Crimes da Informática no Código Penal Brasileiro

Ana C. A. P. Carvalho, Fernando B. Sousa, José F. Neto, Paulo H. C. Neves, Rafael Fragoso, Rodolfo P. Mazzonetto.

Resumo—**O avanço tecnológico trouxe grandes vantagens, mas também viabilizou a utilização do computador como ferramenta para a prática de atos ilícitos. O presente trabalho tem, como objetivo, o estudo das normas reguladoras da prevenção, repressão e punição dos crimes contra o uso, a segurança e a transmissão de informações em sistemas. Ante a inexistência de lei específica a regulamentar a matéria no Brasil e a diversidade de crimes previstos no Código Penal brasileiro, este artigo busca estudar os crimes da informática sob o enfoque da atual legislação em vigor e dos principais projetos de lei que tramitam no Congresso Nacional.**

Palavras-chave—**direito penal, crimes, informática, Internet**

I. Introdução

O advento da informática possibilitou à sociedade adquirir, armazenar e difundir uma vasta quantidade de informações, acompanhadas de muitos beneficios, como a diminuição de rotinas manuais, customização de processos, alto poder de integração entre pessoas, além de abrir novas fronteiras de relacionamentos e negócios. Mas, em contrapartida, vislumbramos graves problemas relacionados aos crimes realizados por meio de computadores, que representam informações mais vulneráveis à quebra de confidencialidade, perda de integridade e indisponibilidade, caso não estejam adequadamente protegidas.

Tal assunto apresenta-se como preocupação constante aos profissionais atuantes nas áreas de Tecnologia da Informação e do Direito, os quais precisam desenvolver técnicas e normas capazes de garantir a segurança das informações.

O Código Penal brasileiro não disciplina, de forma específica, os crimes da informática, cuja prática vem crescendo significativamente, por isso o Poder Legislativo desenvolveu projetos de lei cujo escopo é regulamentar essas infrações de forma a viabilizar a sua apuração e a conseqüente punição dos seus autores.

Os Crimes da Informática como fonte de pesquisa, apresentam-se como um desafio por envolver áreas de conhecimento distintas, envolvendo as ciências exatas, a máquina, a informática e, de outro lado, as ciências humanas, o homem (infrator) e o direito.

A busca do conhecimento sobre este assunto mostra-se bastante relevante, já que discorreremos acerca de um tema bastante atual e que faz parte das preocupações da sociedade de forma geral.

II. A Importância do Estudo dos Crimes Informáticos

O presente trabalho justifica-se por estar inserido em uma área multidisciplinar, preocupando não apenas a profissionais ligados às áreas de Tecnologia da Informação e do Direito, como também a sociedade de modo geral. O tema em comento requer o estudo e o desenvolvimento de alguns pontos indubitavelmente primordiais para a compreensão de que, com todo o aparato tecnológico ora existente, estamos vivendo em um mundo cujas fronteiras se tornam, cada dia, menos visíveis e sem uma legislação adequada, capaz de acompanhar a velocidade estonteante de difusão dos crimes cometidos por meio do computador.

A fragilidade dos sistemas de informática, a condição de legislação omissa por não reprimir ações desta natureza, a grande criatividade dos criminosos e a ausência de soluções técnicas para uma menor proliferação destes atos são fatores que ratificam a importância de discussão sobre este tema.

Simultaneamente, tais circunstâncias acarretam a necessidade de soluções e meios legais para um melhor entendimento acerca de problemas tão relevantes, os quais requerem o auxílio dos profissionais de Tecnologia da Informação e dos juristas, a fim de contribuir para a evolução e democratização do acesso seguro às tecnologias.

Manuscrito recebido em 13 de julho de 2008.

A. C. A. P. Carvalho é advogada, coordenadora da Especialização em Computação Forense e professora da Faculdade de Computação e Informática da Universidade Presbiteriana Mackenzie (e-mail: anacrisazevedo@mackenzie.br).

F. B. Sousa é bacharel em Sistemas de Informação e gestor de Projetos (e-mail: fernando_mack@yahoo.com.br).

J. F. Neto é graduando em Sistemas de Informação e Administrador de Redes (e-mail: neto@francci.net).

P. H. C. Neves é bacharel em Sistemas de Informação, pós-graduando em Computação Forense e gestor de projetos de TI (e-mail: paulo@castroneves.net).

R. Fragoso é bacharel em Sistemas de Informação e analista de controle de qualidade em software (e-mail: rafael.fragoso@linx.com.br).

R. P. Mazzonetto é bacharel em Sistemas de Informação e analista de sistemas mainframe (e-mail: rodolfo.mazzonetto@cpm.com.br).

