direito de Informática em dois ramos principais: o Direito Civil da Informática e o Direito Penal da Informática. No âmbito concernente ao Direito Civil da Informática, este passaria a concentrar seus estudos no conjunto de normas que regulariam as relações privadas que envolvem a aplicação da Informática, quais sejam: computadores, sistemas, programas, cursos, direitos autorais, documentos eletrônicos, assinaturas digitais etc. Já no que se refere ao Direito Penal da Informática, este seria o conjunto de normas destinadas a regular a prevenção, a repressão e a punição relativamente aos fatos que atentem contra o acesso, uso, exploração, segurança, transmissão e sigilo de dados armazenados e de sistemas manipulados por estes equipamentos, os computadores.

Nessa toada, deve o Direito Penal se adequar às novas realidades sociais, tanto pela via do Poder Legislativo, como também pela via do Poder Judiciário, a partir da reanálise e da reinterpretação das normas vigentes de modo a não permitir que novas modalidades de lesão ao direito das pessoas restem sem adequação típica e, consequentemente, sem uma contramedida repressiva por parte do Estado, tais como, por exemplo, a invasão de e-mails pessoais e a instalação de vírus tipo "keylogger"[15] para adquirir senhas de contas, cartões etc. e outras informações pessoais do usuário da internet, práticas que vem se desenvolvendo hodiernamente e são diretamente relacionadas ao Direito Penal da Informática.

[14] ROSA, Fabrizio, *in* Crimes de Informática, Campinas: Bookseller, 2005, p. 26.
[15] A palavra "keylogger" em português significa "registrador do teclado" em nosso vernáculo. Refere-se a um programa de computador do tipo *spyware*, que realiza o registro de tudo que é digitado pela vítima e envia as informações ao *hacker* que o implantou.

2.3.1. O Direito da Personalidade e a *internet*

De fato, atualmente muito se tem discutido sobre a relação do desenvolvimento dos meios de tecnologia e o direito da personalidade, que diuturnamente se confrontam, sendo costumeiras as notícias de violações àquele direito perpetrados pela rede mundial de computadores.

Isso porque, conforme exposto, em uma fração de segundos, imagens fotográficas, vídeos ou áudios relacionados a uma pessoa podem ser compartilhados de modo impetuoso, alcançando usuários da rede que inclusive se situem no outro lado do planeta, por vezes transformando a imagem daquela pessoa em um herói ou em um monstro sem que isto esteja ao seu controle.

De igual modo, os usuários da rede se utilizam do campo virtual para publicarem toda a sorte de opinião e, supostamente sob o manto da liberdade de expressão e de informação, acometem seus alvos com diversos tipos de conteúdo ofensivo ou efetivamente lesivo à sua imagem.

No entanto, temos que referidas liberdades frontalmente colidem com as regras de direito do nosso ordenamento, ainda que carente a legislação sobre o assunto, especialmente no que atine ao Código Civil brasileiro e à Constituição Federal.

Com efeito, o Código Civil, no seu capítulo II, preceitua a inviolabilidade da vida privada das pessoas naturais, outorgando inclusive ao juiz poderes para adotar as previdências que se fizerem necessárias para impedir ou fazer cessar o ato contrário a esse direito[16], bem como protege o direito de a pessoa proibir o uso indevido de sua imagem. Ainda, o art. 5º, V, da Constituição Federal de 1988 assegura o direito de resposta, proporcional ao agravo, além da indenização por dano material, moral ou à imagem do ofendido.

Nesse diapasão, confira-se a lição de Gisele Asturiano (2013):

> As notícias, os furos, são invasões à privacidade. Ora, são pessoas que têm direito a privacidade, estão sendo transformadas, estão sendo maculadas e lesadas. Muito bem posiciona-se Anderson Schreiber sobre a atuação do Judiciário a respeito do tema: "[...] o intérprete e o magistrado têm, nos casos relativos ao uso indevido de imagem, o dever de suprir a omissão legislativa, verificando se a hipótese diz respeito ao exercício da liberdade de

[16] Art. 21 do Código Civil: "A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma".

> informação. Em caso positivo, deve-se proceder à ponderação entre os dois direitos fundamentais em conflito: a liberdade de informação e o direito à imagem. (SCHREIBER, 2011, p. 110)". Há a dicotomia liberdade de expressão vs. direito à privacidade, em ambiente virtual, onde as pessoas são expostas para o mundo como se fosse um portal, onde praticamente não há volta. [...] A internet conta com o acesso de milhões de pessoas, sendo criadas mais de 2 mil homepages por dia, além de comunidades virtuais que representam, tendências e tribos de vários pontos do planeta. O avanço da tecnologia da informação evidentemente não vem acompanhado pelo avanço legal, sendo de responsabilidade do intérprete e do magistrado o dever de suprir a omissão legislativa a fim de verificar se a hipótese proposta diz respeito à liberdade de informação, ponderando o conflito à intimidade e à imagem das pessoas

Recentemente, por exemplo, noticiou-se nacionalmente a morte de uma estudante de apenas 17 anos que, após terem sido espalhadas gravações de vídeo em que aparece tendo relações sexuais com mais duas pessoas, publicou mensagens em suas contas do Instagram e do Twitter pedindo desculpas à sua família e, em seguida, tirou a própria vida[17]. A divulgação da gravação foi impulsionada pelo aplicativo para dispositivos móveis Whatsapp, que, com poucos cliques, permite a transmissão de mídias coletivamente para grupos de até 50 participantes ou individualmente para usuários cadastrados naquele.

A amplitude e a repercussão das transmissões ocorridas pela rede mundial de computadores é deveras incalculável, bem como descobrir o autor das primeiras divulgações não autorizadas é uma árdua tarefa para os órgãos de investigação estatais. Contudo, não pode isso servir de desculpa para a contínua violação do direito da personalidade das pessoas que venham a ser alvo de tais manifestações, que deverão anuir com a utilização de sua imagem para tanto, conforme explica Fabio Siebeneichler de Andrade (2013):

> Quanto ao consentimento, cumpre saber se ele deve ser necessariamente expresso ou pode ser tácito (90). Em se tratando de cessão de direito da imagem, há que se ponderar o caráter excepcional desta modalidade de negócio, razão pela qual a sua interpretação deve ser, em principio, restritiva. Na jurisprudência do Superior Tribunal de Justiça esta tem sido a orientação,

[17] SENA, Yala. PI: Polícia investiga morte de garota após vazar vídeo íntimo na internet, 2013. Disponível em: < http://noticias.terra.com.br/brasil/policia/pi-policia-investiga-morte-de-garota-apos-vazar-video-intimo-na-internet,1bf47a0bb8852410VgnVCM10000098cceb0aRCRD.html>, acessos em 02.12.2013 , às 11:51.

> tendo sido objeto de decisão que não se deve ampliar o disposto em cláusulas contratuais (91). Por conseguinte, somente em situações muito claras deve ser aceito como valido o consentimento tácito em relação a cessão do Direito de imagem, o que corresponde a disposição do artigo 111 (92). Um exemplo neste sentido aparece em decisão que considerou presente a autorização para uso de fotos da pessoa em revista de cunho erótico, em decorrência do conjunto probatório, que continha - a par do contrato firmado pela parte - também entrevista que confirmava o consentimento do uso da imagem (93). Em outro caso, o STJ considerou presente o consentimento tácito ao decidir que se ocorre a exposição da imagem em cenário público - e na hipótese tratava-se de topless - não se poderia considerar como indevida a sua exposição pela imprensa, uma vez que a proteção a privacidade encontra limite na própria exposição realizada (94).

Sobre a matéria, ainda, o Superior Tribunal de Justiça firmou entendimento (Súmula 403) no sentido de que independe de prova do prejuízo a indenização pela publicação não autorizada de imagem de pessoa com fins econômicos ou comerciais.

Nessa senda, sobressai a obrigação de responsabilização do autor de publicação ofensiva à honra de alguém, daquele que vem a divulgar material íntimo pertencente a outrem de forma não autorizada, enfim, de todos aqueles que de alguma forma venham a realizar atos ilícitos em detrimento da personalidade alheia valendo-se das mídias digitais para tanto.

Com vistas à preservação da imagem do ofendido, a justiça dispõe e deve utilizar-se de meios inibitórios ou repressivos às referidas práticas ilícitas quando provocado, tudo de acordo com a lei, seja determinado a interdição de páginas contendo publicações ofensivas, a imposição de filtros nos mecanismos de pesquisa providenciado por sites como o www.google.com ou outras medidas que se fizerem necessárias. Com efeito, o direito à preservação da intimidade daqueles tutelados pelo ordenamento deve sobrepor-se à desenfreada liberdade incutida nos usuários da rede cibernética.

3. LEGISLAÇÃO ESPECÍFICA NO BRASIL E OS PRINCIPAIS CRIMES CIBERNÉTICOS

De fato, o crescente número de acessos à internet, no Brasil, corre de braços dados com o aumento de ocorrências delituosas perpetradas por intermédio da rede.

Segundo a revista eletrônica Techtudo[18], um levantamento feito pela Bitdefender, empresa privada que desenvolve premiados softwares antivírus, revelou que existem mais de 94,2 milhões de pessoas utilizando a internet em nosso país e quase a metade delas (45%) usam algumas das redes sociais existentes (Facebook, Twitter, Instagram etc.). De igual modo, aferiu-se que a cada 15 segundos um brasileiro é vítima de fraudes com informações ou documentos furtados pela internet.

Ademais, de acordo com o Relatório Norton 2013[19], desenvolvido pela empresa de segurança virtual Symantec, 22 milhões de pessoas foram vítimas de crimes virtuais no Brasil entre outubro de 2012 e outubro de 2013, resultando em um custo líquido superior a R$ 18 bilhões para as vítimas.

Em que pese o notório avanço dos meios de tecnologia e a disseminação universal desses, o Poder Legislativo brasileiro, durante muito tempo, adotou uma postura de indiferença à essa importante problemática. Simultânea e progressivamente, pessoas mal intencionadas desenvolviam meios de potencializarem os efeitos das suas práticas delituosas, contando com a deficiência legal existente em nosso ordenamento.

Em face da óbvia incapacidade das regras preexistentes no ordenamento brasileiro de sanarem a crescente onda de crimes perpetrados pela rede, gerando uma indignação generalizada, nosso legislador finalmente saiu da inércia para, em 2012, tratar especificamente daqueles.

Cumpre-nos, nesse momento, tratar da legislação atinente à temática, bem como discorrer sobre os aspectos doutrinários de classificação e terminologia relacionados à temática, para então tratarmos dos crimes mais comumente praticados naquele âmbito e a metodologia utilizada pelos agentes na consumação das suas práticas delitivas amparadas pelos meios informáticos.

---

[18] GALLI. Gabriel. Conheça os crimes virtuais mais comuns e proteja-se. TechTudo, 2013. Disponível em: <http://www.techtudo.com.br/noticias/noticia/2013/08/conheca-os-crimes-virtuais-mais-comuns-em-redes-sociais-e-proteja-se.html>, acesso em: 13.10.2013, às 18:17.

[19] SYMANTEC. Relatório Norton 2013: Custo por Vítima do Cibercrime cresce 50%. Disponível em: <http://www.symantec.com/pt/br/about/news/release/article.jsp?prid=20131002_01>, acessos em: 01.11.2013, às 16:27.

3.1. Lei Federal n. 12.737/12 (Lei Carolina Dieckmann)

A Lei Federal n. 12.737/12, também conhecida extraoficialmente como Lei Carolina Dieckmann, foi sancionada em 2012 e entrou em vigor em abril deste ano no Brasil, elevando à categoria de infrações penais diversas condutas perpetradas pelo meio virtual, contudo somente após 22 do início da comercialização da internet, refletindo o grave atraso do nosso Poder Legislativo em face da matéria.

A aprovação dessa lei foi acelerada em virtude do midiático caso da atriz Carolina Dieckmann, que teve fotos íntimas copiadas do seu computador pessoal por "crackers[20]" e foi chantageada por estes a efetuar o pagamento de R$ 10.000,00 (dez mil reais) para que as imagens não fossem divulgadas. Como a atriz não se dobrou à vontade dos criminosos, as fotos foram divulgadas pela rede e o caso chamou a atenção da mídia nacional.

De fato, esse não foi o primeiro caso de furto de conteúdo privado por intermédio do uso da internet, tampouco a primeira extorsão perpetrada em virtude da obtenção de dados ou informações pessoais de outrem pela rede; contudo, o evento serviu de estopim para que a mídia nacional e a população pressionassem o poder público para legislar acerca da matéria e investir na segurança voltada à tecnologia da informação, visando à punição de condutas que antes não eram crimes, bem como à facilitação da persecução do autor das infrações cibernéticas.

Assim, a Lei Federal n. 12.737/12, dentre outras medidas, felizmente acresceu o art. 154-A ao Código Penal Brasileiro, que criminaliza uma série de condutas que antes poderiam, eventualmente, configurar apenas o dever de reparação pelos danos morais e materiais causados na seara civil.

Com efeito, o *caput* do mencionado artigo dispõe que: invadir (ou seja, entrar sem autorização em) dispositivo alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança, condicionado à finalidade de: i) obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo, ou de; ii) instalar vulnerabilidades para obter

[20] "Crackers" são comumente confundidos com os *hackers*, contudo apresentem acentuadas diferenças que serão melhor vistas no tópico 3.3 desta obra**.** Antecipa-se rasamente que o termo "cracker" se refere àquele que decodifica senhas e informações criptografadas pertencentes a outrem para utilização própria, seja para fins maliciosos, altruísticos ou pelo simples "desafio" de conseguir burlar um mecanismo de segurança digital.

vantagem ilícita, constitui crime ao qual é cominada a pena de três meses a um ano de detenção e multa.

Verifica-se com facilidade que qualquer dispositivo eletrônico se inclui no tipo penal em comento, independentemente de estar conectado à rede mundial de computadores, a exemplo de *pen drives*, *tablets* ou aparelhos celulares.

Contudo, uma importante observação há de ser feita: o *caput* do artigo 154-A do CP menciona que a invasão deve ocorrer "(...) *mediante violação indevida de mecanismo de segurança* (...)", razão pela qual, em respeito ao Princípio da Legalidade, a conduta do agente só se adequará tipicamente se houver a violação de mecanismo de proteção no dispositivo.

