

RESPONSABILIDADE DOS ESTABELECIMENTOS QUE DISPONIBILIZAM LOCAÇÃO DE COMPUTADORES COM ACESSO À INTERNET, NO QUE TANGE AOS CYBERCRIMES

Cibelle Priscila Pinheiro Trindade¹
Sandresson de Menezes Lopes²

RESUMO

Diante da evolução da sociedade e da globalização, os estabelecimentos comerciais que dispõem de computadores para locação à acesso à internet se tornaram palco de crimes cometidos no mundo virtual. Diante da lacuna legislativa, o que causa uma insegurança jurídica, utiliza-se analogicamente o Código Civil de 2002 em seus artigos 186 e 927 e o Código de Defesa do Consumidor. O presente estudo tem por objetivo conceituar os cybercrimes; o instituto da responsabilidade civil, em sua modalidade objetiva e subjetiva; a aplicação do CDC quando os usuários dos estabelecimentos são equiparados a consumidores, a jurisprudência atual e os avanços legislativos, de forma a regulamentar a situação dos cadastros de usuários desses estabelecimentos. A elaboração desse artigo foi desenvolvida através do método dialógico, de acordo com o contexto brasileiro atual, e a pesquisa utilizada foi do tipo bibliográfica. Pela análise desenvolvida verificou-se que o grande causador da insegurança jurídica no campo da internet se deve a ausência de lei específica que regulamenta o tema. Através da pesquisa realizada, conclui-se que é imprescindível a necessidade de lei de âmbito federal que torne obrigatório o cadastro dos usuários para a identificação daqueles que atingem e ferem direitos de terceiros com atos ilícitos, e a devida responsabilização, tanto dos estabelecimentos quanto dos agentes criminosos.

Palavras-chaves: Cybercrimes. Responsabilidade dos Estabelecimentos. Ausência legislativa. Insegurança jurídica.

¹ Discente do curso de Direito da Faculdade Natalense para o Desenvolvimento do Rio Grande do Norte – FARN
E-mail: cibellept@yahoo.com.br

² Orientador, Docente do curso de Direito da Faculdade Natalense para o Desenvolvimento do Rio Grande do Norte – FARN
E-mail: sandresson1@hotmail.com

RESPONSIBILITY OF ESTABLISHMENTS TO PROVIDE RENTAL OF COMPUTERS WITH INTERNET ACCESS, WITH RESPECT TO THE CYBERCRIME

ABSTRACT

The evolution of society and globalization, businesses that have computers to rent the internet access became the scene of crimes committed in the virtual world. Given the legislative gap, which causes legal uncertainty, is used analogously the Civil Code of 2002 in its articles 186 and 927 and the Code of Consumer Protection. This study aims to conceptualize cybercrime, the institution of civil responsibility in its objective and subjective mode, the application of the CDC when users of the establishments are treated as consumers, the current jurisprudence and legislative developments in order to regulate the situation of the records of users of these establishments. The article was developed from elaboration through dialogic method, according to the current Brazilian context and the research used was bibliographic. For the analysis developed it was found that the main cause of legal uncertainty in the field of Internet is due to the absence of specific law regulating the subject. Through research, concludes that it is a compelling need for the federal law to mandate the registration of users to identify those that affect and hurt the rights of others with illegal acts, and proper responsibility, of both criminal agents and establishments.

Keywords: **Keywords:** Cybercrime. Responsibility of the establishments. Absence of legislation. Legal uncertainty.

INTRODUÇÃO

Com o surgimento da internet, muitas oportunidades passaram a ser visualizadas, principalmente como uma forma de diminuir as distâncias entre as pessoas, desenvolvendo novos tipos de relações sociais e a grande troca e armazenamento de informações.

Com a popularização dessa nova forma de comunicação digital, ocorrida ao final da década de 1990, surgiu a necessidade de um estudo maior, para que possamos entender o mundo virtual. Dessa popularização, nasce o que comumente chamamos de ciberespaço, que se constitui, assim como no espaço real, “um ambiente de trocas sociais, econômicas, morais e, ao mesmo tempo, de mudanças cada vez mais rápidas no *modus operandi* de comunicação, informação e interação.” (SOUZA, 2009) Os comportamentos, que antes só eram visualizados na vida real, passaram a ser pauta para discussões sobre os impactos positivos e negativos dessa tecnologia.

Diante desse ciberespaço, a nova cultura que se desenvolve, dá aos seus usuários uma espécie de “liberdade”, pelo fato de circularem pelo mundo virtual, uma grande variedade de informações e pensamentos, onde ninguém é proprietário da internet. Este fato se configura como sendo um dos pontos mais negativos sobre o tema, tendo em vista que dá margem a uma série de crimes que podem ser cometidos nessa esfera ainda muito obscura e emblemática, os chamados cybercrimes.

O mundo virtual deve ser encarado como sendo uma extensão da vida real, não podendo estar, os agentes criminosos, imunes a uma sanção por cometer um ilícito que afeta à coletividade ou um ato prejudicial a um único indivíduo. Diante dessa imensa evolução tecnológica, questões jurídicas tendem a surgir, fazendo nascer um novo ramo no nosso ordenamento: o direito da internet.

Essa nova “onda” de atos antijurídicos que se consumam no mundo virtual, chamados de cybercrimes, vem desafiando o Direito Brasileiro, pois devido a latente velocidade de mutação e à globalização, todos os dias nascem novas modalidades de lesão a interesses e bens que não estão tutelados pelo Estado, causando danos morais e materiais de larga proporção, e que a cada instante é executada de uma maneira diferente, tornando a identificação do agente criminoso quase que impossível.

A falta de legislação específica é um dos fundamentos primordiais que embasam a Era da Insegurança. Por esta razão, como uma forma de garantir uma maior

segurança aos usuários da internet, desperta-se a necessidade de criação de normas regulamentadoras capazes de disciplinar os seus usuários, assim como coordenar as relações travadas no ciberespaço, punir os eventuais crimes que ocorrerem e criar mecanismos que impeçam o uso indevido da internet, protegendo dessa forma os direitos e garantias fundamentais.