III. OBJETIVOS DO TRABALHO

O objetivo do presente trabalho é identificar quais os crimes passíveis de serem cometidos por meios eletrônicos e analisar a legislação pertinente em vigor, inclusive em relação aos meios de prova, definindo os crimes informáticos, apresentando uma visão crítica sobre o uso das modernas tecnologias e o seu impacto na sociedade e apontando as soluções jurídicas existentes.

O tema em questão envolve o estudo do Código Penal Brasileiro, mas não apenas da Parte Geral, que disciplina os crimes e seus elementos, como também da Parte Especial, que traz os crimes em espécie.

A pesquisa enfoca também os Projetos de Lei sobre o assunto, os quais visam a uma regulamentação mais consistente para os crimes da informática.

IV. DEFINIÇÃO DE CRIMES DA INFORMÁTICA

Os crimes da Informática podem ser definidos como a gama de delitos que podem ser promovidos por meio de computador, apresentando-se de várias formas, entre elas o acesso indevido a sistemas, furto de informações, falsificação de documentos com o uso da tecnologia, danos ao computador e às informações, aquisição ilícita de segredos industriais ou comerciais, cópia indevida de softwares, violação do direito autoral, difusão de vírus eletrônico, além dos crimes comumente perpetrados pela Internet, como apologia de crimes, pornografia infantil, ofensas contra a honra e até crimes eleitorais.

V. DA NECESSIDADE DE REGULAMENTAÇÃO

A informática consolida-se como a maior revolução tecnológica já inventada, sendo, através da Internet, capaz de interligar milhares de pessoas, possibilitando a troca de informações e a transferência de diferentes tipos de dados. Entretanto, com o enorme crescimento das tecnologias, cresceram, na mesma proporção, as modalidades de crimes cometidos através da informática.

A razão do crescimento desordenado destes crimes se deve ao grande descompasso existente entre as profundas inovações tecnológicas e a aplicação das normas jurídicas, além da dificuldade de imputação da responsabilidade ao criminoso, já que a legislação brasileira ainda não garante total segurança e punição aos crimes desta modalidade.

Para reforçar a idéia do quanto é importante à regulamentação de uma legislação que puna os crimes informáticos, COSTA (1997) relata que o Direito Civil da Informática atuaria como o conjunto de normas que regulariam as relações privadas envolvendo a aplicação da informática, quais sejam: computadores, sistemas, programas, cursos, direitos autorias etc. Por outro lado, o Direito Penal da Informática seria atuante como o conjunto de normas destinadas a regular a prevenção, a repressão e a punição relativamente aos fatos atentem contra o uso, exploração, segurança, transmissão e sigilo de dados armazenados e de sistemas manipulados por estes equipamentos, os computadores.

Do ponto de vista de soluções técnicas, a arma mais eficiente contra tais crimes seria a própria informação. O conhecimento de como agem estes criminosos, de quais as condutas mais perigosas e vulneráveis a estes crimes e dos cuidados a serem tomados são, portanto, essenciais para a proteção contra qualquer conduta criminosa que atinja o usuário.

Diante dos principais aspectos apresentados, verifica-se que cresce, de forma quase incontida, a corrida ao domínio da informática, devendo, por isso, ser otimizados os procedimentos de pesquisa, intercâmbio e aquisição de tecnologia, bem como ser incentivada a aplicação efetiva do direito da informática.

VI. CONCEITOS ESSENCIAIS DO CÓDIGO PENAL

A vida em sociedade exige um complexo de normas disciplinadoras, denominado direito positivo, que deve ser obedecido e cumprido por todos os integrantes do grupo social, prevendo as conseqüências e sanções aos que violarem seus preceitos. Também designa o sistema de interpretação da legislação penal, ou seja, a Ciência do Direito Penal, visando à sua aplicação aos casos concretos, segundo critérios rigorosos de justiça.

As denominações tradicionais para a matéria referente ao crime e às suas conseqüências são Direito Penal e Direito Criminal, sendo que a primeira é largamente utilizada nos países ocidentais, como Alemanha, Itália, Espanha etc. Entre nós, a denominação passou a ser utilizada no Código Penal da República (1830), ao qual se sucederam a Consolidação das Leis Penais (1936) e o Código Penal vigente (1940), que a consagrou como direito pátrio. Já o Direito Criminal está relacionado com o fato principal do fenômeno jurídico (crime), alongando-se a seus efeitos jurídicos. Subsistem, porém, resquícios da denominação antiga, que ainda é utilizada nas leis da organização judiciária, com a utilização da denominação Varas Criminais.

O fato que contraria a norma de Direito, ofendendo ou pondo em perigo um bem alheio ou a própria existência da sociedade, é um ilícito jurídico, que pode ter conseqüências meramente civis ou possibilitar a aplicação de sanções penais.