Desse modo, pelo mencionado artigo, não pode ser punida a conduta do infrator que invade dispositivo alheio sem ter de violar qualquer mecanismo de defesa. Exsurge-se, de igual modo, a importância - ainda maior - de os usuários de dispositivos eletrônicos utilizarem sempre alguma forma de proteção no seu sistema operacional, tal como o uso de antivírus, *firewall* ou senhas complexas para o acesso às informações ali armazenadas.

No caso supracitado, referente à atriz Carolina Dieckmann, por exemplo, os cinco acusados podem ser condenados pela prática de extorsão, difamação e formação de quadrilha, todos estes crimes previstos no Código Penal. Porém não podem ser punidos pelo ato de devassar os dados contidos no computador da atriz. Isto porque a invasão ao computador da atriz, feita por intermédio da internet, não configurava nenhum tipo penal à época dos fatos, não podendo ser os autores acusados pela infração ao art. 154-A do Código Penal, tendo em vista o basilar princípio da irretroatividade da lei penal incriminadora.

Ademais, o parágrafo primeiro do artigo em relevo pune, com pena igual à prevista no *caput*, quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com intuito de realizar a prática das condutas definidas no *caput*. São penalizados, portanto, o programador que usa suas habilidades e conhecimento técnico para a prática de condutas ilícitas e as pessoas que comercializam meios de invasão cibernética.

Resta agravada a pena, de um sexto a um terço da pena, de acordo com o entendimento do magistrado condutor do feito, quando se afere, no caso concreto, efetivo prejuízo econômico, seja este da proprietária do dispositivo invadido ou de qualquer pessoa que se tornar vítima da invasão, conforme o parágrafo 2º do art, 154-A.

Dentro do artigo em questão, existe uma qualificadora do crime de invasão, qual seja a previsto no parágrafo 3º, que aduz: "*Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido*". Para esta modalidade criminosa, prevê-se pena duas vezes maior àquela cominada no *caput*, ou seja reclusão de seis meses a dois anos.

Com efeito, referido parágrafo denota grande importância no combate aos crimes contra a inviolabilidade dos segredos estatuídos no nosso Código Repressivo. Antes da vigência da lei 12.737/12, contra a devassa das comunicações privadas e a divulgação de segredos comerciais, por exemplo, poder-se-ia enquadrar o infrator nas tenazes dos arts. 151 e 153, respectivamente, cuja soma das penas não ultrapassa um ano de detenção.

Ora, conforme saber rasteiro, a pena de detenção só pode ser cumprida em regime fechado em situações excepcionais, quando o juízo da execução da pena verifica a ineficácia do cumprimento da pena, por parte do condenado, em regime prisional semiaberto ou aberto, momento em que ele pode determinar a transferência para o regime fechado. Já na pena de reclusão, o magistrado sentenciante pode, quando preenchidos os requisitos, determinar o regime inicial de cumprimento da pena pelo condenado já em regime fechado.

Cumpre salientar, ainda, que, para o incurso do infrator na reprimenda do parágrafo 3º do art. 154-A do CPB, basta que ele obtenha os objetos ali descritos. Se além de obtê-los o delinquente ainda os divulgou, comercializou-os ou os transmitiu a terceiro, seja a título oneroso ou gratuito, a pena é aumentada de um a dois terços.

Sobre a invasão qualificada, digna de menção é a observação feita pelo advogado e especialista em Direito Penal Auriney Brito[21], que disserta não só sobre o controle remoto de dispositivo por *hackers*, mas também traz à tona um caso concreto grave, o qual pouco foi divulgado à época de sua ocorrência, consoante se verifica no transcrito a seguir:

> Um ponto interessante a ser ressaltado na Invasão qualificada, é o *controle remoto do dispositivo invadido*. É muito comum hoje a prática do *Distributed Denial of Service Attack (Ddos Attack)* que tem causado prejuízos incomensuráveis à empresas que perdem o seu sistema por um tempo após um ataque como esses. O

[21] BRITO, Auriney. Análise da Lei 12.737/12 – "Lei Carolina Dieckmann". Atualidades do Direito, 2013. Disponível em: <http://atualidadesdodireito.com.br/aurineybrito/2013/04/03/analise-da-lei-12-73712-lei-carolina-dieckmann/>, acesso em: 18.10.2013, às 11:15.

> detalhe é que o sistema da empresa não é invadido, mas em razão de uma sobrecarga de acesso dos seus recursos num mesmo momento.
>
> Pouco se noticiou, mas o mês de março de 2013 foi marcado pelo maior ataque cibernético da história, e essa (Ddos) foi a técnica utilizada. Também chamada de *Ataque de* Amplificação, foi somado à um grande conhecimento de estratégias militares e direcionado à uma empresa que combate *spams* na rede (Spamhaus), o que acabou por atrapalhar o funcionamento da internet em quase todo o mundo. Tem-se notícia que a "guerra" se deu por motivos de disputa empresarial entre duas grandes empresas do ramo.
>
> Isso ocorre quando um *cracker* instala o seu programa malicioso e vários computadores de vários usuários, que passam a obedecer os comandos do seu "líder", tornam-se máquinas "zumbis". Ao seu comando, todos acessam o servidor vítima até que ele esgote sua capacidade de atendimento e trave ou reinicie, causando graves lesões ao seu patrimônio. No ano de 2012, os *sites* de várias empresas como TAM, GOL, Bancos BRASIL, BRADESCO e outros, foram atacados dessa forma. Muitas não assumem o ataque para não transparecer vulnerabilidade e insegurança aos clientes, mas os prejuízos são milionários.
>
> Apenas o *controle remoto* configura crime do 154-A. O Ataque pode configurar o crime do Art. 266 do Código Penal, também introduzido pela nova lei (...)".

O último parágrafo do artigo em comento determina o aumento da pena de um terço até a metade na hipótese de o crime ser praticado contra algum membro da administração pública que, em razão do cargo que ocupa, possui alto poder de direção e, por conseguinte, informações sigilosas e de alta relevância para os interesses do poder público. São eles: I) o Presidente da República, governadores ou prefeitos; II) Presidente do Supremo Tribunal Federal; III) Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa Estadual, de Câmara Legislativa do Distrito Federal ou de Câmara Municipal, e, enfim; IV) dirigente máximo da administração direta e indireta federal, estadual, municipal ou Distrito Federal.

A Lei 12.737/12, seguindo a lógica da seção IV do Código Penal, que dispõe acerca crimes contra a inviolabilidade dos segredos, acresceu o art. 154-B, estatuindo que a ação penal pela infração aos crimes definidos no art. 154-A, em regra, somente será instaurada mediante representação (ação pública condicionada). Contudo, excepcionalmente, a ação penal será pública incondicionada, quando o crime for cometido contra a administração pública direta ou indireta de qualquer dos poderes da União, Estados, Distrito Federal ou Municípios ou, ainda, contra empresas concessionárias de serviços públicos, dada a relevância da finalidade das atividades por eles exercidos.

Em outra linha, a Lei 12.737/12 também acresceu o parágrafo para o art. 266 do Código Repressivo, que criminaliza a interrupção ou perturbação de serviço telegráfico, radiotelegráfico ou telefônico, dificultando-lhe ou impedindo o restabelecimento destes.

Agora, na mesma pena prevista para o *caput* do dispositivo em comento, incorre aquele que interrompe serviço telemático ou de informação de utilidade pública, dificultando-lhe ou impedindo o restabelecimento. Visou o legislador a impedir a atipicidade da conduta daquele que causa transtornos à regular utilização dos meios que compõem a telemática, que pode ser entendido como o conjunto de serviços informáticos fornecidos através de uma rede de telecomunicação[22], que realizam transmissão à distância de informações.

Por fim, cumpre mencionar que também foi acrescido um parágrafo único ao art. 298 do Código Penal pela lei em relevo, que equipara ao documento particular de que trata o *caput* daquele dispositivo os cartões magnéticos de crédito ou débito, cominando pena de um a cinco anos para o falsário.

3.2. Lei Federal n. 12.735/12 (Lei Azeredo)

A Lei Ordinária nº 12.735/12 foi resultado de um longo processo legislativo, cuja origem remonta ao Projeto de Lei nº 84 de 1999, proposto pelo Deputado Federal Luiz Piauhylino.

Referido projeto de lei originalmente continha dezoito artigos que geraram bastante polêmica[23], sendo a maioria deles subtraída pelo seu Relator, o Deputado Federal Eduardo Azeredo, cujo sobrenome tornou-se o nome extraoficial da Lei n. 12.735, que foi sancionada em 2012, bem como outros dos artigos aprovados receberam o veto da então Presidente da República Dilma Roussef.

Em seu texto original, restavam incriminadas diversas condutas, tais como obter, transferir ou fornecer dado ou informação pessoal, sem autorização, por meio da

[22] Definição da palavra "telemática" de acordo com o Dicionário Priberam da Língua Portuguesa, 2013, disponível em <http://www.priberam.pt/dlpo/telem%C3%A1tica>. Acessado em 02.11.2013 às 00:30.

[23] PIAUHYLINO, Luiz. **PL 87/1999**. Projetos de Leis e Outras Proposições, Câmara dos Deputados, disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=15028>, acessos em 18.10.2013, às 16:31.

internet e divulgar, utilizar, comercializar ou disponibilizar dados ou informações pessoais contidas em sistema informatizado com finalidade distinta da que motivou seu registro.

Contudo, o texto final, que foi aprovado e entrou em vigor no ano de 2013, estatui basicamente apenas dois artigos relevantes ao nosso ordenamento.

Primeiramente, o art. 4º da Lei 12.735/12, de caráter eminentemente político, reforça a tarefa de combate contra os crimes cibernéticos por parte do Estado, estatuindo que: "*os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado*".

Com efeito, a criação de delegacias especializadas no combate aos crimes perpetrados pela rede mundial de computadores intensificou-se em meados de 2010. Atualmente, segundo a associação SaferNet[24], entidade voltada ao enfrentamento de crimes e violação a direitos humanos pela internet, já existem diversas delegacias especializadas em pleno funcionamento em pelo menos 12 estados brasileiros.

O artigo 5º da Lei Azeredo, a seu turno, alterou o inciso II do § 3º do art. 20 da Lei n. 7.716/89, que trata do combate ao racismo no Brasil. Anteriormente, estava o juiz autorizado a promover a cessação de transmissões radiofônicas e/ou televisivas que praticassem qualquer das condutas discriminatórias previstas no *caput* do art. 20 da Lei 7.716/89, quais sejam: "Praticar, induzir ou incitar a discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional". Agora, além daquelas transmissões já previstas, o magistrado poderá fazer cessar transmissões eletrônicas ou de publicação por qualquer meio, um avanço significativo no combate a essa sorte de crime.

3.3. Os Crimes Cibernéticos no Brasil

Neste tópico, serão analisados a classificação dos crimes de informática e os termos técnicos relacionados ao tema, que usualmente são desconhecidos ou utilizados de forma errônea não só pela população em geral, mas também por profissionais que de alguma forma trabalham com o tema.

[24] A lista com alguma dessas delegacias pode ser aferida no seguinte link: <http://www.safernet.org.br/site/prevencao/orientacao/delegacias>. Acessado em 23.10.2013, às 21:10.

De igual modo, dar-se-á incurso nas principais infrações criminais praticadas no universo digital, tratando especialmente daquelas modalidades infracionais menos debatidas pelos operadores do Direito, delineando-se, ainda, os principais métodos utilizados pelos delinquentes para lograrem êxito em suas empreitadas criminosas.

3.3.1. Classificação

Com vistas ao enquadramento das condutas realizadas no âmbito virtual do ordenamento jurídico, a doutrina criou diferentes formas de classificar os crimes cibernéticos, que levam em consideração, dentre outros fatores, o tipo de conduta lesiva, o *modus operandi* do agente e o bem jurídico visado por ele.

Com efeito, os atos ilícitos realizados por intermédio de um dispositivo informático podem configurar figuras típicas classicamente apontadas pelo nosso Código Penal, bem como podem configurar uma modalidade delitiva exclusivamente perpetrada no âmbito virtual. Sobre os crimes informáticos, Coriolano Aurelio[25], em preciso escólio, aduz que:

> Segundo Dr. Paulo Quintiliano, crimes informáticos são todos aqueles praticados com a utilização do meio da tecnologia. Ou seja, definimos crimes de alta tecnologia como todos aqueles que se utilizam de ferramentas e instrumentos tecnológicos sofisticados para a práticas de delitos. Por exemplo, os criminosos se utilizam de um sistema de captação de sinais de rádio para captar informações a distância os dados e informações a respeito das operações que estão sendo realizadas naquele momento por caixas eletrônicos com o objetivo de posteriormente promover saques nessas contas. Por outro lado, em um método menos sofisticado, o criminoso pode implantar dentro do terminal bancário uma pequena maquina leitora de dados. Essa máquina pode enviar informações por meio de sinais de radiofrequencia, na versão mais avançada, ou mesmo, deve ser retirada pelo criminoso ao final de um determinado período, para que ele possa colher os dados de que precisa para a pratica do ilícito.

[25] SANTOS, Coriolano Aurelio de almeida Camargo. FRAGA, Ewelyn Schots. As múltiplas faces dos Crimes Eletrônicos e dos Fenômenos Tecnológicos e seus reflexos no universo Jurídico, 2ª ed., São Paulo: OAB-SP, 2010, p. 32. Disponível no endereço: <http://www.oabsp.org.br/comissoes2010/direito-eletronico-crimes-alta-tecnologia/livro-sobre-crimes-eletronicos/Livro2Edicao.pdf/download>, acessado em 04.11.2013, às 21:45

Nessa senda, para Maria Helena Junqueira Reis, citada pela bacharel Virgínia Soprana Dias[26], as infrações cibernéticas podem ser classificadas em razão do seu objetivo. Elucida aquela autora que:

> (...) poder-se-iam separar dois temas, em que constariam do primeiro os crimes regulados pelo instituto do Código Penal e das leis especiais e, do segundo, os demais, decorrentes da tecnologia dos computadores. Isso quer significar que existiriam os crimes em que o sujeito que os pratica visa a um bem juridicamente protegido, mas interno ao universo virtual ou dele dependente – necessariamente ou não –, em que a rede, no caso, seria mera ferramenta para a prática de algum tipo penal; e, diametralmente, existiriam também os crimes em que o agente visa à prática de atos exatamente referentes à rede de computadores, em que o sistema da rede é em si o objetivo material da conduta.