Com a globalização, e no ápice da inclusão digital, tanto o governo como os mais diversos segmentos societários se empenharam em mudar a realidade do privilégio de poucos ao acesso à internet, tornando, hodiernamente, seu acesso, uma questão popular, atingindo a todos os cidadãos, desde aquele de baixo poder aquisitivo, até aquele que tem como adentrar no mundo virtual desfrutando do conforto de sua residência.

Como um meio facilitador desse livre acesso à internet, os empresários vislumbraram uma forma de desenvolver uma atividade econômica de forma lucrativa, fazendo surgir assim, as figuras das “lan houses” e “cybercafés”, que são estabelecimentos comerciais, ou centros de educação, entretenimento e cultura, onde “as pessoas podem pagar para utilizar um computador com acesso à Internet e a uma rede local, com o principal fim de acesso à informação rápida pela rede e entretenimento através dos jogos em rede ou online” (WIKIPÉDIA, 2011).

Entretanto, como tudo há um lado positivo e negativo, por ser de uso público e pelo fato desses estabelecimentos agirem de forma a descumprir as leis e de forma negligente, ignorando as leis inerentes ao exercício da atividade empresarial, facilitando o acesso, os cybercafés e lan houses tornaram-se locais em que a prática dos cybercrimes é comum.

Diante de todo o exposto, alguns parâmetros legais tiveram que ser alterados, e novas leis foram formuladas para abranger e regulamentar essa nova realidade. Alguns Estados, como por exemplo, o Estado de São Paulo, editaram leis que tornam obrigatória o cadastro dos usuários desses estabelecimentos comerciais, a fim de evitar a prática dos cybercrimes e facilitar a identificação dos infratores, assunto este abordado por este trabalho.

1 OS CYBERCRIMES

Apesar de a internet trazer muitos aspectos positivos, trouxe consigo uma série de problemas, que se tornaram impasse jurídico, diante da inexistência ou lacuna legislativa, dentre eles os cybercrimes.

Para o Secretário Executivo da Associação de Direito e Informática do Chile, Claudio Líbano Manzur, esses novos delitos são interpretados como sendo,

todas as ações ou omissões típicas, ilegais e dolosas, tratem-se de incidentes isolados ou de uma série deles, cometidos contra pessoas naturais o jurídicas, realizadas através de um sistema de processamento de informações e destinadas a produzir uma lesão na vítima através atentados à sã técnica de informática, o qual, geralmente, produzirá de maneira colateral lesões a distintos valores jurídicos, reportando-se, muitas vezes, a um benefício ilegítimo ao agente, seja ou não de caráter patrimonial, atuando com ou sem fins lucrativos ³ (MANZUR, 2000, tradução da autora).

Os cybercrimes são os delitos que afetam o interesse da coletividade ou de um único indivíduo. Para Rafael Menezes, “o cybercrime é o crime que utiliza um sistema de informática para atentar contra um bem juridicamente protegido, seja tal bem público ou privado” (MENEZES, 2003).

Esses delitos podem derivar de diversos atos ilícitos, como por exemplo, a violação da propriedade intelectual, ao indevido desrespeito à intimidade, ao envio de mensagens não desejadas e ofensivas à honra, a divulgação de vídeos infamantes, invasão de caixa postal eletrônica, envio de vírus etc.

Para Menezes os crimes que tipificados que podem ser praticados pela internet são: a) homicídio: o criminoso invade o computador da UTI de um hospital e altera os remédios de um paciente, levando uma enfermeira a matá-lo pela dosagem errada; b) Crime contra a honra: caluniar, difamar ou injuriar alguém através de um site; c) Instigação a suicídio através da troca de e-mails ou de mensagens instantâneas; d) Furto: desvio de dinheiro em contas bancárias; e) Estelionato: uso de CPFs e cartões de crédito falsos para fazer compras na internet; f) Violar direito autoral através da cópia de softwares e músicas; g) Pedofilia – divulgação de pornografia infantil, art. 241 do ECA (BRASIL, 1990); h) Favorecimento de prostituição com um site anunciando garotas de programa; i) Tráfico de drogas e de armas que são anunciados pela internet (MENEZES, 2003).

Segundo Renato Ópice Blum, as acusações que mais lideram o ranking de cybercrimes são as de invasão de sistemas e vazamento de informações, ambos os delitos não possuem tipificação específica no ordenamento jurídico brasileiro, gerando a chamada lacuna legislativa (MATSUURA, 2009).

³ “todas aquellas acciones u omisiones típicas, antijurídicas y dolosas, trátense de hechos aislados o de una série de ellos, cometidos contra personas naturales o jurídicas, realizadas en uso de un sistema de tratamiento de la información y destinadas a producir un perjuicio en la víctima a través de atentados a la sana técnica informática, lo cual, generalmente, producirá de manera colateral lesiones a distintos valores jurídicos, reportándose, muchas veces, un beneficio ilícito en el agente, sea o no se caracter patrimonial, actúe con o sin ánimo de lucro.”

Ainda para Blum, essa lacuna está sendo bem preenchida pelo Judiciário Brasileiro que tem comumente aplicado a sabedoria e a inteligência a seu favor. Apesar de não ter leis específicas sobre o assunto, os casos julgados e as decisões judiciais acerca do tema já passam de 18 mil em todo o país (MATSUURA, 2009).

Numa primeira análise, vem a mente de muitos que não há como repreender os agentes, através de uma ação coercitiva do Estado, pois nenhum crime praticado por eles está tipificado no Código Penal, entretanto, deve-se entender que na grande maioria das vezes, a internet é apenas um instrumento de ação dos cybercriminosos. Dessa interpretação imprescindível se faz dividir os cybercrimes em puros, mistos e comuns.

Os crimes virtuais puros são aqueles que, segundo Marco Aurélio Rodrigues da Costa, "toda e qualquer conduta ilícita que tenha por objetivo exclusivo o sistema de computador, seja pelo atentado físico ou técnico do equipamento e seus componentes, inclusive dados e sistemas." (COSTA, 1995). Como exemplo desse tipo de crime encontram-se a figura dos *hackers*, que são pessoas com conhecimento na área de informática e que se utilizam dela para obter um benefício ilícito ou puro vandalismo, como invasão de sites.