Muitas vezes, essas sanções civis se mostram insuficientes para coibir a prática de ilícitos jurídicos graves, que atingem não apenas interesses individuais, mas também bens jurídicos relevantes, em condutas profundamente lesivas à vida social. Arma-se o Estado contra os respectivos autores desses fatos, cominando e aplicando sanções severas por meio de um conjunto de normas jurídicas que constituem o Direito Penal.

Na legislação penal, são definidos esses fatos graves, que passam a ser ilícitos penais, estabelecendo-se as penas e as medidas de segurança aplicáveis aos infratores dessas normas.

Uma característica essencial do Estado liberal do Direito é a busca da redução da criminalização pela prática de ações que, por sua periculosidade e reprovabilidade, exigem e merecem, no interesse da proteção social, inequivocadamente, a sanção penal.

Pode-se dizer, assim, que a finalidade do Direito Penal é a proteção da sociedade e, mais precisamente, a defesa dos bens jurídicos fundamentais (vida, integridade física e mental, honra, liberdade, patrimônio, costumes, paz pública etc).

Discute-se se o Direito Penal é constitutivo, primário e autônomo ou se tem caráter sancionador, secundário e acessório. Afirma-se que se trata de um direito constitutivo porque possui um ilícito próprio, oriundo da tipicidade, uma sanção peculiar (pena) e instrutivos exclusivos, como o sursis.

Revela-se, assim, que a norma penal é sancionadora, reforçando a tutela jurídica dos bens regidos pela legislação extrapenal. O mais correto, como afirma Zaffaroni, seria afirmar que o Direito Penal é predominantemente sancionador e excepcionalmente constitutivo.

Denomina-se o Direito Penal objetivo o conjunto de normas que regulam a ação estatal, definindo os crimes e cominando as respectivas sanções. Sendo, o Estado, o único e exclusivo titular do direito de punir, constitui-se o denominado Direito Penal subjetivo.

O Direito Penal comum se aplica a todas as pessoas e aos atos delitivos, enquanto o Direito Penal especial é dirigido a uma classe de indivíduos de acordo com sua qualidade especial, e a certos atos ilícitos particularizados.

O Direito Penal substantivo é representado pelas normas que definem as figuras penais, estabelecendo as sanções respectivas, bem como os princípios gerais e elas relativos (Código Penal, Lei das Contravenções Penais etc.). O Direito Penal adjetivo constitui-se de preceitos de aplicação do direito substantivo e de organização judiciária.

VII. CRIMES DA INFORMÁTICA

A. Classificação

Quanto ao meio em que são praticados, os crimes da informática podem ser classificados em:

1. Crimes de informática mediatos ou indiretos: ocorrem quando o delito-meio informático é usado para sua consumação. Ex.: acesso não autorizado a sistema bancário (inviolabilidade de dados) e a conseqüente transferência de dinheiro para sua conta (furto). Esta categoria difere dos delitos impróprios, pois aqui há um delito-meio, e não somente a informática como meio, o que aconteceria no caso da difamação, por exemplo.

2. Crimes de informática próprios ou puros: só podem ser praticados através da informática, sem a qual a execução e consumação da infração não poderiam ocorrer. Ex.: violação de e-mail, vandalismo na web, difusão de vírus etc.

3. Crimes de informática impróprios ou comuns: podem ser praticados de qualquer forma, inclusive através da informática (como meio). Ex.: estelionato, calúnia, pedofilia etc.

4. Crimes de informática mistos: abrangem o bem juridicamente protegido, mas sua prática só é possível com a informática. Ex.: obter acesso a sistema de tratamento automático de dados usado pelo serviço eleitoral, para tentar alterar a contagem dos votos.

B. Espécies

1. Crimes contra a honra: calúnia, difamação e injúria.

Caluniar alguém é afirmar que uma pessoa cometeu um crime que ela não cometeu.

Já difamar alguém é espalhar fatos ofensivos à reputação de outra pessoa.

A injúria acontece quando o agente imputa à vitima, não necessariamente em público, alguma ofensa, qualidade ou característica pejorativa.

Através da informática, esses crimes podem ser cometidos utilizando-se uma página criada na Internet, a qual pode ser visitada por qualquer pessoa, ou até mesmo com o uso de salas de bate-papo, em conversas simultâneas de um grupo, ou ainda com o envio de um e-mail para um grupo de pessoas.

2. Ameaça: ameaçar alguém significa causar-lhe mal injusto e grave, por palavra, escrito, gesto ou qualquer outro meio simbólico.

Como a lei não elenca uma forma específica para sua prática, também se torna possível cometê-lo através do computador, utilizando-se, por exemplo, um website e nele inserindo qualquer texto ameaçador, através de conversas on-line ou através de e-mail.

3. Interceptação de Correio Eletrônico: o sigilo das correspondências é garantido pela Constituição Federal e tipificado no artigo 40 do Código Penal.

Correspondência é uma troca de informações entre pessoas ausentes, que pode ser feita também por computador.

