

CRIMINALIDADE VIRTUAL

Felipe Coelho Martins

Bacharel em Direito

1 Introdução

O desenvolvimento tecnológico iniciado no Século XX é reconhecido, nos tempos atuais, como o principal propulsor da “revolução da informação” e do surgimento do conceito de mundo globalizado.

O presente artigo busca delinear alguns aspectos relevantes acerca dos efeitos gerados pelo incremento da tecnologia no contexto de vida de significativa parcela dos indivíduos e suas relações. A criação do computador e o posterior advento de um surpreendente recurso propiciador de troca de informações intersubjetivas – a internet – alteraram a realidade e desencadeou o que se denomina de “era digital”, trazendo, pela primeira vez, conceitos aparentemente intangíveis e inofensivos, mas que rapidamente tomaram proporções imensuráveis.

A ausência de barreiras e a sensação de que estamos diante de um fenômeno incontrolável foi o suficiente para o aparecimento de uma “nova” forma de criminalidade. A internet tornou-se um instrumento de práticas delitivas possíveis de serem realizadas pela habilidade técnica de usuários que viam no espaço virtual um potencial expediente para o implemento de seus desideratos ilegais, mormente pela ilusão do anonimato proporcionada pela impunidade.

Frente a esse panorama, surgem indagações relativas ao enfrentamento dessa “nova” criminalidade: a forma de combate e prevenção das ações lesivas a bens jurídicos acessíveis via computador, a necessidade ou não de atuação legislativa para criminalizar condutas, a aplicação da legislação penal existente para os fatos criminais engendrados no ciberespaço e a suficiência do regramento civil vigente como meio de correspondência eficaz aos anseios das vítimas de lesões patrimoniais e morais.

Abordar-se-ão breves aspectos contextuais da criminalidade virtual na história mundial e sua conceituação; os objetivos iniciais pretendidos pelos idealizadores da internet; a sua posterior aplicação, de forma generalizada, na sociedade, e o desvirtuamento dos objetivos iniciais almejados.

Nesse contexto, serão tecidas algumas considerações sobre pontos

polêmicos do Projeto de Lei Substitutivo (ao PLS 76/2000, PLS 137/2000 e PLC 89/2003), de iniciativa do Senador Eduardo Azeredo, já submetido à análise do Plenário do Senado brasileiro, que busca *tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, de rede de computadores, ou que sejam praticadas contra dispositivos de comunicação ou sistemas informatizados e similares*.

2 Evolução histórico-conceitual dos crimes virtuais e da internet

Importante instrumento militar, criado na década de 1960 pela Agência de Projetos de Investigação Avançada de Defesa dos Estados Unidos (ARPA), em decorrência, notadamente, do clima hostil em que se encontravam os países pós II Guerra Mundial – período em que a tecnologia desenvolvera-se a tal ponto que assombrava a humanidade, tanto pela rapidez, quanto pelo perigo que as inovações poderiam acarretar – a internet tornou-se uma grande arma e importante aliada nesse período de Guerra Fria.¹

Com a fundação da *Advanced Research Projects Agency* (ARPA), nos mesmos moldes que deram início ao surgimento da *National Administration of Space Activities* (NASA), desenvolveram-se estudos com o objetivo de transformar os computadores – antes apenas instrumentos avançados de calcular – em máquinas que interagissem com o homem.²

Percebe-se que a internet nasceu no seio do Estado, com objetivos iniciais de utilização para fins militares, mas que, paulatinamente, transformou-se em um inovador expediente facilitador de realizações de tarefas, com utilização tanto na comunidade acadêmica, quanto para fins comerciais, disseminando-se pelo globo.³ É o que apregoa, nesse sentido, Patrícia Peck Pinheiro⁴:

A Revolução da Informação, plantada em 1957, com a criação do primeiro mainframe, marcou o começo da digitalização da sociedade. Hoje, vivemos uma interdependência completa, globalizada, interativa e em

1 CASTRO, Carla Rodrigues Araújo de. *Crimes de informática*. Rio de Janeiro: Lumen Juris, 2001. p. 3-4.

2 FILHO, Luna ; PEREIRA, Eury. “Internet no Brasil e o direito no ciberespaço”. *Infojus*. Rio de Janeiro, [s.n]. 1999. Disponível em : <<http://www.infojus.com.br>>. Acesso em: 03 dez 2008.

3 ROSSINI, Augusto Eduardo de Souza. *Informática, telemática e direito penal*. São Paulo: Memória Jurídica. 2004, p. 31.

4 PINHEIRO, Patrícia Peck. *Direito digital*. 2. ed. São Paulo: Saraiva, 2007. p. 29-30

rede. Uma simples página gratuita na internet já nasce global, com responsabilidades e obrigações dentro de um cenário complexo de normas. Somos reflexo não apenas de nosso conhecimento, do “penso, logo existo”, mas de nossa expressão, do “comunico-me, logo existo”.

Pierre Lévy⁵ bem acentua a respeito da revolução da escrita na história, desde a criação da imprensa até as inovações surgidas com a internet. Para o autor, tornou-se possível intercomunicar, através de *links* de hipertextos, todos os documentos existentes no mundo e ainda viabilizar o seu acesso simplesmente com cliques em um *mouse*, independentemente do local em que se estiver. Tal revolução, sobreleva destacar, não fora prevista e muito menos desejada pelas empresas multinacionais do setor de informática, telecomunicações e multimídia, mas *explodiu como uma rajada de balas entre os cibernautas*.⁶

Pondera Maria Luisa Fernandez Esteban⁷, em disquisição no Centro de *Estudios Políticos y Constitucionales*, de Madri, que:

Buscava-se criar uma ampla rede de computadores na qual a informação pudesse ir de uns a outros através de vias distintas, de maneira que, se uma área era atacada numa ação bélica, a informação pudesse chegar por um caminho ou outro ao seu destinatário. A chave deste sistema era a inexistência de um centro nevrálgico que controlasse esta rede, pois este seria um ponto vulnerável do sistema. Com esta filosofia nasceu ARPANET, que constitui o antecessor imediato da Internet.

Em sintonia, preleciona Gustavo Testa Corrêa que a internet foi desenvolvida com um princípio bem definido de funcionamento, mantendo-se até os dias de hoje, seria ele: [...] *a procura de vários caminhos para alcançar determinado ponto, ou seja, na hipótese de um dos troncos (caminho pelo qual trafega o sinal eletrônico) estar obstruído, procuraria ela, automaticamente, um outro caminho que o substituisse*.⁸

Ocorre que, paralelamente ao avanço tecnológico e à massificação do uso da internet, criou-se uma situação cujas implicações são

5 LÉVY, Pierre. “A Revolução Contemporânea em Matéria de Comunicação”. In: *Informática e Democracia*. Rio de Janeiro, 2000, p. 151.

6 Idem. Ibidem. p. 151.

7 “Limitaciones constitucionales e inconstitucionales a da libertad de expresión”. *Revista Española de Derecho Constitucional*. Madri : Centro de Estudios Políticos y Constitucionales, n. 53, mayo/ago, 1998. p. 288-289.