Em outro giro, os crimes comuns são aqueles praticados pela internet, mas que já possuem tipificação na lei penal brasileira, sendo a rede mundial de computadores somente um meio diferente do tipificado, para a execução da conduta delituosa, por exemplo, a pornografia infantil, tipificada no art. 241 do ECA, que antes era divulgada por fotos ou vídeos, hoje se encontra em *homepages*, que, por sua vez, são as páginas iniciais de um site (PINHEIRO, 2000).

Por último, os crimes virtuais mistos são aqueles em que o uso da internet é condição *sine qua non* para a efetivação da conduta, mesmo que o bem jurídico lesionado seja diverso do informático, como por exemplo a transferência ilícita de valores de uma *home-banking*, uma espécie de banco online, criado para facilitar "transações, pagamentos e outras operações financeiras e de dados pela Internet por meio de uma página segura de banco" (PINHEIRO, 2000).

Mister se faz ressaltar que, de acordo com Blum, a legislação brasileira cobre 95% dos casos de crimes eletrônicos, mas a falta de legislação específica não implica dizer na não ação coercitiva do Estado para repreender e punir os agentes criminosos, uma vez que a reparação ao bem violado encontra resposta na esfera cível.

Entretanto, difícil é a identificação dos criminosos, seja pela rapidez da internet que possibilita a eliminação de qualquer vestígio criminoso, ou porque há a facilitação e

permissão do direito ao anonimato – que mesmo sendo respeitado não se torna absoluto – tornando mais difícil essa identificação, com a conseqüente responsabilização.

Hodiernamente, a identificação do criminoso é feita através do endereço do IP (Internet Protocol), que por sua vez, é um conjunto de protocolo de comunicação entre computadores de rede (WIKIPÉDIA, 2011). Cada computador tem um endereço de IP diferente, e através dele e da sua localização é possível encontrar o cybercriminoso. O problema reside na seguinte situação: como identificar a agente delitivo se o computador que ele utilizou para a prática antijurídica pertence a uma lan house ou a um cybercafé?

O que ocorre é que nesses estabelecimentos não há a manutenção de um cadastro atualizado de quem utiliza o seu serviço, omissão essa, que acaba por gerar a dificuldade de identificação do criminoso.

Alguns estados brasileiros, como São Paulo, a fim de evitar a prática de cybercrimes e facilitar a identificação dos infratores, editaram leis estaduais que dizem respeito à obrigatoriedade de cadastro nesses estabelecimentos comerciais que disponibilizam o uso à internet. A lei estadual de São Paulo nº 12.228/06 (SÃO PAULO, 2006) traz 5 requisitos como: nome, endereço, data de nascimento, telefone e o número de documento (RG); e mais outros 2 adicionais em caso de o usuário do serviço ser menor de 18 anos, quais sejam, filiação e nome da escola e horário em que estuda, para a realização do cadastro do usuário, e ainda o registro do dia e horário de entrada e saída do usuário, bem como o endereço de IP por ele utilizado.

Entretanto, por negligência de alguns estabelecimentos, ou por inexistência de lei, grande parte deles não faz nenhum tipo de registro dos seus usuários, impossibilitando, conseqüentemente, a identificação do cybercriminoso, à futura reparação do dano e o aumento da sensação de impunidade e de insegurança jurídica.

Desde 1995, a Polícia Civil de São Paulo, combate os crimes virtuais, dando o primeiro passo e sendo a primeira instituição da América Latina a possuir página na Rede Internacional de Dados, ou seja, na internet, com muitas informações acerca da atividade policial desenvolvida no Brasil, orientações de auxílio ao cidadão, bem como espaço destinado a receber denúncias ou sugestões de melhoria, além de arquivos de fotos dos criminosos mais procurados pela polícia e fotos de crianças desaparecidas.

A Polícia Civil de São Paulo, que é a autoridade competente para a investigação de qualquer prática criminosa, através do DCS - Departamento de Comunicação Social, vem, há algum tempo, realizando investigações de cybercrimes, e obtendo nessa empreitada, bastante sucesso.

Apesar de não existir atribuição administrativa para essas investigações, a Polícia Civil continua investigando e combatendo tais condutas delitivas, com o embasamento jurídico nas decisões em inquéritos policiais instaurados com a finalidade de apurar crimes ocorridos no meio virtual, que foram recebidos pelo Ministério Público e pelo Juiz Corregedor da Capital; bem como o embasamento no Código de Processo Penal em seu artigo 6º e incisos (BRASIL, 1941), *in verbis*:

Art. 6º Logo que tiver conhecimento da prática da infração penal, a autoridade policial deverá:

I - dirigir-se ao local, providenciando para que não se alterem o estado e conservação das coisas, até a chegada dos peritos criminais;

II - apreender os objetos que tiverem relação com o fato, após liberados pelos peritos criminais;

III - colher todas as provas que servirem para o esclarecimento do fato e suas circunstâncias;

IV - ouvir o ofendido;

V - ouvir o indiciado, com observância, no que for aplicável, do disposto no Capítulo III do Título VII, deste Livro, devendo o respectivo termo ser assinado por duas testemunhas que lhe tenham ouvido a leitura;

VI - proceder a reconhecimento de pessoas e coisas e a acareações;

VII - determinar, se for caso, que se proceda a exame de corpo de delito e a quaisquer outras perícias;

VIII - ordenar a identificação do indiciado pelo processo datiloscópico, se possível, e fazer juntar aos autos sua folha de antecedentes;

IX - averiguar a vida pregressa do indiciado, sob o ponto de vista individual, familiar e social, sua condição econômica, sua atitude e estado de ânimo antes e depois do crime e durante ele, e quaisquer outros elementos que contribuírem para a apreciação do seu temperamento e caráter. (grifos da autora)

1.1 O COMBATE AOS CYBERCRIMES NO MUNDO – DIREITO COMPARADO

A Convenção sobre o Cybercrime, chamada também de Convenção de Budapeste, foi criada na Hungria em 2001, pelo Conselho da Europa, e entrou em vigor desde 2004, após a ratificação de cinco países. Atualmente, engloba mais de 20 países e tipifica os crimes cometidos na internet.

