I ENCONTRO VIRTUAL DO CONPEDI

CRIMINOLOGIAS E POLÍTICA CRIMINAL I

BARTIRA MACEDO MIRANDA

GUSTAVO NORONHA DE AVILA

THAIS JANAINA WENCZENOVICZ

C928

Criminologias e política criminal I [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Thais Janaina Wenczenovicz

Gustavo Noronha de Avila

Bartira Macedo Miranda – Florianópolis: CONPEDI, 2020.

Inclui bibliografia

ISBN: 978-65-5648-081-7

Modo de acesso: www.conpedi.org.br em publicações

Tema: Constituição, cidades e crise

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Assistência. 3. Isonomia. I Encontro Virtual do CONPEDI (1: 2020 : Florianópolis, Brasil).

CDU: 34

Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

I ENCONTRO VIRTUAL DO CONPEDI

CRIMINOLOGIAS E POLÍTICA CRIMINAL I

Apresentação

Mesmo em um contexto de Pandemia, a pesquisa acadêmica brasileira, no campo das criminologias e das políticas criminais, segue produzindo resultados relevantes socialmente. Parte destes resultados estão incluídos entre os textos a seguir.

Primeiramente, a discussão de violência de gênero, especificamente nas políticas criminais legislativas referentes aos delitos de feminicídio e suas relações com os homicídios passionais são discutidas por Roberto Veloso Carvalho.

Lucas Nogueira e Luiz Fernando Kazmierczak, no campo da política criminal, discutiram as possibilidade da teoria do quatro poder de Bernd Schunemann pode contribuir para o exercício do poder punitivo voltado à racionalidade. A partir deste ponto, analisam o papel da acadêmica na construção de nossa perspectiva político-criminal.

As relações entre a possibilidade de análise das ideias de Giorgio Agamben no sistema de justiça criminal brasileiro, é feita por Luanna Tomaz de Souza e Antonio José Martins. Após, José Serafim da Costa Neto e Maria Luiza de Almeida Carneiro Silva analisam a temática do enfrentamento da criminalidade virtual.

Carolina de Menezes Cardoso, Juliana Horowitz e Débora Soares Dallemole, trabalham os reflexos da Covid-19 no sistema prisional, especificamente as televisitas. Através de técnica de revisão bibliográfica, desde as criminologias críticas latino-americanas, demonstram como os afetos aprisionados precisam ganhar visibilidade acadêmica.

A influência do labelling approach no direito penal brasileiro é analisada por Carolina Carraro Gouvea. Diversas manifestações do enfoque do etiquetamento são trazidas e discutidas pela autora. A seguir, o tema da violência estrutural e as relações de poder nos estabelecimentos carcerários femininos, são discutidas por Larissa Santana da Silva Trindade, Márcio Eloy de lima Cardoso e Fernando Barbosa da Fonseca.

Isabelle Honório discute a intersecção entre subjugação de gênero, feminilização da pobreza e aumento da população carcerária feminina por crimes relacionados ao tráfico de drogas. Também com o objetivo de analisar as privações de liberdade, mas no âmbito juvenil, Clarice Beatriz da Costa Söhngen, realizou pesquisa empírica para compreender as trajetórias de vida

dos adolescentes moradores de bairros periféricos porto-alegrenses contidos nos Centros de Referência Especializados de Assistência Social.

O tema do cárcere é novamente discutido no texto de Érica Lene da Silva Santos, desta vez sob o olhar da dogmática penal trazida na Lei de Execução Penal e nos tratados de Direitos Humanos.

Até que ponto é permitido ao Estado intervir na vida humana subalternizada para curá-la ao convívio comunitário? Este é o problema discutido, a partir do referencial da Biopolítica, por Estela Parussolo de Andrade e Cristiane Andreia Savaris Sima.

Felipe Américo Moraes retoma o tradicional debate entre as correlações entre desemprego e criminalidade. Desde um viés economicista, são problematizadas várias questões trazidas por um certo senso comum criminológico.

Na continuidade, o tema da Covid-19 surge novamente no trabalho de Everson Aparecido Contelli, Ilton Garcia da Costa e Marcelo Agamenon Goes de Souza. Dentro do contexto da segurança pública, são discutidas estratégias de resposta do sistema punitivo na pandemia.

A letalidade policial é discutida criminologicamente por Diogo José da Silva Flora. Afastando-se de uma perspectiva dogmática, é tratada a economia política da pena de morte pela figura dos autos de resistência produzidos pelos policiais militares.

Maria Aparecida Alves e Dalvaney Aparecida de Araújo, discutem a violência doméstica em relação ao contexto atual e as possibilidades do enfrentamento da questão pelo sistema punitivo. O mesmo enfrentamento é discutido, criminologicamente, por Jhulliem Raquel Kitzinger e Caio Henrique Rodrigues, em relação aos crimes de trânsito e os respectivos autores.

Os aspectos sociológicos das primeiras criminalizações da conduta de terrorismo são discutidos por Guilherme Machado Siqueira e Renata Almeida da Costa. Na sequência, temos o trabalho de Rafael Rodrigues de Melo sobre a reincidência ante a seletividade do sistema penal.

As discussões sobre a transgeracionalidade da violência da mulher, sob o enfoque dos estudos decoloniais, são trabalhadas por Thais Janaina Wenczenovicz e Raquel Kolberg. São problematizados dados empíricos como forma de analisar a perpetuação da violência nas relações de gênero.

Por fim, temos o texto “Violência Estrutural na Perspectiva das Desigualdades de Gênero”, de Larissa Santana Trindade, Fernando Barbosa da Fonseca e Márcio Eloy de Lima Cardoso. Desde uma perspectiva teórica, é identificada a proposta da justiça restaurativa como caminho na redução de desigualdades e violências.

Ficam os textos como demonstração da resiliência dos pesquisadores em Direito no Brasil. Mesmo em meio à Pandemia, podemos e queremos reduzir violências. Mesmo na invisibilização dos mais vulneráveis, os textos lançam luz para problemas urgentes e persistentes. Sigamos em frente e Saúde!

Espaço Internético, Evento Virtual do CONPEDI do Primeiro Semestre de 2020,

Bartira Macedo Miranda

Thais Janaina Wenczenovicz

Gustavo Noronha de Ávila

Nota técnica: O artigo intitulado “As trajetórias de adolescentes acompanhados pela assistência social ante a violência: estudos preliminares em segurança pública na cidade de Porto Alegre” foi indicado pelo Programa de Pós-Graduação em Ciências Criminais da PUCRS, nos termos do item 5.1 do edital do Evento.