8 CORRÊA, Gustavo Testa. Aspectos jurídicos da internet. São Paulo: Saraiva, 2000. p. 7.

desconhecidas. Basta imaginarmos que todo e qualquer indivíduo tem livre disponibilidade para veicular na *web* textos, imagens, informações, filmes, músicas, sem qualquer controle ou limite ao atuar que ultrapasse as raias da legalidade e do direito à privacidade, chancelados de forma categórica no texto constitucional pátrio.⁹

Previendo os problemas que o implemento da internet geraria à coletividade, Eric Schmidt, executivo-chefe da empresa *Google*, assim vaticinou: *A internet é a primeira coisa que a humanidade criou e não entende, a maior experiência de anarquia que jamais tivemos.*¹⁰

Nesse contexto, há considerar que o campo para a propagação de condutas desviadas por meio de computadores tornou-se extremamente fértil, desvirtuando do verdadeiro sentido da internet, qual seja o intercâmbio de informações. Surgem, assim, os denominados crimes *virtuais*.

3 Da distinção entre crimes virtuais próprios e crimes virtuais praticados por meio do computador (impróprios)

Inicialmente, há duas grandes classificações que devem ser destacadas, de importância não meramente didática, mas de efeito prático significativo para o próprio enquadramento normativo do fato criminal.

De um lado, existem os denominados delitos virtuais propriamente ditos ou próprios, em que o bem jurídico efetivamente transgredido é a inviolabilidade de dados presentes em um computador. De outro, tem-se os delitos virtuais impróprios, em que o computador é um mero *instrumento* para ataques na rede.¹¹ É o caso, vale dizer, da prática do delito de dano, previsto no Código Penal, que ocorre quando há a *destruição, inutilização ou deterioração de coisa alheia*. Curiosamente, a execução e consumação desse crime poderão ocorrer ainda que o agente se encontre fora do alcance do bem jurídico violado, simplesmente pela utilização de um computador. Tal é o incremento, que a ação criminosa pode, inclusive, ser realizada dentro da própria residência do infrator. Demonstra-se, assim, que essas condutas lesivas só podem ser praticadas por pessoas que possuam certa

9 GUERRA, Sidney César S. O Direito à privacidade e a internet. In: *Internet e direito, reflexões doutrinárias*. Roberto Roland Rodrigues da Silva Junior (org.) et al. Rio de Janeiro, 2001. p. 127.

10 FERREIRA, Érica Lourenço de Lima. Jurisdição Metaterritorial para a Cibernética. *Lex*. São Paulo, [s.n]. Disponível em: <<http://www.lex.com.br>>. Acesso em: 24 dez 2008.

11 JÚNIOR, Délio Lins e Silva. Crimes informático: vitimização e a questão do tipo objetivo. In: *Direito Penal Secundário*. Estudos sobre crimes econômicos, ambientais, informáticos e outras questões. Fábio Roberto D'Avila; Paulo Vinicius Sporleder de Souza (org.). São Paulo: Revista dos Tribunais, 2006. p. 314.

capacidade financeira e intelectual.

Segundo Felipe Cardoso Moreira de Oliveira¹², os delitos virtuais próprios são assim definidos:

Constituem-se em ações realizadas com o intuito de destruir, obter, copiar ou alterar dados (objeto material) de uma unidade de computador ou, ainda, de uma rede. São condutas a serem praticadas especificamente contra os dados e, por consequência contra a capacidade funcional do sistema que os abriga. Como se percebe, sua realização somente se dá envolvendo, pelo menos, um computador. Caso não existissem computadores no mundo, tais delitos jamais seriam cogitados e, muito menos, perpetrados em nossa sociedade.

Quanto aos delitos virtuais impróprios, estes se caracterizam por serem crimes de meio, sendo utilizado o contexto virtual para a obtenção de um fim ilegal. A maioria dos delitos virtuais também ocorre no mundo real, sendo a internet apenas um facilitador, principalmente pelo anonimato que proporciona.¹³

Nessa mesma ordem de considerações, é a lição de Maria de La Luz Lima¹⁴, referente aos crimes virtuais:

Em um sentido amplo é qualquer conduta criminógena ou criminal que em sua realização faz uso da tecnologia eletrônica seja como método, meio ou fim e que, em um sentido estrito, o delito informático, é qualquer ato ilícito penal em que os computadores, suas técnicas e funções desempenham um papel, seja como método, meio ou fim.

Consoante Patrícia Peck Pinheiro¹⁵:

Os crimes virtuais têm modalidades distintas, dependendo do bem jurídico tutelado. Nesse sentido, podemos dar como exemplo o crime de interceptação de dados, que tem como bem jurídico tutelado os dados, ou seja, o que se quer

12 OLIVEIRA, Felipe Cardoso Moreira de. *Criminalidade informática*. Porto Alegre: Pontifícia Universidade Católica do Rio Grande do Sul: PUCRS. 2002. Dissertação de Mestrado, Faculdade de Direito/Ciências Criminais/Pontifícia Universidade Católica do Rio Grande do Sul, 2002.

13 PINHEIRO, Patrícia Peck. *Direito digital*. 2. ed. São Paulo: Saraiva, 2007. p. 249-250.

14 LIMA, Maria de La Luz. *Delitos electrónicos. Criminalia*. Academia Mexicana de ciencias Penales. n. 1-6, año L, Enero-Junio. México, 1984. p. 100.

15 PINHEIRO, Patrícia Peck. *Direito digital*. 2. ed. São Paulo: Saraiva, 2007. p. 249-250.

é proteger a transmissão de dados e coibir o uso dessas informações para fins delituosos, como, por exemplo, captura de informações para envio de “e-mail bombing”¹⁶, o “e-mail com vírus”¹⁷, o “spam”. Esse tipo penal protege também a questão da inviolabilidade das correspondências eletrônicas.

Délio Lins e Silva Júnior¹⁸ não aceita o enquadramento dos delitos praticados por meio de computador como sendo delitos informáticos, justamente por entender que tais práticas são equiparadas aos já tradicionais procedimentos previstos no Código Penal e em legislações esparsas, o que inviabilizaria a sua inserção na categoria dos delitos informáticos, cujo bem jurídico atacado é a inviolabilidade de dados armazenados no computador.

Continua o mesmo autor:¹⁹

A falta de atenção para tal diferenciação leva a doutrina a atribuir aos crimes informáticos conceitos amplos, que albergam não apenas a inviolabilidade de dados constantes em sistemas informáticos, mas também a própria utilização de um computador como mero meio de obtenção dos fins ilícitos pretendidos. Com efeito, se os crimes informáticos visam a tutelar a proteção de dados informáticos, seu corolário lógico deve ser a restrição de sua conceituação.