Segundo o Preâmbulo, a Convenção prioriza “uma política criminal comum, com o objetivo de proteger a sociedade contra a criminalidade no ciberespaço, designadamente, através da adoção de legislação adequada e da melhoria da cooperação internacional” e ainda reconhece “a necessidade de uma cooperação entre os Estados e a

indústria privada no combate à cybercriminalidade, bem como a necessidade de proteger os interesses legítimos ligados ao uso e desenvolvimento das tecnologias da informação” (CONVENÇÃO DE BUDAPESTE, 2001).

O mencionado tratado foi aberto para assinaturas em Novembro de 2001, e estabelece diretrizes para leis e procedimentos que lidam com a criminalidade na internet. O acordo criou um fundamento para a criação de leis em todo o mundo, exigindo que os países que aderissem tratassem o cybercrime de forma uniforme, além de obrigar a criação de redes de contatos entre forças policiais que estivessem disponíveis 24 horas por dia e durante sete dias por semana.

Todavia, um dos pressupostos para a abertura num país, de um processo para apuração de cybercrime, torna-se necessário que a conduta praticada pelo agente seja também crime em qualquer outro país que esteja envolvido nas apurações. Isso se perfaz num dos objetivos da Convenção. O tratado também determina quais tipos de procedimentos de investigações são permitidas, tais como, interceptação de dados ou pesquisas em computadores.

A Convenção de Budapeste é supervisionada pelo Conselho da Europa, fundado em 1949, que também coordena a Convenção Europeia dos Direitos Humanos. Por esta razão, os países integrantes do Conselho da Europa podem assinar o tratado, desde que a legislação interna de cada país, não a contrarie, podendo ratificá-lo.

Os países que estão de fora do Conselho da Europa são convidados a aderir ao tratado. Até agora 32 países ou ratificaram ou aderiram, e outros 15 países assinaram o tratado, mas não o ratificaram, justamente o caso do Brasil.

Infere-se dessa análise que importante será a ratificação dessa Convenção pelo Brasil, pois ela será incorporada às leis brasileiras como sendo lei ordinária e atingirá a todo o país, dando fim a impunidade muitas vezes observada pelos agentes criminosos.

Apesar da inércia do Brasil em ratificar a Convenção sobre os Cybercrimes ou de editar leis específicas sobre o tema, para vigorarem até a ratificação daquela, muitos países já tomaram providências para o combate aos agentes delitivos que praticam seus crimes no mundo virtual. Dentre esses países estão: Estados Unidos, Inglaterra, França, Canadá, México, Portugal e Itália (FILHO, 2011).

Nos EUA há a CYBER ACTION TEAMS – C.A.T.”, unidade do “F.B.I.”, que é responsável pelos cybercrimes praticados no país. As equipes são formadas por poucos agentes, altamente treinados, compostas por analistas e especialistas em computação forense e

códigos maliciosos que viajam ao redor do mundo atuando contra às invasões cibernéticas e delitos relacionados, sempre em defesa dos interesses do governo americano (FILHO, 2011).

Já na Inglaterra, temos o The Police Central e-crime Unit – PCeU, unidade da Metropolitan Police da Inglaterra (Scotland Yard), que tem como objetivo reduzir os danos para o Reino Unido no combate ao cybercrime e aumentar a confiança pública, através da colaboração com parceiros apropriados, buscando melhorar e aperfeiçoar o fluxo de informações e a especialização das unidades policiais inglesas, dando uma resposta rápida nas investigação, tanto a nível nacional como internacional (FILHO, 2011).

L'Office Central de Lutte Contre la Criminalité Liée aux Technologies de l'information et de la Communication (OCLCTIC) é a unidade da Polícia Francesa dedicada ao combate contra os cybercrimes, atuando, em conjunto com unidades de outros países desde que permitido por eles, tanto nos casos envolvendo o crime organizado, como criminalidade financeira e se encontrando subordinada diretamente a Diretoria da Central de Polícia Judiciária francesa. Todos os policiais que atuam nesta unidade devem ser obrigatoriamente detentores da patente de Investigador de Cybercrime (ICC), e N-Tech, sem as quais não lhes será permitido atuar nesta área. Para integrar esta unidade especializada é obrigatório ao interessado ter cursado uma escola para policiais e em seguida obter as devidas certificações em cybercrimes (FILHO, 2011).

Integrated Technological Crime Unit” (ITCU) é uma unidade especializada da “Royal Canadian Mounted Police”, localizada no Canadá. Essa unidade tem como missão a investigação dos cybercrimes, fornecendo subsídios e recursos para pesquisa forense e assistência nesta modalidade criminosa, atuando diretamente na repressão a estes crimes. Os membros da ITCU têm uma ampla gama de experiências na área policial e profundos conhecimentos de computação forense, conhecimento em perícia e coleta de provas nas investigações de crimes cibernéticos, devendo se manter sempre atualizados para poder estar em consonância com as mudanças da tecnologia (FILHO, 2011).

No México temos a Unidad de Policía Cibernética y Delitos Contra Menores, unidade especializada da Polícia do México que atua na investigação de cyberdelitos, pedofilia e na realização de atividades de computação forense. Ainda realiza um trabalho incipiente e busca um melhor treinamento de seus integrantes, principalmente junto a outras unidades especializadas de países tecnicamente mais desenvolvidas (FILHO, 2011).

Em Portugal, a Secção de Investigação de Criminalidade Informática e de Telecomunicações – SICIT – é o órgão de cyber-investigação da Polícia de Portugal, constituída por duas Brigadas de Investigação. Essa secção atua na prevenção criminal na sua

área de investigação e se volta para o aumento da cultura de segurança informática em Portugal. De acordo com a Lei Orgânica da Polícia Judiciária – LOPJ - é da competência reservada da Polícia Judiciária portuguesa a investigação, em todo o território, de determinados crimes de maior gravidade e complexidade, sendo que os cybercrimes são investigados pela SICIT; que detém competência nacional para investigação da chamada criminalidade informática, a qual compreende a generalidade das infrações penais previstas e punidas pela Lei nº 109 de 17 de Agosto 1991 (FILHO, 2011).