Os artigos do Grupo de Trabalho Criminologias e Política Criminal I apresentados no I Encontro Virtual do CONPEDI e que não constam nestes Anais, foram selecionados para publicação na Plataforma Index Law Journals (https://www.indexlaw.org/), conforme previsto no item 8.1 do edital do Evento, e podem ser encontrados na Revista de Criminologias e Políticas Criminais. Equipe Editorial Index Law Journal - publicacao@conpedi.org.br.

A GARANTIA DA ORDEM JURÍDICA E OS CRIMES VIRTUAIS

THE GUARANTEE OF THE LEGAL ORDER AND THE VIRTUAL CRIMES

José Serafim da Costa Neto
Maria Luiza de Almeida Carneiro Silva

Resumo

O presente estudo se propõe a examinar as implicações jurídicas dos crimes virtuais, demonstrando a função do Poder Judiciário, bem como o Poder do Estado enquanto garantidores da segurança jurídica. Ressaltou-se a implicação jurídica de modo crítico, expondo algumas dimensões teóricas e empíricas importantes que costumam ficar excluídas do debate público sobre a matéria. A metodologia utilizada foi à revisão bibliográfica.

Palavras-chave: Crimes virtuais, Ordem jurídica, Dignidade humana, Política criminal, Direito penal

Abstract/Resumen/Résumé

This study aims to examine the legal implications of cybercrime, showing the function of the judiciary and the state power while guaranteeing legal certainty. Was emphasizing the legal implication critically, exposing some of the theoretical and empirical dimensions which tend to be excluded from the public debate on the matter. The methodology adopted was the bibliographical review.

Keywords/Palabras-claves/Mots-clés: Virtual crimes, Legal order, Human dignity, Criminal policie, Criminal law

1. INTRODUÇÃO

O presente estudo busca compreender a garantia da ordem jurídica no Brasil correlacionando com os desafios no combate aos crimes virtuais. A compreensão pretendida não olvidará da legislação pátria, mas também se permitirá discutir experiências estrangeiras, especialmente analisando eventual aplicabilidade de determinados institutos na realidade tupiniquim. Oportunamente, destaca-se que a característica de dinamicidade da sociedade é agravada com a evolução do meio técnico científico e informacional, principalmente sob a perspectiva da internet e das relações jurídicas construídas nesse meio dito virtual.

A relevância social desse tema é indiscutível, na medida em que é ainda não possui ampla produção literário e acadêmica, acrescido do conservadorismo dos tribunais quando da aplicação das normas e pela proliferação de condutas praticadas no meio virtual que precisam receber a guarida estatal.

A metodologia utilizada para a construção do presente artigo foi à revisão bibliográfica, isto é, foi realizado um estudo com base em pesquisas, livros e trabalhos acadêmicos e científicos, bem como a jurisprudência, dos tribunais, sobre a temática do crime virtual.

Desse modo, buscando garantir a maior fluidez possível a leitura do trabalho foi feita a construção em quatro capítulos. Primeiramente, traz-se uma contextualização acerca do tema a ser debatido e dos conceitos inerentes a compressão do trabalho, bem como as próprias origens das problemáticas que geraram a instigação para produzir o presente texto.

Em seguida, avança-se para a compressão do papel do Estado, com especial destaque ao Poder Judiciário, na garantia da ordem jurídica, não olvidando sob qualquer fundamento das previsões constitucionais e legais relacionadas, pois será preciso que se compreenda a complexidade que se relaciona com a efetiva aplicação das normas nos crimes virtuais.

Posteriormente, traz-se à baila maiores detalhes com relação aos crimes virtuais em si até para que possam ser feitas as necessárias ponderações focando na discussão em tela de necessidade de resposta estatal a um novo local de ocorrência de delitos, leia-se o meio virtual, e a necessidade de sua compatibilização com os institutos já estabelecidos na legislação.

Por último, serão expostas considerações acerca do que fora previamente estabelecido e conclui-se com a discussão acerca do papel do Estado no combate a criminalidade e na salvaguarda dos direitos fundamentais de seus cidadãos.

2. A CRIMINALIDADE E SUA DIFUSÃO NA INTERNET

Os meios técnicos científicos e informacionais decorrentes da última revolução industrial, caracterizada pelo posicionamento da informação e dos dados no centro da existência humana, possuem origem já remota no ano de 1957, quando afirmam ter sido criada a internet ou o primeiro protótipo dela, mas os primeiros registros da utilização dela ocorre em 1962. Destacando-se que nesse período, ela limitava-se a circunstâncias deveras restritas e voltadas a pesquisas e estudos propriamente ditos e somente aqueles mais avançados, no entanto ela ganha o cotidiano social na década de 1990, tornando-se hodiernamente para determinados estudiosos um direito fundamental, tamanha sua essencialidade.

A internet pode ser compreendida como a maior criação da história humana, corroborando com tal entendimento temos as lições de Filippo e Sztajnber (1996, p.342):

> Após impulsionar o desenvolvimento da Internet, a NSFNET parou de operar em abril de 1995. Isso ocorreu porque a NSF considerou que já havia cumprido seu papel no fomento à integração do ensino e pesquisa no país. Sendo assim, transferiu para entidades comerciais o controle de seu backbone, o que liberou o tráfego para fins não acadêmicos.
>
> [...]
>
> No início dos anos 80, a importância da tecnologia de redes de computadores já era reconhecida por pesquisadores da área em muitas instituições do país. Nesta época foi criado o LARC – Laboratório Nacional de Redes de Computadores, um consórcio de instituições acadêmicas que tinha o objetivo de fomentar as pesquisas nesta área e de criar uma infraestrutura de redes no país.

Ainda, é oportuno mencionar que a difusão das redes sociais expandiu ainda mais o alcance e a interatividade com o cotidiano dos indivíduos marcando-se pelo ano de 2006, com o popular Orkut, até a chegada do Facebook, Instagram, Twitter, e Youtube, que são os mais utilizados atualmente.

Nesse sentido, a interação das pessoas com esses aplicativos e com a própria internet atraiu o interesse de cidadãos com pretensões criminosas, mas há quem defenda que os primeiros relatos históricos do que se poderia denominar de crimes virtuais ocorreram já em 1960 com os boicotes aos sistemas de computadores, evidentemente são crimes ainda hoje

praticados, mas bastante simples frente a complexidade dos crimes que se observa na contemporaneidade.

