

A INTERNET E SUAS AMEAÇAS VIRTUAIS: UMA ANÁLISE SOBRE AS MEDIDAS UTILIZADAS PELO ESTADO NO COMBATE AOS CRIMES CIBERNÉTICOS.

Felipe Baía Araújo Fernandes Rosado¹

Sandresson de Menezes Lopes²

RESUMO

Neste estudo serão analisados a internet, como um todo, bem como seus desenrolamentos para o direito penal brasileiro. Serão demonstradas as contravenções e os crimes mais encontradas na rede mundial de computadores, bem como o entendimento de tribunais brasileiros sobre os casos mais relevantes e, por fim, o que já foi apresentado como forma de legislação específica para a Internet.

Palavras-chave: Internet, legislação, tribunais, contravenções.

ABSTRACT

This study will analyze the internet as a whole as well as its unrolling for the Brazilian criminal law. Will be demonstrated the most common contraventions and crimes found on the worldwide web as well as the understanding of Brazilian courts on relevant cases and, finally, what has been presented as a way of legislation specific to the Internet.

Keywords: Internet, legislation, court, contraventions, crimes

¹ Graduando do curso de Direito pelo Centro Universitário do Rio Grande do Norte.

² Advogado especialista em Direito Penal e professor de graduação do Centro Universitário do Rio Grande do Norte

1 INTRODUÇÃO

O presente estudo visa demonstrar a abrangência da rede mundial de computadores, iniciando com a elucidação de toda a criação do que veio a se tornar a Internet, ferramenta imprescindível nas relações interpessoais humanas, devido a facilidade em seu uso, sua celeridade e, principalmente, a possibilidade de não ser necessário obedecer limites geográficos nos atos praticados virtualmente.

Após análise de seu surgimento e sua chegada ao Brasil, ocorrida ao final da década de 80, serão tecidos comentários sobre privacidade e anonimato, figuras muito presentes na rede como um todo e a disposição da Constituição Federal brasileira sobre essas modalidades. Será, também, analisada a facilidade na manutenção das relações interpessoais através das chamadas redes sociais.

Será, então, explanado o que vem a ser considerado crime, no Brasil, utilizando a classificação fornecida pelo doutrinador e professor Damásio de Jesus e como vem sendo aplicada a definição de crime pela doutrina.

Ingressaremos, então, no mundo cibernético com a diferenciação entre um *hacker* e um *cracker*, os usuários do mundo virtual que, muitas vezes, confrontam a legalidade, mas, não necessariamente, o fazem buscando proveito além do acadêmico.

Mostrou-se necessário, também, tecer comentários sobre o “*hacktivismo*”, modalidade que veio a ser conhecida com a tentativa de diversos governamentais de cercear a liberdade cibernética. Recheados com ideologias políticas, os praticantes dessa modalidade de ataque não se sentem intimidados ao confrontarem os mais altos órgãos de investigação do mundo. Será mencionado o grupo conhecido por seu anonimato, os Anonymous, que já entraram em atrito com gigantes do mundo físico e virtual, tais como PayPal, Visa e MasterCard, não poupando, nem mesmo o FBI, órgão de investigação pertencente ao governo dos Estados Unidos, e a presidente brasileira, Dilma Rousseff, que teve informações pessoais vazadas na internet após a assinatura da Lei nº 12.965/14, o Marco Civil da Internet.

Serão, então, expostos os crimes virtuais encontrados com maior frequência na rede, bem como o posicionamento da jurisprudência ante tais delitos e a inércia do Congresso Nacional em manifestar-se sobre a rede mundial de computadores, com raras exceções já votadas.

Por fim, demonstrarei o que vem sendo feito para tornar a legislação brasileira aos avanços tecnológicos, visto que o usuário comum possui pouco, ou nenhum, conhecimento sobre o que poderá ocorrer, caso não tenha prudência ao ingressar na rede, uma vez que a legislação não abrange atos virtuais, não coibindo esse tipo de ato.

As informações constantes nesse estudo foram adquiridas através de pesquisas a material produzido no Brasil e no exterior, bem como em pesquisa feitas na própria Internet e decisões proferidas por tribunais pátrios.

Esse estudo objetiva, principalmente, demonstrar que a Internet ainda é uma terra sem lei e a inércia da legislação vem obrigando a utilização quase exclusiva da analogia ao lidar com esse tipo de transgressão.

2 A INTERNET

2.1 O QUE É A INTERNET – UMA BREVE ANÁLISE DE SUA CRIAÇÃO E EVOLUÇÃO

Antes de falarmos o surgimento da internet, e, a fim de um estudo mais aprofundado sobre o tema, devemos primeiro definir o que significa a palavra “internet”. O dicionário Michaelis conceitua:

Internet

In.ter.net **sf** (**inter+ingl net**, rede) **Inform** Rede remota internacional de ampla área geográfica, que proporciona transferência de arquivos e dados, juntamente com funções de correio eletrônico para milhões de usuários ao redor do mundo.

Para Adriano Roberto Vancim e Jefferson Luiz Mattioli, “*a internet é tida como meio de comunicação, interligando milhões de microcomputadores no mundo todo e permitindo o acesso a uma quantidade de informações quase que inesgotáveis*”. (VANCIM, 2011. p.28)

Após o entendimento do presente, passo a manifestar sobre o surgimento e a evolução da ferramenta conhecida como internet até os tempos modernos. Até meados do século XX, a ideia de uma rede interligada de aparelhos eletrônicos que trocariam dados rapidamente não passava de ilusão, mas o término da 2ª Guerra Mundial e o advento da Guerra Fria obrigaram as duas potências mundiais – Estados Unidos e União Soviética – a correrem em busca de avanços tecnológicos e científicos que pudessem coloca-las permanentemente no topo do poderio global. Segundo o Emerson Wendt e Higor Vinicius Nogueira Jorge, “*com a finalidade de automatizar o cálculo de tabelas balísticas, no ano de 1946 foi construído o primeiro computador digital, denominado ENIAC*”. (WENDT, 2013. p.5).

Em 1957, o lançamento do satélite espacial Sputnik, pelos Soviéticos fez o presidente norte-americano, Dwight Eisenhower começar a tomar providências para impedir que seu país fosse, novamente, colocado para trás em relação aos comunistas liderados por Stalin. Foi criada, assim, a Advanced Research Projects Agency – ARPA, cuja função era desenvolver mecanismos de defesa mais evoluídos que os existentes até então.

A outra ofensiva americana aos russos foi o lançamento da Apollo 2, a bordo da qual encontravam-se Neil Armstrong, Buzz Aldrin e Michael Collins.

Manuel Castells ilustra que: *“No ano de 1962, a Força Aérea, com a preocupação de proteger-se de uma eventual guerra ou ataque nuclear, solicitou à empresa Rand Corporation um estudo sobre uma rede militar descentralizada.”* (CASTELLS, 2001, p.14).

Tal rede deveria ser capaz de se manter em funcionamento ainda que diversas de suas células fossem destruídas, permitindo, portanto, que as informações continuassem a ser manuseadas, mesmo que o sistema não estivesse operando em sua capacidade total.

A empresa *Rand Corporation* analisou o pedido e redigiu um relatório, no qual indicava à Força Aérea que buscasse junto à American Telephone & Telegraph – AT&T, para que esta implementasse o projeto. Entretanto, a empresa de telefonia mostrou-se contrária à implementação do proposto, visto que, nas palavras de Emerson Wendt e Higor Vinicius Nogueira Jorge: *“implementar o projeto que envolvia a criação de uma rede digital de pacotes seria concorrer com ela mesma, que tinha uma rede analógica baseada em comutação de circuitos.”* (WENDT, 2013, p.6)

O medo de um ataque, principalmente Soviético, contra instalações americanas durante a guerra fria, se mostrou o maior incentivo à criação do que viria a se tornar a rede mundial de computadores, largamente utilizada na atualidade.

Posteriormente, segundo o Brasil Escola, a ARPA desenvolveu um projeto, denominado ARPANET, para interligar os computadores dos seus departamentos de pesquisa. Tal rede teve seu início conectando as Universidades de Stanford, situada em Santa Cruz, da Califórnia, em Los Angeles e Santa Bárbara, e a Universidade de Utah, em Salt Lake City, todas nos Estados Unidos. (BRASIL ESCOLA).

Para Antônio Cruz, *“apenas organismos militares e grandes Universidades estavam ligados entre si pela ARPANET, e, com o tempo, foi permitida a entrada de empresas”* (CRUZ, apud VANCIM, 2011, p.29). O que significou um aumento exponencial na utilização do projeto criado em 1969.

Emerson Wendt afirma que: *“No ano de 1973 realizou-se a primeira conexão internacional da ARPANET, que interligou a Inglaterra e a Noruega.”* (WENDT, 2013, p.7)

Mostrando, assim, a capacidade de interconectividade da ARPANET e a possibilidade de conectarem-se dispositivos cada vez mais distantes.

Somente em 1986, quando, *“foi convencionada a possibilidade de sua utilização para fins comerciais”* (PINHEIRO, 2010, p. 59) que a ARPANET passou a ser denominada “INTERNET”, nomenclatura utilizada até os dias atuais, e não cessou seu crescimento exponencial, alcançando cada vez mais usuários pelo globo.

2.2 A INTERNET NO BRASIL

O primeiro contato do Brasil com a internet ocorreu, segundo a reportagem “o Homem no Espaço”, veiculado pela superinteressante, em 1988, com a Fundação de Amparo à Pesquisa do Estado de São Paulo – FAPESP e com o Laboratório Nacional de Computação Científica – LNCC. Ainda assim, o cidadão comum só teve a oportunidade de conectar-se à rede em 1994, quando foi criado o primeiro provedor de internet brasileiro.