Polizia Postale e delle Comunicazioni é uma unidade especializada da Polizia di Stato da Itália, cujo foco principal é prevenir e combater a criminalidade informática, garantindo o sigilo dos valores constitucionais e a liberdade de todas as formas de comunicação. Todos os esforços desta unidade da polícia italiana se voltam para os Correios e comunicações, buscando novas estratégias e formas de combate as novas fronteiras tecnológicas do crime. Esta unidade especializada está presente em todo o território italiano através de 20 unidades, com um foco regional, e 80 seções com competência provincial, coordenados centralmente pela diretoria da Polizia Postale e delle Comunicazioni (FILHO, 2011).

2 O INSTITUTO DA RESPONSABILIDADE CIVIL

A palavra responsabilidade tem sua origem no latim *spondeo*, pela qual se vincula o devedor, solenemente, nos contratos verbais do direito romano. Dentre as várias acepções existentes, a da doutrina do livre-arbítrio ou motivações psicológicas, destaca-se a noção de responsabilidade como aspecto da realidade social.

Toda atividade que trazer prejuízo traz na sua essência, como fato social, o problema da responsabilidade. Destina-se a restaurar o equilíbrio moral e patrimonial provocado pelo autor do dano, sendo a fonte geradora da responsabilidade civil o restabelecimento do direito violado, consistindo dessa forma a restauração do equilíbrio, da contraprestação e da reparação de dano.

Diante disso, coloca-se o responsável pela violação de determinada norma, exposto as consequências não desejadas decorrentes de sua conduta danosa, podendo ser compelido a restaurar o *statu quo ante*.

O instituto da responsabilidade civil é parte integrante do direito obrigacional, pois a principal consequência de uma prática delitiva é a obrigação que acarreta, para o seu autor, de reparar o dano, seja essa conduta dolosa ou culposa. A responsabilidade civil, seja em ambas as modalidades, está prevista no Código Civil de 2002 (BRASIL, 2002).

O artigo 186 do Código Civil estabelece que a modalidade subjetiva é aquela em que há a necessidade de comprovação de culpa. E em seu artigo 927, a objetiva, é a que não há a necessidade de comprovação de culpa, bastando para sua caracterização, o nexo de causalidade existente entre a conduta danosa e o dano causado.

Os elementos essenciais para o estabelecimento da responsabilidade civil são: uma ação ou omissão, que cause culposamente ou dolosamente, em que pese a necessidade de comprovação ou não da culpa, a relação nexo-causal, entre a conduta do agente e o dano experimentado pela vítima, conforme aduz os artigos do Código Civil, *in verbis*:

Art. 186. Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito.

Art. 927. Aquele que, por ato ilícito causar dano a outrem, fica obrigado a repará-lo.

Parágrafo único. Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por natureza, risco para direitos de outrem.

Observando o exposto no art. 186, percebemos que ele consagra uma regra universalmente aceita, qual seja, a de que todo aquele que causar dano a outrem é obrigado a repará-lo. Entretanto, tal artigo se baseia tão somente na culpa, conseqüentemente, em regra, não havendo culpa não há obrigação de reparar o dano.

A culpa é a inobservância de um dever que o agente deveria conhecer e observar, que segundo José de Aguiar Dias (apud, VENOSA, 2009, p. 23):

A culpa é a falta de diligência na observância da norma de conduta, isto é, o desprezo, por parte do agente, do esforço necessário para observá-la, com o resultado não objetivado, mas previsível, desde que o agente se detivesse na consideração das consequências eventuais de sua atitude.

Segundo o doutrinador Carlos Roberto Gonçalves, a culpa pode ser: *in eligendo*, que decorre de má escolha do representante; *in vigilando*, decorrente da ausência de fiscalização; *in committendo*, que decorre de uma ação, ou seja, de um ato positivo; *in*

omittendo, decorrente de uma omissão, quando havia o dever de fazer e não o fez; e por fim a culpa *in custodiendo*, decorrente de uma falta de cuidados na guarda de um animal ou de algum objeto (GONÇALVES, 2009, p. 36).

Segundo Maria Helena Diniz (2007, p.11), a responsabilidade civil evoluiu também na dimensão da culpa, uma vez que a obrigação de reparar passa a existir não apenas no seu lado subjetivo, nascendo o caráter objetivo da reparação que advém do risco, independente de culpa, sob a alegação de que o risco deve ser garantido como proteção aos direitos da pessoa.

Já o artigo 927 do Código Civil de 2002, dispõe que, pode em determinadas situações, a reparação de um dano cometido sem culpa, sendo nesse caso a responsabilidade objetiva, porque prescinde da culpa e se satisfaz apenas com o dano e o nexo de causalidade. Essa teoria também é chamada de Teoria do Risco, tendo como fundamento, que todo dano é indenizável, e deve ser reparado por quem a ele se liga por um nexo de causalidade (ALVIM, apud GONÇALVES, 2009, p. 30).

Segundo Silvio Rodrigues (2001, p.11), a teoria do risco

é a da responsabilidade objetiva. Segundo essa teoria, aquele que, através de sua atividade, cria risco de dano pra terceiros deve ser obrigado a repará-lo, ainda que sua atividade e seu comportamento sejam isentos de culpa. Examina-se a situação, e, se for verificada, objetivamente, a relação de causa e efeito entre o comportamento do agente e o dano experimentado pela vítima, esta tem o direito de ser indenizado por aquele.

Portanto, qualquer atividade ilícita que venha a causar prejuízo a direito da sociedade ou de outrem, enseja o direito à reparação, relação análoga e extensiva aos cybercrimes, que a depender do caso concreto pode ser aplicada a teoria subjetiva ou objetiva para que seja exigível a reparação do dano.

3 A RESPONSABILIDADE DAS LAN HOUSES OU CYBERCAFÉS NO QUE TANGE AOS CYBERCRIMES PRATICADOS EM SEU INTERIOR

O uso disseminado da internet, muitas vezes por meio da acessibilidade que trazem os estabelecimentos comerciais, os atos ilícitos cometidos, se produzem com a mesma

facilidade que no espaço real. Daí a necessidade de o Direito acompanhar essa evolução, para que possa garantir a tutela ao bem jurídico dos cidadãos.