Não é essa a opinião, todavia, de Augusto Eduardo de Souza Rossini²⁰. Afirma o autor que a denominação “delitos informáticos” abrange toda e qualquer conduta em que haja relação (tanto de meio quanto de fim) com sistemas informáticos, e não somente as condutas perpetradas no contexto da internet. Ainda, o conceito englobaria os delitos em que a utilização do computador fosse uma mera ferramenta, *sem a imprescindível conexão à Rede Mundial de Computadores, ou a qualquer outro meio telemático. Ou seja, no caso de fraude em que o computador é usado como instrumento do crime, fora da internet.*

16 *E-mail bombing* : envio de *e-mails* imensos ou vários *e-mails*. Causa atraso na recepção e gasto adicional com conta telefônica.

17 E-mail com vírus – envio de vírus anexado ao *e-mail*.

18 JÚNIOR, Délio Lins e Silva. *Crimes informáticos: vitimização e a questão do tipo objetivo*. In: *Direito Penal Secundário*. Estudos sobre crimes econômicos, ambientais, informáticos e outras questões. Fábio Roberto D’Avila; Paulo Vinícius Sporleder de Souza (org.). São Paulo: Revista dos Tribunais, 2006. p. 315.

19 Idem. Ibidem. p. 315.

20 ROSSINI, Augusto Eduardo de Souza. *Informática, Telemática e Direito penal*. São Paulo: Memória Jurídica, 2004. p. 110.

Oportuno que se apresentem as especificações relativas às duas principais modalidades de condutas virtuais praticadas na *web*, sob o enfoque dos bens jurídicos que visam tutelar e das características do próprio agir criminoso.

3.1 A recepção tipológica dos crimes virtuais impróprios: a legislação existente

Com a enorme efusão da internet e a aparente impunidade dos atos criminosos de alguns maus usuários, o campo para a propagação de crimes cibernéticos tem se tornado extremamente atrativo. Notadamente pela possibilidade do anonimato das condutas transgressoras e a insipiência em que se encontram os estudos relativos a essa “novel” criminalidade, é imperioso que avancemos em certos dogmas arraigados em nossa cultura, principalmente a busca exclusivamente da lei penal como meio para a solução das mazelas sociais, para que consigamos combater com eficácia a inevitável disseminação dessa forma de prática delitiva.

Tratando-se dos crimes virtuais impróprios, tais condutas transgressoras instrumentalizadas pela internet em nada se diferem daquelas já previstas em nossa legislação penal, exceto pela necessidade de um computador.

Como bem acentuado por Angela Bittencourt Brasil²¹, *a semelhança dos crimes comuns com esses ‘novos’ crimes termina pela utilização do computador, para alcançar e manipular o seu sistema em proveito próprio ou para lesionar outrem.*

A necessidade de legislação específica sobre crimes de computador é irrelevante quando estivermos diante de condutas delituosas que já estejam previstas no estatuto repressivo e em leis esparsas, inexistindo qualquer alteração no que tange à adequação das condutas lesivas, via internet, com os tipos penais já existentes.

Nessa mesma ordem de considerações, preleciona José Henrique Barbosa Moreira Lima Neto, especializado em informática e segurança de informações, em lembrança adequada por Gustavo Testa Corrêa²², que *A Internet não precisa de leis especiais, mas ser incorporada à realidade do país, bem assim, Toda legislação existente, seja de natureza penal, comercial ou civil, se aplica à internet.*

Patrícia Peck Pinheiro²³ refere que, especificamente no caso do

21 BRASIL, Angela Bittencourt. *Informática jurídica: o ciber direito*. Rio de Janeiro: [s.n]. 2000. p. 37.

22 CORRÊA, Gustavo Testa. *Aspectos jurídicos da internet*. São Paulo: Saraiva, 2000. p. 59-60.

23 PINHEIRO, Patrícia Peck. *Direito digital*. 2. ed. São Paulo: Saraiva, 2007. p 252.

Brasil, as infrações penais mais usuais, praticadas via rede mundial de computadores, são aquelas associadas ao delito de estelionato e à pedofilia.

Não destoam Luiz Gustavo Grandinetti Castanho de Carvalho²⁴, ao afirmar que:

Se a rede é usada para a prática de crimes, usam-se os tipos penais existentes. Se se trata de pedofilia, serve-se do artigo 241 do ECA. Se ela for usada para o tráfico de drogas, a Lei de Tóxicos, ou mesmo o tipo da apologia de fato criminoso. Quando ocorrer violação de correspondência pela forma do e-mail, aplica-se o artigo 151 do Código Penal.

Em artigo publicado no *site* Espaço Vital²⁵, intitulado *Levantamento mostra que já existem mais de 17 mil decisões judiciais envolvendo problemas na Internet*, há um elenco de alguns tipos penais que se amoldam às condutas danosas de usuários do ciberespaço:

A lista de ilícitos é extensa: insultar a honra de alguém (calúnia – artigo 138), espalhar boatos eletrônicos sobre pessoas (difamação – artigo 139), insultar pessoas considerando suas características ou utilizar apelidos grosseiros (injúria – artigo 140), ameaçar alguém (ameaça – artigo 147) e utilizar dados da conta bancária de outrem para desvio ou saque de dinheiro (furto – artigo 155).

Também comentar, em chats, e-mails e outros, de forma negativa, sobre raças, religiões e etnias (preconceito ou discriminação – artigo 20 da Lei nº 7.716/89), enviar, trocar fotos de crianças nuas (pedofilia – artigo 247 da Lei nº 8.069/90, o Estatuto da Criança e do Adolescente).

Grande parcela das ocorrências delitivas que se apresentam na seara da informática, frize-se, já encontra tutela no ordenamento jurídico vigente. Talvez não de forma adequada, contudo não é crível que se infra que certos delitos virtuais *estejam entregues a um limbo legal, sendo impossível a solução dos conflitos que se apresentam ao mundo jurídico sem a elaboração de um ou vários novos diplomas normativos*.²⁶

24 CARVALHO, Luiz Gustavo Grandinetti Castanho de. Direito de informação, liberdade de expressão e internet. In: *Internet e Direito, Reflexões Doutrinárias*. Roberto Roland Rodrigues da Silva Junior (org.) et al. Rio de Janeiro: Lumen Júris, 2001. p. 87.

25 S.n. *Levantamento mostra que já existem mais de 17 mil decisões judiciais envolvendo problemas na Internet*. Espaço Vital. Porto Alegre: [s.n.], 2008. Disponível em: <<http://www.espacovital.com.br>>. Acesso em: 08 dez 2008.

26 MARTINS, Júlio César Werneck. O Hackerismo e a defesa da propriedade virtual: O Patrimônio da

Em ilustrativo caso de possibilidade de aplicação dos tipos penais existentes para os “fatos informáticos” de caráter delituoso, em especial atenção aos crimes de estelionato e extorsão, previstos, respectivamente, nos artigos 171 e 158, ambos do Estatuto Repressivo, Júlio César Werneck Martins²⁷ traz à baila os chamados “sequestros virtuais”.

Tal denominação deu-se em razão de uma prática que surgiu por ações de *hackers*, que invadiam sistemas informáticos e modificavam todas as senhas de acesso existentes, impedindo, com isso, que os titulares, proprietários dos dados contidos em um sistema digital, tivessem livre acesso a esses.