A figura do *hacker* como são corriqueiramente denominados os praticantes de crimes virtuais surge com essa denominação da década de 1970 e fortalecem as perspectivas relacionados aos crimes cibernéticos. No entanto, o crescimento de crimes dessa natureza amplia-se na década seguinte, pois esse *hackers* não mais se satisfazem com crimes de boicotes e invasão as redes, mas também com crimes mais complexos, tais com a pirataria e a própria pedofilia.

No cenário brasileiro esse avanço não ocorreu exatamente nesse período, pois nosso avanço tecnológico intensificou-se mais na década de 1990, e também os crimes virtuais no Brasil, na medida em que nossa legislação já estimulava a informatização, mas sem se preocupar tanto com a criminalidade no cyber espaço.

A principal problemática, nesse contexto, é a ineficácia dos institutos tradicionais quando relacionados aos ditos crimes virtuais com a consequente impunidade, ou, pelo menos, dificuldade de aplicar políticas públicas eficientes de combate a esses crimes sem a legislação adequada. A garantia da ordem legal pelo Estado torna-se prejudicada, sob essa perspectiva, pois a carência de tipificação de condutas ou sua não especificidade dificulta as ações punitivas causando prejuízos aos envolvidos na conduta criminosa.

3. A GARANTIA DA ORDEM LEGAL PELO ESTADO

A história do Estado é longa e no curso dela as exigências que lhe são apresentadas e seu papel no tecido social alterou-se profundamente, no entanto a perspectiva de que o Estado precisa ser o garantidor da ordem legal é uma constante. Nesse sentido, a segurança pública é uma função essencialmente estatal e a sensação de segurança do cidadão é um termômetro da eficiência do Estado nesse contexto, mas não se trata apenas de assegurar a segurança, no seu modo prático, afastando a população da violência existente por meio de medidas paliativas, devendo, pois, reduzir a conduta ilegal e conduzi-la ao bem geral, utilizando-se meios de prevenção e aplicabilidade do texto constitucional.

A vítima, por sua vez, busca a satisfação dos seus interesses através de uma resposta ao mal causado, não bastando exclusivamente à aplicação da lei penal e suas sanções, mas também, uma reparação aos danos produzidos pelos criminosos, seja morais ou materiais. Todavia, conforme sobredito, a inexistência da lei para os crimes virtuais, faz com que o sentimento de impunidade seja banalizado.

Dessa forma, vale consignar que o ordenamento jurídico pátrio fez um arranjo superficial criando a Lei Federal nº 12.735/2012, com o intuito de tornar crime as condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares. A simplicidade da lei e seu caráter genérico para resolver problemática tão profunda beira ao absurdo e a inocência.

Posto isso, não se olvida da relevância de que seja garantida maior proteção jurídica as relações nos meios virtuais, mas isso não ocorrerá com leis dessa natureza, tendo em vista a escassez que regula a matéria. Nesse sentido, a sociedade se torna refém e exige uma opressão e a conseqüente punição dos autores de crimes virtuais.

Jorge (2011) ainda afirma que a dependência da tecnologia torna o assunto ainda mais grave, pois "se com apenas um pendrive infectado com vírus foram provocados danos em reatores de uma usina nuclear no Irã, não é demais dizer que todos os países são suscetíveis ao ciberterrorismo".

Portanto, pode-se observar o perigo iminente a que está submetida à sociedade, e o quanto a segurança jurídica nesse meio ainda é ineficiente, havendo a necessidade então de se vislumbrar a falta de garantias nesse aspecto e assim gerá-las para que ninguém seja alvo de condutas ilegais, uma vez que cabe ao Estado sim reprimir a ilegalidade, mas antes de tudo é seu dever reprimi-la.

Vislumbra-se políticas públicas também como meios eficientes de combate a criminalidade, dentre as quais se podem destacar as delegacias especializadas nos crimes cibernéticos, como por exemplo, as que existem nos estados do Espírito Santo, Goiás, Mato Grosso do Sul, Minas Gerais, Pará, Paraná, Pernambuco, Rio de Janeiro, Rio Grande do Sul, São Paulo e no Distrito Federal. Essas delegacias são especializadas em casos de aliciamento on-line e Ciberbullying.

No primeiro caso, é necessário um cuidado redobrado em relação às crianças, pois estas são o maior alvo dos criminosos em decorrência da sua inocência e inexperiência, bem como pela exposição aos meios virtuais de maneira descontrolada e sem fiscalização. Já nos casos de ciberbullying, caracterizam-se por repetitivos envios de mensagens para o celular da vítima, e-mails, recados em diferentes redes sociais, vídeos e áudios com palavras de baixo calão e xingamentos, ofensas e humilhações, tendo como alvo as crianças e adolescentes, trazendo consigo vários prejuízos psicológicos às vitimas.

Igualmente, nos casos de roubo de dados, que estão diretamente ligados ao crime de falsa identidade, uma vez que o criminoso atua nos moldes do art. 307 do Código Penal, atribuindo-lhe falsa identidade, se age no intuito de lesar um terceiro, como por exemplo, nos

casos de “roubo” de perfil/blog clonado numa rede de relacionamentos virtuais. Vale salientar que, o criminoso não atinge somente a vítima, mas o Estado também é lesado, uma vez que toda conduta criminosa em si já configura afronta a figura do Estado, mas o crime previsto no art. 307 do Código Penal especificamente vai contra a fé pública.

Diante de toda essa problemática, o SarfeNet (2012), site especializado na prevenção de crimes virtuais, esclarece como se configuram os crimes de falsa identidade na esfera virtual:

> A primeira conduta é atribuir-se ou atribuir a outrem a falsa identidade, ou seja, fazer-se passar ou a terceiro por outra pessoa existente ou imaginária. Identidade, no sentido natural, é o conjunto de caracteres próprios e exclusivos de uma pessoa: nome, idade, estado, profissão, qualidade, sexo, defeitos físicos, impressões digitais etc. Vale dizer que o crime se configura quando o agente se atribui identidade e não qualidade qualquer.
>
> É indispensável para a caracterização do ilícito que a falsa atribuição de identidade seja praticada para que o agente obtenha vantagem, em proveito próprio ou alheio, ou para causar dano a outrem. É necessário, assim, que o fato seja ou possa vir a ser juridicamente relevante pois, se não houver a possibilidade de resultar efeito jurídico, não ocorre o ilícito. A lei em vigor não distingue a espécie de vantagem, que poderá ser de caráter patrimonial, social, sexual ou moral.