Com o surgimento das leis e com a aplicação do Código Civil de 2002 e do Código de Defesa do Consumidor (BRASIL, 1990) aplica-se a responsabilidade civil a estes estabelecimentos, como lan houses ou cybercafés.

A Lei Estadual 12.228/06 do Estado de São Paulo passou a exigir o cadastramento obrigatório de seus usuários, conforme dispõe o seu artigo 1º e 2º, *in verbis*:

Artigo 1º. São regidos por esta lei os estabelecimentos comerciais instalados no Estado de São Paulo que ofertam a locação de computadores e máquinas para acesso à Internet, utilização de programas e de jogos eletrônicos, abrangendo os designados como „lan houses“, „cibercafés“ e „cyber offices“, entre outros.

Artigo 2º. Os estabelecimentos de que trata esta lei ficam obrigados a criar e manter cadastro atualizado de seus usuários, contendo:

- I - nome completo;
- II - data de nascimento;
- III - endereço completo;
- IV - telefone;
- V - número de documento de identidade.

§ 2º. O estabelecimento deverá registrar a hora inicial e final de cada acesso, com a identificação do usuário e do equipamento por ele utilizado.

§ 4º. As informações e o registro previstos neste artigo deverão ser mantidos por, no mínimo, 60(sessenta) meses.

Com base nessa lei, o Estado de São Paulo conferiu aos estabelecimentos a responsabilidade subjetiva quando em algum de seus equipamentos for cometido um cybercrime. Entretanto, as lan houses, por latente negligência, deixam de cumprir com o estabelecido na lei e gerando para a investigação do delito, a impossibilidade de identificação do agente. Neste caso, a lan house incorre em culpa *in ommittendo*, pois tem a obrigação de realizar o cadastro e por alguma razão não o faz, causando a possibilidade de alguém cometer um ato ilícito.

Há atualmente, em tramitação perante o Senado Federal um projeto de lei nº 296 de 2008, que disciplina acerca da obrigatoriedade de cadastro atualizado dos seus usuários, pelos estabelecimentos de “locação de terminais de computadores”.

De acordo com Antônio Jeová Santos (apud, GONÇALVES, 2009, p. 89), a responsabilidade do provedor é objetiva, quando se trata da hipótese de *information*

providers, em que incorpora a página ou o site, pois “uma vez que aloja a informação transmitida pelo site ou pela página, assume o risco de eventual ataque a direito personalíssimo de terceiro”. Ainda continua dizendo que, a respeito do conteúdo de terceiros ou indiretos, os chamados *links*, a responsabilidade também é objetiva, já que antes de acessá-lo necessariamente deve ser o conteúdo analisado e estudado.

Já no tocante à *internet service providers*, que são aqueles em que há apenas a entrega de serviço para possibilitar a conexão à internet, e ao *hosting service*, aqueles em que tem como função abrigar sites e páginas, atuando como hospedeiro tecnológico virtual, não havendo interferência no conteúdo que o usuário coloca na página ou site. Entende Santos que a responsabilidade de quem explora esses tipos de serviços será sempre subjetiva, somente ocorrendo se atuarem com alguma modalidade de culpa.

É pacífico o entendimento nos Tribunais em todo o país, de que o fato de as obras e as informações transmitidas pela Internet estarem sob a forma digital não retira delas a característica de criação humana, passíveis de proteção jurídica, configurando a verossimilhança do direito alegado, hábil a antecipação da tutela (AgI 122.834/4-SP, TJSP, 2ª Câmara. Dir. Priv., rel. Des. Cintra Pereira, julgado em 26-10-1999).

Sob a ótica do Código de Defesa do Consumidor, o terceiro prejudicado é equiparado a consumidor, pois os usuários irão utilizar dos serviços ofertados pelas *lan houses* e *cybercafés*.

Ao utilizarem tais serviços, os usuários presumem que estes estabelecimentos dispõem dos aparelhos e softwares capazes de proteger o computador contra, por exemplo, *spams* - que são mensagens enviadas eletronicamente em massa, sem a solicitação - e que em sua grande maioria estão com vírus. Por esta razão, não há a necessidade de toda vez que o usuário for utilizar o computador, analisar se a máquina está em perfeitas condições de uso, o que garantirá a sua segurança e de seus direitos, pois, consiste em obrigação de quem presta o serviço de manter seus aparelhos livres de qualquer meio que possa vir a resultar em dano a alguém, sendo presumido o risco.

Dessa maneira, se por algum defeito no serviço ou nos equipamentos, houver danificação por exemplo, de um arquivo, por um vírus contraído no computador da *lan house*, esta será responsável, na modalidade objetiva, por reparar o dano causado tanto aos seus usuários como a terceiros. Sobre este risco o Código de Defesa do Consumidor declara o seguinte em seu artigo 14, caput, § 1º, II, e artigo 17:

Art.14. O fornecedor de serviços responde, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação de serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos.

§1º o serviço é defeituoso quando não fornece a segurança que o consumidor dele pode esperar, levando-se em consideração as circunstâncias relevantes, entre as quais:

 II – o resultado e os riscos que razoavelmente dele se esperam;

Art. 17. Para os efeitos desta Seção, equiparam-se aos consumidores todas as vítimas do evento.

Este entendimento foi firmado pelo juiz da 39ª Vara Cível da capital do Estado de São Paulo, que condenou uma lan house a pagar a quantia de R\$ 10 mil reais a título de indenização para uma administradora de empresas, que foi vítima de ofensas por mensagem eletrônica enviadas de um usuário de uma lan house. No caso, o estabelecimento oferecia o serviço de internet via conexão sem fio (wireless), que mesmo com a identificação do endereço do IP não há como chegar na máquina de onde partiu a ofensa. Partindo do pressuposto que nenhum crime cometido pela internet fica sem a devida responsabilização, a conduta praticada pelo estabelecimento foi enquadrada na teoria do risco, restando para esta, a responsabilização por danos materiais e morais à administradora.