Aduz o autor, ainda, que esse agir infracional seria o mesmo *que invadir uma residência e trocar todas as fechaduras das portas, impedindo o acesso dos verdadeiros donos ou locatários*.

Diante da impossibilidade de disporem de informações e conteúdos importantes de uso exclusivo e sigiloso, comprometendo sobremaneira o exercício de atividades corriqueiras, empresários submetem-se a legítimas extorsões, tornando-se vítimas das ações criminosas dos *hackers*. Sem alternativa, efetivam-se os pagamentos das quantias exigidas pelos invasores de modo a recuperar o controle dos dados extraviados.

Ademais, continua o autor: *Poderia a empresa adotar postura mais radical, simplesmente derrubando o sistema e reinstalando um novo, porém tal atitude implicaria na destruição de suas informações homem homem, não apenas a homem-máquina, o que seria desastroso*.²⁸

Carla Rodrigues Araújo de Castro²⁹ menciona outros tipos penais instrumentalizados por computador (crimes virtuais impróprios):

artigo 208 (Escárnio por Motivo de religião); artigo 228 (Favorecimento da Prostituição); artigo 233 (Ato obsceno); artigo 234 (Escrito ou objeto obsceno); artigo 286 (Incitação ao Crime); artigo 287 (Apologia de Crime ou Criminoso); artigo 50 do Decreto-Lei n.º 3.688/41 (Jogos de Azar); artigo 241 da Lei n.º 8.069/90 (Pedofilia); artigos 1.º e 20 da Lei n.º 7.716/89 (Crime de Preconceito e Discriminação); artigos 22 e 23 da Lei n.º 7.170/83 (Crimes Contra a Segurança Nacional); Lei n.º 9.279/96 (Crimes Contra a Propriedade Industrial), artigo 1.º da Lei 9.613/98 (Crime de Lavagem de Dinheiro).

Informação. In: *Internet e Direito, Reflexões Doutrinárias*. Roberto Roland Rodrigues da Silva Junior (org.) et al. Rio de Janeiro: Lumen Juris, 2001. p. 185.

27 Idem. Ibidem. p. 185.

28 Idem. Ibidem. p. 185.

29 CASTRO, Carla Rodrigues Araújo de. *Crimes de informática*. Rio de Janeiro: Lumen Juris, 2001. p. 16-69.

Os crimes contra a propriedade imaterial (de múltiplas condutas), artigo 184 do Código Penal – praticados via computador, também podem ser classificados em crimes virtuais impróprios, ou seja, são realizáveis por meio da utilização de um sistema computacional, o qual é apenas instrumento para a prática infracional.

3.2 A recepção tipológica dos crimes virtuais próprios: a legislação existente

Anotação que se faz necessária, é a delimitação da abrangência dos delitos virtuais próprios, realizada a partir de uma análise do bem jurídico tutelado, sugerida por Felipe Cardoso Moreira de Oliveira³⁰, *in verbis*:

Os delitos informáticos constituem-se em ações realizadas com o intuito de destruir, obter, copiar ou alterar dados (objeto material) de uma unidade de computador ou, ainda, de uma rede. São condutas a serem praticadas especificamente contra os dados e, por consequência contra a capacidade funcional do sistema que os abriga.

Relativamente aos delitos em espécie, previstos no Diploma Penal e em legislações especiais, Carla Rodrigues Araújo de Castro³¹ apresenta as seguintes hipóteses de condutas violadoras da “capacidade funcional do sistema computacional” (crimes virtuais próprios):

Interceptação de *E-mail* (Comunicações):

O sigilo das correspondências constitui uma garantia constitucional prevista no artigo 5.º, XII. Correspondência é uma troca de informações entre pessoas ausentes, que pode ser feita por cartas, bilhetes e agora por computador. O e-mail nada mais é do que uma correspondência enviada pela Internet.³²

Segundo a autora, em nossa legislação haveria duas regras aptas a proteger o *e-mail*, perfazendo um conflito aparente de normas. São elas: O

30 OLIVEIRA, Felipe Cardoso Moreira de. *Criminalidade informática*. Porto Alegre: Pontifícia Universidade Católica do Rio Grande do Sul: PUCRS. 2002. Dissertação de Mestrado, Faculdade de Direito/Ciências Criminais/Pontifícia Universidade Católica do Rio Grande do Sul, 2002.

31 CASTRO, Carla Rodrigues Araújo de. *Crimes informática*. Rio de Janeiro: Lumen Juris, 2001. p.21.

32 Idem. Ibidem. p. 21.

artigo 40³³ da Lei n.º 6.538/78 e o artigo 10³⁴ da Lei n.º 9.296/96, que traz eficácia ao inciso XII, parte final, do artigo 5.º da Constituição Federal. Por ser regramento especial, parece razoável inferir-se que o último dispositivo é que deveria prevalecer.³⁵

Trata-se de norma penal que visa a tutelar a comunicação telefônica e telemática, *sendo esta a junção da comunicação com os meios de informática*.³⁶

Inserção de Dados Falsos em Sistema de Informações – Artigo 313-A³⁷ do Código Penal:

Esse tipo penal foi inserido no CP pela Lei n.º 9.983 de 14/07/2000, no capítulo dos crimes praticados por funcionário público contra a Administração Pública. Os bens jurídicos tutelados são a probidade da Administração Pública e o sistema de informação e programas por ela utilizados. Trata-se de crime de informática próprio, posto que só pode ser praticado com o auxílio do computador.³⁸

Da mesma forma que o artigo 313-A do Estatuto Repressivo, o delito de Modificação ou Alteração não Autorizada de Sistema de Informação (Artigo 313-B³⁹ do mesmo Diploma) surgiu com o implemento da Lei n.º 9.983/2000. Somente pode ser praticado por funcionário público contra a Administração Pública. Os bens jurídicos tutelados são a probidade da Administração Pública e o sistema de informação por ela utilizado.⁴⁰

4 Crítica ao Projeto de Lei

A iminente aprovação do Projeto de Lei Substitutivo (ao PLS

33 Art. 40. Devassar indevidamente o conteúdo de correspondência fechada dirigida a outrem:

Pena – detenção, até 6 (seis) meses, ou pagamento não excedente a 20 (vinte) dias-multa.

34 Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei:

Pena – reclusão, de 2 (dois) a 4 (quatro) anos, e multa.

35 CASTRO, Carla Rodrigues Araújo de. *Crimes de informática*. Rio de Janeiro: Lumen Juris, 2001. p. 22.

36 Idem. Ibidem. p. 22

37 Art. 313-A. Inserir ou facilitar, o funcionário público autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano:

Pena – reclusão, de 2 (dois) a 12 (doze) anos, e multa.

38 CASTRO, Carla Rodrigues Araújo de. *Crimes de Informática*. Rio de Janeiro: Lumen Juris, 2001. p. 22.

39 Art. 313-B. Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente:

Pena – detenção, de (três) meses a 2 (dois) anos, e multa.