Postulamos a classificação doutrinária dos crimes virtuais aduzida por Túlio Lima Vianna, em Fundamentos de Direito Penal Informático, que classifica os crimes informáticos em quatro espécies, quais sejam os crimes informáticos impróprios, próprios, mistos e mediatos ou indiretos. Conforme explica Emanuel Alberto (2013)[27], para aquele autor, classificar-se-iam em *crimes informáticos impróprios* "(...) 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)"; já os *crimes informáticos próprios* seriam "(...) aqueles em que o bem jurídico protegido pela norma penal é a inviolabilidade das informações automatizadas (dados)"; os *delitos informáticos mistos*, a seu turno, seriam "(...) crimes complexos em que, além da proteção da inviolabilidade dos dados, a norma visa a tutelar bem jurídico de natureza diversa" e; por fim, os *crimes informáticos mediatos ou indiretos* seriam os delitos-fim não informáticos que herdam esta característica do delito-meio informático, o qual foi realizado para possibilitar a sua consumação.

Sucintamente, passemos ao detalhamento dessas espécies.

Veja-se que, nos crimes virtuais propriamente ditos, o agente necessariamente faz uso do sistema informático para lesionar a vítima, violando as

---

[26] DIAS, Virginia Soprana. Aspectos da Segurança Jurídica no Âmbito dos Crimes Cibernéticos**.** *Proceedings of the Second Internacional Conference of Forensic Computer Science Investigation*, 2007, p. 87. Disponível em: <http://www.icofcs.org/2007/ICoFCS2007-pp12.pdf>, acessado em 22.11.2013 às 07:55.

[27] GIMENES, Emanuel Alberto Sperandio Garcia. Crimes Virtuais. Revista de Doutrina da 4ª Região, Porto Alegre, n. 55, ago. 2013. Disponível em: <http://www.*revistadoutrina*.trf4.jus.br/index.htm?http://www.revistadoutrina.trf4.jus.br/artigos/edicao055/Emanuel_Gimenes.html>, acesso em: 22.11.2013, às 08:21.

informações contidas em seu domínio cibernético pessoal, constituindo, desse modo, o sistema informático um objeto e meio para a execução de uma conduta tipificada. Exemplificando essa modalidade delitiva, pode-se citar a interceptação de comunicações telefônicas, de informática ou telemática, sem autorização ou com objetivos não autorizados em lei, conduta típica prevista no art. 10º da Lei Federal n. 9.296/96, para a qual é cominada a pena de dois a quatro anos de reclusão.

No que atine aos crimes virtuais impróprios, o computador, na verdade, é utilizado como instrumento para a execução de um determinado crime não-informático que não envolva ofensa ao bem jurídico inviolabilidade da informação automatizada (dados). É dizer, o dispositivo tecnológico é meio para a consumação de um delito-fim, que se enquadra em uma figura típica, cujo *iter criminis* não envolve o acesso ao dispositivo pessoal de outrem. Por exemplo, a utilização de um computador para, conectando-se a uma rede social como o *facebook*, o infrator cometer crimes contra a honra de um desafeto seu.

A seu turno, os crimes informáticos mistos previstos em lei tem o escopo de tipificar a conduta de violação das informações automatizadas e, simultaneamente, tutelar um bem juridicamente relevante para o ordenamento que possua natureza diversa. Em elucidação, pode-se mencionar o crime previsto no art. 72, I, da Lei Federal n. 9.504/97 (conhecida como Lei das Eleições), no qual é cominado a pena de cinco a dez anos de reclusão ao agente que "obter acesso a sistema de tratamento automático de dados usado pelo serviço eleitoral, a fim de alterar a apuração ou a contagem de votos".

Finalmente, os delitos informáticos mediatos ou indiretos herdam esta característica em virtude do delito-meio informático que foi utilizado para que fosse aquele consumado, ocorrendo, na espécie, pelo menos duas figuras típicas. Conforme o caso, pode ser aplicado o princípio da consunção na espécie, por exemplo, na medida em que o delito-meio informático é meio necessário ou normal fase de preparação ou de execução de outro crime[28], como na invasão a dispositivo informático alheio, crime previsto no art. 154-A do Código Penal, por parte do agente que visa exclusivamente à obtenção dos dados pessoais e do cartão de crédito da vítima para a transferência de numerários desta para ele. Com efeito, nesse contexto fático, o infrator responderia pela subtração dos valores, não sendo cabível ser ele punido em relação à invasão, atividade-meio.

[28] GRECO, Rogério. Curso de Direito Penal, vol. I. 13. Ed., Rio de Janeiro: Impetus, 2011, p. 30

3.3.2. Terminologia do Sujeito Ativo

Os crimes intentados no ambiente virtual destoam essencialmente dos demais tipos de crime em razão do distanciamento físico entre o agressor e o ofendido; de fato, ao invés de uma ação física movida diretamente à pessoa do ofendido, os criminosos cibernéticos utilizam-se de dispositivos eletrônicos para emanar ordens de quebra de senhas, transferências de arquivos, dados, valores monetários etc., ou códigos criptografados que são convertidos em mensagens, tudo com o fito de perpetrar o ato ilícito.

Com efeito, esse distanciamento torna a internet um fecundo campo para a prática de delitos por parte de *hackers* e de *crackers* mal intencionados, principais sujeitos autores de crimes cibernéticos.

A definição do termo *hacker* é controversa, explicando o juiz federal Emanuel Gimenes que se entende como *hacker*:

> (...) uma pessoa com grande conhecimento na área de informática. Mas, segundo Plantullo, (19) **"**é uma pessoa física que detém, como objeto, a investigação da integridade e da segurança de um sistema qualquer de computador. Utilizasse de técnicas avançadas para invadir sistemas e detectar suas respectivas falhas. Todavia, não os destrói ou prejudica".[29]

Em que pese a conotação pejorativa usualmente imputada ao termo *hacker* pela mídia e pela população como um todo, tem-se que os *hackers* não necessariamente atuam de modo danoso à sociedade. São eles pessoas que detém conhecimento acima da média na área da informática, sendo capazes de inventar ou modificar mecanismos tecnológicos, encontrar brechas de segurança e, utilizando-se desses métodos, destinar uma finalidade diversa da originalmente pretendida pelo mecanismo.

Michael Simpson, na obra "Hands-on Ethical Hacking and Network", explica que "*hackers* éticos" são contratados por empresas para aferirem o nível de segurança das redes e dos sistemas privados delas, por meio de testes de segurança e de penetração.

---

[29] GIMENES, Emanuel Alberto Sperandio Garcia. Crimes Virtuais. Revista de Doutrina da 4ª Região, Porto Alegre, n. 55, ago. 2013. Disponível em: <http://www.revistadoutrina.trf4.jus.br/index.htm?http://www.revistadoutrina.trf4.jus.br/artigos/edicao055/Emanuel_Gimenes.html>, acesso em: 01.11.2013, às 13:50.

Segundo o autor, ditas empresas utilizam-se da máxima que "*você somente está seguro na medida do seu elo mais fraco*", sendo esses expertises da informática essenciais para descobrir o elo mais fraco da segurança da tecnologia de informação da empresa. *Ipsis litteris*, aduz o referido autor:

> Remember the old adage: You're only as secure as your weakest link. The bad guys spend a lot of time and energy trying to find weak links. (…)
> Companies sometimes hire ethical hackers to conduct penetration tests. In a penetration test, an ethical hacker attempts to break into a company's network to find the weakest link in the network or a network system. In a security test, testers do more than attempt to break in; they also analyze a company's security policy and procedures and report any vulnerabilities to management[30].

O *cracker*, a seu turno, conforme definição apresentada pelo website da TechTarget[31], é aquele que se especializa em invadir computadores de outras pessoas, normalmente por meio de acesso à mesma rede à qual pertence o alvo. Podem burlar senhas ou licenças necessárias para a utilização de softwares pagos ou, em outra linha, invadem e superam a segurança de dispositivos eletrônicos alheios.

A finalidade do ataque de um *cracker* varia bastante, podendo ser ela delitiva – a mais usual em nosso país -, altruística ou pelo simples "prazer" de vencer o desafio. Um exemplo de "cracking" se deu no notório caso da atriz Carolina Dickmann, em que um *cracker* enviou um programa malicioso, por *spam,* à caixa de e-mails da atriz, que, após o download desse, ficou exposta à invasão do *cracker*, sendo consequentemente furtadas diversas fotos pessoais do seu computador.

---

[30] Traduz-se: "Lembre-se do velho adágio: V*ocê somente está seguro na medida do seu elo mais fraco. Os caras maus gastam uma enorme porção de tempo e de energia tentando achar elos fracos. (...) Companhias algumas vezes contratam hakers éticos para conduzirem testes de penetração. Em um teste de penetração, um haker ético tentar invadir a rede de uma companhia para achar o elo mais fraco na rede ou no sistema da rede. Em um teste de segurança, aqueles que testam fazem mais do que tentar invadir; eles também analisam a política e os procedimentos de segurança de uma companhia e reportam qualquer vulnerabilidades à gerência"*. Em: SIMPSON, Michael T. BACKMAN, Kent. CORLEY, James E. Hands-on Ethical Hacking and Network Defense, Boston: Course Technology Cengage Learning, 2013, p. 1.

[31] ROUSE, Margaret. *Cracker definition.* TechTarget SearthSecurity Disponível em: <http://searchsecurity.techtarget.com/definition/cracker>, acesso em 01.11.2013, às 14:53.

3.3.3. Principais Infrações e os métodos utilizados pelos criminosos

Existem diversos tipos de ataques perpetrados por criminosos no universo virtual, configurando alguns desses figuras tipicamente previstas na lei.

Os diversos sítios eletrônicos que noticiam sobre a matéria, bem como a doutrina relacionada[32], apontam uma unanimidade: no Brasil, o crime mais comumente cometido pela internet trata-se do roubo de identidade. De igual modo, afere-se a usual ocorrência de furtos de dados (arquivos) pessoais, crimes relacionados à pedofilia e materiais pornográficos contendo crianças e adolescentes, atos ofensivos à honra de outrem (calúnia, injúria, difamação), ameaças, crimes de discriminação e, ainda, a ocorrência de espionagem industrial.

De fato, no roubo de identidade e no furto de dados, os criminosos, utilizando-se de variados métodos, obtém informações ou arquivos pessoais da vítima para a realização de diversos crimes, a depender do nível de ousadia, conhecimento técnico e de periculosidade do infrator.

Veja-se, inicialmente, que a utilização da tecnologia pode constituir meio para a prática de outras figura típicas que não estão vinculadas à informática e que de outro modo poderiam ser perpetradas, amoldando-se à classificação supra exposta dos chamados crimes informáticos impróprios, mistos ou mediatos, de acordo com o caso. Nessa toada, as informações e os arquivos pessoais obtidos são utilizadas para realizar transações comerciais ilícitas, transferências financeiras, extorquir a vítima etc., podendo os delinquentes responderem pelos crimes de estelionato (art. 171, CP), furto qualificado (art. 155, § 4º, II, CP), extorsão (art. 158, CP), formação de quadrilha (art. 288, CP), dentre outros.

Contudo, afere-se igualmente a configuração de crimes cibernéticos propriamente ditos que estão previstos na nossa legislação, devendo ser aferido o tipo

[32] Sobre o tema, valiosas lições se extraem da obra de SANTOS, Coriolano Aurelio de almeida Camargo. FRAGA, Ewelyn Schots. As múltiplas faces dos Crimes Eletrônicos e dos Fenômenos Tecnológicos e seus reflexos no universo Jurídico, 2010, São Paulo: OAB-SP, disponível no endereço: <http://www.oabsp.org.br/comissoes2010/direito-eletronico-crimes-alta-tecnologia/livro-sobre-crimes-eletronicos/Livro2Edicao.pdf/download>, acessado em 04.11.2013, às 21:45. Outrossim, importantes são as seguintes matérias no trato da temática: GALLI, Gabriel. Conheça os crimes virtuais mais comuns em redes sociais e proteja-se, disponível em: <http://www.techtudo.com.br/noticias/noticia/2013/08/conheca-os-crimes-virtuais-mais-comuns-em-redes-sociais-e-proteja-se.html>; CARPANEZ, Juliana. Conheça os Crimes Virtuais mais comuns. Jornal Folha de S. Paulo. Disponível em: <http://www1.folha.uol.com.br/folha/informatica/ult124u19455.shtml>, todos acessados em 04.11.2013, às 21:45.

penal incorrido pelo agente, no caso concreto, de acordo com a via por ele eleita para a obtenção das informações e dos arquivos pessoais

Com efeito, cumpre-nos, neste momento, abordar com maior profundidade os crimes de informática propriamente ditos, esclarecendo em que linha ocorre o *modus operandi* desses delitos e outras importantes observações, uma vez que os demais crimes já estão por demasiado debatidos pela rica doutrina e jurisprudência pátria, fugindo do nosso objetivo.

Assim, para a obtenção dos dados, uma das principais formas de invasão a dispositivos eletrônicos, utilizada por *hackers* mal intencionados, é infectando-os com m*alwares* (softwares maliciosos), que, de acordo com Abhisek Singh (2008), são programas feitos para causar danos e/ou interromper a máquina infectada e outras máquinas ligadas a ela em rede[33], podendo também fazer o furto de informações pessoais de usuários do dispositivo infectado, seja este móvel (computadores de bolso, como *smartphones*, *tablets* e *laptops*) ou não.

Os *malwares* podem ser classificados em 4 tipos: *worms*, *trojans*, vírus e, por fim, *spywares* e *adwares.*

Os *worms* são softwares maliciosos que são programados automaticamente para se espalharem de uma máquina para outra com finalidades diversas. Como ensina Abhishek Singh (2008), os *Mass-Mailing Worms*, por exemplo, espalham-se por meio do envio em massa de mensagens para vários endereços de e-mail que são coletados da máquina da vítima, resultando na famosa prática de *Spam*. Uma espécie desse tipo de *worm*, citado pelo autor[34], trata-se do *mass-mailing worm* W32.Assarm@mm, que envia mensagens respondendo a todas as mensagens não lidas que estão na caixa de entrada do *software Microsoft Outlook.* O problema é que, normalmente, ditas mensagens vem acompanhadas de outros tipos de *malwares*, que acabam entrando despercebidamente na máquina do usuário e resultam em graves consequências.