Um bom exemplo da prática desse crime poderia ser a conduta praticada pelos administradores de redes empresariais, os quais podem acessar as contas de e-mail de todos os funcionários e, sem a sua autorização, ler os e-mails trocados.

Nesse sentido, é importante lembrar que recentes decisões proferidas pela Justiça do Trabalho brasileira têm reconhecido o direito que as empresas têm de monitorar os e-mails trocados pelos seus empregados através da conta da empresa.

Porém, ainda no que concerne à violação de e-mail, se o computador for apreendido em um procedimento de busca e apreensão, determinado pela autoridade competente, seus programas, arquivos e inclusive os e-mails nele contidos poderão, indubitavelmente, ser lidos durante a análise pericial.

4. Furto: consiste em subtrair, para si ou para outrem, coisa

alheia móvel.

É um crime que pode ser cometido através de violação de um sistema bancário visando à transferência de valores para a conta, ou ainda subtração de números de cartões de crédito em sites de comércio eletrônico, para futura tentativa de fraude. Estes são dois dos crimes mais praticados eletronicamente, porém pouco divulgados, pois as instituições preferem arcar com o prejuízo a tornar pública sua vulnerabilidade.

Há também os casos em que computadores são invadidos pelo criminoso, para subtração de documentos ou arquivos diversos, porém, para que se configure o delito, é necessário que o objeto subtraído possua valor econômico.

5. Envio de programas maliciosos: na ausência de legislação específica, é aplicável o tipo penal do dano, que é destruir, inutilizar ou deteriorizar coisa alheia.

É necessário que haja prejuízo econômico, portanto, se o agente criminoso envia um vírus, no entanto, o destinatário não chega a executar os vírus por saber do que se tratava, é certo que nenhum prejuízo econômico terá sofrido, logo, tratar-se-ia de conduta atípica.

Existem várias espécies de programas maliciosos, os quais têm, como finalidade, executar tarefas inesperadas e não solicitadas, ao sistema do computador. Entre os mais comuns estão os vírus, os vermes e os cavalos de tróia.

Vírus é um programa criado com a finalidade de destruir arquivos ou alterar seus dados e programas, porém, exige que haja intervenção direta do usuário para que ele se manifeste, ou seja, seria preciso executá-lo.

Os vermes, por sua vez, são capazes de se propagarem de um sistema para outro sem a intervenção humana e destruir dados e arquivos.

Já os cavalos de tróia são especializados em subtrair informações pessoais do usuário, como senhas de acesso a serviços de Internet Banking e afins. Normalmente, chegam sob a forma de um inofensivo programa, vídeo ou foto que vem anexado em um falso e-mail orientando a vítima a executar o arquivo. No final, o que ocorre é a instalação de um vírus programado para registrar as informações da vítima e depois enviá-las ao seu criador.

Infelizmente, esses programas são cada vez mais comuns na Internet.

6. Estelionato: é um crime que pressupõe dois resultados, senão, vantagem ilícita e prejuízo alheio, os quais devem ser obtidos mediante artifício, ardil ou qualquer outro meio fraudulento.

É nesse ponto que entra a informática, uma vez que o agente pode utilizar páginas na Internet, salas de bate-papo ou e-mails para induzir alguém a erro, seja mediante ardil, artifício ou qualquer outro meio.

A fraude pode ocorrer quando alguém compra, vende ou investe via Internet, e é enganado de alguma forma.

Uma situação muito comum é o vendedor disponibilizar um produto na Internet, receber o dinheiro do pedido, mas não entregar o produto.

7. Ato Obsceno: é tudo aquilo que ofende o pudor público, podendo ser real ou simulado, porém, deve ter conotação sexual.

É muito comum, na Internet, encontrarem-se páginas com conteúdo de cenas de sexo explícito, as quais podem ser acessadas por qualquer pessoa, às vezes por um ato involuntário.

Alguns casais chegam a instalar câmeras dentro de suas casas, para gravar suas relações sexuais e, em seguida, disponibilizá-las na Internet, o que pode ser caracterizado como ato obsceno, caso se considere que a Internet é um lugar aberto ao público.

8. Incitação ao crime: corresponde à conduta de publicar algo que estimule alguém à prática de crime.

A lei exige que a conduta seja praticada publicamente para haver o crime, o que possibilita o uso da Internet para cometê-lo. O agente pode colocar anúncios em uma página na Internet, estimulando a prática de algum crime, como, por exemplo, a utilização de entorpecentes. Como as páginas podem ser acessadas por qualquer pessoa que tenha acesso à rede, a incitação se torna pública.

Além de páginas na Internet, o agente pode utilizar salas de bate-papo, com várias pessoas conversando ao mesmo tempo, para praticar esse crime.