40 CASTRO, Carla Rodrigues Araújo de. *Crimes de informática*. Rio de Janeiro: Lumen Juris, 2001. p. 22.

76/2000, PLS 137/2000 e PLC 89/2003), de iniciativa do Senador Eduardo Azeredo, já submetido à análise do Plenário do Senado brasileiro, que busca *tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, de rede de computadores, ou que sejam praticadas contra dispositivos de comunicação ou sistemas informatizados e similares*, suscita alguns questionamentos referentemente aos reflexos que surtirá em nosso contexto.

Fruto de um processo legislativo calcado em um ideário de extrema repressão, o Projeto de Lei Substitutivo define como criminosas algumas condutas na internet, até então inofensivas, e o estabelecimento de penas severas para os pretensos infratores.

Percebe-se, mais uma vez, que o Direito Penal alcança *status* de apaziguador dos problemas sociais oriundos do natural incremento da tecnologia e do aperfeiçoamento, por via de consequência, dos métodos de cometimento de ilícitos. O Estado, não cumprindo com o dever social que lhe é peculiar, utiliza-se do Direito Penal como *prima ratio* e estabelece regime extremamente rigoroso em pleno Estado Democrático de Direito.

Não adianta valer-se de leis penais, cumpre dizer, violadoras de princípios constitucionais, com o pretexto de apaziguar a coletividade e restaurar a tranquilidade ameaçada por certos transtornos sociais se esse aparente restabelecimento da normalidade cria verdadeiras ficções jurídicas e rompe com garantias individuais categoricamente chanceladas no texto constitucional.

Tais medidas excepcionais transmitem erroneamente à sociedade e, principalmente, aos meios de comunicação impresso e digital – formadores de opinião –, a sensação de que não há alternativa para a proteção do patrimônio e para a segurança de outros bens igualmente relevantes a não ser por meio do rigorismo penal.

Sob essa ideologia de enfrentamento dos problemas sociais e, diante da política criminal adotada pelo Estado, é que se encaminha a vindoura “Lei dos Crimes na Internet”, que transformará a rede num espaço virtual de medo, território em que todos seremos suspeitos e potenciais criminosos.

Não por outras razões, pesquisadores e professores brasileiros encaminharam ao Congresso Nacional um manifesto, intitulado: *Em defesa da liberdade e do progresso do conhecimento na internet brasileira*, reivindicando aos parlamentares a rejeição do Projeto Substitutivo do Senador Eduardo Azeredo, conforme trecho que segue:

Se, como diz o projeto de lei, é crime “obter ou transferir dado ou informação disponível em rede de computadores, dispositivo de comunicação ou sistema informatizado, sem autorização ou em desconformidade à autorização, do legítimo titular, quando exigida”, não podemos mais fazer nada na rede. O simples ato de acessar um site já seria um crime por “cópia sem pedir autorização” na memória “viva” (RAM) temporária do computador. Deveríamos considerar todos os browsers ilegais por criarem caches de páginas sem pedir autorização, e sem mesmo avisar ao mais comum dos usuários que eles estão copiando. Citar um trecho de uma matéria de um jornal ou outra publicação on-line em um blog, também seria crime. O projeto, se aprovado, colocaria a prática do “blogging” na ilegalidade, bem como as máquinas de busca, já que elas copiam trechos de sites e blogs sem pedir autorização de ninguém!

Se formos aplicar uma lei como essa às universidades, teríamos que considerar a ciência como uma atividade criminosa já que ela progride ao “transferir dado ou informação disponível em rede de computadores, dispositivo de comunicação ou sistema informatizado”, “sem pedir a autorização dos autores” (citamos, mas não pedimos autorização aos autores para citá-los). Se levarmos o projeto de lei a sério, devemos nos perguntar como poderíamos pensar, criar e difundir conhecimento sem sermos criminosos.⁴¹

Vê-se, assim, que o Projeto de Lei Substitutivo apresenta relevantes indagações que necessitam ser enfrentadas, com repercussão direta em atividades realizáveis por meio do uso do computador e da internet. Sobre os dispositivos mais polêmicos da iminente “Lei dos Crimes na Internet” o tópico que se segue abordará o tema de forma pormenorizada.

4.1 A análise dos artigos

Conforme texto veiculado pelo Centro de Tecnologia e Sociedade da Escola de Direito da Fundação Getúlio Vargas⁴², do Estado do Rio de Janeiro, é possível fazer algumas ponderações acerca dos tipos penais

41 LOBATO, Elvira. Baixar arquivo na internet pode virar crime. *Folha On Line*. São Paulo: [s.n.], 2008. Disponível em : <<http://www.folha.com.br>>. Acesso em: 16 dez 2008.

42 PROTASIO, Arthur. *Esclareça suas dúvidas sobre os vários problemas do Projeto de Ciber Crimes, aprovado pelo Senado*. A2kbrasil. Rio de Janeiro: [s.n.], 2008. Disponível em : <<http://www.a2kbrasil.org.br>>. Acesso em: 16 dez 2008.

constantes no Projeto de Lei Substitutivo, aprovado no dia 9 de julho de 2008, pelo Plenário do Senado Federal.

O Projeto de Lei prevê a criminalização de algumas condutas de usuários do ciberespaço. Necessitam de especial atenção, pela polêmica que encerram, as seguintes modalidades infracionais:

Artigo 285-A. Acessar, mediante violação de segurança, rede de computadores, dispositivo de comunicação, ou sistema informatizado, protegidos por expressa restrição de acesso: Pena - reclusão, de 1 (um) a 3 (três) anos, e multa. Parágrafo único. Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada de sexta parte.

Tal previsão do projeto transforma condutas banais de usuários da internet em tipos criminais, com apenamento extremamente severo como forma de sancionamento. Ainda, pela circunstância de não haver qualquer menção do que seria *expressa restrição de acesso*, isso dá ensejo a uma série de possibilidades de restrições, como a legal, contratual ou tecnológica.⁴³

Exemplo 1: Desbloqueio de celular de uma operadora para ser acessado em outra. Configura ‘acesso a dispositivo de comunicação protegido por expressa restrição de acesso, mediante violação de segurança’.⁴⁴

Exemplo 2: Desbloquear um aparelho de DVD (para que ele funcione com filmes de qualquer região). Configura ‘acesso a sistema informatizado protegido por expressa restrição de acesso, mediante violação de segurança’.⁴⁵

Artigo 285-B. Obter ou transferir, sem autorização ou em desconformidade com autorização do legítimo titular da rede de computadores, dispositivo de comunicação ou sistema informatizado, protegidos por expressa restrição de acesso, dado ou informação neles disponível: Pena - 1 (um) a 3 (três) anos de reclusão, e multa. Parágrafo único. Se o dado ou informação obtida desautorizadamente é fornecida a terceiros, a pena é aumentada de um terço.