A seu turno, os *trojans*, ou "cavalos de Tróia" como são popularmente conhecidos, são programas que se disfarçam de *softwares* bons e enganam o usuário a executá-los, existindo atualmente uma infinidade de *trojans* criados por *hackers* maldosos. Uma vez executados, os *trojans* podem, dentre outras tarefas, enviar e-mails

[33] Texto na íntegra: "Malware stands for Malicious Software. Malicious softwares are programs, which are designed to damage and/or disrupt the infected machine and/or other networked machines. It can be classified into four types". SINGH, Abhishek. SINGH, Baibhav. JOSEPH, Hirosh. Vulnerability Analysis and Defense for the Internet. Nova Iorque: Springer Science+Business Media, p. 169, 2008.

[34] No original, aduz o autor: "For example, W32.Assarm@mm is a mass-mailing worm that sends messages in reply to all unread messages in the Microsoft Outlook Mailbox", *ibid*, p. 170.

(como no caso dos *mass-mailing worms)*, destruir dados da máquina, fazer o download de arquivos, fornecer acesso remoto do computador infectado ao *hacker* que programou o *malware* etc – lembrando que o controle remoto não autorizado do dispositivo invadido, por si, já constitui crime previsto no art. 154-A, parágrafo 3º, do CPB.

Especialmente, existem os chamados *Password-Stealing* (PSW) *Trojans*, que, segundo Abhishek Singh (2008), roubam senhas e/ou informações (de cartões de crédito, contas de e-mail etc) diretamente do computador da vítima e mandam para o autor do vírus por e-mail ou por arquivo para uma unidade de armazenamento remoto. É o caso do clássico *Trojan-IM. Win-32*, que rouba senhas de programas de mensagens instantâneas como o *ICQ* e o *Msn Messenger*.

Por sua vez, o vírus trata-se de um código executável (programa) que pode se replicar de um lugar para outro, repetidas vezes, e atingir a sua finalidade no sistema, seja ela benigna ou maligna. Diferencia-se do *trojan*, basicamente, em razão de o vírus ser potencialmente ofensivo à operacionalidade do dispositivo infectado como um todo (por exemplo, ele pode impedir que um computador inicialize o sistema operacional, tornar defeituoso o funcionamento do mouse, do teclado etc), enquanto o outro, disfarçado como um *software* bom para a máquina, busca na verdade criar uma porta dos fundos no sistema para que o autor do *malware* possa utilizar a máquina infectada como se fosse administrador desta, devassando o conteúdo ali contido, enviando mensagens em nome do proprietário etc.

Por fim, os *spywares* e os *adwares* são *softwares* que, uma vez introduzidos secretamente na máquina invadida, ajudam o seu autor a juntar informações sobre o usuário ou sobre uma organização sem que estes tenham conhecimento, tais como os horários de funcionamento da máquina, quais as páginas mais acessadas, que tipo de propagandas da *web* são logo cortadas pelo usuário etc. Em posse dessas informações, o autor dos *softwares* repassam a pessoas ligadas à publicidade ou outros interessados.

De fato, os *malwares* claramente são ferramentas configuradoras dos novos delitos introduzidos em nosso ordenamento pela Lei Federal nº 12.737/12. Com efeito, no que atine ao delito previsto no art. 154-A daquele diploma, os *malwares* se enquadram tanto como instrumentos de violação de mecanismo de segurança para a obtenção de dados ou informações do titular do dispositivo, como também se tratam de vulnerabilidades para a obtenção de vantagem ilícita.

De igual modo, não se pode perder de vista o disposto no parágrafo terceiro do artigo em comento, que remonta aos típicos crimes de espionagem, porquanto

criminaliza a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais e informações sigilosas por meio da invasão do dispositivo eletrônico.

Cumpre salientar, ainda, que a produção, mero oferecimento, distribuição, venda ou difusão dos *softwares* maliciosos constitui crime no ordenamento pátrio, consoante o disposto no parágrafo 1º do art. 154-A do CPB.

Com efeito, uma outra poderosa ameaça na rede virtual trata-se das chamadas "Botnets", que são redes de computadores que obedecem às ordens de um *hacker* ou de um grupo de criminosos em virtude do êxito destes na invasão a diversos dispositivos, como se fossem as máquinas verdadeiros "zumbis", podendo serem utilizadas para diversas finalidades. Sobre o tema, confira-se a didática abordagem de Fausto Salvadori em matéria veiculada pelo *website* da Revista Galileu[35]:

> "Uma das funções das botnets é atuar em operações de "negação de serviço": basta ao dono da rede ordenar que seus milhares de computadores acessem ao mesmo tempo um determinado site. O volume de tráfego será tão grande que o servidor não dará conta da movimentação, e o site sairá do ar - uma ação que tanto pode ser *feita* para prejudicar empresas como para desestabilizar serviços estatais. O principal uso das botnets, contudo, é espalhar spams: sem que os donos das máquinas percebam, os computadores-zumbis são usados para enviar e-mails não solicitados para milhões de usuários, boa parte deles carregados de programas maliciosos. Graças às botnets, os spams respondem por 85% de todos os 100 bilhões de e-mails que os terráqueos trocam diariamente entre si".

Conforme visto anteriormente, a ordenação desse tipo de ataque requer o controle remoto da máquina e, portanto, trata-se do crime de invasão qualificada previsto no art. 154-A, parágrafo 3º, do CPB. Contudo, uma importante observação merece ser feita no que atine aos *spams* realizados por *hackers* criminosos, seja por meio das *botnets*, *worms* ou outra forma utilizada.

Em virtude da crescente conscientização dos usuários da internet sobre os riscos aos quais eles são expostos, bem como pela evolução dos *softwares* antivírus, cada vez mais as formas de ataques dos criminosos cibernéticos vem se aperfeiçoando, especialmente para ludibriar a vítima, camuflando-se a lesão que se está cometendo, ao

[35] SALVADORI, Fausto. Crimes Vrituais. Revista Galilei, Editora Globo. Disponível em: <http://revistagalileu.globo.com/Revista/Common/0,,EMI110316-17778,00-CRIMES+VIRTUAIS.html> acesso em 08.11.2013, às 10:31.

revés de simplesmente oferecer à vítima o download de um arquivo nocivo, como anteriormente era feito.

Nessa toada, uma prática que se tornou forte e assombrosamente presente na rede se trata do "phishing", que é disseminado usualmente por meio do *spam*, ou seja, o envio em massa de mensagens para diversos usuários da internet.

O termo "phishing" é uma derivação utilizada pelos *hackers* para se referir à palavra inglesa *fishing*, que, traduzindo para o português, significa "pescaria". Consiste o *phishing* realmente na "pesca" de informações e dados pessoais da vítima, que pode ser feita por métodos mais ou menos tecnológicos, mas sempre induzindo a vítima em erro.

Nos ataques mais primitivos, o *phishing* é feito mediante o envio de uma mensagem falsa para a vítima por e-mail, em que o criminoso se faz passar por uma empresa ou um órgão os quais possuem credibilidade notória, tais como bancos ou até mesmo órgãos do poder judiciário, e alega a necessidade de a vítima realizar alguma medida de urgência. De outro modo, a vítima pode ser levada a acreditar que está diante de uma grande oportunidade financeira por um anúncio publicitário, enquanto navega na internet.

Diante de tais situações, a vítima é induzida a urgentemente preencher cadastros, fornecendo endereço, número de cartão de crédito, dados pessoais, como o número da carteira de identidade e da sua inscrição no cadastro de pessoas físicas etc., que são utilizados pelos criminosos para a realização de empréstimos bancários, transações financeiras indevidas a partir da conta da vítima ou para a aplicação de outras fraudes.

Nessas condições, pensamos não existir a ocorrência de uma figura delitiva própria do direito penal da informática, mas se afere, na verdade, a consumação do crime de estelionato, previsto no art. 171 do Código Penal, em razão de a vítima, induzida a erro, voluntariamente fornecer meios para que o criminoso obtenha vantagens em detrimento daquela.

Mencione-se, ademais, que o crime *phishing* pode envolver o emprego de meios mais avançados de tecnologia, como o *defacement* e a efetiva utilização de *malwares*.

Com efeito, o *defacement*, conforme noticiado pela revista Consultor Jurídico[36], consiste em "alterar um *site* visualmente e se equivale a uma pichação na internet. *Sites* de instituições públicas são alvos constantes desse tipo de invasão, utilizada por grupos *hackers* para fazer protestos de cunho político". Desse modo, os *hackers* criminosos utilizam-se da técnica para maquiar um *website* e enganar a vítima que, por exemplo, acreditando estar realmente navegando do sítio eletrônico do seu banco, uma vez que digitou corretamente o endereço eletrônico daquele, inscreve os dados referentes à sua conta bancária nos campos ali demonstrados, os quais serão todos encaminhados, contudo, para o(s) autor(es) do truque.

Quando o sítio eletrônico da empresa almejada possui uma defesa superior à técnica de invasão do *hacker*, um outro caminho a ser percorrido por ele é a criação de um *website* em moldes muitos parecidos ao da instituição original. Desse modo, o criminoso envia mensagens alertando as vítimas sobre a necessidade de atualização de dados, ou alguma outra estória para ludibriá-la, juntamente com o *link* do *website* por ele criado para que a vítima forneça seus dados supondo estar no endereço eletrônico correto, e, da mesma forma acima descrita, as informações acabam parando nas mãos dos criminosos.

Por fim, o *phishing* pode ser ainda mais nocivo à vítima, quando ela, além de ter sido ludibriada pela estória dos delinquentes, faz o *download* de *malwares* para o seu dispositivo ao verificar o anexo da mensagem ou efetivamente visitar o *link* enviado pelos autores dessa. Aqui, independentemente do fornecimento voluntário da vítima dos seus dados e informações pessoais, os infratores invadem a máquina dela e, deste modo, estão aptos a realizar as diversas finalidades já estudadas por meio dos *malwares* maliciosos.

[36] Na matéria, informa-se sobre um ataque, que houve em março deste ano, por um grupo de *hackers* ao site do Tribunal Regional Federal da 5º Região, no qual eles substituíram a página do Tribunal por uma gravura apologista ao nazismo e teceram diversas críticas. A notícia pode ser lida na íntegra pelo *link* <http://www.conjur.com.br/2013-mar-23/site-trf-invadido-grupo-hacker-coloca-ilustracao-hitler-ar>, acessado em 08.11.2013, às 10:53.

4. A COMPROVAÇÃO DA AUTORIA E DA MATERIALIDADE NOS CRIMES CIBERNÉTICOS

Uma vez discorrida a importância da problemática no nosso atual contexto social, a resposta do Estado ante os crimes cibernéticos com a promulgação de leis voltadas ao combate contra aqueles, nos moldes estabelecidos pela nossa Carta Magna, bem como os principais meios utilizados por criminosos nesse âmbito, é chegada a hora de entrarmos no incurso da comprovação dos elementos que compõem o tipo penal cibernético no caso concreto, necessários à punibilidade do agente infrator.

Nos é mister, neste momento, tratar da responsabilidade e dos limites inerentes aos órgãos de investigação criminal e persecução penal, para, adiante, analisarmos a configuração material do crime cibernético e em que medida a computação forense e os demais elementos de investigação se amoldam às regras penais do nosso ordenamento na busca da condenação dos criminosos virtuais.

4.1. A investigação criminal cibernética, no ordenamento brasileiro, para a persecução criminal

A Constituição Federal de 1988 elenca, em seu art. 144, os órgãos que devem diretamente exercer a preservação da ordem pública, da incolumidade das pessoas e do patrimônio destas. Dentre outras maneiras, o exercício dessa preservação pode ocorrer, em um momento preliminar, mediante a prevenção da ocorrência de um crime (mediante vigilância ostensiva por parte da polícia militar, por exemplo), bem como quando da apuração dos elementos que constituem a infração penal ocorrida concretamente, extraindo-se substrato probatório suficiente para a deflagração de uma ação penal e a consequente absolvição ou condenação do acusado.

Conforme saber rasteiro, a persecução criminal, buscando a apuração da infração penal e sua respectiva autoria em nosso ordenamento, em sua forma ordinária, divide-se em duas fases essenciais, a saber: a primeira, trata-se da fase inquisitiva, onde a autoridade policial realiza o inquérito policial; a segunda é a denominada fase processual, marcada notoriamente pela presença do contraditório e da possibilidade de

ampla defesa por parte do investigado, que se eleva da categoria de mero suspeito para efetivamente tornar-se acusado, pelo Estado, de ser o autor do fato típico.

Nas palavras de Nestor Távora[37], com a ocorrência da infração criminal, "(...) é salutar que se investigue com o fito de coligir elementos que demonstrem a autoria e a materialidade do delito, viabilizando-se o início da ação penal". Especialmente, nos crimes virtuais, é necessária a imediata provocação da força policial ou do Ministério Público para que seja possível a investigação do delito, uma vez que o rastro deixado pelos criminosos nesse âmbito, além de escassos e difíceis de serem seguidos, rapidamente podem sumir, seja pela reorganização dos dados internos do dispositivo invadido, seja em virtude da limpeza dos vestígios por parte dos delinquentes.

Para tanto, referidos órgãos se utilizarão de diversas técnicas periciais exclusivas do âmbito informático e outros meios de prova para a obtenção da verdade real dos fatos. Nas palavras de Fernando Capez[38], o meio de prova "(...) compreende tudo quanto possa servir, direta ou indiretamente, à demonstração da verdade que se busca no processo. Assim, temos: a prova documental, a pericial, a testemunhal etc."

Vigora na processualística penal brasileira o entendimento da não-limitação dos meios de prova, especando os tutelados da injusta aplicação da lei penal no caso concreto. Segundo Fernando Capez[39], a jurisprudência e a doutrina são unânimes em assentir que os meios de prova elencados no Código de Processo Penal são meramente exemplificativos, sendo possível a produção de outras provas distintas daquelas ali enumeradas, respeitando-se, logicamente, as demais regras e princípios previstos em nosso ordenamento.