9. Apologia ao crime ou criminoso: significa enaltecer ou elogiar o crime. É necessário que seja pública a prática dessa conduta.

É muito comum a prática desse crime em páginas da Internet ou salas de bate-papo, através das quais as pessoas incitam a prática de crimes, sem se preocuparem com suas conseqüências para elas mesmas ou para terceiros.

Igualmente, no Orkut, esse crime é freqüentemente praticado, cujos detalhes serão posteriormente discutidos.

10. Inserção de dados falsos em sistemas de informação: o crime de inserir ou facilitar a inserção de dados falsos, alterar ou excluir indevidamente dados corretos em sistemas informatizados, aplica-se apenas à Administração Pública.

Somente o funcionário público pode ser o sujeito ativo, enquanto apenas a Administração Pública pode ser sujeito passivo.

C. Legislação Extravagante

Existem alguns crimes que não são tipificados pelo Código Penal, porém têm leis específicas que os disciplinam. Vale a pena citá-los, pois, além de serem cometidos através da informática, são crimes comuns nessa área, e suas práticas são abordadas de forma freqüente.

1. Crimes de Preconceito e Discriminação. Preconceito é

uma opinião formada sem reflexão, um conceito antecipado sobre pessoas ou lugares, seja por raça, cor, etnia ou religião. Já a discriminação é o ato de tratar uma ou mais pessoas com restrição e diferenças, em razão do preconceito.

A prática desses crimes é muito comum em salas de bate-papo e páginas de Internet, onde pessoas criam sites e fóruns de discussão sobre determinados assuntos que caracterizam esses crimes. Houve polêmica na página de relacionamento Orkut na Internet, pois algumas comunidades criadas acabavam por incentivar o preconceito e a discriminação.

Saliente-se que a lei combate quaisquer formas de preconceito e discriminação, como ocorre nos atos praticados contra a mulher, contra o deficiente físico ou mental e contra o pobre.

2. Interceptação de Comunicações. Interceptar é o ato de captar o conteúdo de comunicação telefônica ou telemática.

É necessário o dolo do agente para que se configure o crime, portanto, no exemplo de linhas cruzadas, não haverá crime.

Por outro lado, ocorreria o crime em uma conversa de bate-papo on-line, se alguém a interceptasse para dela tomar conhecimento, ou ainda um arquivo interceptado e capturado no momento de sua transferência.

3. Pedofilia. Trata-se de um crime que merece atenção especial, pois se tornou absurdamente praticado através da Internet.

A lei diz que nenhuma criança ou adolescente será objeto de qualquer forma de negligência, discriminação, exploração, violência, crueldade e opressão, punindo qualquer atentado, por ação ou omissão, aos seus direitos fundamentais.

O Estatuto da Criança e do Adolescente cuida dos direitos das crianças e adolescentes e dispõe que, até os doze anos incompletos, a pessoa é considerada criança, enquanto adolescente é aquela entre doze e dezoito anos.

Algumas pessoas utilizam-se da Internet para divulgar materiais obscenos relativos à pedofilia, ou até mesmo vendê-los anonimamente, sendo um crime que causa revolta e repúdio na sociedade, pois é incalculável o constrangimento a que crianças e adolescentes são submetidos para saciar o prazer e o desejo de pessoas imorais.

Esse crime merece punição severa, seja pela sociedade, denunciando os criminosos e páginas na Internet que armazenam conteúdos desse tipo ou que incentivam essa prática, seja pelo Poder Público, que deve punir as pessoas que praticam esse crime.

É importante mencionar que o simples ato de disponibilizar, por qualquer meio, inclusive e-mail ou site, fotos ou cenas de sexo explícito envolvendo crianças e adolescentes, é suficiente para configurar a conduta criminosa.

D. O Caso do Orkut

O caso do Orkut repercutiu muito e gerou polêmica em nossa sociedade, motivo pelo qual merece ser discutido.

O Orkut é uma página da Internet, no qual as pessoas podem criar comunidades e convidar amigos para participarem delas, sendo também interessante por permitir que as pessoas deixem recados, disponibilizem fotos, descrevam seus perfis pessoais, entre outras funcionalidades.

O serviço em questão foi lançado em 2004 pelo grupo Google, e fez tanto sucesso entre os brasileiros, que o Brasil passou a ser o país com maior número de usuários do Orkut no mundo, conseqüentemente o Orkut ganhou uma versão em língua portuguesa para atender ao público brasileiro, que, em 2006, já ultrapassara 17 milhões de usuários cadastrados.

Por se tratar de um site na Internet, o Orkut é livre, e qualquer pessoa cadastrada pode acessar e visitar o perfil de outro usuário, escrever mensagens e investigar a vida das pessoas, caso estas tenham preenchido seu perfil e deixem que ele fique visível para qualquer usuário, e não apenas para pessoas que estejam ligadas a sua rede de amigos.