43 Idem.Ibidem.

44 Idem.Ibidem.

45 Idem.Ibidem.

Novamente são criminalizadas condutas absolutamente triviais, cabendo ao legítimo titular a prerrogativa de “completar” a lei, podendo escrever como quiser a sua “autorização”, que, uma vez violada, configura o delito.⁴⁶

Exemplo 1: Acessar um site em violação a seus termos de uso. Configura ‘obtenção de dados em desconformidade com autorização do legítimo titular de sistema informatizado protegido por expressa restrição de acesso’.⁴⁷

Ademais, Note que a “expressa restrição de acesso” consiste nos próprios termos de uso do site. Para sites que não possuem termos de uso (um blog, por exemplo) o problema continua, já que o conteúdo dos mesmos é protegido pela lei de direitos autorais (ou seja, esta também é uma “expressa restrição de acesso”, que como dito acima, pode ser tecnológica, jurídica ou contratual).⁴⁸

Exemplo 2: “Resgatar música de um iPod de volta para o computador. Configura ‘obter dado em desconformidade com a autorização do legítimo titular do dispositivo de comunicação ou sistema informatizado’.⁴⁹

Artigo 163-A. Inserir ou difundir código malicioso em dispositivo de comunicação, rede de computadores ou sistema informatizado. Parágrafo 1.º. Se do crime resulta destruição, inutilização, deterioração, alteração, dificuldade do funcionamento, ou funcionamento desautorizado pelo legítimo titular, de dispositivo de comunicação, de rede de computadores, ou de sistema informatizado: Pena - 2 (dois) a 4 (quatro) anos, e multa.

A conduta tipificada traz uma abrangência que ultrapassa o conceito de “vírus”:

Ele diz respeito a qualquer programa que resulte na ‘alteração’, ‘dificultação do funcionamento’ ou ‘funcionamento desautorizado pelo legítimo titular’.⁵⁰

Exemplo 1: Desbloqueio do iPhone utilizando um software compatível, configura ‘inserir código malicioso em dispositivo de comunicação que resulta em funcionamento desautorizado pelo legítimo titular’.⁵¹

Artigo 22. O responsável pelo provimento de acesso a rede de computadores mundial, comercial ou do setor público é

46 Idem.Ibidem.

47 Idem.Ibidem.

48 Idem.Ibidem.

49 Idem.Ibidem.

50 Idem.Ibidem.

51 Idem.Ibidem.

obrigado a: III. informar, de maneira sigilosa, à autoridade competente, denúncia que tenha recebido e que contenha indícios da prática de crime sujeito a acionamento penal público incondicionado, cuja perpetração haja ocorrido no âmbito da rede de computadores sob sua responsabilidade. Estes são os principais equívocos do dispositivo: A denúncia não deveria ser feita diretamente à autoridade competente? O provedor, nesse sentido, não tem a obrigação de receber denúncias. Como não existe restrição para que qualquer interessado possa enviar denúncias aos provedores, isso cria uma espécie de ‘indústria de denúncias’. Além disso, a própria definição de ‘provedor’ não é clara no texto da lei (há vários tipos de provedores de acesso: à rede, a conteúdo, a serviços online etc.).⁵² Exemplo: Cria-se um blog em um provedor brasileiro por algum usuário, este blog possui ‘links patrocinados’. Alguém denuncia a pessoa ao provedor, que por sua vez é obrigado a denunciá-lo à autoridade competente.⁵³

Se isso não bastasse, o profano – provedor – ainda deve possuir conhecimento técnico-jurídico suficiente para aferir se determinada conduta de usuário seu é ou não ensejadora de um “acionamento penal público incondicionado”. Ainda:

Com o novo dispositivo, interessados (como a indústria do conteúdo) podem evitar completamente um processo prévio de identificação, ficando prejudicado o direito constitucional de devido processo legal. Isso ocorre porque a partir da simples denúncia ao provedor de acesso, este fica obrigado a encaminhá-la imediatamente à autoridade competente, conforme prevê o dispositivo, podendo inclusive mandar os dados do usuário vinculado ao IPs “denunciado”. Dessa forma, ocorrerá automaticamente a identificação do usuário, ao arrepio do devido processo legal.⁵⁴

Evidente, pois, a ausência de cientificidade na proposta parlamentar que visa à regulamentação do agir no âmbito informático, estando em total desintonia com o princípio constitucional implícito da proporcionalidade e da razoabilidade, este agora expressamente esculpido no artigo 5º da *norma normarum*, conforme se clarividencia no comando que subjaz de seu inciso LXXVII.

52 Idem.Ibidem.

53 Idem.Ibidem.

54 Idem.Ibidem.

A natureza subsidiária e fragmentária do Direito Penal de mínima intervenção está longe de ser alcançada no Projeto de Lei Substitutivo, sendo oportuna a lição de Claus Roxin⁵⁵, quando aduz, com grande proficiência, que: *onde bastarem os meios do direito civil ou do direito público, o direito penal deve retirar-se*.

5 Criminalidade contemporânea e a tutela penal subsidiária

Conforme referido em tópicos precedentes, é notório que a propalação crescente das facilidades trazidas pela internet e a inevitável sensação de impunidade dos atos criminosos de alguns usuários, que veem na rede um encorajador espaço para a prática de atividades ilegais até então impensáveis, traz como apanágio o aumento dos crimes cibernéticos, peculiar às reflexões atinentes à criminalidade contemporânea.

A presença do meio digital, permeando todas as atividades humanas, já havia sido motivo de preocupação da magistratura do Estado do Rio Grande do Sul, de forma pioneira, ainda no ano de 1983.

No início, a inserção da computação no meio jurídico e social no Brasil demandava uma discussão mais aprofundada sobre os efeitos da informática nas relações intersubjetivas, bem como o aperfeiçoamento dos novos conceitos que estavam sendo apresentados ao judiciário.

Na obra *Juscibernética*⁵⁶, publicada pelo Departamento de Estudos da Associação dos Juízes do Rio Grande do Sul, foram apresentadas as noções de cibernética e a sua relação com o computador. Juscibernética seria um termo convencional que indica as relações entre Direito e cibernética. O direito do qual se ocupa a informática jurídica é o direito positivo, isto é, o conjunto das normas da convivência social, providas de sanção.

Como advertiu Júlio César Werneck Martins⁵⁷, *ao operador do direito que tencione aventurar-se no mundo do “direito e internet”, não é permitido o “analfabetismo cibernético”*.

Tal advertência é uma realidade que não podemos ignorar, segundo dados publicados pelo Comitê Gestor da Internet no Brasil e outros⁵⁸:

55 ROXIN, Claus. Sentido e limites da pena estatal. In: *Problemas fundamentais de direito penal*. Lisboa: Veja, 1986. p. 29.

56 LOSANO, Mario G. Juscibernética. Edição da Diretoria da Revista de Jurisprudência e Outros Impressos do Tribunal de Justiça. *Ajuris*, [s.n.], 1983. p. 11.

57 MARTINS, Júlio César Werneck. O Hackerismo e a defesa da propriedade virtual: o patrimônio da informação. In: *Internet e Direito, Reflexões Doutrinárias*. Roberto Roland Rodrigues da Silva Junior (org.) et al. Rio de Janeiro: Lumen Juris, 2001. p. 173.