Por fim, é manifesto que o Poder Judiciário e o Estado tem para si a responsabilidade de zelar e proteger as vítimas, sendo incumbido ao Estado o direito de punir aquele que infringir a lei. Em se tratando de Direito Penal, aqui incluso o Processo Penal, as regras em relação à liberdade têm interpretação extensiva, enquanto que as regras em relação à prisão têm interpretação restritiva, desse modo para que possa ser cerceada a liberdade do indivíduo, sendo ela um direito fundamental, a lei é o maior respaldo que se pode ter, e o Código Penal em seu artigo 1° deixa claro esse enfoque, não sendo à toa que é com base nele que se tem o Princípio da Legalidade Penal em sentido estrito.

Sendo assim, a ausência de legislação gera impunibilidade, mas também a ineficiência de políticas públicas e o sucateamento da estrutura estatal, não oportunizando a vítima o retorno que ela espera através da penalização do agente infrator mediante uma sentença condenatória ou por meio da reparação dos danos causados.

A segurança jurídica se concretiza com a certeza do Direito e da Justiça, e para que essa aliança não seja quebrada, e os direitos não sejam violados sem consequências para tanto, o Estado e o Poder Judiciário devem cumprir os seus papéis, punido e solucionando os conflitos, respectivamente, respeitadas as garantias constitucionais e legais.

4. A COMPLEXIDADE DOS CRIMES VIRTUAIS

O ato criminoso já é considerado complexo, inclusive sendo um dos principais objeto de uma ciência específica que é a criminologia. O feixe de situações e particularidades envolvendo condutas criminosas no meio virtual traz uma pluralidade de conceitos, apenas com fins ilustrativos tem-se o conceito de Senise (2005, p. 261):

> Atos dirigidos contra um sistema de informática, tendo como subespécies atos contra o computador e atos contra os dados ou programas de computador. Atos cometidos por intermédio de um sistema de informática e dentro deles incluídos infrações contra o patrimônio; as infrações contra a liberdade individual e as infrações contra a propriedade imaterial.

Contribuindo o conceito de crimes cibernéticos tem-se os apontamentos de Rosa (2002, p. 53):

> 1. [...] É a conduta atente contra o estado natural dos dados e recursos oferecidos por um sistema de processamento de dados, seja pela compilação, armazenamento ou transmissão de dados, na sua forma,compreendida pelos elementos que compõem um sistema de tratamento, transmissão ou armazenagem de dados, ou seja, ainda, na forma mais rudimentar; 2. o 'Crime de Informática' é todo aquele procedimento que atenta contra os dados, que faz na forma em que estejam armazenados, compilados, transmissíveis ou em transmissão; 3. assim, o 'Crime de Informática' pressupõe does elementos indissolúveis: contra os dados que estejam preparados às operações do computador e, também, através do computador, utilizando-se software e hardware, para perpetrá-los; 4. A expressão crimes de informática, entendida como tal, é toda a ação típica, antijurídica e culpável, contra ou pela utilização de processamento automático e/ou eletrônico de dados ou sua transmissão; 5. nos crimes de informática, a ação típica se realiza contra ou pela utilização de processamento automático de

> dados ou a sua transmissão. Ou seja, a utilização de um sistema de informática para atentar contra um bem ou interesse juridicamente protegido, pertença ele à ordem econômica, à integridade corporal, à liberdade individual, à privacidade, à honra, ao patrimônio público ou privado, à Administração Pública, etc.

Ainda com relação aos conceitos tem-se a perspectiva de Roque (2007, p. 25), segundo o qual o crime de informática é "toda conduta, definida em lei como crime, em que o computador tiver sido utilizado como instrumento de sua perpetração ou consistir em seu objeto material".

Como todo instituto novo, o crime virtual possui várias formas de ser conceituado, mesmo assim há pontos em comum nesses posicionamentos, que é o de considerá-lo um crime contra o patrimônio no âmbito da internet, como também acerca dos sujeitos desse crime e da intenção criminosa.

A imputação objetiva ao autor do crime virtual e sua comprovação é extremamente difícil frente à ausência física do sujeito ativo, uma vez que se trata de um crime cometido em um espaço cibernético onde o anonimato é peça chave para seu cometimento, diante disso surgiu a figura do *hacker*, conforme já citado anteriormente, uma pessoa que usa seu conhecimento técnico a respeito de informática para ganhar acesso a sistemas privados, e esse conhecimento por ser considerado ímpar, tanto pode ser utilizado para atos negativos quanto positivos, ao se tratar de crimes virtuais certamente é negativo.

Já o sujeito passivo dessa infração penal pode ser qualquer um, seja pessoa física, ou até mesmo pessoa jurídica, tendo em vista que ela pode ter seus bens desviados ou suas informações violadas. É válido também abordar a intenção do criminoso nesse tipo de crime, que pode ser de ludibriar uma pessoa para obter uma vantagem financeira ou pessoal ou até mesmo furtar informações particulares com o intuito de utilizá-las em proveito próprio.

Algumas modalidades do crime virtual têm se tornado recorrentes no nosso dia a dia, como é o caso do envio de e-mail simulando ser de algum órgão estatal conhecido, como é o caso da Receita Federal, Polícia Federal e Serasa, fazendo com que o proprietário do e-mail pense que existe alguma pendência com o órgão e clique em um algum link para solucionar tal problema, quando na verdade ao clicar no link se tem instalado em seu computador um programa capaz de colher e repassar dados sigilosos pertencentes a vítima. Outra modalidade é de querer mostrar o quanto são frágeis os sistemas privados e o quanto eles estão expostos aos próprios *hackers*, como é o caso das recentes invasões as páginas de órgãos oficiais. Nesta

modalidade o criminoso é motivado por uma questão de desafiar a segurança de sites do governo, mas também de exigir grandes montantes em dinheiro para liberar esses recursos.

Existe uma enorme gama de possibilidades de crimes virtuais, muitos ainda nem possuem um *modus operandi* conhecido, outros ainda nem foram descobertos, em se tratando de crimes é realmente muito difícil lidar com a evolução, pois ela acontece de maneira muito célere, como nos ensina a criminologia, no entanto a preocupação deve ser pautada no futuro e no presente, devendo-se buscar políticas criminais e estratégias que garantam a mantença da ordem pelo Estado.

Enquanto a competência nesses casos, ela será definida territorialmente, se firmando pelo local em que estiver hospedado o provedor do site, ocorre que o ambiente virtual não tem fronteiras sobrevindo casos em que resultado é típico no país em que o comando é dado, porém atípica no Estado onde ocorra o resultado fático.