A liberdade que a Internet oferece facilita as ações criminosas, o que demanda o cuidado das prestadoras de serviços relativos à Internet, sejam elas provedores de acesso, fóruns ou salas de bate-papo. Essas empresas devem evitar que ocorram violações à lei ou, uma vez ocorridas, colaborar na sua apuração, o que não constitui tarefa fácil, à medida em que requer um rastreamento dos atos praticados por seus clientes e ainda a disponibilização dos seus bancos de dados ao Ministério Público em caso de investigação.

Sob essa ótica, o Orkut é um website mundial, acessado e utilizado em diversas jurisdições, com milhões de acessos diários, e está sujeito a situações diversas, que podem incluir a prática de crimes contra honra, contra o patrimônio, pedofilia, racismo e muitos outros, dentro das comunidades ou através dos recados trocados entre os usuários, principalmente no que diz respeito à pedofilia.

É certo que os crimes não acontecem apenas no Orkut, pois já foram relatados diversos outros casos, como crianças participando de diálogos com conteúdo obsceno em salas de bate-papo disponibilizadas por provedores nacionais. Além da pedofilia, grupos neonazistas brasileiros pregaram mensagens de ódio, tendo sido registrada uma imagem contendo a seguinte mensagem em um site da Internet: “Vamos encarar um mundo sem judeus e negros, seria como um mundo sem ratos e baratas”.

No final de 2004, a Procuradoria da República em São Paulo começou a receber numerosas *notitiae criminis* relacionadas à prática de delitos envolvendo ódio e pornografia infantil no Orkut.

A Google, como detentora do Orkut, porém, esclareceu que não fazia nenhum tipo de verificação ou validação dos dados informados pelos usuários, possibilitando a criação de perfis falsos e comunidades criminosas de todo tipo, tais como: terrorismo, racismo, instigação e auxílio ao suicídio, pornografia infantil, tráfico ilícito de entorpecentes, comercialização de medicamentos de uso restrito, apologia e incitação ao crime, exercício arbitrário das próprias razões,

formação de quadrilha, estelionato, além de penosos casos de ofensas à honra de celebridades e pessoas comuns (criação de perfis falsos contendo injúrias, calúnias e difamações de todas as espécies).

Por tais motivos, o Ministério Público Federal, através da Procuradoria da República, entrou com uma ação civil pública com pedido de antecipação de tutela, descrevendo a realidade brasileira em hospedagem de sites contendo pornografia infantil: em 2003, o Brasil estava em quarto lugar no ranking mundial dos países com esse tipo de conteúdo.

Em 2005, o grupo Google comprou a empresa brasileira Akwan Information Technologies e passou a operar diretamente no Brasil, que se tornou o primeiro país na America Latina a possuir uma subsidiária da companhia, cujo objetivo declarado era o lucro fácil, através da venda de espaços comerciais nas suas páginas Google.

A princípio, parece não haver problema algum no fato de instalar-se, no país, uma companhia transnacional buscando o lucro, pois a Constituição brasileira assegura a todos o livre exercício do trabalho, contanto que respeitem a soberania nacional.

No entanto, mesmo diante de um número superior a 34 mil denúncias anônimas, envolvendo casos de crianças mostradas seminuas ou nuas, com práticas sexuais com adultos, com outras crianças e adolescentes e até mesmo com animais, a Google não auxiliava as investigações do Ministério Público, criando obstáculos à medida em que retardava a extinção das comunidades ou não respondia às suas solicitações.

As primeiras ações do Ministério Público requerendo a quebra de sigilos de dados das comunidades do Orkut foram encaminhadas em 2005.

Após ser intimada, a Google informou que forneceria as informações de usuários e endereços IP, mas ainda assim houve desobediência e informações insuficientes.

Devido aos descumprimentos da Google, foi solicitado à Justiça, pelo Ministério Público, que impusesse a aplicação de multas, com valor não inferior a R$ 200.000,00 (duzentos mil reais), para cada decisão judicial não atendida, e valor não inferior a R$ 130.000.000,00 (cento e trinta milhões de reias) de indenização por danos morais coletivos, o qual seria revertido ao Fundo Nacional para a Criança e o Adolescente. Na eventualidade de persistir no descumprimento às ordens da Justiça Federal, requereu o Ministério Público o encerramento das atividades da Google.

Em 2 de julho de 2008, o Ministério Público Federal em São Paulo e a Google Brasil assinaram o TAC (Termo de Ajustamento de Conduta), visando ao combate da pedofilia na Internet. O acordo foi firmado durante a sessão da CPI da Pedofilia no Senado.

Após a assinatura do acordo, o Ministério Público se comprometeu a suspender as ações em curso contra a Google Brasil.