58 Fontes: Comitê Gestor da Internet no Brasil, Febraban, FBI, Consultoria em Segurança Iron Port. S.n. Golpe

1,5 bilhão é quanto os bancos gastam por ano no combate a fraudes eletrônicas; 300 milhões foi o prejuízo dos bancos com fraudes em 2005 (último dado informado) e 3 de cada 4 spams estão contaminados com códigos maliciosos e podem conter programas para roubar senha bancárias.

Estamos enfrentando o completo desvirtuamento do verdadeiro sentido do uso do computador e da internet. Diante disso, torna-se impreterível a implementação de estudos que objetivem a inibição dos efeitos danosos surgidos com o aprimoramento da tecnologia.

São positivas as perspectivas de uma gradativa adaptação dos conceitos e interpretação das normas criminais, de forma mais condizente com as práticas infracionais virtuais, todavia não parece razoável que se persista na elaboração sistemática de leis penais a cada adaptação do agir criminoso, em completo desprestígio aos demais mecanismos de controle existentes.

Talvez seja essa uma das razões que levou Pedro J. Montano Gómez⁵⁹ a tecer o seguinte posicionamento:

La consecuencia en la actualidad, es que apesar de existir esas leyes específicas e innovadoras, éstas han sido de escasa aplicación y también han presentado lagunas y dificultades de interpretación porque, al ingresar en la casuística descripción de nuevas situaciones, forzosamente ya han quedado obsoletas, a pesar del corto lapso transcurrido. Puede afirmarse que – a pesar de los esfuerzos – no han sido aun una verdadera solución al problema.

Apregoa o autor uruguaio, ainda, que o combate aos crimes perfectibilizados com o auxílio de recursos tecnológicos não seria uma novidade para a história do Direito Penal. Basta recordarmos, por exemplo, do surgimento da energia elétrica, quando delitos passaram a ser praticados por meio da utilização dessa tecnologia, sem que com isso fosse necessária a implementação de novos tipos penais.⁶⁰

Termina Pedro J. Montano Gómez⁶¹: *El automóvil se vio como un nuevo instrumento u objeto para cometer delitos clásicos, como las lesiones, el homicidio, el hurto o el daños.*

Eletrônico. Reportagem Especial. Jornal Zero Hora. Porto Alegre, 9 de setembro de 2008. p. 5.

59 GÓMEZ, Pedro J. Montano. Delitos Informáticos y los Tipos que Exigen la “Cosa Ajena Mueble”. Justiça Penal 7. In: *Críticas e Sugestões*. Justiça Criminal Moderna. São Paulo: Revista dos Tribunais, 2000. p. 337.

60 Idem. Ibidem, p. 337.

61 Idem Ibidem, p. 339.

Imperioso observar, as legislações que procuraram adaptar-se às ovas roupagens de apresentação dos delitos não resolveram de forma eficiente o que objetivavam, isto é: fornecer obstáculos às condutas desregradas. Com a possível aprovação da “Lei dos Crimes na Internet”, a tendência, pelo que se tem observado nos últimos anos, deverá ser o insucesso da tentativa do Estado de depositar novamente no Direito Penal uma responsabilidade que não lhe deveria caber.

É justamente nesse contexto que se insere a discussão acerca da necessidade da *intervenção do Direito Penal na seara do mais moderno, revolucionário e emblemático conhecimento humano*, aduz Rossini.⁶²

Em linha meridiana, indaga o autor:

Qual dos ramos do Direito, dentre todos, fornecerá a ferramenta para que se chegue o mais rapidamente à solução.⁶³ Ainda: Há a efetiva necessidade de se estabelecer um sistema composto por novos tipos penais que, juntamente com outros delitos já consagrados, constituiriam as “infrações penais telemáticas”?⁶⁴

A “Lei de Direitos Autorais” (n.º 9.610/98), de abrangência civil, que protege *os direitos de autor e os que lhes são conexos*, é o Diploma Legal apropriado para dispor acerca de direitos violados na seara virtual.

Havendo na legislação pátria dispositivo legal suficiente para coibir o agir cibernético ilegal, resta indagar se há real necessidade de tutelar, de forma mais rigorosa, as condutas comuns na seara virtual. Acresce-se a esse dilema, a circunstância de que se está tratando de direitos individuais consagrados na Lei Maior, e que devem ser considerados, em toda sua amplitude, quando da busca de um controle social por meio de legislação repressiva. Aí a relevância de se ponderar os princípios norteadores da razoabilidade e proporcionalidade, porquanto limitam os excessos punitivos.

Conforme apregoado por Carlos Bernal Pulido⁶⁵:

62 ROSSINI, Augusto Eduardo de Souza. *Informática, Telemática e Direito penal*.: São Paulo: Memória Jurídica, 2004. p. 127.

63 Idem. Ibidem, p. 127.

64 Idem. Ibidem, p. 126.

65 PULIDO, Carlos Bernal. *El Principio de proporcionalidad y los derechos fundamentales*. Madrid: CEPC, 2002. p. 805.

A proporcionalidade possui uma dupla face: de proteção positiva e de proteção de omissões estatais. Ou seja, a inconstitucionalidade pode ser decorrente de excesso do Estado, caso em que determinado ato é desarrazoado, resultando desproporcional o resultado do sopesamento (*Abwägung*) entre fins e meios; de outro, a inconstitucionalidade pode advir de proteção insuficiente de um direito fundamental.

Não destoa Ingo Sarlet⁶⁶ quando informa que o princípio da proporcionalidade deve servir tanto para controlar os excessos do Estado, em detrimento dos direitos fundamentais, quanto para cobrar uma efetiva prestação que não esteja sendo atendida e que venha, consequentemente, acarretar algum prejuízo a direito individual ou social. É o que se denominou de dupla face de proteção dos direitos fundamentais, uma positiva e outra negativa. Frente ao Estado e por meio do Estado.

Em defluência, reitera-se a desnecessidade de criação legislativa, de coloração repressivo-penal, porquanto representaria um efetivo rigorismo legal, excesso punitivo, em havendo regramento em vigor no país, de natureza civil, mais condizente para a obtenção do restabelecimento de bens e direitos de titularidade de usuários da *web*, eventualmente atingidos por práticas ilícitas. E o mais relevante, sem afrontar direitos individuais esculpidos categoricamente na Carta política de 1988.

6 Considerações finais

O desenvolvimento dos estudos iniciais e o efetivo surgimento da internet remontam a um período da história mundial em que a tecnologia avançava a passos largos. Fruto das inovações advindas com a nova realidade presenciada na época, o campo para a propagação de condutas desviadas por meio de computadores tornou-se extremamente fértil.