2.3 A INTERNET COMO FERRAMENTA FACILITADORA DO COTIDIANO

2.3.1 CONTRATO ELETRÔNICO

Para o ilustre magistrado Semy Glanz: “*Contrato eletrônico é aquele celebrado por meio de programas de computador ou aparelhos com tais programas. Dispensam assinatura ou exigem assinatura codificada ou senhas*”. (GLANZ, Semy *apud* VANCIM, 2011, p.29.)

Desta forma, é possível inferir que um contrato eletrônico é realizado utilizando computadores ou a internet como mediadores, não havendo a obrigatoriedade da presença física de nenhum dos interessados durante qualquer fase do processo.

Para Adriano Roberto Vancim: “*o contrato eletrônico, como regra, é aquele firmado entre pessoas ausentes*” (VANCIM, 2011, p.29)

Tal afirmação pode ser comprovada ao se realizar uma compra na internet, onde o vendedor não se encontra, necessariamente, conectado à rede no momento de sua celebração, somente tomando ciência em momento posterior, ao receber notificação informando-o do negócio realizado. Não havendo, portanto, uma aceitação imediata por nenhuma das partes.

Apesar da falta de regulamentação específica em relação à internet na legislação brasileira, em contratos eletrônicos é possível aplicar o Código de Defesa do Consumidor para as relações de consumo virtuais, como pode ser visto a seguir.

“CONSUMIDOR. REPARAÇÃO DE DANOS MATERIAIS E MORAIS. AQUISIÇÃO DE PRODUTO VIA INTERNET. PRODUTO NÃO ENTREGUE. DIREITO DE EXIGIR O ADIMPLEMENTO DA OBRIGAÇÃO DA VENDEDORA. DANOS MORAIS NÃO CONFIGURADOS.

Sentença que reconhece o direito do consumidor ao recebimento do produto adquirido, estando tal matéria pacificada, na falta de recurso da ré. Recurso apenas da parte autora, insistindo no pleito de reparação por danos morais. Ausência de configuração. Os danos morais somente podem ser reconhecidos quando há ofensa à dignidade da pessoa humana e aos seus direitos de personalidade, e somente excepcionalmente são concedidos em casos de descumprimento contratual, Situação dos autos que não enseja reparação por suposta lesão à personalidade. RECURSO DESPROVIDO. (TJRS – Recurso Cível Nº 71002458883, Terceira Turma Recursal Cível, Turmas Recursais, Relator: Eugênio Facchini Neto, Julgado em 27/05/2010).”

2.3.2 REDES SOCIAIS

Para o Info Escola, denomina-se rede social o complexo de relações entre pessoas que fazem parte de um grupo e que facilitam a interação.(INFO ESCOLA)

Diante dessa informação, é possível perceber que “redes sociais” são anteriores à internet, fazendo parte da própria evolução humana, quando grupos primitivos reuniam-se para trocar experiências e aumentar o aprendizado de seus indivíduos.

A história humana é marcada pelas, cada vez mais, céleres interações entre os indivíduos da raça. O advento da revolução industrial, ocorrida no século XVIII, na Inglaterra, reduziu drasticamente o tempo que as famílias utilizavam para interagirem. Até mesmo mulheres e crianças trabalhavam pesado e ganhavam muito pouco. A jornada de trabalho

variava de 14 a 16 horas por dia para mulheres e de 10 a 12 horas por dia para crianças.(INFO ESCOLA)

Ao ser criada, a internet não possuía nenhuma outra utilização que não militar ou acadêmica, mas o acesso ao público permitiu que fossem criados sítios a serem utilizados por pessoas que não possuíam qualquer relação com as forças armadas ou grandes universidades, permitindo, assim, novos usos da ferramenta.

Nesse meio, surgiram redes sociais, que são estruturas que inter-relacionam empresas ou pessoas, conectadas pelas mais diversas relações. Cada qual se relacionando de acordo com suas preferências e particularidades. (INFO ESCOLA)

2.3.3 SOBRE PRIVACIDADE E ANONIMATO

A internet trouxe consigo um fluxo de informações onde cada pessoa tem a oportunidade de buscar na rede tudo aquilo que julgar necessário. Com isso, tornou-se aparentemente impossível proteger a privacidade de todos os indivíduos.

A Constituição Federal, no entanto, já prevê, em seu artigo 5º, inciso X, proteção à privacidade daqueles sob sua égide, aduzindo que: *“são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação”*. (BRASIL, Constituição Federal)

A Carta Magna brasileira, também em seu artigo 5º, inciso IV, leciona que: *“É livre a manifestação do pensamento, sendo vedado o anonimato”* (BRASIL, Constituição Federal) Ocorre que, a própria natureza da internet permite que tal subterfúgio seja utilizado, ainda que não seja permanente, uma vez que, segundo Patrícia Peck Pinheiro: *“a própria tecnologia nos permite rastrear o emissor”* (PINHEIRO, 2010, p.85). Ainda assim, a quase inexistente fiscalização virtual obriga a vítima a buscar todo o auxílio que necessitar antes de ser possível uma reparação.

3 CRIME

3.1 O QUE É UM CRIME

Para o eminente doutrinador Damásio de Jesus, existem quatro sistemas para a conceituação de crime (JESUS, 2011, p.192), sendo elas:

i) Formal: através da qual verifica-se que crime consiste em um fato típico acrescido de antijuridicidade.

Por fato típico, devemos entender a conduta humana, uma ação ou omissão, que gera um resultado, previsto na lei penal como ilícito.

A antijuridicidade ocorre quando o fato praticado choca-se com a lei penal vigente;

ii) Material: O que se busca no conceito material de um crime é sua relevância jurídica sobre o bem protegido. Como exemplo, é possível afirmar que o bem jurídico protegido no artigo 121 do Código Penal - *“matar alguém”* (Decreto Lei Nº 2.848) - seria a vida daquele que vier a ser considerado vítima;

iii) Formal e Material: Essa maneira de conceituar o crime o examina tanto formalmente (fato típico e antijurídico) quanto materialmente (bem jurídico protegido);

iv) Por fim, o crime pode ser conceituado como Formal, Material e Sintomático, quando, além da tipicidade e antijuridicidade do fato, acrescenta a personalidade do agente para averiguar a conduta criminosa.

Quanto ao Brasil, o código penal adota a teoria bipartite, onde são analisados o fato típico e a antijuridicidade – o conceito formal do professor Damásio de Jesus, no entanto, a doutrina vem entendendo que além do aspecto formal, também se faz necessário demonstrar a culpabilidade do agente no ato praticado, onde a culpabilidade é a reprovação do fato pela ordem jurídica vigente.

4 AGENTES VIRTUAIS – A SUTIL DIFERENÇA ENTRE UM HACKER E UM CRACKER

Embora existam muitas semelhanças em seus modos de agir, o que pode gerar confusão entre os leitores, os termos *hacker* e *cracker* são utilizados para designar dois tipos distintos de indivíduos.

Um *hacker*, para Robert W. Taylor: “*is an individual with a profound interest in computers and technology, that has used this knowledge to access computer systems with or without authorization from the system owners*”³. (SCHELL apud TAYLOR, 2011, p. 62).

Hackers agem por diversos motivos distintos, mas boa parte desse grupo de indivíduos seguem um código de ética próprio que, apesar de não haver obrigatoriedade alguma em segui-lo, é respeitado por boa parte da comunidade. Segundo Robert W. Taylor, o código de ética *hacker* envolve, mas não se limita a: i) *Do not profit from intrusion*; ii) *Do not intentionally harm a computer system*; iii) *Attempt to inform a system administrator of security flaws*⁴ (TAYLOR, 2011, p.68). Importante mencionar, também, que diversos atos ilegais causam tanta repulsa em *hackers* quanto em qualquer pessoa tecnologicamente leiga.

Hackers, ainda de acordo com Robert W. Taylor, podem ser classificados em três grupos distintos, sendo eles: *White hat*, *Gray hat* e *Black hat hackers*⁵ (TAYLOR, 2011, p.68-69).

White hat hackers são aqueles que ingressaram no ramo da segurança computacional, muitas vezes contratados por empresas para testar a segurança de novos softwares a serem lançados no mercado; verificar falhas de funcionamento e segurança em softwares; engenharia reversa, buscando e corrigindo falhas; e, por fim, para treinarem funcionários da empresa contratante. Nem sempre *White hats* são bem vistos na comunidade *hacker*, pois envolveram-se por demais com “o lado correto da lei”, o que significaria, em parte, a troca da liberdade, muito prezada por eles, por lucro, ferindo, assim, um dos preceitos do código de ética.

Gray hat é o termo utilizado para designar aqueles que passam a maioria do tempo agindo legalmente, mas que podem, eventualmente, infringir a lei. Assim, para Taylor: “*a*

³ É um indivíduo com um profundo interesse em computadores e tecnologia, que usou tal conhecimento para acessar sistemas de computadores com ou sem autorização de seus donos.

⁴ i) não lucrar com a invasão; ii) Não causar, intencionalmente, dano ao sistema de computadores invadido; iii) Tentar informar um administrador do sistema invadido sobre suas possíveis falhas de segurança, em tradução livre.

⁵ Chapéus brancos, chapéus cinza e chapéus negros, respectivamente.

typical gray hat is a penetration tester who would not attack a client, but hacks and intrudes recreationally”⁶ (TAYLOR, 2011, p.68). Assim, é possível classificar como “gray hats” a maior parte dos frequentadores da comunidade *hacker*, pois, apesar de manterem-se a maior parte do tempo na legalidade, não estão presos a ela, mantendo, assim, a liberdade, que é a base da comunidade *hacker*.