Pelo termo, o Google Brasil se compromete a filtrar suspeitos de pedofilia e pôr em prática uma série de medidas de controle no sistema. Se a empresa descumprir qualquer cláusula do acordo, poderá ser punida com o pagamento de multa no valor de R$ 25.000,00 (vinte e cinco mil reais) por dia de descumprimento.

Segundo o termo, as medidas devem ser implementadas imediatamente e relacionam 13 cláusulas. O principal ponto do acordo é que a Google se compromete a cumprir de forma "integral a legislação brasileira" no que se refere a crimes cibernéticos praticados por brasileiros ou por meio de conexões de Internet efetuadas no Brasil.

Na lista com as cláusulas, a Google também assume responsabilidade de responder em, no máximo, 15 dias as reclamações que receber. Pelo acordo, a empresa se compromete ainda a desenvolver tecnologia eficiente para filtrar e impedir a publicação de imagens de pornografia infantil no Orkut.

O termo define também a notificação automática de todas as ocorrências de pornografia infantil detectadas em perfis e comunidades do Orkut e a retirada de conteúdos ilícitos, mediante ordem judicial, requerimento de autoridade policial ou do Ministério Público, e preservação dos dados necessários à identificação dos autores e conteúdos.

Segundo o acordo, a empresa terá ainda que desenvolver campanhas de educação para o uso seguro e não criminoso da Internet, além de financiar a confecção de 100.000 cartilhas que serão distribuídas a crianças e adolescentes de escolas públicas (sobre o uso seguro da Internet).

VIII. PROJETOS DE LEI SOBRE CRIMES DA INFORMÁTICA

No Brasil, ainda não existe legislação em vigor que verse especificamente sobre os crimes da informática, seja ela penal ou processual penal, mas apenas propostas para tal regulamentação.

Tem-se, primeiramente, o Projeto de Lei n.º 1.713, do então Deputado Cássio Cunha Lima, apresentado em 27 de março de 1996, dispondo sobre o acesso, a responsabilidade e os crimes cometidos nas redes integradas de computadores. Este projeto não foi devidamente apreciado devido ao término da legislatura e acabou sendo arquivado.

Em 24 de fevereiro de 1999, o Deputado Luiz Piauhylino apresentou, na Câmara dos Deputados, o Projeto de Lei n.º 84/99, caracterizando como crime informático ou virtual os ataques praticados por *hackers* e *crackers*, em especial as alterações em *home pages* e a utilização indevida de senhas.

Em seguida, o Projeto de Lei da Câmara n.º 89/2003, também de autoria do Deputado Luiz Piauhylino, representou um aperfeiçoamento do PL n.º 1.713/96 e, mais uma vez, propôs a disciplina dos crimes cometidos contra sistema de computador ou por meio de computador.

Por outro lado, o Senado criara, em 2000, dois projetos de lei que passaram a tramitar em conjunto: o PL n.º 76/2000, do Senador Renan Calheiros, definindo e tipificando os delitos informáticos, e o PL n.º 137/2000, do Senador Leomar Quintanilha, o qual estabelece nova pena aos crimes cometidos

com a utilização dos meios de tecnologia de informação e telecomunicação.

Em 2005, os Projetos de Lei do Senado n.º 76/2000 e 137/2000 passaram a tramitar em conjunto com o Projeto de Lei da Câmara n.º 89/2003.

Em 09 de julho de 2008, o Projeto de Lei da Câmara n.º 89/2003 foi aprovado pelo Senado com emendas, de forma que um Substitutivo foi enviado para votação na Câmara dos Deputados.

IX. Conclusão

Observando a grande importância do tema, concluímos que a disciplina dos crimes da informática depende da análise de peculiaridades relativas a duas áreas do conhecimento bem distintas, senão, Direito e Tecnologia da Informação, ou, como alguns já denominam, o Direito da Informática.

Uma das constatações deste trabalho é a indubitável necessidade de um controle, por parte da sociedade, dos atos praticados através da informática.

Não se pode negar que, no Brasil, há legislação em vigor disciplinando a prática dos atos através da informática, mas essas leis não se mostram suficientemente eficazes para investigar e punir os infratores, por serem normas gerais, aplicáveis a uma grande diversidade de situações.

Alterações na legislação, inserindo dispositivos técnicos especificamente aplicáveis aos atos praticados com a utilização da informática, poderiam aumentar a eficácia das leis existentes hoje no Brasil.

Portanto, a conclusão a que se chega é no sentido de que há grandes possibilidades de redução na prática dos crimes informáticos se houver dispositivos legais contendo uma especificação técnica maior, tanto acerca da forma como são praticados, quanto no tocante à sua investigação.

No entanto, enquanto a legislação permanece como está, dificultando a repressão a essa modalidade de crimes, resta à sociedade enfatizar as ações preventivas, como divulgar as sanções aplicáveis aos infratores, na tentativa de que não pratiquem as condutas, e, ao mesmo tempo, buscar a segurança da informação através das ferramentas cabíveis.