Diante desse panorama, incrementou-se o agir criminoso mediante um *modus operandi* que, sob certo aspecto, trouxe novos contornos às práticas delitivas tradicionais, tornado-as “requintadas” em razão da complexidade exigida para o manuseio técnico do computador – execução – e, consequentemente, consumação do desiderato criminoso arquitetado. Não poderiam, evidentemente, o Estado e suas instituições, bem como o Direito e os estudos criminológicos, negarem o enfrentamento dessas

66 SARLET, Ingo. Constituição e proporcionalidade: o direito penal e os direitos fundamentais entre proibição de excesso e de insuficiência. *Revista de Estudos Criminais*, Sapucaia do Sul, n. 12, ano 3, 2003. p. 87.

questões. Impulsionou-se, assim, uma construção dogmática no sentido de classificar e especificar, em tipos penais existentes no ordenamento jurídico pátrio, alguns dos delitos virtuais que vinham sendo perpetrados, bem assim definir qual seria o bem jurídico violado na prática do delito virtual puro.

O Projeto de Lei Substitutivo (ao PLS 76/2000, PLS 137/2000 e PLC 89/2003), aprovado pelo Plenário do Senado brasileiro, trouxe à tona a problemática da criminalização de fatos sociais como forma de coibir ações transgressoras decorrentes da inovação tecnológica. O Projeto de Lei prevê a tipificação de algumas condutas de usuários do ciberespaço, até então consideradas corriqueiras e inofensivas, rompendo com garantias constitucionais basilares do cidadão. Para a aprovação de qualquer documento regulamentador em nosso país, máxime o de natureza sancionatória, mister proposta parlamentar que contenha tecnicidade e cientificidade suficientes para que não se incorra em equívoco legislativo, comprometendo garantias individuais.

Destarte, desnecessária a elaboração de leis de coloração repressivo-penal na seara virtual, porquanto representaria um efetivo rigorismo legal, excesso punitivo, quando já há normatizações em vigor no país – tanto de repercussão civil (Lei n.º 9.610/98), que trata dos Direitos Autorais, quanto criminal (artigo 184 do Código Penal) – mais propícias à obtenção do restabelecimento de bens e direitos de titularidade de usuários do ciberespaço, eventualmente atingidos por práticas ilegais, sem qualquer afronta a direitos individuais de rubrica categórica na Lei Maior.

Referências

BRASIL, Angela Bittencourt. *Informática jurídica : O ciber direito*. Rio de Janeiro: [s.n.], 2000.

CARVALHO, Luiz Gustavo Grandinetti Castanho de. Direito de informação, liberdade de expressão e internet. In: *Internet e direito, reflexões doutrinárias*. Roberto Roland Rodrigues da Silva Junior (org.) et al. Rio de Janeiro: Lumen Juris, 2001.

CASTRO, Carla Rodrigues Araújo de. *Crimes de informática*. Rio de Janeiro: Lumen Juris, 2001.

CORRÊA, Gustavo Testa. *Aspectos jurídicos da internet*. São Paulo: Saraiva, 2000.

FERREIRA, Érica Lourenço de Lima. Jurisdição Metaterritorial para a Cibernética. *Lex*, São Paulo, [s.n], 2006. Disponível em: <<http://www.lex.com.br>>. Acesso em: 24 dez. 2008.

FILHO, Luna; PEREIRA, Eury. Internet no Brasil e o Direito no Ciberespaço. *Infojus*, Rio de Janeiro, [s.n], 1999. Disponível em: <<http://www.infojus.com.br>>. Acesso em: 03 dez. 2008.

GÓMEZ, Pedro J. Montano. Delitos informáticos y los tipos que exigen la “Cosa Ajena Mueble”. Justiça Penal 7. In: *Críticas e Sugestões*. Justiça Criminal Moderna. São Paulo: Revista dos Tribunais, 2000.

GUERRA. Sidney César S. O Direito à Privacidade e a Internet. In: *Internet e Direito, Reflexões Doutrinárias*. Roberto Roland Rodrigues da Silva Junior (org.) et al. Rio de Janeiro: Lumen Juris, 2001.

JÚNIOR, Délio Lins e Silva. Crimes informáticos: vitimização e a questão do tipo objetivo. In: *Direito Penal Secundário: Estudos sobre crimes econômicos, ambientais, informáticos e outras questões*. Fábio Roberto D’Avila; Paulo Vinícius Sporleder de Souza (org.). São Paulo: Revista dos Tribunais, 2006.

LÉVY, Pierre. A Revolução Contemporânea em Matéria de Comunicação. In: *Informática e Democracia*. Rio de Janeiro: UERJ, 2000.

LIMA, Maria de La Luz. Delitos Electrónicos. Criminalia. *Academia Mexicana de ciencias Penales*, México, Porrúa, Enero-Junio, n. 1-6, año L., 1984.

LOSANO, Mario G. Juscibernética. Edição da Diretoria da Revista de Jurisprudência e Outros Impressos do Tribunal de Justiça. *Ajuris*, [s.n], 1983.

MARTINS, Júlio César Werneck. O Hackerismo e a defesa da propriedade virtual: O patrimônio da informação. In: *Internet e Direito, Reflexões Doutrinárias*. Roberto Roland Rodrigues da Silva Junior (org.) et al. Rio de Janeiro: Lumen Juris, 2001.

OLIVEIRA, Felipe Cardoso Moreira de. *Criminalidade Informática*. Porto Alegre: Pontifícia Universidade Católica do Rio Grande do Sul/PUCRS. 2002. Dissertação de Mestrado, Faculdade de Direito/Ciências Criminais/Pontifícia Universidade Católica do Rio Grande do Sul, 2002.

PINHEIRO, Patrícia Peck. *Direito digital*. 2. ed. São Paulo: Saraiva, 2007.

PROTASIO, Arthur. Esclareça suas Dúvidas sobre os vários problemas do Projeto de Ciber Crimes aprovado pelo Senado. In: *A2kbrasil*. Rio de Janeiro: [s.n.], 2008. Disponível em :<http://www.a2kbrasil.org.br>>. Acesso em: 16 dez. 2008.

PULIDO, Carlos Bernal. *El Principio de proporcionalidad y los derechos fundamentales*. Madrid: CEPC, 2002.

ROSSINI, Augusto Eduardo de Souza. *Informática, telemática e Direito penal*. São Paulo: Memória Jurídica, 2004.

ROXIN, Claus. Sentido e limites da pena estatal. In: *Problemas fundamentais de direito penal*. Lisboa: Veja, 1986.

SARLET, Ingo. Constituição e proporcionalidade: o direito penal e os direitos fundamentais entre proibição de excesso e de insuficiência. In: *Revista de estudos Criminais*, Sapucaia do Sul, n. 12, ano 3, 2003.

S.n. Limitaciones constitucionales e inconstitucionales a da libertad de expresión. In: *Revista Española de Derecho Constitucional*, Centro de

Estudios Políticos y Constitucionales. Madri, n. 53, mayo/agosto , 1998.

S.n. *Levantamento mostra que já existem mais de 17 mil decisões judiciais envolvendo problemas na Internet*. Espaço Vital. Porto Alegre: 2008. Disponível em: <<http://www.espacovital.com.br>>. Acesso em: 08 dez. 2008.