Nessa toada, uma vez tendo a autoridade policial ciência da notícia do crime (*notitia criminis*), provocada ou espontaneamente, a primeira medida-chave em geral da investigação, conforme explica a Procuradoria da República no Estado de São Paulo (2006), é identificar o meio utilizado para a perpetração do crime. *Ipsis litteris*, aduz o manual disponibilizado por aquele órgão federal[40]:

---

[37] TÁVORA, Nestor. ALENCAR, Rosmar Rodrigues, em "Curso de Direito Processual Penal", 5º ed. ver. ampl. e atual., Bahia : JusPODIVM, 2011, p. 89,

[38] CAPEZ, Fernando. Curso de Processo Penal. 19ª ed., São Paulo: Saraiva, 2012, p. 394.

[39] CAPEZ, Fernando, loc. cit.

[40] MINISTÉRIO PÚBLICO FEDERAL. Procuradoria da República no Estado de SP. Crimes Cibernéticos. Manual Prático de Investigação, 2006, p. 15. Disponível em: <http://www.mpce.mp.br/orgaos/CAOCRIM/pcriminal/ManualdeCrimesdeInform%C3%A1tica-versaofinal.pdf>. Acessos em 21.11.2013, às 00:45.

> Quando recebemos a notícia de um crime cibernético, a primeira providência a tomar é a identificação do meio usado: trata-se de a) um *website*?; b) um e-mail?; c) programas de troca de arquivos eletrônicos (do tipo Kazaa)?; d) arquivos ou mensagens ofensivas trocados em programas de mensagem instantânea (do tipo MSN Messenger ou ICQ)?; e) arquivos ou mensagens ofensivas trocados em salas de bate-papo (chats)?; f) grupos de discussão (como yahoo groups)?; ou g) comunidades virtuais como o Orkut? As características de cada um desses meios são diferentes e, por isso, as medidas a serem tomadas são igualmente distintas.

Segundo informa o manual de investigação supra mencionado, o mais importante elemento para a investigação de um crime cibernético, com efeito, trata-se do número do IP (*Internet Protocol*) do autor do fato típico. Esse número é recebido pelo usuário sempre que ele se conectar à rede mundial de computadores e, durante o tempo em que ele estiver conectado, o IP será o seu identificador. O tema será aprofundado quando tratarmos da comprovação da autoria dos delitos cibernéticos.

Usualmente, a colheita do depoimento da vítima ou do depoimento do denunciante, mostra-se cabal para o fornecimento dos elementos preliminares que nortearão os rumos do procedimento investigatório dos delitos cibernéticos.

Nos crimes que envolvam material pornográfico envolvendo crianças e adolescentes (crimes informáticos impróprios), por exemplo, o depoimento do denunciante revelará quem lhe enviou o material ou qual o sítio eletrônico em que ele foi disponibilizado, possibilitando à polícia seguir uma trilha em busca daquele que produziu o material pornográfico ou, pelo menos, daquele que primeiramente disponibilizou na internet o conteúdo.

Em outra linha, nos crimes de invasão a dispositivos eletrônicos (crimes cibernéticos propriamente ditos, mistos ou mediatos), o depoimento da vítima será cabal para o direcionamento das investigações, informando quais foram os primeiros sinais de comportamento estranho na operação do dispositivo, tais como lentidão do computador ou da navegação na internet, quais os *websites* estranhos que foram ultimamente acessados etc.

Empós a colheita dos depoimentos pertinentes, revela-se de extrema importância o imediato recolhimento do dispositivo pessoal, que foi objeto de invasão ou que teve acesso direto ao "local do crime" (a página da rede social contendo as ofensas ou o *link* para o download do arquivo pornográfico envolvendo menores etc.).

Em posse da máquina pessoal, ou não, diversas técnicas serão utilizadas pelos investigadores em prol da persecução criminal. Algumas destas, para a colheita de provas impossíveis de serem repetidas em juízo durante a instrução processual, em virtude do rápido desaparecimento dos vestígios.

Interessa-nos, neste momento, abordar os meios de provas aplicáveis, especialmente aqueles que são exclusivos para essa seara criminal, na persecução dos crimes cibernéticos, todas eles destinadas à realização dos consectários constitucionais de vigilância e preservação dos bens humanos, materiais ou não, uma vez que formarão o lastro probatório mínimo suficiente para a deflagração da ação penal (indícios de autoria e de materialidade do delito) ou confirmarão, em juízo, a existência dos fatos típicos imputados e a autoria dos respectivos, conforme se verá.

4.2. Materialidade dos crimes cibernéticos - o dano real

A comprovação da materialidade do delito é de todo importante para a persecução criminal. Isto porque, se inexistente ela, estará ausente na espécie um requisito mínimo para a deflagração da ação penal, qual seja justa causa, devendo o Ministério Público requerer o arquivamento da denúncia e a homologação deste pelo magistrado, com a aplicação analógica do art. 395, III, do CPP.

Consoante a precisa lição de Nestor Távora[41], "o exercício da ação penal não pode ser uma aventura irresponsável, só assistindo razão ao início do processo se existirem elementos mínimos que façam concluir pela ocorrência da infração e dos seus autores".

A matéria é de tal ordem de importância que os tribunais superiores já pacificaram o entendimento de ser cabível a impetração de *habeas corpus*, excepcionalmente, para o trancamento do inquérito policial, ou até mesmo da ação penal, em razão da ausência de justa causa. Para tanto, deve restar comprovada na espécie, de forma cristalina, a atipicidade da conduta, a incidência de causa de extinção da punibilidade, a falta de indícios de autoria ou de prova da materialidade do delito[42].

[41] TÁVORA, Nestor. ALENCAR, Rosmar Rodrigues, em "Curso de Direito Processual Penal", 5º ed. ver. ampl. e atual., 2011, p. 119, Bahia : JusPODIVM.
[42] BRASIL. Superior Tribunal de Justiça – STJ. *Habeas Corpus* nº 165.805/RS. Voto do Relator: Min. Og Fernandes, Sexta Turma, julgado em 14/05/2013, DJe 23/05/2013. Disponível em:

De igual modo, se não restar comprovado durante a instrução processual a materialidade dos fatos típicos imputados na inicial acusatória, ao juízo condutor do feito não restará alternativa senão a aplicação do art. 386, II, do CPP, absolvendo o réu em razão de estarem ausentes provas da existência do fato criminoso.

Nessa senda, a investigação dos crimes cibernéticos tem de demonstrar a contento, ao final da instrução processual, a ocorrência da(s) conduta(s) descrita(s) no tipo penal no caso concreto, bem como, eventualmente, a presença de substrato probatório suficiente que indique a presença dos elementos subjetivos contidos no tipo, de modo a possibilitar a valoração das provas (art. 155 do CPP) e a fundamentação da sentença (art. 381, III e IV, do CPP) por parte do magistrado.

De fato, nos crimes cibernéticos, a prova da materialidade pode ser obtida por diversas modalidades usuais de produção de prova, tais como: depoimentos testemunhais, interrogatório do acusado, acareação, busca e apreensão etc., possuindo especial valor, a depender da espécie, o conteúdo arquivado no dispositivo da vítima e no dispositivo utilizado pelo ofensor, bem como a prova pericial.

No caso dos crimes relacionados à pornografia infantil (crimes virtuais impróprios), previstas nos arts. 240 ao 241-E da Lei n. 8069/90 (Estatuto da Criança e do Adolescente), por exemplo, a busca e apreensão dos materiais (computador, celular, *laptop*, *tablet*, dentre outros) que contenham registros pornográficos envolvendo crianças e adolescentes se mostram, a contento, suficientes para a condenação do acusado, logicamente quando também demonstrada a sua autoria.

Isso porque a mera conduta de adquirir, possuir ou armazenar, por qualquer meio (fotografia, vídeo etc.) cenas de sexo explícito ou pornográficas envolvendo menores é crime, ao qual é cominado a pena de um a quatro anos de reclusão e multa (art. 241-B). Portanto, pouco importa se tais arquivos são impressos ou se estão contidos em um dispositivo eletrônico: a existência deles em posse de alguém comprova a materialidade do delito, por si.

Nesse sentido, confira-se o julgamento da apelação nº 70044107191 pelo Tribunal de Justiça do Rio Grande do Sul, no qual a Desembargadora relatora fez mencionar tratar-se do tipo de crime de mera conduta aquele previsto no art. 241-B do Eca:

<https://ww2.stj.jus.br/revistaeletronica/Abre_Documento.asp?sSeq=1234277&sReg=201000476719&sData=20130523&formato=PDF>. Acesso em 16 de novembro de 2013, às 10:45. Em igual sentido, confira-se os seguintes julgados: HC 244.737/RS, Rel. Ministro Jorge Mussi e HC 244.671/AP, Rel. Ministro Marco Aurélio Belizze, ambos do Superior Tribunal de Justiça.

> Embora seja pouco crível a versão do réu no sentido de que baixou os arquivos "sem querer" (para si ou para clientes que solicitaram filmes pornográficos, cabendo atentar que, na fase policial, o réu negou a existência deste tipo de material), a simples constatação de armazenamento de material contendo cena de sexo explícito ou pornográfica envolvendo criança ou adolescente, como ocorreu no caso, por si já caracteriza o tipo penal previsto no art. 241-B, do ECA, que é crime de mera conduta.[43]

Naquela ocasião, o réu restou também condenado pela prática do delito previsto no art. 241-A[44] do mesmo diploma legal, com base nas declarações prestadas pelas testemunhas na fase inquisitiva e durante a instrução processual, as quais alegavam que o réu divulgava e disponibilizava, em seu computador pessoal, o material pornográfico para os amigos.

Já em outras espécies de crime, existem aspectos que demandam atenção redobrada.

Conforme já visto quando tratamos da Lei Federal n. 12.737 de 2012, no crime de invasão de dispositivo informático previsto no art. 154-A do Código Penal, deverá ficar demonstrado que houve a violação indevida de mecanismo de segurança no dispositivo para a obtenção de um dos resultados finalísticos previstos no mencionado tipo penal.

Desse modo, caberá a um profissional especialista a elaboração de laudo pericial que constate a ocorrência da violação de algum tipo de mecanismo de segurança existente na espécie, que pode variar desde a decodificação de uma senha pessoal utilizada pela vítima à desativação do antivírus ou *firewall* da máquina invadida.

Com efeito, realizando uma varredura no sistema invadido, o perito poderá constatar a presença de alguma espécie de *malware* que foi responsável pela violação da segurança, como um *keylogger*, usualmente utilizado por *crackers* brasileiros para obter senhas pessoais da vítima e, em posse destas, acessar a caixa de e-mail dela ou fazer outros tipos de devassa.

---

[43] BRASIL. Tribunal de Justiça do Rio Grande do Sul – TJRS. Apelação nº 70044107191. Voto da Relatora: Des. Isabel de Borba Lucas, Oitava Câmara Criminal, julgado em 19/10/2011, DJe 21/11/2011. Em igual sentido, confira-se os seguintes julgados: Apelação nº 70039406616, Rel. Desa. Fabiane Breton Baisch, julgado pelo TJRS.

[44] Art. 241 da Lei Federal n. 8.069/90: Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa.

Em outra linha, nas modalidades mais primitivas do *phishing*, feitas exclusivamente por meio da engenharia social, em que o criminoso é capaz de induzir a vítima a fornecer voluntariamente dados pessoais e outras informações para locupletar-se em detrimento daquela, entendemos não ser possível a constatação da materialidade do delito previsto no art. 154-A do CPB, em virtude da ausência de um dos elementos desse, qual seja a violação de mecanismo de segurança de um dispositivo.

Nessas condições, pensamos não existir a ocorrência de uma figura delitiva própria do direito penal da informática, mas se afere, na verdade, a consumação do crime de estelionato, previsto no art. 171 do Código Penal, em razão de a vítima, induzida a erro, voluntariamente fornecer meios para que o criminoso obtenha vantagens em detrimento daquela.

Importante é que a máquina invadida por outrem ou que, de outro modo, tornou-se efetivamente "um corpo de delito" seja mantida intacta até que seja ela submetida ao manuseio dos profissionais da computação forense.

Isso porque, da invasão ao dispositivo em que o *hacker* vem a obter conteúdo de comunicações eletrônicas privadas, conteúdo pessoal, informações sigilosas etc., alguns vestígios restam na máquina que só serão apagados mediante a utilização diária daquela, formatação da unidade de armazenamento, intencionalmente pelo *hacker* etc. Dentre eles, sobressaem os chamados *logs* de eventos do sistema operacional[45], cuja informação neles contida pode devidamente ser "traduzida" para uma linguagem acessível aos operadores de Direito e, assim, ser utilizada em juízo para a constatação da ocorrência de infração na espécie.

Acerca daqueles, confira-se o informe da multinacional Microsoft[46], cuja essência é aplicável analogicamente aos *logs* de eventos de outros sistemas operacionais, como os que utilizam o núcleo Linux:

> Os logs de eventos são arquivos especiais que registram eventos importantes no computador (por exemplo, quando um usuário faz logon ou quando um programa encontra um erro). Sempre que esses tipos de eventos ocorrem, o Windows registra o evento em um log de eventos que pode ser lido com o recurso Visualizar Eventos. Os detalhes nos logs de eventos podem ser úteis

[45] Existem, também, os *logs* de evento no âmbito da utilização da internet, consoante será visto somente no próximo tópico em virtude de esses cumprirem melhor papel no rastreamento do autor da infração cibernética.

[46] MICROSOFT. "Que informações aparecem nos logs de eventos? (visualizar eventos)", disponível em: <http://windows.microsoft.com/pt-br/windows-vista/what-information-appears-in-event-logs-event-viewer>, acessado em 19.11.2013 às 23:00.

> para usuários avançados que precisem solucionar problemas com o Windows e outros programas.

Cumpre salientar, ainda, uma importante ferramenta que está diretamente no alcance das vítimas de crimes perpetrados pela internet: trata-se da Ata Notarial, documento lavrado por um tabelião, a pedido do interessado, que é capaz de preservar evidências voláteis, atribuindo-lhe fé pública e, deste modo, fazendo prova plena do fato em juízo.

Nela, o agente cartorário relatará fielmente tudo aquilo que presenciou Para ter validade, a ata notarial deve preencher os requisitos do art. 215 do Código Civil Brasileiro. Ademais, aduz o art. 364 do Código de Processo Civil que: "O documento público faz prova não só da sua formação, mas também dos fatos que o escrivão, o tabelião, ou o funcionário declarar que ocorreram em sua presença".