Black hat são, basicamente, *hackers* maliciosos, *crackers* e criminosos virtuais. Embora nenhum *hacker* siga, obrigatoriamente, um código de conduta e, apesar de, no geral, não receberem nenhuma vantagem pessoal, sentem prazer no caos gerado. Black hats são indivíduos com um profundo conhecimento de computação e que não possuem qualquer senso moral que os impeça de vandalizarem o ambiente virtual, com ou sem ganhos pessoais.

5 UM BREVE COMENTÁRIO SOBRE O HACKTIVISMO

O barateamento do acesso à tecnologia e o, cada vez mais, cedo acesso à internet resultou em uma geração com maior capacidade de buscar informações na rede. Isso culminou com uma maior quantidade de *hackers* com ideologias políticas das mais diversas e que estão dispostos a demonstrá-las de formas igualmente diversas. Tais indivíduos são denominados “hacktivistas”.

O grupo mais conhecido de hacktivistas da atualidade são, ironicamente, denominados “Anonymous”, ou “Anônimos”, em português. O motivo do nome é exatamente para manter a imagem de que eles podem ser qualquer um e estar em qualquer lugar todo o tempo, não sendo possível designar exatamente o que são, pois não é possível classificá-los como uma organização ou qualquer denominação semelhante.

Trata-se de um grupo de pessoas, embora nenhuma possa ser considerada membro oficial do grupo, com interesses em comum, não havendo qualquer forma de hierarquia. Em sua maioria, os membros são *hackers* classificados como “gray hats”, termo já explanado anteriormente, mas não é necessária participação ativa no mundo virtual para ser considerado um “Anonymous”, visto que, como não existe uma organização do grupo, qualquer indivíduo poderá se autodenominar como membro do grupo.

Os “Anonymous” buscam, em sua quase totalidade, a liberdade, principalmente a virtual, utilizando diversas artimanhas para disseminarem sua causa, dentre suas táticas, a mais utilizada é denominada “*Distributed Denial of Service – DDoS*”, a ser explanada no próximo tópico.

O grupo, iniciado em 2003, é responsável por diversas contravenções na *web*, tais como a invasão do e-mail pessoal da então candidata à vice-presidência dos Estados Unidos, Sarah Palin, em 2008, bem como a união com o conhecido *site* de *downloads* piratas, The Pirate Bay⁷, para a criação de um endereço eletrônico onde iranianos poderiam protestar contra a vitória de Mahmoud Ahmadinejad, declarado presidente do Irã. O governo iraniano buscou impedir os protestos, mas não obteve êxito.

No ano de 2010 o grupo Anonymous obteve notoriedade mundial ao apoiar o Wikileaks, *site* sueco utilizado por Julian Assange, seu criador, e diversos outros voluntários

⁶ Um típico chapéu cinza é um testador de invasão que não atacaria um cliente, mas *hackeia* e invade como forma de recreação.

⁷ A Baía dos Piratas, em tradução livre.

para divulgar documentos sigilosos dos governos. A repercussão do site atingiu escala global ao serem divulgados diversos documentos sigilosos do governo dos Estados Unidos. Tal atitude culminou com ações tomadas pelo governo norte americano para impedir que o site recebesse apoio financeiro, a maior parte em forma de doações feitas através dos sites Amazon, PayPal, Mastercard, Visa e o site do Banco Suíço. Tais páginas pararam de emitir pagamentos ao WikiLeaks, deixando-o sem fundos, numa tentativa de impedir suas ações. Nesse momento, o grupo Anonymous declarou seu apoio ao WikiLeaks e lançou uma operação chamada “*payback*”⁸, através da qual os *hackers* do Anonymous lançaram diversos ataques *DDoS* contra os referidos sites, que não estavam mais repassando as doações ao WikiLeaks, tirando-os do ar por alguns dias, antes de suspenderem os ataques.

6 DELITOS VIRTUAIS

6.1 DISTRIBUTED DENIAL OF SERVICE⁹

Segundo Taylor: “*a DoS attack uses multiple systems to attack one or more victim systems or Web sites with the intent of denying service to legitimate users wishing to log on or utilize the attacked server*”¹⁰ (TAYLOR, 2011, p. 123)

Conforme explanado anteriormente, a Internet funciona com a troca de dados entre a rede e o aparelho do usuário. Um *DDoS*, como é mais conhecido no mundo virtual, afeta essa distribuição de dados, inundando-a de tal forma que o sistema fica sobrecarregado, impedindo o ingresso de novos usuários naquela rede e tornando-a extremamente lenta para aqueles que já a estavam utilizando, ou, em uma versão mais violenta do ataque, derrubando o alvo, de maneira que todos os usuários são expulsos daquela conexão e ela não pode ser acessada enquanto o ataque durar, o que pode levar horas.

Para que um *DDoS* tenha capacidade para negar o acesso ao servidor de uma grande empresa, é necessário um grande número de aparelhos, para que o tráfego no alvo seja aumentado exponencialmente. A maneira mais comum de realizar tal feito é através de “computadores zumbi”, ou computadores já infectados por outros programas anteriormente e que, mesmo sem o conhecimento do usuário, está sendo utilizado para abarrotar a rede outra rede de dados.

Não há, exatamente, uma maneira de se prevenir contra um *DDoS*, visto que não se trata de uma ameaça direta, por assim dizer, mas de uma sobrecarga repentina daquela rede de dados. Embora seja uma técnica muito utilizada por *hackers* iniciantes, visto que não há necessidade de criar uma ferramenta para o ataque por eles mesmos, sendo fácil encontra-las na web, também é utilizada por *hackers* avançados, dada a eficácia dos resultados. Quanto maior o nível de conhecimento do atacante, maior será a sua predileção por criar os programas que causam os ataques por si próprios, visto que podem inserir um toque pessoal no ataque ou, ainda que a base do ataque seja a mesma, aumentar o grau de dificuldade para a vítima se defender ou parar o ataque, visto que nenhum programador com intenção de utilizar esse tipo de ferramenta irá copiar o *script* de outro.

⁸ Retorno; Retribuição, em tradução livre.

⁹ Negação de distribuição de serviço, em tradução livre.

¹⁰ Um ataque DoS utiliza múltiplos sistemas contra um ou mais sistemas ou web sites alvo com o objetivo de negar serviço a usuários legítimos que desejam ingressar ou utilizar no servidor atacado. Tradução livre.

6.2 PHISHING SCAM

Phishing Scam é uma das condutas mais encontradas na rede. Trata-se de uma mensagem, geralmente enviada através de e-mail ou redes sociais, na qual a vítima é induzida a clicar em um *link* e inserir, em uma página falsa, dados pessoais e outras informações importantes.

Este termo é derivado da palavra “fishing”, pescaria, em inglês, pois o agente utiliza uma isca e aguarda que a vítima a obtenha. (WENDT, 2013, p. 39).

O grau de sofisticação dos beneficiados por essa prática cresce a todo momento, tendo se tornado comum a qualquer indivíduo abrir seu correio eletrônico e encontrar mensagens da Receita Federal do Brasil, do Banco do Brasil, dentre outros, entidades que já fizeram anúncios públicos que não tentam contato com a população através de meios eletrônicos.

As mensagens envolvem uma dívida perante a entidade, ou supostos erros cadastrais, vindo acompanhadas por um *link*, o qual, se clicado, encaminhará a vítima a um site extremamente semelhante ao verdadeiro, este último pertencente verdadeiramente à entidade.

O site para o qual a vítima é direcionada informa que, para continuar o acesso e ser encaminhada à sua área pessoal, deverá preencher campos com informações diversas, tais como seus documentos pessoais, número de seu cartão de crédito, número da conta bancária, bem como outras informações que o agente criminoso poderá utilizar para se locupletar às custas da falta de conhecimento da vítima ou seu despreparo em lidar com a rede.

O objetivo do Phishing Scam nada mais é que a obtenção de dados da vítima, que serão utilizados em momento posterior para prejudica-la diretamente, ou a terceiros, ao tentar utilizar as informações da vítima para efetuar aquisições.

Agentes com um maior grau de conhecimento informático elaboram o golpe de tal maneira que, ao clicar no *link* em sua caixa de entrada, a vítima estará encaminhando a mensagem para toda a sua lista de contatos, perpetuando, assim, a conduta criminosa, ainda que inconscientemente.

Phishing Scam não é um crime tipificado no Código Penal brasileiro, no entanto, por analogia, é possível utilizar o artigo 171 do mesmo código, o qual informa: “*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*” (Decreto Lei N^a 2.848), conforme visto a seguir:

“CRIMINAL. HABEAS CORPUS. FRAUDES POR MEIO DA INTERNET. PRISÃO PREVENTIVA. GRAVIDADE DO CRIME. NECESSIDADE DA CUSTÓDIA DEMONSTRADA. PRESENÇA DOS REQUISITOS AUTORIZADORES. CONDIÇÕES PESSOAIS FAVORÁVEIS. IRRELEVÂNCIA. PEDIDO DE EXTENSÃO. SUPRESSÃO DE INSTÂNCIA. ORDEM PARCIALMENTE CONHECIDA E DENEGADA.