No que diz respeito a classificação dos crimes virtuais, diversos doutrinadores acreditam que o crime virtual divide-se em dois tipos: crime virtual puro (próprio) e impuro (impróprio).

O primeiro é aquele em que o sujeito utiliza-se do sistema do computador de terceiros – sujeito passivo – para executar o crime, invadindo seus dados, sem autorização, seja para modificar, alterar ou inserir dados de origem falsa.

Viana (2003, p. 13) ensina que os crimes virtuais próprios "são aqueles em que o bem jurídico protegido pela norma penal é a inviolabilidade das informações automatizadas (dados)", ou seja, o crime puro só se consumará se forem praticados e se realizados por meio eletrônicos. Nele, a informática é o bem jurídico tutelado.

Já o segundo, os crimes virtuais impróprios são aqueles realizados na própria máquina, ou seja, na utilização do computador para configuração de condutas ilícitas, atingindo o bem jurídico. Vele salientar que, esses crimes já são tipificados, como por exemplo, nos casos de pedofilia, onde o criminoso age através do computador, mas não necessariamente precisa dele para chegar ao fim desejado.

Asseverando tal afirmação, Castro (2003) aponta que "[...] impróprios admitem a prática por diversos meios, inclusive os meios informáticos".

Todavia, mesmo havendo essas classificações, ainda não são consideradas eficazes, sendo aplicadas, na maior parte das vezes, em casos didáticos. Isso acontece porque a realidade dos computadores e da internet são dinâmicas, tendo em vista a sua evolução grandiosa, tornando essas classificações obsoletas.

Contudo, as acepções ao crime virtual são bastante amplas e divergentes, variando de acordo com o ponto de vista de cada pessoa.

Por isso, aponta Bueno; Coelho (2008) o crime virtual pode ser classificado em puro, misto e comum:

> O crime virtual puro seria toda e qualquer conduta ilícita que tenha por objetivo exclusivo o sistema de computador, pelo atentado físico ou técnico ao equipamento e seus componentes, inclusive dados e sistemas. Crime virtual misto seria aquele em que o uso da internet é condição para efetivação da conduta, embora o bem jurídico visado seja diverso do informático, como, por exemplo, as transferências ilícitas de valores em uma homebanking, onde o racker retira de milhares de contas correntes, diariamente, pequenas quantias que correspondem a centavos e as transfere para uma única conta. Embora esses valores sejam ínfimos para o correntista, que, na maioria das vezes, nem se dá conta do furto, representam para o cibercriminoso uma expressiva quantia em seu montante. Por derradeiro, crime virtual comum seria utilizar a internet apenas como instrumento para a realização de um delito já tipificado pela lei penal. Assim, a Rede Mundial de Computadores acaba por ser apenas mais um meio para a realização de uma conduta delituosa. Se antes, por exemplo, o crime como o de pornografia infantil era instrumentalizado por meio de vídeos ou revistas, atualmente, dá-se por salas de bate-papo, ICQ, como também pela troca de fotos por e-mail entre pedófilos e divulgação em sites. Mudou a forma, mas a essência do crime permanece a mesma.

Ainda, conforme, os autores supracitados acrescentam:

> Os crimes de informática se distinguem em duas categorias:
> 1 - os atos dirigidos contra um sistema de informática, por qualquer motivo, verdadeiro núcleo da criminalidade informática, por se tratarem de ações que atendem contra o próprio material informático (suportes lógicos ou dados dos computadores);

> 2 - os atos que atendem contra outros valores sociais ou outros bens jurídicos, cometidos através de um sistema de informática, que compreenderiam todas as espécies de infrações previstas em lei penal.

Portanto, mesmo havendo varias definições distintas, o meio para chegar a consumação sempre será o mesmo, isto é, utilizando-se da internet para prática de atos ilegais. Consoante os posicionamentos expostos, Mazzardo (2013) esclarece que as redes sociais tornam possível que determinados crimes ocorram:

> A redução da segurança das pessoas ocorre por exposições feitas por elas mesmas, como as publicadas em redes sociais, a saber: Facebook, Twitter, Flicker, Youtube, etc. Infelizmente as exibições vão de local do trabalho, estudos, viagens, denotando o nível financeiro e aplicativos com registro geográfico onde a pessoa se encontra no momento. Isso potencializa que crimes realizados na roupagem antiga, passem a ser realizados pelo meio virtual ou com a ajuda das informações virtuais, como por exemplo, estelionato, pornografia infantil, extorsão, furto, ameaça, sequestro, etc.

Diante do exposto, fica evidente que as práticas ilegais são tendenciosas a crescer, tanto pelos usuários que expõem abertamente suas vidas pessoais, como pela falta de meios de combate, ferindo assim, os direitos fundamentais da pessoa humana. Era comum que a comunicação ocorre-se, mediante cartas tradicionais, e hoje, utilizam-se meios eletrônicos, ambos com o mesmo intuito, de fornecer informações e pensamentos, porém, estes devem ser protegidos pela Constituição Federal, como aponta Guardia (2012):

> Embora distintos o suporte empregado e o canal de circulação de comunicação, tanto a carta como o correio eletrônico são meios de difusão de ideias e pensamentos que utilizam principalmente caracteres escritos. O caráter íntimo da comunicação, destinada a um receptor determinado, exige total reserva de conhecimento de terceiros. Por razão, o regime de inviolabilidade das comunicações postais igualmente se aplica às interceptações ou acessos a mensagens de correio eletrônico. Concluída a comunicação, não cessa a tutela

> jurisdicional para o conhecimento de seu conteúdo, portanto, não há que diferenciar a proteção das comunicações e a proteção dos em si mesmos.