Justificando sua decisão o juiz entendeu que

Quem disponibiliza terminais de computadores ou rede sem fio para uso de internet assume o risco do uso indevido desse sistema para lesar direito de outrem. Sendo assim, diante do evidente conteúdo difamatório da mensagem eletrônica enviada à autora origina no estabelecimento da ré, de rigor a condenação nas perdas e danos morais já que a agressão aos bens materiais configura prejuízo moral. São invioláveis a honra e a imagem das pessoas, assegurando o direito à indenização pelo dano material ou moral consequente à sua violação (Ação Cível nº 583.00.2006.243439-5, TJSP, 39ª vara cível, sentença publicada dia 10-03-2008).

Neste mesmo diapasão, a jurisprudência já reconheceu a responsabilidade dos estabelecimentos que disponibilizam computadores com acesso à internet, qual seja:

“AÇÃO DE OBRIGAÇÃO DE FAZER CUMULADA COM PERDAS E DANOS – Mensagem eletrônica recebida pela autora de teor ofensivo à sua honra - Obrigação do estabelecimento de onde partiu o envio de manter cadastro atualizado dos usuários, a fim de que estes não se favoreçam do anonimato quando da prática de ilícitos - Aplicação da Lei Estadual nn 12.228/06 que obriga os estabelecimentos que fornecem serviços de acesso à Internet de manter referido cadastro - Atividade destes estabelecimentos que

pode ser considerada de risco, caso não tomem as medidas necessárias que possibilitem a identificação dos usuários (art. 927, parágrafo único, do Código Civil) - Responsabilidade civil pelos danos causados caracterizada - Cabimento do pedido alternativo para conversão em perdas e danos - Procedência mantida - Recurso desprovido.” (Apelação nº 604.346-4/7-00, TJ/SP, Rel. Des. Salles Rossi, Julgado em 10/12/2008).

Observa-se que, no que tange a responsabilidade subjetiva aos fornecedores de acesso à internet, o fundamento é o da omissão quanto à obrigatoriedade de cadastro de usuários que gera como consequência a impossibilidade de identificação do criminoso. Já na responsabilidade objetiva, pauta-se a responsabilização na teoria do risco, que pode gerar um dano da prestação do serviço a seus clientes e a terceiros, não havendo a necessidade de se especificar a conduta dolosa ou culposa, bastando somente identificar o nexo de causalidade, entre a conduta praticada ou, neste caso, o risco oferecido e o dano sofrido pela vítima.

Assim sendo, no mundo virtual, que não está excluído do direito, quando ocorre um dano, a responsabilidade deverá ser atribuída: ao provedor, aos usuários desses provedores como, por exemplo, bancos online, supermercados virtuais, sites de compra coletiva; ou ao próprio cidadão que por meio de sua vontade cometeu ato ilícito; ou ainda a todos solidariamente, o que nunca ocorrerá é a não reparação ao dano causado.

4 CONSIDERAÇÕES FINAIS

Com o avanço da tecnologia e da globalização a internet se tornou um meio fácil para o cometimento de novos crimes ou crimes já conhecidos, mas com a utilização da internet para a sua consumação. Isso se configura como sendo um novo desafio a ser enfrentado pelo direito positivo, tornando-se necessária não só a tutela dos bens de terceiros com mais segurança, como também elaborando leis tipificando essas condutas, não permitindo que os delitos fiquem impunes e dêem margem à insegurança jurídica.

Para essa garantia verificou-se que o instituto da responsabilidade civil se adequa perfeitamente aos crimes cometidos no mundo virtual, aplicando-se não somente aos autores do delito, mas bem como aos estabelecimentos, ou usuários da internet, como bancos *online*, e todos aqueles que concorrerem na culpa, para a impossibilidade de identificação dos que geram riscos a terceiros.

O que ocorre no meio virtual reflete diretamente no mundo real e na sociedade, exigindo-se uma adequação dos países relativa ao tema. Diante da lacuna legislativa ou da inércia Estatal em ratificar a Convenção de Budapeste, é de encargo de cada Estado da Federação editar sua lei quanto ao cadastramento dos usuários e a sua devida responsabilização. Entretanto, por tratar-se de uma discricionariedade, imperioso se faz a necessidade de uma lei que atinja todos os Estados, e que venha regular essa situação.

Visando regulamentar essa matéria com uma lei de âmbito nacional, o projeto de lei do Senado Federal nº 296 de 2008, aprovado recentemente pela Comissão competente e já enviado à Câmara dos Deputados para a devida revisão, prevê a obrigatoriedade, em âmbito federal, o cadastro dos clientes de estabelecimentos que fazem a locação de computadores com acesso à internet.

Se aprovada esta lei, assim que entrar em vigor em toda a Federação, extinguirá a insegurança jurídica causada pela lacuna legislativa, e o instituto da responsabilidade civil subjetiva será estendido aos agentes que cometerem danos a terceiros pela internet, e aos proprietários dos estabelecimentos que por negligência ou falta de fiscalização, favorecem a prática delitiva nas lan houses e cybercafés, por não realizarem o cadastro do usuário dificultando a identificação dos criminosos.

Isto posto, conclui-se que não basta apenas novas leis, pois os cybercrimes só serão eficazmente combatidos caso ocorra uma interação adequada entre o Poder Judiciário, Ministério Público e Polícia Civil; OAB; empresas de telecomunicações, para propiciar aos cidadãos uma conscientização acerca do uso seguro e legal da internet ou ainda para orientar acerca dos crimes virtuais já existentes; provedores de acesso e instituições financeiras.

Além disso, os profissionais do direito e as autoridades policiais devem estar preparados e treinados para apurar e reprimir os cybercrimes, imprescindível para isso, uma atualização das técnicas de prática forense e também um curso para a ampliação dos conhecimentos de computação forense. Ainda para o avanço da represália aos cybercrimes é importante a colaboração dos estabelecimentos como lan houses e cybercafés, bem como dos provedores de internet, que devem priorizar além do lucro, os valores éticos-morais e os direitos de terceiros, para ajudar as autoridades competentes a identificar e reprimir essa conduta criminosa, que se alastra por todo o país.