Por outro lado, uma vez aperfeiçoada a legislação sobre os crimes da informática, com a devida eficácia de suas leis, o Brasil poderá iniciar uma preocupação mais direcionada à cooperação internacional, dispondo de fundamentos para colaborar com os outros países no combate ao crime e exigir que estes façam o mesmo.

Referências

[1] ARAÚJO JÚNIOR, João Marcelo de. *Computer Crime*: Conferência Internacional de Direito Penal. Rio de Janeiro: Procuradoria Geral da Defensoria Pública, 1998.

[2] AZEREDO, Eduardo, O Brasil contra o cibercrime. Disponível em http://www.valoronline.com.br/seminarios/crimes_digitais/Senador%20Eduardo%20Azeredo.ppt, acessado em: 23/04/2007.

[3] CASTRO, Carla Rodrigues Araújo de. Crimes de Informática e seus aspectos processuais, Rio de Janeiro: Lumen Juris, 2003.

[4] CORRÊA, Gustavo Testa. Aspectos jurídicos da Internet. 1ª edição. São Paulo: Saraiva, 2000.

[5] COSTA, Marco Aurélio Rodrigues da. Crimes de Informática. Disponível em http://jus2.uol.com.br/doutrina/texto.asp?id=1826, acessado em 13/07/08.

[6] DELMANTO, Celso. Código Penal Comentado. 3ed. Rio de Janeiro: Renovar, 1991.

[7] FRAGOSO, Heleno Cláudio. Observações sobre o princípio da reserva legal. Disponível em http://www.fragoso.com.br/cgi-bin/heleno_artigos/arquivo11.pdf , acessado em 13/07/08.

[8] FRANCO, Alberto Silva. As margens penais e a pena relativamente indeterminada. Julgados do Tribunal de Alçada Criminal de São Paulo. São Paulo, v. 45, p.29-36, set./out., 1976.

[9] GIRALDI, Renata. Google e Ministério Público assinam acordo para combater pedofilia no Orkut. Disponível em: http://www1.folha.uol.com.br/folha/informatica/ult124u418420.shtml, acessado em: 10/07/2008.

[10] GOUVÊA, Sandra. O Direito na era digital. 1ª edição. Rio de Janeiro: Mauad, 1997.

[11] GOUVEIA, Flávia. Tecnologia a serviço do crime. Cienc. Cult., vol.59, n.º 1, p.6-7, jan./mar. 2007.

[12] GUIMARÃES COLARES, Rodrigo. Cybercrimes: os crimes na era da informática. Disponível em http://jus2.uol.com.br/doutrina/texto.asp?id=3271, acessado em 28/04/2007.

[13] JESUS, Damásio E. de. Direito Penal. V.1. Parte Geral. 20ed. rev. e atual. – São Paulo: Saraiva, 1997.

[14] LANGE, Denise Fabiana. O impacto da tecnologia digital sobre o direito de autor e conexos. 1ª edição. São Leopoldo: Unisinos, 1996.

[15] LICKS, Otto Banho e JUNIOR, João Marcelo de Araújo. Aspectos penais dos crimes de informática no Brasil. 1ª edição. Rio Grande do Sul: Revista dos Tribunais, 1994.

[16] LUCCA, Newton de, FILHO, Adalberto Simão. Direito e Internet – Aspectos jurídicos relevantes. 1ª edição. São Paulo: Edipro, 2000.

[17] MIRABETE, Julio Fabbrini. Código de processo penal interpretado: referências doutrinárias, indicações legais, resenha jurisprudencial. 6ed. São Paulo: Atlas, 1999.

[18] _____. Manual do Direito Penal. 20ed. São Paulo: Atlas, 2003.

[19] PIMENTEL, Alexandre Freire. O Direito Cibernético em enfoque teórico e lógicoaplicativo, 1ª ed. Rio de Janeiro: Renovar, 2000.

[20] REINALDO FILHO, Demócrito, O projeto de Lei sobre crimes tecnológicos. Disponível em http://jus2.uol.com.br/doutrina/texto.asp?id=5447, acessado em: 28/04/2007.

[21] SENADO FEDERAL. Disponível em: http://www.senado.gov.br/sf/atividade/Materia/detalhe.asp?p_cod_mate=43555, acessado em: 21/04/2007.

[22] VIANNA, Túlio L. Dos crimes por computador. Disponível em http://www.cbeji.com.br/artigos/DosCrimesporComputador.PDF, acessado em: 28/04/2007.

[23] _____. Fundamentos de Direito Penal Informático, São Paulo: Forense, 2002.

[24] ZAFFARONI, Eugenio Raul e PIERANGELI, José Henrique. Manual de direito penal brasileiro. São Paulo: RT, 2004.