Nessa toada, referido documento público poderá ser utilizado para comprovar diversos elementos do crime virtual, tais como o conteúdo da mensagem eletrônica enviada, o remetente desta, a presença de textos ofensivos e o conteúdo destes publicados em alguma página da internet, o *IP* (I*nternet Protocol*) do emissor da mensagem eletrônica ou do autor do texto etc, antecipando o trabalho das autoridades e resguardando a incolumidade e validade jurídica das provas do crime, atestando não só pela materialidade do delito como, quando possível, a autoria daquele.

4.3. Rastreamento e a imputação da Autoria nos crimes cibernéticos

Trata-se este ponto do mais vital na tarefa investigativa contra os infratores cibernéticos, uma vez que a rede mundial de computadores permite que um usuário, localizado a milhares de quilômetros de distância de sua vítima, perpetre atos que violem os direitos daquela, o que imbui o agente infrator com uma sensação de impossibilidade de responsabilização pelos seus atos.

Contudo, atualmente existem diversos meios de se rastrear a exata localização do usuário conectado a uma rede local ou à rede mundial de computadores, bem como precisar a hora em que ocorreu o ataque, informações estas que, somadas às outras provas deixadas pela atividade criminosa, resultarão na punição do agente infrator.

Com efeito, para que o usuário conecte-se à rede mundial, ele necessita dos serviços de uma provedora de internet, que lhe dará acesso àquela, tais como, no Brasil, a Claro, Telefônica, Oi Velox, etc. No ato de sua conexão, e normalmente enquanto perdurar esta, ele será identificado por meio de um número de IP, que será utilizado pelo protocolo TCP (*Transmission Control Protocol*, ou protocolo de controle de transmissão em português) para o recebimento e o envio de dados pela rede.

O endereço de IP é dividido em quatro campos separados por pontos finais, cada um desses campos correspondendo a um número entre 0 e 255 (por exemplo: 186.215.111.11), e será vital para que as autoridades possam chegar ao local de funcionamento da máquina utilizada para cometer crimes.

Importa ao perito verificar, além do endereço de IP que originou a infração criminal, a data, a hora em que ocorreu a conexão ou da comunicação e o fuso horário do sistema, conforme explicação do Ministério Público Federal[47]:

> Como a Internet é uma rede mundial de computadores, os registros indicam a hora local (05:41:12, no exemplo) e a referência à hora GMT (no caso -08:00). Às vezes, é feita apenas a menção à hora GMT (por exemplo, "Tue, 09 Mar 2004 00:24:28 GMT"). Nos pedidos feitos aos provedores de acesso e às companhias telefônicas, é imprescindível que haja, no mínimo, a menção a esses três indicadores: a) o número IP; b) a data da comunicação; e c) o horário indicando o fuso horário utilizado – GMT ou UTC. Sem eles, não será possível fazer a quebra do sigilo de dados telemáticos.

Como o IP emprestado pela provedora faz parte de um banco de endereços pertencentes a esta, cabe ao investigador verificar à qual das provedoras pertence o endereço, utilizando-se de ferramentas diversas atualmente existentes, como a disponibilizada pelo site http://network-tools.com e o centralops.net.

Por exemplo, foi pesquisado, no primeiro daqueles sítios eletrônicos, o endereço de IP que estava sendo utilizado para a elaboração desta monografia, no dia 20 de novembro de 2013 às 22:05, qual seja o nº 187.58.74.34, obtendo-se como resposta o seguinte nome de servidor: 187.58.74.34.static.host.*gvt*.net.br. Revelado, portanto, que o provedor responsável pelo IP, na espécie, trata-se da empresa Gloval Village Telecom (GVT).

---

[47] MINISTÉRIO PÚBLICO FEDERAL. Procuradoria da República no Estado de SP. Crimes Cibernéticos. Manual Prático de Investigação, 2006, p. 15. Disponível em: <http://www.mpce.mp.br/orgaos/CAOCRIM/pcriminal/ManualdeCrimesdeInform%C3%A1tica-versaofinal.pdf>. Acessos em 20.11.2013, às 22:08.

Em posse dessa informação, deve o provedor imediatamente ser acionado, diretamente ou por intermédio do Poder Judiciário, para fornecer os dados do usuário vinculado ao IP e todas as informações acerca da conexão, devendo serem esses preservados, de modo a se comprovar a existência de elo entre a conexão à rede e a ocorrência do ato infracional.

Contudo, em face da demora do fornecimento dessas informações, ou nos casos de comprovada urgência, acreditamos seja possível a utilização de outras ferramentas de localização do endereço de IP para que seja possível, de pronto, a busca e a apreensão do material que se está sendo utilizado para a prática delitiva, logicamente desde que autorizada a medida por determinação judicial quando não houver flagrante delito.

Para tanto, algumas ferramentas estão disponíveis para uso pelos investigadores. A título de exemplificação, dentre essas ferramentas existe o VisualRoute[48], que é um programa desenvolvido pela empresa Visualware capaz de determinar onde e como o tráfego virtual está fluindo dentro da rota entre o destinatário (ponto sendo acessado) e de onde está vindo a tentativa de acesso. O *software* providencia um mapa geográfico da rota e informa a performance em cada porção daquela rota.

No caso de crimes cometidos por intermédio de *e-mails*, é possível detectar o endereço de IP do ofensor, bem como a data e a hora do envio da mensagem, verificando-se o cabeçalho da mensagem, especificamente no campo do remetente.

A verificação do real autor pode ser dificultada, contudo, em virtude do forjamento do real endereço remetente da mensagem pelo autor da mensagem, prática conhecida como *e-mail spoofing*.

O forjamento é possível em razão de o SMTP (*Simple Mail Transfer Protocol*, que em português, ao pé da letra, quer dizer protocolo de transferência de simples mensagem), o principal protocolo utilizado para o envio de *e-mails*, não inclui um mecanismo de autenticação. Desta forma, o usuário pode inserir comandos no cabeçalho do *e-mail* que irão alterar a informação da mensagem, conforme explica o sítio eletrônico da TechTarget[49].

---

[48] VISUALWARE. VisualRoute features and Benefits. Disponível em: <http://www.visualroute.com/detail.html>, acessado em 20.11.2013 às 22:57.

[49] ROUSE, Margaret. *E-mail spoofing definition*. TechTarget SearthSecurity, 2007. Disponível em: <http://searchsecurity.techtarget.com/definition/email-spoofing>, acessado em 21.11.2013 às 00:33.

Em que pese a possibilidade de tal prática, uma análise mais apurada no código fonte da mensagem por parte do perito, permitirá a ele ter ciência de todos os passos que foram dados pela mensagem eletrônica e, examinando a origem de todos os servidores pelos quais ela passou, descobrir de onde realmente partiu ela, obtendo-se o IP e as demais informações.

Existem ferramentas que não só facilitam e efetivamente concluem essa tarefa, mas que simultaneamente permitem ao investigador localizar geograficamente a rota traçada pela mensagem desde a fonte dessa. São eles: o VisualRoute, acima mencionado, o centralops.net e o www.abika.com.

Na hipótese de não ser possível a localização do número IP que originou a mensagem, mas se obteve o endereço eletrônico real do remetente, explica o Manual Prático de Investigação do Ministério Público Federal[50] que:

> (...) a autoridade policial ou o membro do Ministério Público podem requerer judicialmente a quebra do sigilo de dados telemáticos para que o provedor do e-mail (no exemplo, o Terra) forneça o número IP da máquina que autenticou esta conta, na data e horário do e-mail remetido (ver modelo anexo). Caso queiram uma abrangência maior, poderão pedir a relação de todos os IPs gerados no momento de autenticação da conta, num determinado período (um mês, por exemplo).
>
> Se o provedor do e-mail não estiver sediado no Brasil (exemplos: xxxxxxxx@hotmail.com ou xxxxxxxx@yahoo.com), o investigador encontrará dificuldades para obter as informações necessárias ao prosseguimento das investigações. O provedor de e-mails Hotmail, um dos mais populares do mundo, é mantido pela Microsoft. A empresa possui uma filial brasileira, sediada em São Paulo e, em reunião com o Ministério Público Federal de São Paulo, disse que, "a título de colaboração", encaminha as ordens judiciais de quebra de sigilo de dados telemáticos à sua matriz americana, para atendimento. Nem sempre, porém, esse atendimento é feito com presteza. Além disso, a empresa não faz interceptações de dados telemáticos (o "grampo" de e-mails), pois alega que a legislação americana não autoriza essa medida. Sugerimos que as ordens judiciais de quebra de sigilo de dados telemáticos continuem a ser enviadas às filiais nacionais desses provedores.

[50] MINISTÉRIO PÚBLICO FEDERAL. Procuradoria da República no Estado de SP. Crimes Cibernéticos. Manual Prático de Investigação, 2006, p. 31. Disponível em: <http://www.mpce.mp.br/orgaos/CAOCRIM/pcriminal/ManualdeCrimesdeInform%C3%A1tica-versaofinal.pdf>. Acessos em 21.11.2013, às 00:45.

Sobre o tema, relevante a matéria veiculada pelo *website* do *The United States Department of Justice*[51], que relata o caso do estadunidense James L. Rudzavice, 44, que foi condenado pelo crime de receptação de material pornográfico infantil.

Narra a notícia que o criminoso, em setembro de 2006, passou a ser investigado por uma entidade que trata de crianças desaparecidas e exploradas a partir de um relato da empresa Yahoo! (dentre outros serviços, esta é uma provedora de e-mails) noticiando a presença de imagens eróticas envolvendo menores em um endereço particular de IP.

A partir do rastreamento do IP, os agentes descobriram que o endereço era utilizado em Mansfield, município do Texas, e foram capazes de identificar o James Rudzavice como o indivíduo que comprou o acesso à internet da residência ali localizada.

Em 20 de dezembro de 2006, os oficiais da Dallas Police Department, aliados aos inspetores da U.S. Postal Inspection Service, executaram um mandado de busca federal na residência do investigado no momento em que este se encontrava em sua residência. Os agentes, por meio do exame do computador e dos arquivos ali armazenados (computação forense), encontraram mais de 10 imagens de pornografia infantil e mais de 20 videoclipes pornográficos envolvendo crianças. Na ocasião, o acusado assumiu ter recebido imagens e vídeos de crianças, entre 8 e 17 anos de idade, posando e realizando atos sexuais, bem como admitiu ter sido ele quem salvou o conteúdo em seu disco de armazenamento.

Veja-se, no caso em comento, que o rastreamento do IP tratou-se de medida cabal para que fosse encontrado o autor do delito, o qual, em nosso ordenamento, seria enquadrado no art. 241-B da Lei Federal n. 8.069/90. A materialidade e a autoria do crime ficou sobejamente demonstrada pelos elementos colhidos durante a fase inquisitiva. Com efeito, as imagens e os vídeos ilícitos foram efetivamente encontrados no dispositivo que pertencia ao indiciado, cuja apreensão foi permitida por meio da ordem judicial de constrição daquele bem, bem como o acusado confessou ser o autor do delito.

Uma outra relevante elucidação da aplicação das técnicas ora discutidas, reside no notório caso da atriz da Rede Globo Carolina Dickmann, que teve fotos

[51] COLVIN, Kathy. Tarrant County Man Pleads Guilty to Federal Child Pornography Charge. U.S. Department of Justice. Disponível em: <http://www.justice.gov/usao/txn/PressRel07/rudzavice_PSC_ple_pr.html>, acesso em: 21.11.2013, às 01:08.

íntimas suas furtadas por cinco *crackers* que tentaram extorqui-la, sob pena de serem reveladas aquelas.

Conforme se extrai da entrevista com o inspetor Rodrigo Mello, da Delegacia de Repressão aos Crimes de Informática, publicada pelo sítio eletrônico da Revista Info[52], os principais elementos da investigação consistiram no depoimento da vítima e na análise de seu computador de uso pessoal.

Da análise do computador, os peritos constataram que as imagens haviam sido furtadas do *e-mail* da atriz. Então, os investigadores resolveram traçar um padrão de acesso da vítima à sua conta de *e-mail*, prática bastante comum na investigação dos crimes cibernéticos, de modo a notar a existência de acessos fora do padrão dela, tais como de madrugada ou durante o seu expediente de trabalho, quando ela não estaria utilizando sua máquina em casa.

Logrou-se êxito na tarefa, descobrindo a polícia quais os acessos incomuns estavam ocorrendo, que possivelmente eram realizados pelos criminosos, passando estes a serem rastreados.

Desse modo, os policiais puderam levantar informações sobre quem e quando acessaram o *e-mail*, quem realizou a publicação das imagens em sítios eletrônicos estrangeiros etc., concluindo-se com a identificação dos cinco suspeitos que, ainda, utilizavam programas para mascarar o endereço IP.

Para superar tais *softwares*, explica o inspetor Rodrigo Mello que a polícia "(...) possui convênio com a maior parte das empresas que oferecem esses softwares para mascarar IP. Não importa se o *cracker* usar a solução X ou Y, se criar roteadores virtuais usando servidores na Islândia ou Finlândia… sempre há um rastro que podemos seguir".

Ora, no caso de crimes menos complexos, ou perpetrados por agentes de menor conhecimento técnico informático, normalmente o rastreamento do endereço de IP é uma tarefa mais simples, em virtude de esses realizarem a conduta delituosa fazendo uso do computador em sua própria residência, como no caso ora comentado. Deste modo, é uma questão de tempo até que a polícia consiga localizar o infrator para que responda penal e civilmente por seus atos.

[52] ZMOGINSKI, Felipe. Saiba como a polícia identificou os crackers do caso Carolina Dieckmann. INFO Online, Editora Abril S.A, 2012. Disponível em: <http://info.abril.com.br/noticias/blogs/trending-blog/geral/saiba-como-a-policia-identificou-os-crackers-do-caso-carolina-dieckmann>, acessos em 21.11.2013, às 01:34.

Contudo, na medida em que se desenvolveram os meios de rastreamento de IP dos usuários da internet, outros métodos de disfarçar aquele endereço, ocultá-lo completamente ou dificultar a atividade policial também se desenvolveram.

Com efeito, as duas práticas a seguir estudadas são apenas exemplos dos incontáveis meios que podem ser utilizados tanto isoladamente como, na maioria dos casos, em conjunto com outros para dificultar o trabalho da polícia e garantir a impunidade do *hacker* ou *cracker* mal intencionado, uma vez que o *hacker* se conecta à rede mundial de computadores, ou a uma rede local, de forma indireta, maquiando o seu endereço IP.