1. Hipótese em que o paciente foi denunciado pela suposta prática dos crimes de estelionato e formação de quadrilha, pois seria integrante de grupo hierarquicamente organizado com o fim de praticar fraudes por meio da

Internet, concernentes na subtração de valores de contas bancárias, em detrimento de diversas vítimas e instituições financeiras do Brasil e do exterior. 2. O réu ocupava, em tese, a função de programador, responsável técnico pelo software e pelos e-mails por onde circulavam grande quantidade de informações bancárias. 3. Não há ilegalidade na decretação da custódia cautelar do paciente, tampouco no acórdão confirmatório da segregação, pois a fundamentação encontra amparo nos termos do art. 312 do Código de Processo Penal e na jurisprudência dominante. 4. A gravidade do delito pode ser suficiente para motivar a segregação provisória como garantia da ordem pública. Precedente. A liberdade do réu poderia, facilmente, ensejar a reiteração da atividade delitiva, tendo em vista que praticada via computador. I. Condições pessoais favoráveis do agente não são garantidoras de eventual direito subjetivo à liberdade provisória, se a manutenção da custódia encontra respaldo em outros elementos dos autos. II. O pleito de extensão dos efeitos do decisor que concedeu liberdade provisória a alguns co-réus não foi examinado pelo Tribunal a quo. III. A análise da matéria por esta Corte ocasionaria indevida supressão de instância. IV. Ordem parcialmente conhecida e denegada. (STJ - *Habeas Corpus* 34.965/PA, DJ de 20 de setembro de 2004. Relator: Ministro Gilson Dipp).

É possível, também, aplicar o artigo 155 do Código Penal, em seu parágrafo 4º, inciso II, o qual trata de furto mediante fraude. O Excelentíssimo Ministro Gilson Dipp, relator do voto supra, já proferiu voto no qual utilizou tal ferramenta para fundamentar sua decisão, senão vejamos:

CRIMINAL. RECURSO EM HABEAS CORPUS. FURTO QUALIFICADO. PRISÃO EM FLAGRANTE. IMPRESTABILIDADE DAS PROVAS. IMPROPRIEDADE DO MEIO ELEITO. COMPETÊNCIA DA JUSTIÇA FEDERAL. OFENSA A BENS DA CAIXA ECONÔMICA FEDERAL. LIBERDADE PROVISÓRIA. INDEFERIMENTO. POSSIBILIDADE CONCRETA DE REITERAÇÃO CRIMINOSA. NECESSIDADE DA CUSTÓDIA DEMONSTRADA. RECURSO DESPROVIDO.

I. A via eleita não se presta ao exame de alegações relacionadas à imprestabilidade da prova produzida no auto de prisão em flagrante no inquérito policial, em virtude da necessidade de revolvimento no conjunto fático-probatório. II. Maiores incursões a respeito da matéria devem ser efetivadas no decorrer da instrução criminal. III. Impõe-se o processamento da ação penal no âmbito da Justiça Federal, conforme expresso no art. 109, IV, da Constituição, pois, ainda que os saques tenham sido empreendidos de conta de particulares, o crime, em tese, atingiu diretamente bens e interesses da referida empresa pública, tendo em vista que o dinheiro subtraído encontrava-se ainda na posse do ente federal. IV. A hipótese dos autos evidencia a suposta prática de saques em contas-correntes, inclusive via Internet, sendo que em poder do réu foram encontradas senhas de acesso a contas bancárias, cartões magnéticos e numerário. V. Trata-se de acusado proveniente de uma localidade onde, segundo o Magistrado singular, tal tipo

de prática criminosa estaria ocorrendo de forma reiterada, não sabendo o paciente explicar o motivo pelo qual mudou o distrito da culpa. VI. Constata-se, pelas evidências concretas do caso em tela, a real possibilidade de reiteração criminosa, o que é suficiente para fundamentar a segregação do paciente para garantia da ordem pública. VII. Recurso desprovido. (STJ – *HABEAS CORPUS* nº 19.846/GO (2006/0153072-3) Relator: Ministro Gilson Dipp. DJ de 9/10/2006)

Tais votos demonstram que sim, existe a conduta criminosa, que deverá ser punida, mas que não há pacificação sobre o assunto, nem mesmo no Colendo Superior Tribunal de Justiça, abrindo margem para a total interpretação do Magistrado sobre o assunto, resultando em duas punições distintas, visto que a pena por furto envolvendo fraude (artigo 155, §4, II, do CP) é mais severa que a pena por estelionato (artigo 171, também do CP).

6.3 VÍRUS

São, indubitavelmente, o tipo de malícia mais recorrente na rede mundial de computadores. Vírus são programas codificados que possuem, como principal objetivo, a replicação na máquina hospedeira e sua propagação enquanto não forem tornados obsoletos.

No entanto, variações quase infinitas nos códigos de sua criação podem gerar agentes com diferentes utilidades. Um mesmo vírus, ao ser escrito de maneira diferenciada, poderá driblar programas de proteção e causar um dano diferente do esperado, prejudicando, assim, o computador infectado e, principalmente, o usuário de boa-fé daquela máquina.

Dentre os vírus, é válido mencionar os seguintes:

6.3.1 VÍRUS DE INICIALIZAÇÃO, OU BOOT VIRUS

Vírus de inicialização figuram como uma das espécies iniciais de programas maliciosos a afetarem computadores. Emerson Wendt informa que esse vírus teria surgido no final da década de 80, causando muitos transtornos a usuários de computador. (WENDT, 2013, p. 24).

O método de contaminação por esse tipo de arquivo é através de um disquete contaminado, que, ao ser inserido na máquina, executaria um arquivo escondido de seu usuário – o próprio vírus. A máquina, então, seria utilizada para a multiplicação do programa, infectando quaisquer outros disquetes que fossem inseridos no hospedeiro.

O vírus de inicialização seria ativado logo que a máquina fosse inicializada, antes que qualquer programa de proteção pudesse ser ativado. O *malware*¹¹, então, faria com que a máquina entrasse em um ciclo de reinicializações por tempo indeterminado, não permitindo que o usuário tivesse acesso a seus arquivos pessoais.

Como a forma de contágio e transmissão desse vírus é bastante específica, a própria evolução tecnológica encarregou-se de limitar seu alcance, levando-o quase à extinção. No entanto, ainda é possível encontrar esse tipo de programa em funcionamento e os usuários de

¹¹ Termo utilizado para designar arquivo malicioso

computador, principalmente aqueles com aparelhos mais antigos, ainda são suscetíveis a esse malefício.

6.3.2 BOMBA RELÓGIO, OU TIME BOMB

Um vírus pertencente a esta espécie, como seu nome já indica, infecta a máquina do usuário – geralmente através de e-mail, portas dos fundos ou cavalos de Troia, estes últimos a serem explicados em momento oportuno – mas só entrará em atividade quando for atingido um momento específico, definido por seu programador.

Contrário a outros tipos de arquivos maliciosos desta espécie – vírus -, não há como prever a extensão de seu dano ou, até mesmo, o que fará com a máquina infectada, uma vez que somente entrará em funcionamento quando cumprido o pré-requisito estipulado.

Um vírus desta espécie que atingiu notoriedade na Internet chama-se Conficker, ou 1º de Abril, em sua nomenclatura mais conhecida. Este arquivo estaria programado para se ativar em primeiro de abril, o que não veio a ocorrer. Ainda assim, este arquivo em particular ainda pode ser considerada uma ameaça, mesmo que classificada com nível entre baixo e médio, pois, como jamais foi ativado, a extensão do dano poderá surpreender programas de defesa, tornando-os inúteis contra o ataque.

6.3.3 WORMS¹²

Apesar de estar classificado nesta categoria, um worm possui um diferencial dos outros vírus: ele não visa atacar diretamente a máquina, mas apenas replicar-se.

Para tanto, este tipo de arquivo irá utilizar os recursos de seu hospedeiro no cumprimento de seu objetivo, ocupando cada vez mais espaço em seu disco rígido, a medida que se multiplica, sobrecarregando os processadores da máquina e deixando-a demasiadamente lenta ou incapaz de realizar determinadas tarefas que exigiriam um pouco mais do computador.

Ainda assim, dependendo de sua codificação, um worm poderá ser utilizado para outros fins, tais como a criação de uma porta dos fundos, a qual o invasor poderá utilizar para ganhar acesso à máquina em momento futuro, bem como utilizar os e-mails registrados na máquina para enviarem novas mensagens, possivelmente contendo cópias do arquivo.

6.4.4 CAVALOS DE TROIA, OU TROJAN HORSES

Este é um dos arquivos maliciosos mais difundidos na Internet, devido a sua incrível versatilidade.

Como na lendária guerra de Troia, onde o herói grego Odisseu sugeriu a construção de um gigantesco cavalo de madeira – a ser recheado com soldados gregos – e entrega-lo como presente aos troianos – culminando com a vitória grega -, o vírus conhecido como Cavalo de Troia utiliza este mesmo subterfúgio para ingressar na máquina, escondendo-se em outro arquivo – mais atrativo à atenção da vítima – para efetuar a invasão.

¹² Em tradução literal, vermes ou minhocas

Ao abrir o arquivo contaminado, o usuário permite a entrada do vírus em seu aparelho. O criador do Cavalo de Troia poderá, então, utilizar o *malware* para instalar remotamente outros arquivos igualmente perigosos, tais como *keyloggers* e *screenloggers* – os quais serão explicados com maiores detalhes a seguir.

O Cavalo de Troia, por sua própria natureza, poderá, também, ser utilizado como uma porta dos fundos pelo agente criminoso, garantindo seu acesso à máquina infectada enquanto o programa não for eliminado ou destruído – pelo agressor ou pela vítima. Através do acesso fornecido por tal artimanha, o criminoso poderia utilizar a máquina para reenviar o vírus – aproveitando-se do computador da vítima (abusando da imagem do alvo para enganar aqueles que lhe são próximos a permitirem novas malícias em suas máquinas) ou realizar quaisquer outras atividades ilícitas.

Curiosamente, apesar de estar classificado nesta categoria, o Cavalo de Troia possui uma particularidade que o diferencia de outros vírus: ele não se multiplica, devendo ser instalado diretamente no alvo. Acredita-se que o Cavalo de Troia não possa ser considerado um vírus por essa característica, no entanto, seu modo de agir e de contágio são semelhantes a outros vírus e, por tal motivo, classifiquei-o como um.