Destarte, Cassanti (2013), através do site “Crimes Pela Internet”, especializado em crimes virtuais, classificou os crimes mais comuns no meio tecnológico:

> INSULTOS: falar mal ou insultar alguém que pode gerar processo com base no Artigo 140 do Código Penal, que pune “a injúria que ofende a dignidade ou decoro”;
> CALÚNIA: inventar histórias falsas sobre alguém pode ser enquadrado no Artigo 138 do Código Penal;
> DIFAMAÇÃO: associar uma pessoa a um fato que ofende sua reputação. Artigo 139 do Código Penal;
> DIVULGAÇÃO DE SEGREDO: revelar segredos de terceiros na internet ou divulgar material confidencial de documentos/correspondências que possam causar danos, pode levar a processo com base no Artigo 153 do Código Penal;
> ESCÁRNIO POR MOTIVO DE RELIGIÃO: criar comunidade online que menospreze ou zombe de pessoas religiosas e religiões. Artigo 208 do Código Penal;
> FAVORECIMENTO DA PROSTITUIÇÃO: Artigo 228 do Código Penal;
> ATO OBSCENO: Artigo 233 do Código Penal;
> ESCRITO OU OBJETO OBSCENO: Artigo 234 do Código Penal;
> INCITAÇÃO AO CRIME: Artigo 286 do Código Penal;
> APOLOGIA DE CRIME: criar comunidades virtuais (fóruns, blogs, etc) para ensinar como burlar a legislação ou divulgar ações ilícitas realizadas no passado, que estão sendo realizadas no presente ou serão realizadas no futuro: Artigo 287 do Código Penal;
> FALSA IDENTIDADE: criar um perfil falso pode levar a processo judicial com base no Artigo 307 do Código Penal;

> PRECONCEITO OU DISCRIMINAÇÃO: comentar em chats, e-mails blogs e outros, de forma negativa sobre raças, religiões, etnias, etc. Artigo 20 da Lei 7.716/89;
> PEDOFILIA: troca de informações ou imagens envolvendo crianças ou adolescentes. Artigo 241-A/241-B/241-C/241-De241-E da Lei no 8.069/90 ECA.

E completou:

> No Brasil, dos 83,4 milhões de usuários de Internet, 90,8% acessam as redes sociais. Entre as redes mais acessadas, a que mais ganhou novos usuários nos últimos três meses foi o Facebook, contando com mais de 50 milhões de brasileiros conectados. Com números tão expressivos não é de se estranhar que pessoas, mal intencionadas ou que desconhecem a existência de leis que regem o ambiente virtual, executam diversos crimes nas redes.

Por todo exposto, fica evidente que o desenvolvimento das novas tecnologias e sua aproximação com o cotidiano dos indevidos nos torna frágeis com relação aos crimes virtuais, entretanto, a legislação pátria, as políticas públicas e a conscientização do usuário ainda são bastante precárias.

5. O DESAFIO DO COMBATE AOS CRIMES VIRTUAIS E O PAPEL DO ESTADO DE GARANTIR OS DIREITOS FUNDAMENTAIS E A ORDEM LEGAL

Os direitos fundamentais são norteadores do Estado Democrático de Direito, como aponta Sarlet (2007, p. 77) que são “todas aquelas posições jurídicas concernentes às pessoas, que, do ponto de vista do direito constitucional positivo, foram, por seu conteúdo e importância, integradas ao texto da Constituição [...]”.

À vista disso, vislumbram-se quatro dimensões que são asseguradas a qualquer pessoa no que alcança as garantias e direitos fundamentais, sendo a primeira ensinada por Sarlet (2007, p. 56) como “particular relevo no rol desses direitos, especialmente pela sua

inspiração jusnaturalista, os direitos à vida, à liberdade, à propriedade e à igualdade perante a lei.”.

Já a segunda dimensão satisfaz ao direito cultural e social, alcançando até ao direito a saúde e educação possuem cunho prestacionista e exigem uma posição ativa do Estado na garantia de direitos vinculados a concepção de igualdade material.

No que se refere à terceira dimensão, Luño (1991, p. 206) preleciona que é uma “resposta ao fenômeno denominado poluição das liberdades, que caracteriza o processo de erosão e degradação sofrido pelos direitos e liberdades fundamentais, principalmente em face do uso de novas tecnologias”.

A quarta dimensão trata do futuro da cidadania e, subsequentemente, da liberdade de todos os povos, ou seja, pode-se afirmar que contempla-se o direito à democracia e a informação. Todavia há estudiosos que defendam divisões distintas dos direitos fundamentais e que merecem tanta atenção, quanto os citados no presente texto.

Adentrando-se ao princípio da dignidade da pessoa humana, sabe-se que todo ser humano é dotado desse preceito e que, assim como os direitos fundamentais, este princípio é norteador do Estado Democrático de Direito.

Na visão de Sarlet (2012, p. 73) a dignidade da pessoa humana integra uma:

> [...] qualidade intrínseca e distintiva reconhecida em cada ser humano que o faz merecedor do mesmo respeito e consideração por parte do Estado e da comunidade, implicando, neste sentido, um complexo de direitos e deveres fundamentais que assegurem a pessoa tanto contra todo e qualquer ato de cunha degradante e desumano, como venham a lhe garantir as condições existenciais mínimas para uma vida saudável, além de propiciar e promover sua participação ativa e co-responsável nos destinos da própria existência e da vida em comunhão com os demais seres humanos, mediante o devido respeito aos demais seres que integram a rede da vida.

Desse modo, o princípio em estudo opera diretamente ligado aos direitos fundamentais, opondo-se a mudança do homem em objeto.

Por conseguinte, os crimes informáticos, afrontam esse valoroso postulado constitucional, sendo importante e indispensável a tutela de tais direitos por meio de um combate efetivo.

Entretanto, o poder judiciário brasileiro ainda é falho no que tange aos crimes virtuais, seja pela falta de tipificação especifica para o tema em apreço, porém, é comum a aplicação da lei já citada anteriormente para que sejam utilizados os crimes já tipificados em nosso ordenamento para moldar os crimes cibernéticos. Ainda se enfrenta a carência de estrutura e de conhecimento técnico acerca do tema.

Os magistrados utilizam-se, na maior parte das vezes, como fundamento o Código Penal Brasileiro, em seu art. 171, *in verbis*: "Art. 171: Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento.". Essa analogia utilizada pelos magistrados em seus julgados é considerada por muitos como uma interpretação mais extensiva no delito tipificado, sendo assim, o local do crime não é propriamente físico, mas por equiparação existe e o resultado buscado pelo criminoso ao cometer tal conduta na internet fora alcançado.