A primeira a se mencionar trata-se da clonagem/adulteração do endereço *MAC* (*Media Access Control*), conhecida como *MAC Spoofing*.

Ao criar uma rede doméstica ou comercial a partir de um roteador, o criador pode optar por deixa-la aberta (pública), compartilhá-la apenas com máquinas interligadas por cabos ou com os usuários que tenham conhecimento da senha de proteção da rede *Wi-Fi* (aquela disponibilizada sem a necessidade de ligação de cabos), ou, por fim, pode permitir o acesso à rede apenas pelas máquinas cujo endereço *MAC* esteja cadastrado pelo servidor. O endereço *MAC*, conforme ensina Alexandre Guiss[53], consiste no endereço de controle de acesso da placa de rede de um dispositivo eletrônico, que contém doze dígitos hexadecimais, identificando a placa em uma rede à qual ela venha se conectar.

Por intermédio de *malwares*, *hackers* mal intencionados podem vir a clonar o endereço *MAC* o qual está habilitado para acessar uma determinada rede e, utilizando o endereço clonado em seu dispositivo, vir a ter pleno acesso à rede. Uma vez dentro dessa, e ela estando habilitada ao acesso à rede mundial de computadores, o *hacker* poderá se utilizar do endereço IP da rede local para realizar os teus atos ilícitos, dificultando sobremaneira o rastreamento do IP da sua máquina. De igual modo, os usuários da rede local estão suscetíveis ao ataque do intruso, razão pela qual se faz importante sempre possuir um antivírus atualizado, que poderá combater o ataque do *hacker* ao endereço *MAC* da máquina que sofre as tentativas de invasão.

[53] GUISS, Alexandre. O que é um Endereço MAC e como fazer para descobri-lo no seu computador ou smartphone. TecMundo. Disponível em: <http://www.tecmundo.com.br/5483-o-que-e-um-endereco-mac-e-como-fazer-para-descobri-lo-no-seu-computador-ou-smartphone.htm>, acessos em: 21.11.2013, às 08:00.

Outra ferramenta de acesso indireto bastante utilizada pelos *hackers* trata-se do uso de servidor *Proxy*. Sobre este, confira-se a precisa lição extraída do Manual Prático de Investigação do Ministério Público Federal[54]:

> Com efeito, o usuário pode optar por utilizar um método de acesso indireto, que funciona da seguinte maneira: o usuário se conecta a um servidor específico, que lhe serve de "ponte" para acessar o verdadeiro conteúdo desejado. O servidor conectado utiliza um IP próprio e "esconde" o IP original do usuário, de forma que toda mensagem que chega no servidor é redirecionada a usuário e toda mensagem que parte do usuário é identificada apenas pelo IP do servidor. Este tipo de serviço chama-se Proxy.
>
> Para nós, o maior problema é que há na Internet servidores Proxy que garantem ao usuário o anonimato do IP de acesso, e ainda muitos programas gratuitos para fazer as configurações necessárias à utilização dessa forma de acesso indireto à rede. Há ainda a possibilidade do usuário se utilizar de múltiplos servidores Proxy, de forma a dificultar ainda mais o rastreamento.
>
> De todo o modo, a identificação do usuário depende da colaboração dos servidores Proxy envolvidos.

Existem diversos servidores de *proxy* na rede atualmente, tanto gratuitos como pagos, cuja finalidade pode ser criminosa ou benéfica à utilização da internet, existindo uma lista deles que pode ser verificada sítio eletrônico www.publicproxyservers.com.

Como exemplo de um servidor de *proxy* de finalidade benéfica trata-se daquele disponibilizado pela Universidade Federal do Ceará, que permite aos usuários que se conectem ao servidor utilizarem serviços na rede mundial que são restritos ao domínio ufc.br, tais como o portal de periódicos da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (Capes) e o acesso a diversos livros eletrônicos para download gratuitamente[55].

Maleficamente, o servidor *proxy* pode assumir incontáveis facetas, em razão de prestar o anonimato ao usuário que se conecta à rede mundial de computadores por intermédio dele, conforme visto anteriormente.

---

[54] MINISTÉRIO PÚBLICO FEDERAL. Procuradoria da República no Estado de SP. Crimes Cibernéticos. Manual Prático de Investigação, 2006, p. 39. Disponível em: <http://www.mpce.mp.br/orgaos/CAOCRIM/pcriminal/ManualdeCrimesdeInform%C3%A1tica-versaofinal.pdf>. Acessos em 21.11.2013, às 08:22.

[55] Especificamente sobre esse servidor de *proxy*, mais informações podem ser obtidas em: SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO. Como acessar o proxy. Universidade Federal Do Ceará. Disponível em: <http://proxy.ufc.br/>. Acessos em 21.11.2013, às 08:47.

Contudo, a Kapersky Lab, uma das principais empresas especializadas em segurança da tecnologia de informação no mundo, apresentou na última conferência da *Virus Bulletin*, ocorrida em 2012 na cidade de Berlim, um trabalho inédito que detalhava uma técnica de ataque cibernético, associada ao uso de servidores de *proxy*, que foi aprimorado no Brasil e passou a ser exportada para outros países, com o intuito se obter ilicitamente contas bancárias e credenciais de acesso de incontáveis usuários da rede mundial de computadores.

Sobre o ataque, confira-se os principais trechos noticiados no comunicado de imprensa da empresa supra mencionada (sem destaques no original)[56]:

> O recurso chamado PAC (Proxy Auto-Config) é uma funcionalidade legítima que existe em todos os navegadores modernos, ela tem sido abusada em ataques que fazem com que o acesso a determinadas páginas de internet sejam direcionadas para **um servidor de proxy sob controle de um cibercriminoso**. O proxy malicioso pode ser inserido nas configurações do navegador usando uma URL apontando para um arquivo online ou para um pequeno arquivo, geralmente menor de 1 kb, salvo no computador da vítima.
>
> (...) esse recurso tem sido usado por cibercriminosos brasileiros, que desde 2009 tem aprimorado esses ataques visando redirecionar vítimas para sites falsos de Bancos, empresas de cartão de crédito, serviços de webmail, etc.
> 'Diversos trojans brasileiros tem usado esse recurso: em média de cada 10 trojans brasileiros, 6 deles possuem essa função de alterar o proxy do navegador,' afirma Assolini. 'É uma mudança pequena, silenciosa, não percebida pelo usuário, porém efetiva para direcionar usuários para páginas falsas. O ataque pode afetar todos os navegadores: Chrome, Firefox e Internet Explorer'".

Em outra linha, um importante recurso que foi implantado em 2006 no Brasil trata-se de uma parceria existente entre a Microsoft Brasil e a Polícia Federal, que lançaram a versão local do CETS (Child Exploitation Tracking System) ou Sistema de Rastreamento da Exploração Infatil.

O programa permite que a polícia se comunique em tempo real por todas as cidades e países que estejam ligadas à solução em comento. Esta, a seu turno, possui entre outras funcionalidades, "(...) um repositório de informações estruturado pelos

[56] KASPERSKY LAB. PAC: o problema dos proxies maliciosos. Comunicado de Imprensa. Disponível em: <http://brazil.kaspersky.com/sobre-a-kaspersky/centro-de-imprensa/comunicados-de-imprensa/pac-o-problema-dos-proxies-maliciosos>, acessado em: 21.11.2013, às 08:31.

próprios investigadores, facilitando o trabalho de investigação da força policial em sua luta contra a exploração sexual de crianças pela Internet"[57].

Resultados diretos de medidas como essas, em conjunto com outras já estudadas, tem sido obtidos hodiernamente pela Polícia Federal do Brasil, que recentemente, em novembro de 2013, realizou uma das maiores ações de combate contra o crime de pornografia na internet: a operação "Glasnost".

Conforme explicou o delegado responsável pela operação, Flavio Setti, ao site de notícias G1[58], para a captura dos infratores cibernéticos, as investigações já ocorriam há mais de dois anos e começou com a prisão anterior de outros pedófilos, que mencionavam a utilização, para troca e divulgação de pornografia infantil para várias outras partes do mundo, de uma página russa da *web*.

O fato chamou a atenção da PF e, com a consequente prisão de outros criminosos, notou-se que o site se tornou um ponto de convergência citado por muitos dos pedófilos presos, que relatavam a existência de troca de materiais pornográficos, pelo sítio eletrônico, envolvendo vítimas entre seis meses e 16 anos de idade.

Com base naquelas informações, a PF passou a investigar unicamente os brasileiros que de algum modo faziam parte do site. Segundo os relatos do delegado Flavio Setti, eram aproximadamente 200 os brasileiros investigados, que criavam um perfil e, por meio deste, postavam álbuns com as fotos ilícitas.

As fotos que eram públicas foram alvos de rastreamento por parte dos investigadores que, com sucesso, conseguiram efetuar a prisão de 20 criminosos, sendo 18 deles pegos em flagrante, em diversos estados brasileiros, na ação que envolveu aproximadamente 400 policias federais, 86 mandados de busca e apreensão e 30 de condução coercitiva.

Muito embora tenhamos presenciado importantes avanços na repressão aos crimes cibernéticos no Brasil, sobretudo com a edição da Lei 12.737/12, é de se mencionar que ainda não existe no Brasil, atualmente, legislação específica que estabeleça os direitos e os deveres por parte de empresas provedoras de internet, de

[57] CORTEZZE, Priscilla. Microsoft coopera com Polícia Federal no desenvolvimento de um Sistema de Rastreamento de Exploração Infantil, 2006. Disponível em: <http://www.microsoft.com/brasil/pr/2006/ms_cet.aspx>, acessado em 21.11.2013, às 09:05.

58 JUSTI, Adriana. Operação da PF prende suspeitos de pedofilia em 11 estados brasileiros, 2013. Disponível em: <http://g1.globo.com/pr/parana/noticia/2013/11/operacao-da-pf-prende-suspeitos-de-pedofilia-em-11-estados-brasileiros.html> , acessos em 21.11.2013 , às 09:12.

serviços online, como *e-mails* ou comunidades virtuais (os populares Facebook e o Orkut, por exemplo), ou de hospedagem de páginas virtuais.

Desse modo, denota-se evidente prejuízo na tutela das relações ocorridas entre aquelas empresas, os usuários brasileiros da rede mundial de computadores e estes entre si. Na esfera cível, não se tem claramente delineada em que medida ocorre a responsabilização dessas empresas quando da ocorrência de atos ilícitos dentro dos seus domínios.

Especialmente na seara penal, resta sobremaneira dificultada a já árdua tarefa da polícia e do Ministério Público de buscar a identificação e a comprovação da autoria do infrator cibernético, salientando-se que o processo penal exige a certeza da autoria delitiva para que o réu venha a ser condenado, não sendo suficiente uma rala produção probatória que ateste nesse sentido. Com efeito, dentre outros aspectos prejudiciais, inexiste atualmente um prazo legal mínimo de armazenamento das informações, nos bancos de dados das provedoras de serviços, contendo o endereço de IP, data e hora da conexão e a região onde esta ocorreu pelos usuários da rede, informações estas de vital importância, conforme visto, para que os investigadores possam localizar o autor da infração virtual.

Nessa senda, sobressai a importância de uma atuação conjunta dos diversos entes envolvidos na prática delitiva virtual para que a instrução probatória logre êxito em punir quem realmente seja responsável pelo ato criminoso.

No que atine à vítima, esta pode, dentre outras medidas estudadas, ajudar com a precoce denúncia da infração criminal e manter intacto o dispositivo invadido. Contudo, no âmbito cibernético, a contramedida mais eficaz, com certeza, trata-se da prevenção, sendo importante que a sociedade seja informada dos riscos inerentes à utilização da rede mundial de computadores e de que formas elas poderão evitar serem lesadas.

Salta aos olhos também a necessidade de os provedores de serviços no âmbito da internet, a seu turno, realizarem o armazenamento dos dados de acesso dos seus usuários, em virtude da vertiginosa dinâmica com a qual se desenvolvem os atos nessa seara. A polícia e o Ministério Público, especialmente, devem buscar sempre se atualizar em face das modernizações dos meios de perpetração de crimes virtuais, assim como, por fim, o Poder Judiciário deve estar atento à aplicação das medidas cautelares que se fizerem necessárias para a efetiva persecução criminal, não se olvidando que a

efetividade da prestação jurisdicional depende também da celeridade com a qual nossos magistrados realizem suas funções constitucionalmente atribuídas.

5. CONCLUSÃO

Restou sobejamente demonstrado que o aparente anonimato, tão reverenciado pelos infratores que se utilizam universo digital para a prática delitiva, pode, sim, ser aclarado com o emprego de técnicas investigativas que, como consectário, levarão o agente a responder por seus atos perante a justiça, independentemente da modalidade de crime informático por ele perpetrado.

De fato, a questão dos crimes informáticos há muito tempo já se desenvolve, dentre outras razões, em virtude das inovações tecnológicas que diuturnamente são oferecidas à sociedade e da presença cada vez maior de usuários utilizando-se dessas tecnologias e interligados a redes de acesso, como a rede mundial de computadores, o que tornou o âmbito cibernético cada vez mais atrativos para pessoas mal intencionadas.

Nessa senda, vimos que *hackers* e *crackers* maliciosos criaram e atualizaram diversas ferramentas as quais lhes permitiam devassar e controlar dispositivos informáticos de outras pessoas para, consequentemente, vir a lesá-las com ainda maior intensidade, especialmente com a prática do roubo de identidade, amplamente tratado na obra.

As práticas ilicitamente ocorridas no âmbito virtual, no entanto, continuavam sem receber uma resposta à altura por parte do nosso Estado, especialmente na esfera do Poder Legislativo, o qual remanescia inerte em face dos incontáveis prejuízos arcados anualmente pelo nosso ordenamento, até que em 2012 resolveu ativamente lidar com a situação, promulgando as leis federais n. 12.735 e 12.737, que supriram parcialmente a falta de normas atinentes à matéria em nosso país.

De igual modo, aferiu-se que diversas pessoas, com menor conhecimento técnico informático ou não, também se utilizam da rede mundial de computadores para a prática de figuras delitivas clássicas, tais como as relacionadas à pornografia infantil e aos crimes contra a honra, imaginando elas estarem albergadas pelo manto da impunidade em face da vastidão do universo cibernético e da rapidez com a qual os escassos vestígios do delito praticado no âmbito informático normalmente se esvaem.