Os principais alvos de um Cavalo de Troia são os computadores domésticos, objetivando a busca de uma senha específica, visto que este arquivo pode trazer consigo outros *malwares* os quais podem monitorar tudo o que a vítima fizer.

Os programas de proteção estão constantemente atualizando suas defesas contra esse tipo de vírus, tamanho é o dano que ele pode causar.

A jurisprudência pátria vem considerando o uso de Cavalos de Troia como furto mediante fraude (artigo 155, §4º, inciso II do Código Penal), senão vejamos:

CRIMINAL. HABEAS CORPUS. FURTO QUALIFICADO. FRAUDES POR MEIO DA INTERNET. PROGRAMA TROJAN. OPERAÇÃO CONTROL/ALT/DEL. PRISÃO PREVENTIVA. POSSIBILIDADE CONCRETA DE REITERAÇÃO CRIMINOSA. NECESSIDADE DA CUSTÓDIA DEMONSTRADA. PRESENÇA DOS REQUISITOS AUTORIZADORES. ORDEM DENEGADA.

I – Hipótese na qual o paciente foi denunciado pela suposta prática do crime de furto qualificado, pois seria integrante de grupo organizado com o fim de praticar fraudes por meio da internet, concernentes na subtração de valores de contas bancárias, em detrimento de diversas vítimas e instituições financeiras, entre elas a Caixa Econômica Federal, a partir da utilização de programa de computador denominado TROJAN.

II – Não há ilegalidade na decretação da custódia cautelar do paciente, tampouco no acórdão confirmatório da segregação, pois a fundamentação encontra amparo nos termos do art. 312 do Código de Processo Penal e na jurisprudência dominante.

III – As eventuais fraudes podem ser perpetradas na privacidade da residência, do escritório ou, sem muita dificuldade, em qualquer lugar em que se possa ter acesso à rede mundial de computadores.

V – A real possibilidade de reiteração criminosa, constatada pelas evidências concretas do caso em tela, é suficiente para fundamentar a segregação do paciente para garantia da ordem pública.

VI – Ordem denegada.

(STJ – Habeas Corpus nº 81.638/PA (2007/0087811-8) Relator: Ministro Gilson Dipp. DJ de 6/08/2007)

Os instrumentos de *Habeas Corpus*, utilizados para a liberação de indivíduos quando este: “sofrer ou se achar na iminência de sofrer violência ou coação ilegal na sua liberdade de ir e vir, salvo nos casos de punição disciplinar” (Decreto Lei nº 3.689) vêm sendo rechaçados, com base no artigo 312 do mesmo dispositivo legal, o qual informa que a prisão preventiva poderá ser utilizada para a manutenção da ordem pública, visto que o agente desta modalidade de crime poderia facilmente cometê-lo novamente ao obter acesso a um microcomputador.

HABEAS CORPUS. OPERAÇÃO TROJAN. PRISÃO PREVENTIVA. GARANTIA DA ORDEM PÚBLICA. DECISÃO FUNDAMENTADA. PRÁTICA DELITUOSA REITERADA. LIBERDADE PROVISÓRIA. CONSTRANGIMENTO ILEGAL. INEXISTÊNCIA. PRECEDENTES. 1. Estando a decisão denegatória da liberdade provisória satisfatoriamente fundamentada, nos termos do artigo 93, inciso IX, da Constituição Federal, não há que se falar em constrangimento ilegal. 2. **Presença dos requisitos elencados no art. 312 do CPP, para a garantia da ordem pública, justificando a custódia cautelar da paciente.** 3. Decreto de prisão preventiva motivado na garantia da ordem pública, considerando a existência de fortes indícios de que o paciente integrava quadrilha especializada em praticar furtos de valores depositados em contas bancárias, sendo o grupo bem organizado, dispondo de equipamentos tecnológicos e programas espões inseridos em computadores ligados à internet, colocando em risco o patrimônio de milhares de pessoas. 4. As investigações demonstraram que o paciente insistia na prática costumeira e reiterada de crimes, impondo-se o desbaratamento do grupo para a cessação da atividade delituosa, considerando a facilidade para o cometimento das fraudes, mediante o uso de programas capazes de capturar dados bancários e transferir valores para outras contas, pagamentos de boleto e aquisição de créditos para telefone celular. 5. Os bons antecedentes, o endereço certo e o desempenho de ocupação lícita não asseguram, por si só, o direito à liberdade provisória, quando a segregação cautelar imposta ao paciente encontra amparo legal e mostra-se plenamente justificada. Precedentes. 6. Inexistência de excesso de prazo na formação da culpa. 7. Ordem de habeas corpus denegada. (TRF-1 - HC: 56684 TO 0056684-28.2010.4.01.0000, Relator: DESEMBARGADOR FEDERAL CARLOS OLAVO, Data de Julgamento: 26/10/2010, TERCEIRA TURMA, Data de Publicação: e-DJF1 p.216 de 12/11/2010) (grifo meu)

6.5 PORTA DOS FUNDOS, OU BACK DOOR

Uma porta dos fundos, conforme já mencionado anteriormente, é um programa malicioso, através do qual o cibercriminoso implanta um ponto de acesso à máquina infectada, garantindo seu acesso futuro, despercebido pelo usuário de boa-fé.

Através desse acesso remoto, é possível utilizar o computador com este dispositivo para o cometimento de outros atos ilícitos, como um *DDoS*, explanado no ponto 6.1. Ao possuir diversos computadores em seu poder, o cibercriminoso poderia lançar um ataque utilizando estas máquinas para gerar e enviar os pacotes necessários à sobrecarga de seu alvo, sem qualquer conhecimento da vítima infectada pelo backdoor, que poderiam ser rastreadas, caso o alvo do ataque final (no exemplo, um *DDoS*) consiga realizar engenharia reversa.

Este tipo de arquivo é muito utilizado por ser de difícil detecção pela vítima e qualquer ato praticado dessa forma terá o computador da vítima rastreado em possíveis casos de engenharia reversa. Este tipo de arquivo pode ser destruído pelo indivíduo de má-fé a qualquer tempo, caso não tenha sido estabelecido um tempo limite para seu funcionamento naquela máquina (pelo próprio criminoso).

6.6 KEYLOGGER E SCREENLOGGER

Keylogger, ou registrador de teclado, em português, é um programa utilizado por criminosos virtuais com o objetivo de obter informações do possuidor da máquina infectada, para que possam, posteriormente, utilizar as informações adquiridas em proveito próprio. Um dos usos mais comuns para este tipo de arquivo é a obtenção de informações do cartão de crédito da vítima, ou de seus registros bancários, caso utilize o sistema de *home banking* fornecido pela empresa.

Tal programa registra as teclas pressionadas no teclado e as envia, geralmente por e-mail, ao agente criminoso.

Para Emerson Wendt: *“boa parte dos casos de phishing scams são praticados em conjunto com Keyloggers, através de programas de spam, que permitem o envio de e-mail em massa para milhares de pessoas”* (WENDT, 2013, p.31). Apesar de correta esta informação, ela está levemente incompleta, na medida em que um Cavalo de Troia também é um veículo popular para a instalação deste tipo de arquivo. Possivelmente, o segundo seria mais ameaçador que o primeiro, pois as chances de um cavalo de Troia ser enviado por alguém conhecido à vítima – o primeiro já infectado com um cavalo de Troia, conforme explicado no ponto anterior – é claramente maior, o que reduziria a possibilidade daquela mensagem – veículo de um keylogger ou screenlogger – ser ignorada.

Já um screenlogger, ou registrador de tela, seria a versão evoluída de um keylogger, funcionando de maneira semelhante – registrando informações da vítima e enviando-as ao criminoso – mas sua forma de funcionamento difere de seu análogo na medida em que as informações registradas são provenientes da tela do computador, não de suas teclas.

Versões mais avançadas deste tipo de programa mesclam ambas as atividades, registrando tudo o que o usuário fizer em seu computador – tanto as teclas, quanto a tela -, o que, praticamente, impossibilita qualquer tentativa de esconder tais informações uma vez inseridas no micro.

O resultado, no geral, é a utilização da conta bancária da vítima – seja através do sistema de *home banking* ou do cartão de crédito – prejudicando não só a vítima, mas também o sistema bancário nacional, visto que existem tribunais aplicando a teoria do risco e determinando a indenização do indivíduo pela instituição financeira, como pode ser

observado nessa decisão do Tribunal de Justiça de Minas Gerais, tendo como relator o Desembargador Lucas Pereira.

APELAÇÃO. AÇÃO DE INDENIZAÇÃO POR DANOS MORAIS E MATERIAIS. TUTELA ANTECIPADA. ART. 273. REQUISITOS PRESENTES. PRELIMINAR REJEITADA. MOVIMENTAÇÃO BANCÁRIA POR TERCEIROS VIA INTERNET. RESPONSABILIDADE DA INSTITUIÇÃO FINANCEIRA PELOS DANOS ADVINDOS AO CLIENTE. RESPONSABILIDADE OBJETIVA. PREJUÍZOS COMPROVADOS. INDENIZAÇÕES DEVIDAS.

Existindo o fundado receio de dano irreparável ou de difícil reparação, requisitos do art. 273 do CPC, e prova inequívoca que convença o julgador da verossimilhança das alegações invocadas, deve ser deferida a antecipação da tutela. Se a instituição bancária disponibiliza acesso à conta corrente, como também, uma série de serviços bancários e movimentações financeiras através da Internet, compete-lhe garantir a segurança do sistema. Restando demonstrado que o serviço é falho, haja vista que permitiu o acesso à conta do cliente por terceiro, quando foram efetuadas operações de contratação de crédito, transferências e pagamentos, inafastável a responsabilidade do Banco, competindo-lhe reparar os prejuízos decorrentes do defeito na prestação do serviço.