Dessa forma, Carneiro (2012) preleciona as modalidades de atos ilícios elencados pela DRCI – Delegacia de Repressão aos Crimes de Informática:

> Esses crimes em sua maioria são cometidos por meio da internet, mas não necessariamente por esse meio, portanto a previsão legal em sua maioria não o trata como crime virtual e sim como crime penal ao qual independente do meio utilizado para sua consumação se for realizado será enquadrado na lei penal em questão:
> Calúnia - Art. 138 do Código Penal ("C.P.")
> Difamação - Art. 139 do C.P.
> Injúria - Art. 140 do C.P.
> Ameaça - Art. 147 do C.P.
> Furto - Art. 155 do C.P.
> Dano - Art. 163 do C.P.
> Apropriação indébita - Art. 168 do C.P.
> Estelionato - Art. 171 do C.P.
> Violação ao direito autoral - Art. 184 do C.P.
> Pedofilia - Art. 247 da Lei 8.069/90 (Estatuto da Criança e do Adolescente)
> Crime contra a propriedade industrial - Art. 183 e segs. da Lei 9.279/96

Interceptação de comunicações de informática - Art. 10 da Lei 9.296/96

Interceptação de E-mail Comercial ou Pessoal - Art. 10 da Lei 9.296/96

Crimes contra software -“Pirataria” - Art. 12 da Lei 9.609/98

Sendo assim, não restam dúvidas que os avanços globais foram de enormes proporções, mas que a legislação brasileira não acompanhou tais avanços, ocasionando a utilização de tipos penais já existentes em novos crimes, bem como a ineficiência nas políticas públicas de combate aos crimes virtuais.

Conforme já citado previamente a Lei n.º 12.735 de 2012 (BRASIL, 2012) tipifica as condutas realizadas mediante uso de sistema eletrônico, digital ou semelhante, que sejam praticadas contra sistemas informatizados e similares. Tal lei é considerada um amparo para as demais legislações que venham a ser aprovadas no ordenamento brasileiro, pois traz em seu artigo 4º a determinação de que os órgãos da polícia judiciária devem estruturar setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado.

Ademais, o seu artigo 5º incluiu o inciso II no § 3º do artigo 20 da Lei n.º 7.716 de 5 de janeiro de 1989 (BRASIL, 1989), que define os crimes resultantes de preconceito de raça ou de cor, prevendo agora a possibilidade de o juiz, verificando a ocorrência de crimes cometidos na esfera virtual relacionados a raça, cor, etnia, religião ou procedência nacional, determinar a cessação da transmissão que contenha o referido delito.

O advento da Lei 12.737 de 2012 (BRASIL, 2012) logo após, que dispõe sobre a tipificação criminal de delitos informáticos, já é considerado um avanço na tipificação correspondente por ter dado um pontapé para o surgimento de novas leis que estipulassem uma punição, apesar de lamentavelmente ela só ter inserido três crimes, ficando várias condutas ainda sem tipificação.

No entanto, alguns erros foram encontrados na referida lei, já que ela tipifica a infração dentro de três critérios: invasão do dispositivo mediante violação do mecanismo de segurança para adulterar ou destruir dados com a obtenção de vantagens ilícitas. Ou seja, se a pessoa invadir o equipamento, mas não subtrair ou copiar nada, não há a caracterização. Se não houver alguma dessas condicionantes, provavelmente, o crime vai se caracterizar apenas na esfera cível. O que certamente não é ideal.

Essa lei recebeu a alcunha de Lei Carolina Dieckmann pela grande comoção social e midiática, decorrente da prática de um crime virtual contra a atriz, e inclui ainda como crime a interrupção de serviços informáticos, mas apenas os que contêm informações de utilidade pública, ou seja, sites de particulares ficaram fora da norma.

No entanto, a lei em comento introduziu também aspectos de grande ajuda em seu bojo, o seu artigo 2º alterou o Código Penal Brasileiro (BRASIL, 1940), incluindo os artigos 154-A e 154-B ao diploma legal referido.

O caput do artigo 154-A inclui no ordenamento o crime de invasão de dispositivo informático, estipulando uma pena de detenção de 3 meses a 1 ano, além de multa, para quem invadir dispositivo informático, mediante violação dos mecanismos de segurança, visando a obtenção, alteração ou destruição de dados computacionais sem a devida autorização de seu proprietário, ou, ainda, para instalar vulnerabilidades no dispositivos a fim de obter vantagem ilícita.

Já o artigo 154-B estabelece que as ações penais que versem sobre delitos informáticos só poderão ser processadas mediante representação, exceto se o crime é cometido contra a administração direta ou indireta federal, estadual, distrital ou municipal, ou, ainda, contra empresas concessionárias de serviços públicos.

É possível perceber então que tais leis apesar de já serem de grande ajuda no cenário atual, não bastam para a solução dos problemas, até mesmo pelo simples de fato de serem muito enxutas, contendo poucos artigos, não tendo a oportunidade assim de abranger todo o tema.

Nesse dialeto, ao que se refere a legislação brasileira, Azeredo (2011, p. 9) é persuasivo em dizer que é preciso “adaptar o sistema jurídico ao novo contexto tecnológico, porém a legislação vigente não é suficiente e muitos projetos relevantes encontram-se ainda tramitando há anos no Congresso Nacional”. Dar-se como exemplo, a lei n° 84/99, conhecida popularmente como “Lei Azeredo”, que tipifica punições nos crimes digitais.

6. CONSIDERAÇÕES FINAIS

Por fim, então, constatou-se que os crimes virtuais estão ganhando seu espaço no território nacional e isso pede uma atitude para combatê-los de modo eficaz. Sem dúvida os avanços tecnológicos foram benéficos para a sociedade, no entanto essa nova modalidade de crimes acompanhou tal evolução, e é em razão do anonimato da rede mundial de computadores, da falta de tipificação de tais crimes, de forma específica, e da mora na

aplicação da punição por parte do Poder Judiciário que se há a facilitação do cometimento desses ilícitos, o que acaba a obrigar a população a buscar mecanismos de prevenção contra eles.

O Brasil está entre os dez países que mais utilizam a internet, em um mercado promissor e crescente, porém, sem uma legislação que defina e classifique quantos e quais são os crimes cometidos virtualmente não existe um amparo específico para os usuários desse serviço, sendo considerado um atraso no aspecto jurídico, enquanto que na criminalidade é notório o progresso realizado por meios virtuais, violando direitos fundamentais e deixando a sociedade à margem de uma proteção efetiva.

O Direito, por ser instrumento regulador dos fatos juridicamente relevantes, deve acompanhar essas mudanças tecnológicas, buscando se adaptar as transformações de modo direto, a fim de trazer adequação efetiva e gradual perante a mudança na realidade, obtendo como fim a segurança jurídica.

Apesar de existir apenas duas leis completamente dedicadas aos crimes informáticos atualmente em vigor no Brasil, havendo, também poucos julgados dedicados à legislação, a jurisprudência nacional tem se mostrado a favor da responsabilização e condenação dos indivíduos que cometem delitos por meio da internet, mas por haver lacunas na lei a respeito do tema, ainda existem criminosos que não podem ser condenados ou lhe são aplicadas sanções não adequadas.