Contudo, vimos que a imediata provocação da força policial ou do Ministério Público para a investigação da ocorrência pode efetivamente resultar na captura do infrator. Com efeito, referidos órgãos, cada vez mais especializados em nosso país, em especial a polícia, dispõem de ferramentas que possibilitam a

preservação das provas na espécie, de modo a possibilitar a comprovação da materialidade do delito em juízo.

Essa tarefa também está ao alcance da vítima a partir do emprego dos meios aqui vistos, tais como deixar incólume o dispositivo invadido, acionar precocemente as autoridades policiais e procurar a lavratura da competente ata notarial, que é capaz de preservar evidências voláteis, atribuindo-lhe fé pública e, deste modo, fazendo prova plena do fato em juízo.

Referidas práticas e ferramentas, empregadas conjuntamente pela população e pelos agentes públicos, não só possibilitarão a preservação das evidências que atestem pela materialidade do delito como também terão papel determinante na identificação do autor.

Conforme visto, para que o usuário conecte-se à rede mundial, ele necessita dos serviços de uma provedora de internet, a qual lhe fornecerá um número de IP que o identificará durante todo o tempo em que ele permanecer conectado. Toda transmissão de dados realizadas por ele, bem como a sua o ato de sua conexão, serão identificados pelo seu IP em conjunto com a data, hora e o fuso horário GMT do dispositivo utilizado para a navegação.

Trata-se o número de IP do principal meio de rastreamento do infrator que pratique crimes no âmbito virtual, existindo atualmente diversos programas que permitem a exata localização geográfica da máquina utilizada pelo usuário. De igual modo, em posse dessa informação, pode o provedor ser acionado, diretamente ou por intermédio do Poder Judiciário, para fornecer os dados do usuário vinculado ao IP e todas as informações acerca da conexão, sendo mister a preservação desses de modo a se comprovar a existência de elo entre a conexão à rede e a ocorrência do ato infracional.

Em uma última análise, concluímos pela importância de uma atuação conjunta dos diversos entes que estejam envolvidos nos crimes informáticos, tais como a polícia, a vítima, os provedores de serviços de *internet* e o próprio Poder Judiciário. Deste modo, possibilitar-se-á a formação de lastro probatório suficiente para a confirmação, em juízo, da existência dos fatos típicos imputados e da autoria dos respectivos, elementos esses necessários em nosso ordenamento para que seja possível a condenação do agente infrator.

REFERÊNCIAS

ANDRADE, Fabio Siebeneichler de. **The protection of personality rights in the Brazilian legal system/A tutela dos direitos da personalidade no direito brasileiro em perspectiva atual**. Revista de Derecho Privado, .24 (January-June 2013), p. 81.

ASTURIANO, Gisele. REIS, Clayton. **Os Reflexos Do Ciberdireito Ao Direito Da Personalidade: Informação Vs. Direito À Intimidade**. Revista da SJRJ, 2013, Vol.20(37). Disponível em: <http://www4.jfrj.jus.br/seer/index.php/revista_sjrj/article/viewFile/450/351>. Acesso em 02.12.2013, às 12:04.

BITTENCOURT, Cezar Roberto. **Tratado de Direito Penal: Parte Geral, 1**. São Paulo: Saraiva, 2011.

BRASIL. **Lei Federal n. 8.069/90 (Estatuto da Criança e do Adolescente)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8069.htm>. Acesso em: 16 de novembro de 2013, às 11:51.

BRASIL. **Lei Federal n. 11.343/2006 (Lei de Drogas)**. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11343.htm>. Acesso em: 20.11.2013, às 15:12

BRASIL. **Lei Federal n. 10.406/2002 (Código Civil)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm>. Acesso em: 02.12.2013, às 11:11.

BRASIL. Superior Tribunal de Justiça – STJ. *Habeas Corpus* nº 165.805/RS. Voto do Relator: Min. Og Fernandes, Sexta Turma, julgado em 14/05/2013, DJe 23/05/2013. Disponível em: <https://ww2.stj.jus.br/revistaeletronica/Abre_Documento.asp?sSeq=1234277&sReg=201000476719&sData=20130523&formato=PDF>. Acesso em 16 de novembro de 2013

BRASIL. Superior Tribunal de Justiça – STJ. **Súmula nº 403**. Disponível em: <http://www.stj.jus.br/SCON/sumulas/doc.jsp?livre=s%FAmula+403&&b=SUMU&p=true&t=JURIDICO&l=10&i=1>. Acesso em: 02.12.2013, às 13:09.

BRASIL. Tribunal de Justiça do Rio Grande do Sul – TJRS. Apelação nº 70044107191. Voto da Relatora: Des. Isabel de Borba Lucas, Oitava Câmara Criminal, julgado em 19/10/2011, DJe 21/11/2011.

BRITO, Auriney. **Análise da Lei 12.737/12 – "Lei Carolina Dieckmann"**. Atualidades do Direito, 2013. Disponível em: <http://atualidadesdodireito.com.br/aurineybrito/2013/04/03/analise-da-lei-12-73712-lei-carolina-dieckmann/>, acesso em: 18.10.2013, às 11:15.

CAPEZ, Fernando. **Curso de Direito Penal, Parte Geral: (arts. 1º a 120)**. 15. São Paulo: 2011.

CAPEZ, Fernando. **Curso de Processo Penal**. 19ª ed., São Paulo: Saraiva, 2012.

CARPANEZ, Juliana. **Conheça os Crimes Virtuais mais comuns**. Jornal Folha de S. Paulo. Disponível em: <http://www1.folha.uol.com.br/folha/informatica/ult124u19455.shtml>, acessado em 04.11.2013, às 21:45.

CENTRAL INTELLIGENTE AGENCY. **Top 10 Lists for Mobile Phone and Internet Usage**. Disponível em: <https://www.cia.gov/news-information/featured-story-archive/2012-featured-story-archive/mobile-phone-and-internet-usage.html>. Acesso em 10.10.13, às 21:46.

COLVIN, Kathy. **Tarrant County Man Pleads Guilty to Federal Child Pornography Charge**. U.S. Department of Justice. disponível em: <http://www.justice.gov/usao/txn/PressRel07/rudzavice_PSC_ple_pr.html>, acessado em: 21.11.2013, às 01:08.

CORTEZZE, Priscilla. **Microsoft coopera com Polícia Federal no desenvolvimento de um Sistema de Rastreamento de Exploração Infantil**, 2006. Disponível em: <http://www.microsoft.com/brasil/pr/2006/ms_cet.aspx>, acessado em 21.11.2013, às 09:05.

DIAS, Virginia Soprana. **Aspectos da Segurança Jurídica no Âmbito dos Crimes Cibernéticos.** *Proceedings of the Second Internacional Conference of Forensic Computer Science Investigation*, 2007. Disponível em: <http://www.icofcs.org/2007/ICoFCS2007-pp12.pdf>, acessado em 22.11.2013 às 07:55.

Dicionário Priberam da Língua Portuguesa. Definição "telemática", 2008-2013, disponível em <http://www.priberam.pt/dlpo/telem%C3%A1tica>. Acessado em 02.11.2013 às 00:30.

GALLI. Gabriel. **Conheça os crimes virtuais mais comuns e proteja-se**. TechTudo, 2013. Disponível em: <http://www.techtudo.com.br/noticias/noticia/2013/08/conheca-os-crimes-virtuais-mais-comuns-em-redes-sociais-e-proteja-se.html>, acesso em: 13.10.2013, às 18:17.

GIMENES, Emanuel Alberto Sperandio Garcia. **Crimes Virtuais**. Revista de Doutrina da 4ª Região, Porto Alegre, n. 55, ago. 2013. Disponível em: <http://www.*revistadoutrina*.trf4.jus.br/index.htm?http://www.revistadoutrina.trf4.jus.br/artigos/edicao055/Emanuel_Gimenes.html>, acesso em: 22.11.2013, às 08:21.

GRECO, Rogério. **Curso de Direito Penal, vol. I**. 13. Ed., Rio de Janeiro: Impetus, 2011.

GUIMARÃES, Deocleciano Torrieri. **Dicionário Técnico Jurídico**. 10ª ed., São Paulo: Rideel, 2008.

GUISS, Alexandre. **O que é um Endereço MAC e como fazer para descobri-lo no seu computador ou smartphone**. TecMundo. Disponível em: <http://www.tecmundo.com.br/5483-o-que-e-um-endereco-mac-e-como-fazer-para-descobri-lo-no-seu-computador-ou-smartphone.htm>, acessos em: 21.11.2013, às 08:00.

IANZEN, Adriane. PINTO, José Simão De Paula. CORREIO, Egon Walter Wildauer. **Os sistemas de proteção de direito digital (DRM): Tecnologias e tendências para *e-books***. Encontros Bibli: Revista Eletrônica de Biblioteconomia e Ciência da Informação, Vol.18 (36), 2013.

JUSTI, Adriana. **Operação da PF prende suspeitos de pedofilia em 11 estados brasileiros**, 2013. Disponível em: <http://g1.globo.com/pr/parana/noticia/2013/11/operacao-da-pf-prende-suspeitos-de-pedofilia-em-11-estados-brasileiros.html>, acesso em 21.11.2013, às 09:12.

KASPERSKY LAB. **PAC: o problema dos proxies maliciosos**. Comunicado de Imprensa. Disponível em: <http://brazil.kaspersky.com/sobre-a-kaspersky/centro-de-imprensa/comunicados-de-imprensa/pac-o-problema-dos-proxies-maliciosos>, acessado em: 21.11.2013, às 08:31.

LIMA, Alberto Jorge C. de Barros. **Direito Penal Constitucional: A imposição de Princípios Constitucionais Penais**, São Paulo: Saraiva, 2012

MICROSOFT. **Que informações aparecem nos logs de eventos? (Visualizar eventos),** disponível em: <http://windows.microsoft.com/pt-br/windows-vista/what-information-appears-in-event-logs-event-viewer>, acessado em 19.11.2013 às 23:00.

MINISTÉRIO PÚBLICO FEDERAL. Procuradoria da República no Estado de SP. **Crimes Cibernéticos. Manual Prático de Investigação**, 2006. Disponível em: <http://www.mpce.mp.br/orgaos/CAOCRIM/pcriminal/ManualdeCrimesdeInform%C3%A1tica-versaofinal.pdf>. Acessos em 21.11.2013, às 00:45.

PIAUHYLINO, Luiz. **PL 87/1999**. Projetos de Leis e Outras Proposições, Câmara dos Deputados, disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=15028>, acessos em 18.10.2013, às 16:31.

REVISTA CONSULTOR JURÍDICO. **Site do TRF 5ª Região é invadido por grupo hacker**. Consultor Jurídico, 2013, disponível em: <http://www.conjur.com.br/2013-mar-23/site-trf-invadido-grupo-hacker-coloca-ilustracao-hitler-ar>, acessado em 08.11.2013, às 10:53.

ROSA, Fabrizio. **Crimes de Informática**, Campinas: Bookseller, 2005.

ROUSE, Margaret. ***Cracker definition***. TechTarget SearthSecurity. Disponível em: <http://searchsecurity.techtarget.com/definition/cracker>, acesso em 01.11.2013, às 14:53.

ROUSE, Margaret. ***E-mail spoofing definition***. TechTarget SearthSecurity, 2007. Disponível em: <http://searchsecurity.techtarget.com/definition/email-spoofing>, acessado em 21.11.2013 às 00:33.

SAFERNET BRASIL. **Delegacias Cibercrimes**. Disponível em: <http://www.safernet.org.br/site/prevencao/orientacao/delegacias>. Acessado em 23.10.2013, às 21:10:

SALVADORI, Fausto. **Crimes Vrituais**. Revista Galilei, Editora Globo. Disponível em: <http://revistagalileu.globo.com/Revista/Common/0,,EMI110316-17778,00-CRIMES+VIRTUAIS.html> acesso em 08.11.2013, às 10:31.

SANTOS, Coriolano Aurelio de Almeida Camargo. FRAGA, Ewelyn Schots. **As múltiplas faces dos Crimes Eletrônicos e dos Fenômenos Tecnológicos e seus reflexos no universo Jurídico**, 2ª ed., São Paulo: OAB-SP, 2010. Disponível no endereço: <http://www.oabsp.org.br/comissoes2010/direito-eletronico-crimes-alta-tecnologia/livro-sobre-crimes-eletronicos/Livro2Edicao.pdf/download>, acessado em 04.11.2013, às 21:45

SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO. **Como acessar o proxy**. Universidade Federal Do Ceará. Disponível em: <http://proxy.ufc.br/>. Acessos em 21.11.2013, às 08:47.

SENA, Yala. PI: **Polícia investiga morte de garota após vazar vídeo íntimo na internet**, 2013. Disponível em: <http://noticias.terra.com.br/brasil/policia/pi-policia-investiga-morte-de-garota-apos-vazar-video-intimo-na-internet,1bf47a0bb8852410VgnVCM10000098cceb0aRCRD.html>, acessos em 02.12.2013, às 11:51.

SIMPSON, Michael T. BACKMAN, Kent. CORLEY, James E. **Hands-on Ethical Hacking and Network Defense**. Boston: Course Technology Cengage Learning, 2013.

SINGH, Abhishek. SINGH, Baibhav. JOSEPH, Hirosh. **Vulnerability Analysis and Defense for the Internet**. Nova Iorque: Springer Science+Business Media, 2008.

SYMANTEC. **Relatório Norton 2013: Custo por Vítima do Cibercrime cresce 50%**. Disponível em: <http://www.symantec.com/pt/br/about/news/release/article.jsp?prid=20131002_01>, acessos em: 01.11.2013, às 16:27.

TÁVORA, Nestor. ALENCAR, Rosmar Rodrigues. **Curso de Direito Processual Penal**, 5º ed. ver. ampl. e atual., Bahia : JusPODIVM, 2011.

ZMOGINSKI, Felipe. **Saiba como a polícia identificou os crackers do caso Carolina Dieckmann**. INFO Online, Editora Abril S.A, 2012. Disponível em: <http://info.abril.com.br/noticias/blogs/trending-blog/geral/saiba-como-a-policia-identificou-os-crackers-do-caso-carolina-dieckmann>, acessos em 21.11.2013, às 01:34.