(TJMG, 17ª CC. APELAÇÃO CÍVEL Nº 1.0145.08.440243-0/001. REL. SR. DES. LUCAS PEREIRA. Publ. 01/12/2009)(grifos próprios)

Apesar da aplicação da culpa à instituição financeira, obrigando-a a restituir o que fora tomado de seu correntista, alegando a falta de segurança por parte do banco, não restou comprovada o que resultou em tal movimentação ilícita. O próprio correntista poderia estar com seu computador comprometido, o que resultou em tais danos à sua conta bancária.

6.6 DISCRIMINAÇÃO E ÓDIO NA REDE

Apesar dos esforços governamentais brasileiros e exteriores, a Internet permanece, em sua maioria, entregue à anarquia, à completa falta de regulamentação.

Acobertados pela sensação de impunidade gerada pela capacidade de ser completamente anônimo na rede (embora tal subterfúgio seja vedado pela Constituição Federal brasileira), é comum encontrar formas de discriminação das mais diversas, principalmente em redes sociais, onde a falta de fiscalização permite a criação de perfis falsos, que podem ser utilizados para a disseminação de discursos de ódio.

O alcance da Internet pode se mostrar um empecilho – bem como, possivelmente, na mesma medida, um auxílio – no combate a essas posturas, pois a repercussão de qualquer ato pode tomar proporções colossais atingindo inúmeros indivíduos, o que facilita o rastreamento de sua fonte, mas não há como retirar por completo o que foi praticado.

Nos Estados Unidos, grupos defensores da “supremacia branca” utilizam a Internet não apenas para disseminar seus ideais discriminatórios, mas para recrutarem novos adeptos a seus ideais.

Uma das maneiras mais utilizadas para “comprovar” o ideal de supremacia se propaga através da desumanização e da demonização dos indivíduos discriminados, bem como a retirada da sensibilidade para os atos cometidos contra as vítimas.

Para Robert W. Taylor: *“One of the more effective and therefore more dangerous techniques these sites use to dehumanize de “enemy” or desensitize the consumer toward violence is computer games that are filled with extremist belief”*.¹³ (TAYLOR, 2011, p. 196)

Ao serem expostos a esses tipos de jogos por tempo suficiente, os indivíduos (geralmente jovens, possivelmente alvos de recrutamento para esses grupos) passariam a observar como normais as atrocidades cometidas.

A Constituição Federal brasileira, em seu artigo 5º, iguala todos os indivíduos presentes em território brasileiro, devendo todos ser tratados com a mesma deferência, sendo vedada qualquer forma de discriminação, em especial o racismo, o qual conta, além da constituição (artigos 4º, VIII e 5º XLII) com o Código de Processo Penal, em seu artigo 323, inciso I. O artigo 4º, inciso VIII, informa que a República Brasileira repudiará o racismo, enquanto os artigos 5º, XLII, da Constituição e o artigo 323, I, do CPP elevam o crime de racismo a crime inafiançável.

RACISMO. Ré que ofende não só a vítima pessoalmente, mas toda a raça negra. Crime do art. 20, da Lei nº 7.716/89, caracterizado. Afastamento da preliminar de desclassificação da conduta para injúria racial (art. 140, § 3º, do CP), perseguida por ação penal privada. Confissão da ré em plena harmonia com a prova colhida. Condenação mantida. Penas aplicadas no dobro do piso, sem justificativa idônea. Condenação ao pagamento das custas processuais inafastável. Eventual impossibilidade de pagamento que deve ser discutida perante o juízo da execução. Apelo parcialmente provido para, afastada a matéria preliminar, reduzir as penas ao piso legal e substituir a corporal, na forma do art. 44, § 2º, 1ª parte, do Código Penal, por dez dias-multa, no piso.

(TJ-SP - APL: 990101542404 SP , Relator: Tristão Ribeiro, Data de Julgamento: 02/12/2010, 5ª Câmara de Direito Criminal, Data de Publicação: 02/12/2010)

No Brasil, apesar da inexistência de lei específica para a internet, mostra-se possível a aplicação dos artigos 138, 139 e 140 do Código Penal (Calúnia, Difamação e Injúria, respectivamente) para buscar reparação pela discriminação proferida na rede, e é assim que vem demonstrando a jurisprudência pátria, sobre o crime de calúnia:

APELAÇÃO CRIMINAL. QUEIXA-CRIME. CALÚNIA. RECURSO ACUSATÓRIO. AUSÊNCIA DE DOLO ESPECÍFICO. NÃO OCORRÊNCIA. AUSÊNCIA DE TIPIFICAÇÃO DO CRIME IMPUTADO FALSAMENTE. DESNECESSIDADE. MEIO QUE FACILITA A DIVULGAÇÃO DA CALÚNIA. SITES DE INTERNET. ART. 141, III, CP. RECURSO PROVIDO.

¹³ Uma das técnicas mais eficazes e, portanto, mais perigosos esses sites usam para desumanizar de "inimigo" ou dessensibilizar o consumidor para a violência são jogos de computador, preenchidos com crenças extremistas. Tradução livre.

Não se fala em ausência de dolo específico do querelado que admite ter apontado irregularidades na Prefeitura, mas nega que visasse atingir a honra do Prefeito.

A ausência de tipificação expressa do crime, que o querelado teria imputado falsamente ao querelante, não impossibilita a procedência da Queixa-crime, pois na Ação Penal Privada, assim como na pública, o réu se defende dos fatos.

A divulgação da calúnia por meio de sites de Internet configura a causa de aumento estabelecida no art. 141, III, do CP.

(TJMS. Processo nº 2007.003364-6. Órgão Julgador: 2ª Turma Criminal. Relator: Exmo. Sr. Des. Claudionor Miguel Abss Duarte. Julgado em 23/05/2007)(grifos próprios)

Pelo exposto acima, a falta de tipicidade de crime de calúnia cometido na rede não afasta a possibilidade de enquadramento do agente criminoso.

Em relação aos crimes de injúria e difamação, podemos citar o seguinte julgado, emitido pelo douto Magistrado Luis Gustavo, da 2ª Turma Recursal do Tribunal de Justiça do Distrito Federal.

JUIZADO ESPECIAL. CIVIL. INJÚRIA E DIFAMAÇÃO. SÍTIO DA INTERNET. VIOLAÇÃO DA DIGNIDADE. DANO MORAL CONFIGURADO. INDENIZAÇÃO RAZOÁVEL E PROPORCIONAL. RECURSO DESPROVIDO.

1.A regra inscrita no art. 333 do CPC impõe ao autor o ônus de comprovar os fatos constitutivos do seu direito e ao réu o dever de demonstrar a inexistência desses fatos ou a presença de outros que lhe sejam impeditivos, modificativos ou extintivos. 2. No caso em exame, o autor comprovou a exibição de palavras ofensivas à sua honra no “blog” do requerido, enquanto esse se limitou a negar que tal fato violou a dignidade do requerente. **3. A injúria e a difamação atingem a honra objetiva e subjetiva da vítima, bem como ensejam a indenização por dano moral, sobretudo quando as ofensas são irrogadas em sítio da rede mundial de computadores.** 4. O dano moral é *in re ipsa*, ou seja, decorre do próprio fato ou ato causador da lesão, não havendo que se falar em prova da alteração do estado anímico do agente. 5. Se no arbitramento do valor da reparação observaram-se os princípios da razoabilidade e da proporcionalidade, não há razão para a sua revisão pela instância *ad quem*. 6. Recurso conhecido e desprovido. 7. Decisão tomada nos termos do art. 46, da Lei 9.099/95, servindo a ementa de acórdão. 8. Condene o recorrente no pagamento das custas e honorários advocatícios, os quais arbitro em 10% (dez por cento) do valor da condenação, cuja exigibilidade resta suspensa em face da gratuidade de justiça, nos termos da Lei nº 1.060/50.

(TJ-DF – ACJ: 1049443520108070001 DF 0104944-35.2010.807.0001, Relator: Luis Gustavo B. de Oliveira. Data de julgamento: 14/02/2012, 2ª Turma Recursal dos Juizados Especiais do Distrito Federal. Data de Publicação: 06/03/2012, DJe Pág. 187)

Embora os julgados não tenham sido proferidos por Magistrados das varas criminais, resta comprovada a culpabilidade dos agentes nesses casos.

6.7 CYBERBULLYING

Emerson Wendt leciona que Bullying é uma *“palavra originada da língua inglesa que significa valentão, caracteriza-se pela prática de agressões físicas ou psicológicas de forma habitual, traumática e prejudicial às vítimas”* (WENDT, 2013, p. 102).

As constantes evoluções tecnológicas fizeram essa prática evoluir, adaptando-se à rede mundial de computadores, surgindo, assim, uma nova modalidade, o *cyberbullying*. Sua prática tornou-se mais facilmente encontrável, visto que, agora, não ocorrem mais em salas escuras ou em corredores de pouca circulação, mas são postadas na rede onde diversas outras pessoas, não relacionadas com o que está ocorrendo, podem observar, sendo, também, possível que estes terceiros ingressem na prática, tomando parte do lado agressor ou do lado agredido.

A Internet, nesse caso, estaria atuando como uma ferramenta disseminadora e perpetuadora dessas agressões, principalmente em redes sociais, onde é possível repassar a “piada” com um mero clique.

O Bullying – e sua versão virtual – são muito recorrentes entre jovens em ambiente escolar – mas não se limita a tanto, Emerson Wendt informa que tais práticas também podem ocorrer no em ambiente corporativo, quando seria, então, denominado “mobbing” (WENDT, 2013, p.102). Tais práticas podem ser consideradas, também, formas de preconceito, uma vez que o agente estaria se aproveitando de uma característica – física, mental ou situacional – para realizar suas agressões.