Dessa forma, faz-se primordial, em razão da complexidade do tema, que medidas sejam tomadas, e essas medidas dependem estritamente da excelente relação entre o Direito e os Órgãos Especializados da Justiça, para que haja o tratamento dessas questões por meio de legislação específica que aborde o tema de forma a inibir condutas similares.

Assim, ao final deste estudo é possível detectar que se faz extremamente necessário que o legislador trabalhe no sentido de editar legislações mais completas, que atinjam todas as vertentes dos crimes informáticos. Outrossim, deve-se criar instrumentos legais adaptáveis às contínuas mudanças tecnológicas, evitando, assim, a criação de normas antiquadas, presas à realidade vigente a época de sua concepção e que, consequentemente, não tem os mecanismos necessários ao combate dos delitos informáticos desenvolvidos após a sua edição, bem como a garantia do combate a esse crimes através de capacitação dos profissionais de segurança pública, políticas eficientes e estrutura física adequada.

REFERÊNCIAS

AZEREDO, Eduardo. **Uma lei para combater delitos digitais.** Revista Jurídica Consulex. Ed Consulex. ano XV. n 343 maio 2011.
BRASIL. **Constituição da República Federativa do Brasil de 1988.** Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm> Acesso em: 12 de março de 2015.
BRASIL. **Código Penal de 1940.** Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 20 de março de 2015.
BRASIL. **Lei n.º 7.716 de 5 de Janeiro de 1989**. Define os crimes resultantes de preconceito de raça ou de cor. Disponível em:http://www.planalto.gov.br/ccivil_03/leis/l7716.htm. Acesso em: 18 de março de 2015.
BRASIL. **Lei nº 12.735, de 30 de Novembro de 2012.** Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12735.htm. Acesso em: 20 de março de 2015.
BRASIL. **Lei nº 12.737, de 30 de Novembro de 2012.** Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 20 de março de 2015.
BUENO, James Nogueira Bueno; COELHO, Vânia Maria Bemfica Guimarães. **Crimes de Internet.** (2008) Disponível em: <http://fadiva.edu.br/documentos/jusfadiva/2008/12.pdf> Acesso em: 12 de abril de 2015.
CARNEIRO, Adeneele Garcia. **Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação.** In: Âmbito Jurídico, Rio Grande, XV, n. 99, abr 2012. Disponível em: <http://www.ambito-juridico.com.br/site/index.php/?n_link=revista_artigos_leitura&artigo_id=11529&revista_caderno=17>. Acesso em 3 de maio de 2015.
CASSANTI, Moisés de Oliveira. Crimes virtuais nas redes sociais. (2013) Disponível em: <http://www.crimespelainternet.com.br/crimes-virtuais-nas-redes-sociais/> Acesso em: 17 de abril de 2015.
CASTRO, Aldemario Araújo. **Internet e os Tipos Penais que Reclamam Ação Criminosa em Público.** In: Webly. Disponível em: <http://www.webly.com.br/forum/lofiversion/index.php/t11293.html>. Acesso em: 13 de abril de 2015.
DEL RE FILIPPO, Denise; SZTAJNBERG, Alexandre. **Bem-vindo à Internet.** Rio de Janeiro: Brasport, 1996.
FERREIRA, Ivette Senise. **Direito & Internet: Aspectos Jurídicos Relevantes.**2 ed. São Paulo: Quartier Latin , 2005, p.261.
GUARDIA, Gregório Edoardo Raphael Selingardi. **Comunicações eletrônicas e dados digitais no processo penal.** São Paulo: USP, 2012. Disponível em: <http://www.teses.usp.br/teses/disponiveis/2/2137/tde-02042013-102504/publico/Disserta_Parcial_Gregorio_Edoardo_Raphael_Selingardi_Guardia.pdf>. Acesso em: 17 de abril de 2015.

JUNIOR, Sergio Jose Barbosa. **Crimes informáticos - breves considerações sobre os delitos virtuais no ordenamento jurídico brasileiro.** Disponível em: http://jus.com.br/artigos/29634/crimes-informaticos#ixzz3ZQaFXLd3. Acesso em: 04 de março de 2015.

JORGE, Higor Vinicius Nogueira. **Lei de crimes virtuais deve agilizar processos e reduzir impunidade.** Disponível em: <http://www.higorjorge.com.br/755/lei-de-crimes-virtuais-deve-agilizar-processos-e-reduzir-impunidade-higorjorge-gazeta-de-limeira/>. Acesso em: 29 de abril de 2015.

_____. **Crimes Cibernéticos e a polícia.** Revista Jurídica Consulex. Ed Consulex. ano XV. n° 345. junho 2011.

MAZZARDO, Luciane de Freitas. **A Proteção de Direitos Fundamentais à Luz da Tipificação de Novos Crimes Cibernéticos.** Disponível em: <http://ebooks.pucrs.br/edipucrs/anais/cienciascriminais/IV/07.pdf> Acesso em: 10 de março de 2015.

MENDES, Maria Eugenia Gonçalves; VIEIRA, Natália Borges. **Os crimes cibernéticos no ordenamento jurídico brasileiro e a necessidade de legislação específica.** Disponível em: <http://www.gcpadvogados.com.br/artigos/os-crimes-ciberneticos-no-ordenamento-juridico-brasileiro-e-a-necessidade-de-legislacao-especifica-2>. Acesso em: 29 de abril de 2015.

ROQUE, Sérgio Roque. **Criminalidade Informática – Crimes e Criminosos do Computador.** 1 ed. São Paulo: ADPESP Cultural, 2007.

ROSA, Fabrízio. **Crimes de Informática**. Campinas: Bookseller, 2002.

SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais.** 8. ed. rev. atual. Porto Alegre: Livraria do Advogado, 2007. p.77.

_____. **Dignidade da pessoa humana e direitos fundamentais na Constituição Federal de 1988.** 9. ed. rev. atual. Porto Alegre: Livraria do Advogado, 2012. p.73.

SARFENET. **Roubo de dados – falsa identidade.** (2012) Disponível em: <http://www.safernet.org.br/site/prevencao/orientacao/roubo> Acesso em: 13 de abril de 2015.

SILVA, Rita de Cássia Lopes. **Direito Penal e Sistema Informático.** São Paulo: Revista dos Tribunais, 2003.

TOURAINE, Alain. **O que é a Democracia?** Petrópolis: Vozes. 2ª ed. 1996.

VIANA, Marco Túlio. **Fundamentos de direito penal informático. Do acesso não autorizado a sistemas computacionais.** Rio de Janeiro: Forense, 2003, p. 13-26.