Os resultados são avassaladores para a vítima, sendo constantemente encontrados agredidos com sintomas de depressão e inferioridade, podendo escalar para o suicídio, o que já ocorreu.

Embora não esteja tipificado como crime, Wendt informa que o bullying (e sua forma virtual) podem incorrer nos crimes de calúnia, difamação e injúria, estes já explicados no tópico anterior, mas também podem ser classificados como ameaça (WENDT, 2013, p.103-104) – modalidade bastante comum, pois serviria para diminuir a capacidade de defesa da vítima, fazendo-o elevar o agressor à qualidade de inatingível, por medo de sofrer novas agressões. Também há o constrangimento ilegal, muito utilizado em conjunto com a ameaça, para que a vítima realize algo que não deseja, sob pena de ter uma ação tomada contra ela ou aqueles que lhe são próximos.

Outro crime, também mencionado pelo doutrinador supra, é a falsa identidade (WENDT, 2013, p.104), sendo muito comum de encontrar na versão virtual da agressão, por não haver baixa ou nenhuma fiscalização na criação de perfis virtuais. O criador do perfil falso pode, então, apropriar-se de imagens e informações de um perfil pré-existente em sua empreitada (incorrendo, também, no crime de falsidade ideológica). Esta modalidade possui duas vítimas distintas, com diferentes resultados.

A primeira vítima é o alvo direto do agressor. Geralmente, ao ser criado um perfil falso, o indivíduo já possui, ao menos, o desejo de buscar realizar um ataque contra um indivíduo, aproveitando-se do disfarce. A segunda vítima pode não ser objetivo do agressor, sendo atingido pelo reflexo de seus atos. Trata-se do indivíduo que teve seu perfil clonado para a realização do ataque e, por muitas vezes, a primeira a ser acionada para reparar os danos causados. Muitas vezes o perfil falsificado é de uma personalidade pública ou

personagem fictício, no entanto, não existe impeditivo para que o agressor copie qualquer um da rede.

Por fim, a última finalidade dessa modalidade não é, exatamente, um crime, mas uma contravenção penal. Trata-se da perturbação da tranquilidade de um usuário. É o método mais utilizado pelos *trolls* da internet, ou *cybertrolls*. Estes são indivíduos que sentem prazer em irritar outrem, virtualmente ou não. Para tanto, utilizarão diversas táticas para atrair e prender um usuário incauto em discussões sem fim, sempre discordando do mesmo (até mesmo mudando sua própria argumentação inicial, apenas para prolongar o debate) até que este fique irritado. Sua presença é maior na Internet, onde podem passar horas buscando vítimas. Geralmente, seu “ataque” se inicia com um ataque direto à opinião proferida por um indivíduo, bem como ao próprio, garantindo que seja notado.

Os crimes – e a contravenção – aqui elencados são alvos não apenas do direito penal – no caso das três primeiras modalidades – mas recaem, também, sobre o direito civil e sobre a própria Constituição Federal.

Nossa Carta Magna protege, dentre outros fatores, a honra e a imagem das pessoas, garantindo a possibilidade da vítima buscar reparação – através de indenizações por danos morais e/ou materiais.

Acompanhando a Constituição, o Código Civil, em seus artigos 186, 187 e 927, demonstra a culpabilidade pelo ato praticado e o dever de repará-lo.

Também no Código Civil, em seu artigo 953, parágrafo único, existe a permissão para que o juiz fixe o valor da indenização a ser paga, caso o ofendido não consiga comprovar o prejuízo material.

O seguinte julgado comprova a capacidade de acionar, até mesmo a instituição de ensino, caso o fato ocorra sob sua guarda.

RECURSO INOMINADO. MUNICÍPIO DE SANTA MARIA. AÇÃO INDENIZATÓRIA. ESCOLA DE ENSINO FUNDAMENTAL. BULLYING. AGRESSÕES E HUMILHAÇÕES. MENOR COM SÍNDROME DE DOWN. RESPONSABILIDADE CIVIL DO MUNICÍPIO CONFIGURADA. DANO MORAL CARACTERIZADO. QUANTUM INDENIZATÓRIO REDUZIDO.

A Administração Pública responde objetivamente pelos danos advindos de atos ou omissões de seus agentes, contra terceiros, nos termos do artigo 37, § 6º da Constituição Federal. No caso, restou comprovada a responsabilidade extracontratual do Estado, porquanto demonstrado o evento danoso, bem como o nexo causal com a omissão do ente público. Inegável a ocorrência de bullying contra o menor, tendo em vista que as provas documentais carreadas, bem como os depoimentos das testemunhas, demonstram, cabalmente, que este sofria agressões e humilhações de crianças mais velhas no ambiente escolar. Presente o dever do Estado de promover o bom convívio dos alunos matriculados nas escolas, bem como a inclusão social das pessoas com deficiência. Diante da omissão estatal e comprovado o nexo causal, resta caracterizado o dever de indenizar pelos danos extrapatrimoniais. Isto porque o dano moral é aquele que atinge o âmago de uma pessoa, os seus direitos de personalidade, de modo a causar dor,

angústia, tristezas e sofrimentos, não se confundindo com os meros dissabores cotidianos. No entanto, o quantum indenizatório restou fixado em valor superdimensionado, merecendo redução, em razão dos princípios da razoabilidade e proporcionalidade. DERAM PARCIAL PROVIMENTO AO RECURSO. (Recurso Cível Nº 71004620498, Turma Recursal da Fazenda Pública, Turmas Recursais, Relator: Luís Francisco Franco, Julgado em 28/11/2013)

(TJ-RS - Recurso Cível: 71004620498 RS , Relator: Luís Francisco Franco, Data de Julgamento: 28/11/2013, Turma Recursal da Fazenda Pública, Data de Publicação: Diário da Justiça do dia 16/12/2013)

7 PORNOGRAFIA INFANTIL

Pornografia infantil é uma modalidade da pornografia caracterizada pela utilização de crianças e adolescentes em situações eróticas.

Para Emerson Wendt, trata-se de uma das maiores preocupações da internet, visto que o suposto anonimato, representado pela rede mundial de computadores, torna-se um campo fértil para a proliferação desse tipo de conteúdo. (WENDT, 2013, p. 98)

Essa modalidade de crime não está tipificada no código penal, mas no estatuto da criança e do adolescente (Lei 8.069/90) em seus artigos 240 e 241

PENAL. APELAÇÃO CRIMINAL. PEDOFILIA. PUBLICAÇÃO DE IMAGENS CONTENDO PORNOGRAFIA INFANTIL NA INTERNET. ART. 241, CAPUT, LEI Nº 8.069/90. DELITO CONSUMADO. CÚMULO MATERIAL. AUTORIA E MATERIALIDADE COMPROVADAS.

1. Comprovada, através de prova técnica, a publicação em site de doze fotos contendo pornografia infantil, assim como a disponibilização de arquivos de fotos, do mesmo gênero, na rede mundial de computadores. 2. Todos os meios tecnológicos utilizados que provoquem o resultado "publicar" são suficientes para a configuração do delito na sua forma consumada. 3. Materialidade e autoria delitivas da prática, por três vezes, do crime tipificado no art. 241, caput, do ECA, comprovadas pelo conjunto probatório constante dos autos, não possuindo qualquer sustentação a tese defensiva.

(TRF-4 - ACR: 5802 RS 2005.71.04.005802-7, Relator: TADAAQUI HIROSE, Data de Julgamento: 20/03/2007, SÉTIMA TURMA, Data de Publicação: D.E. 20/03/2007)

Esta modalidade de crime gera revolta até mesmo entre *hackers*, mas é absurdamente difícil comprovar a existência desse tipo de crime na rede, visto que os domínios onde estão hospedados esse tipo de conteúdo são propriedade da chamada *deep web*¹⁴, que é, a princípio, o reduto onde se encontram a grande maioria dos arquivos maliciosos da internet e todos aqueles que tem habilidades *hackers*.

¹⁴ Rede profunda, em tradução literal.

Nem toda a deep web é perigosa, o site de downloads piratas chamado The Pirate Bay, mencionando anteriormente, surgiu lá e, atualmente, é um dos maiores endereços para downloads ilegais no mundo.

É consistida dos endereços que não podem ser encontrados por servidores de busca, tais como o Google e o Yahoo, e tornou-se um porto seguro onde qualquer indivíduo com o devido conhecimento pode ingressar. Embora seja possível acessá-la com qualquer *browser*¹⁵ não é recomendado fazê-lo, pois, no local onde reina o verdadeiro anarquismo virtual, utilizar um navegador comum deixaria o IP (protocolo de internet, na sigla em inglês. É a digital do computador) a mostra para todos, tornando-o, certamente, um alvo para qualquer um que desejasse tentar a invadi-lo.

Na deep web existem fóruns de notícias das mais diversas, tal como na *surface web*¹⁶, como é chamada a internet acessada pela maioria esmagadora de seus usuários, desde discussões sobre futebol a endereços onde as notícias são mais repugnantes, como a pornografia infantil.

Os hacktivistas do grupo Anonymous em outubro de 2011 realizaram um ataque contra diversos endereços eletrônicos desse tipo de pornografia, retirando mais de 40 deles do ar e divulgando os nomes de mais de 1500 usuários para órgãos de investigação, como o FBI americano, convidando-os a juntarem-se nesta causa. Esta operação ficou conhecida como “DarkNet¹⁷”, mas não resultou em maiores frutos, devido a resistência do órgão federal em se aliar a *hackers* que não constavam nas fileiras do governo.

8 O QUE ESTÁ SENDO FEITO

A legislação brasileira ainda está quase inerte com relação aos crimes de internet, havendo poucos já tipificados e outros muito utilizados analogicamente a outros delitos já existentes no código penal, o que poderia ser uma afronta até mesmo ao artigo 1º do CP, o qual informa: “*Art. 1º - Não há crime sem lei anterior que o defina. Não há pena sem prévia cominação legal.*” (Decreto Lei 2848/41).

Neste íterim, faz-se necessário demonstrar a necessidade de Leis como a 12.737, de 2012, popularmente conhecido como Lei Carolina Dieckmann, surgida após a divulgação de imagens íntimas retiradas de aparelhos pertencentes à atriz na Internet. Esta lei veio como um marco, ao demonstrar o quão despreparados estava a legislação pátria para lidar com esse tipo de atividade, cuja prática vem se tornando mais comum a cada momento.

Tal lei modificou o código penal, acrescentando os artigos 154-A e B, pronunciando-se, finalmente, sobre invasão de aparelhos alheios mediante a Internet com o fim de prejudicar o proprietário da máquina.

Casos como o da goianiense Fran Santos, o qual teve imagens divulgadas em momentos sensíveis, gerando toda uma agitação, não apenas na internet, mas, também, na mídia, visto que, corajosamente, a jovem buscou auxílio judicial para lidar com o caso.

¹⁵ Navegador, em tradução livre.

¹⁶ Rede da superfície, em tradução livre

¹⁷ Rede sombria; rede escura, em tradução livre

A celeridade do mundo virtual vem superando, e muito, a morosidade do Congresso Nacional, expondo pessoas a situações vexatórias, podendo resultar em atitudes tomadas contra essas pessoas, que deveriam estar sendo protegidas em um momento de fragilidade.

As recentes denúncias de espionagem contra diversos órgãos, empresas e, até mesmo, a presidenta brasileira, demonstraram a necessidade da criação de uma regulamentação mais severa para a rede. Isso culminou com a aprovação da Lei 12.965/14, denominada Marco Civil da Internet, o qual possui disposições iniciais sobre como deverá ser utilizada a rede mundial de computadores, mas não ingressou em nenhum ponto sensível ao direito penal, dispondo apenas inicialmente sobre direitos e garantias dos usuários da rede no Brasil.

9 CONSIDERAÇÕES FINAIS

Diante de tudo o que foi exposto, restou comprovada a insegurança existente na rede e a quase inexistente representação de tal modalidade criminosa por parte do Poder Legislativo, engessando o Judiciário a aplicação de analogias e, quando não houver tipificação na lei penal sequer para uma analogia, estará configurada, por força do artigo 1º do Código Penal, o qual informa não haver crime antes de haver lei prévia, a impunidade virtual.

O surgimento das Leis 12.737/12 e 12.965/14, denominadas popularmente como Lei Carolina Dieckmann e Marco Civil da Internet, respectivamente, vem como as primeiras possibilidades de defesa contra os males que utilizam a Internet como meio de propagação e perpetuação, uma vez que a presença do Estado serviria para coibir agentes de má-fé virtuais que não possuem conhecimento suficiente para ultrapassarem as barreiras impostas.

O constante barateamento da tecnologia trará cada vez mais usuários para a rede, onde existem poucas defesas para um indivíduo mal informado, visto que, até mesmo, os melhores programas de antivírus (vendidos por lojas especializadas como única solução para os problemas virtuais) presentes no mercado não são capazes de prever o que ainda será criado, tamanha é a diversificação dos códigos geradores de arquivos maliciosos, limitando-se a proteger as máquinas, e seus usuários, contra aquilo que já existe, impedindo que mais dano seja causado.

Todo usuário da rede acaba, por um momento, inserindo informações sensíveis sobre sua pessoa na Internet, seja ao utilizar o sistema de *home banking* fornecido por sua instituição bancária, ou ao criar um perfil na mais interessante rede social do momento, e a proteção do Estado seria de bom tamanho para demonstrar que os cidadãos de boa-fé teriam, ao menos, garantia de reparação.

Assim, mostra-se imprescindível o não retorno à inércia original, uma vez que a mera analogia não será capaz de abranger todas as condutas que ocorrem com frequência na rede.

10 REFERÊNCIAS

MICHAELIS, Dicionário. **Dicionário Online.** Disponível em <http://michaelis.uol.com.br/moderno/portugues/index.php?lingua=portugues-portugues&palavra=Internet> Acesso em 08 de abril de 2014.

VANCIM, Adriano Roberto. **Direito & Internet: contrato eletrônico e responsabilidade civil na WEB: Jurisprudência selecionada e legislação internacional correlata** / Adriano Roberto Vancim, Jeferson Luiz Mاتيولli – Leme: Lemos e Cruz, 2011.

WENDT, Emerson. **Crimes cibernéticos: ameaças e processos de investigação** / Emerson Wendt; Higor Vinicius Nogueira Jorge. – 2. Ed – Rio de Janeiro, Brasport, 2013. p. 5

Castells, Manuel. **A Galáxia da Internet: reflexões sobre a internet, os negócios e a sociedade**. Rio de Janeiro: Jorge Zahar Editor, 2001.

BRASIL ESCOLA. **Internet**. Disponível em: <http://www.brasilecola.com/informatica/internet.htm> Acessado em 09 de Abril de 2014.

CRUZ, Antonio *apud* VANCIM

PINHEIRO, Patrícia Peck. **Direito digital**. / Patrícia Peck Pinheiro. – 4. Ed. Revista, atualizada e ampliada. – São Paulo: Saraiva, 2010.

O Homem no espaço. **Super Interessante**. Editora Abril. Disponível em <http://super.abril.com.br/tecnologia/homem-espaco-442035.shtml> Acessado em 17 de abril de 2014

GLANZ, Semy *apud* VANCIM, op., cit., p.29.

BRASIL. Tribunal de Justiça do Rio Grande do Sul. Recurso Cível Nº 71002458883, Terceira Turma Recursal Cível, Turmas Recursais, Relator: Eugênio Facchini Neto, Julgado em 27/05/2010.

INFO ESCOLA. **Redes Sociais**. Disponível em <http://www.infoescola.com/sociedade/redes-sociais-2> Acessado em 14 de abril de 2014.

INFO ESCOLA. **Revolução Industrial**. Disponível em <http://www.infoescola.com/historia/revolucao-industrial/> Acesso em 14 de abril de 2014

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil. Brasília: Senado Federal, 1988.

JESUS, Damásio de. **Direito penal, volume 1: Parte geral** / Damásio de Jesus. – 32 ed. – São Paulo: Saraiva, 2011.

BRASIL. Código Penal. Decreto Lei nº 2848. Rio de Janeiro. Presidência da República, 1940.
BRASIL. Superior Tribunal de Justiça. HC 34965/PA. Relator: Ministro Gilson Dipp. DJ 20/11/2004

BRASIL. Superior Tribunal de Justiça. HC 19846/GO. Relator: Ministro Gilson Dipp. DJ 09/10/2006

BRASIL. Código de Processo Penal. Decreto Lei nº 3689. Rio de Janeiro, 1941.

BRASIL. Lei 12.737 de 30 de Novembro de 2012. Congresso Nacional, 2012.

BRASIL. Lei 12.965/2014 de 23 de Abril de 2014. Congresso Nacional, 2014.

BRASIL. Superior Tribunal de Justiça. Habeas Corpus nº 81.638/PA (2007/0087811-8) Relator: Ministro Gilson Dipp. DJ de 6/08/2007

BRASIL. Tribunal Regional Federal da 1ª Região. HC: 56684 TO 0056684-28.2010.4.01.0000, Relator: DESEMBARGADOR FEDERAL CARLOS OLAVO, Data de Julgamento: 26/10/2010, TERCEIRA TURMA, Data de Publicação: e-DJF1 p.216 de 12/11/2010

BRASIL. Tribunal de Justiça de Minas Gerais. TJMG, 17ª CC. APELAÇÃO CÍVEL Nº 1.0145.08.440243-0/001. REL. SR. DES. LUCAS PEREIRA. Publ. 01/12/2009

BRASIL. Tribunal de Justiça de São Paulo. TJ-SP - APL: 990101542404 SP , Relator: Tristão Ribeiro, Data de Julgamento: 02/12/2010, 5ª Câmara de Direito Criminal, Data de Publicação: 02/12/2010

BRASIL. Tribunal de Justiça do Mato Grosso do Sul. TJMS. Processo nº 2007.003364-6. Órgão Julgador: 2ª Turma Criminal. Relator: Exmo. Sr. Des. Claudionor Miguel Abss Duarte. Julgado em 23/05/2007

BRASIL. Tribunal de Justiça do Distrito Federal. TJ-DF – ACJ: 1049443520108070001 DF 0104944-35.2010.807.0001, Relator: Luis Gustavo B. de Oliveira. Data de julgamento: 14/02/2012, 2ª Turma Recursal dos Juizados Especiais do Distrito Federal. Data de Publicação: 06/03/2012, DJe Pág. 187

BRASIL. Tribunal de Justiça do Rio Grande do Sul. TJ-RS - Recurso Cível: 71004620498 RS , Relator: Luís Francisco Franco, Data de Julgamento: 28/11/2013, Turma Recursal da Fazenda Pública, Data de Publicação: Diário da Justiça do dia 16/12/2013

GRABOSKY, Peter N. **Crime in the digital age: controlling telecommunications and cyberspace illegalities.** / Peter N Grabosky; Russel G Smith. – USA - Transaction Publishers. 2007.

Crimes na Internet: interpretados pelos tribunais: repertório de jurisprudência e legislação. / supervisão editorial Jair Lot Vieira. – Bauru, SP: EDIPRO, 2009

TAYLOR, Robert W. *et al.* **Digital Crime and Digital Terrorism.** / Robert W. Taylor *et al.*
– USA - PEARSON, 2011.

ANONYMOUS. **A Brief History of Anonymous Hacktivism.** / ANONYMOUS. ISBN
9781489587701