REFERÊNCIAS

BRASIL. Lei nº 10.406 de 10 de janeiro de 2002. **Código Civil – CC/02**. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/L10406.htm>. Acesso em 10 nov. 2011.

BRASIL. Lei nº. 8.069 de 13 de julho de 1990. **Estatuto da criança e do adolescente - ECA**. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L8069.htm>. Acesso em: 10 nov. 2011.

BRASIL. Lei nº 3.689 de 03 de outubro de 1941. **Código de Processo Penal – CPP**. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del3689Compilado.htm>. Acesso em: 23 nov. 2011.

BRASIL. Lei nº 8.078 de 11 de setembro de 1990. **Código de Defesa do Consumidor – CDC**. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L8078compilado.htm>. Acesso em: 10 nov. 2011.

BRASIL. **Projeto de Lei do Senado Federal nº 296/2008**. Disponível em: <http://www.senado.gov.br/atividade/materia/detalhes.asp?p_cod_mate=86846>. Acesso em 13 nov. 2011.

CONVENÇÃO SOBRE O CIBERCRIME. Disponível em: <http://ccji.pgr.mpf.gov.br/informes-e-documentos/documentos/docs_documentos/convencao_cibercrime.pdf>. Acesso em: 24 nov. 2011.

DINIZ, Maria Helena. **Curso de direito civil brasileiro**. 21. ed. São Paulo: Saraiva, 2007.

FILHO, José Mariano de Araújo. **A investigação dos crimes eletrônicos no Brasil e no mundo**. Disponível em: <<http://www.slideshare.net/jmarfilho/a-investigao-dos-cybercrimes-no-brasil-e-no-mundo>>. Acesso em: 23 nov. 2011.

FILHO, José Mariano de Araújo. **Convenção sobre o Cybercrime será discutida esta semana, apesar de controvérsias em todo o mundo**. In weblog: Cybercrimes – Delegado Mariano. Disponível em: <<http://mariano.delegadodepolicia.com/tag/delegado-jose-mariano-de-araujo-filho/>>. Acesso em: 23 nov. 2011.

GONÇALVES, Carlos Roberto. **Direito Civil Brasileiro**, volume IV: responsabilidade civil/Carlos Roberto Gonçalves. - 4. ed. rev. - São Paulo: Saraiva, 2009.

MATSUURA, Lilian. **A era da tecnologia é também a era da insegurança**: entrevista de Renato Opice Blum à Conjur. Disponível em: <<http://www.conjur.com.br/2009-mar-22/entrevista-renato-opice-blum-especialista-direito-eletronico>>. Acesso em: 13 nov. 2011.

MENEZES, Rafael de. **Responsabilidade civil na internet e cybercrimes**. Disponível em: < <http://www.rafaeldemenezes.adv.br/artigos/internet.htm>>. Acesso em: 15 nov. 2011.

MORAES, Paulo Francisco Cardoso de. **A vedação constitucional do anonimato aplicada à internet. O papel do estado brasileiro na identificação dos usuários e responsabilização dos provedores**. In: Âmbito Jurídico, Rio Grande, 91, 01/08/2011. Disponível em: < http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=9964>. Acesso em: 15 nov. 2011.

PINHEIRO, Reginaldo César. **Os cybercrimes na esfera jurídica brasileira**. Jus Navigandi, Teresina, ano 5, n. 44, 1 ago. 2000. Disponível em: <<http://jus.com.br/revista/texto/1830>>. Acesso em: 17 nov. 2011.

PINHEIRO, Patrícia Peck. PRATTI, Vivian. MARTES, Rogério. **Análise dos últimos 10 anos do Direito Digital no Judiciário Brasileiro. II Consolidado de Jurisprudência - Direito Digital**. In: Âmbito Jurídico, Rio Grande, 81, 01/10/2010. Disponível em: < http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=8396>. Acesso em: 17 nov. 2011.

RODRIGUES, Silvio. **Direito civil**. São Paulo: Saraiva, 2000.

SANTOS, Gustavo de Oliveira; ANDRADE, Izabella Lucena Medeiros de; MORAIS, Lucas Andrade de. **A responsabilidade dos estabelecimentos fornecedores de serviço de acesso à internet nos “cybercrimes”**. Disponível em: < http://docs.google.com/viewer?a=v&q=cache:74_8-60qn9EJ:www.unieducar.org.br/artigos/A%2520RESPONSABILIDADE%2520CIVIL%2520DOS%2520ESTABELECIMENTOS%2520FORNECEDORES.pdf+responsabilidade+civil+da+lan+house+pelos+crimes+cibern%C3%A9ticos&hl=pt-BR&gl=br&pid=bl&srcid=ADGEESgYQ_KJwr1OhU4FfV4C2Uyd0pgSM1r4yG6iUPMgdD6AtaMSTNXPeKntIUfrAKgfjoo9kPSX6LpjvACyZXVorvEYfCM-sWOy9LljEPuQEAilucboJDMmYQ7IdhfHGFBrgIa4f6n_&sig=AHIEtbSRgkOU8jlg3_VGjkdFd-iRPIWnnA>. Acesso em 19 nov. 2011.

SÃO PAULO. **Lei estadual nº 12.228/06**. Disponível em: < <http://lanhouse2d.com/lei.pdf>>. Acesso em 18 nov. 2011.

SOUZA, Gills Lopes Macêdo; PEREIRA, Dalliana Vilar. **A Convenção de Budapeste e as Leis Brasileiras**. Disponível em: < <http://www.charlieoscartango.com.br/Images/A%20convencao%20de%20Budapeste%20e%20as%20leis%20brasileiras.pdf>>. Acesso em: 23 nov. 2011.

SOUZA, Gills Lopes Macêdo; PEREIRA, Dalliana Vilar. **O Cibercrime e as Relações Internacionais**. Disponível em: < <http://www.mundialistas.com.br/blog/?p=304>>. Acesso em: 12 nov. 2011.

TRIBUNAL DO ESTADO DE SÃO PAULO. **Jurisprudência**. Disponível em: <<http://www.tj.sp.gov.br/servico/ConsultaCapital.aspx>>. Acesso em: 19 nov. 2011.

VENOSA, Sílvio de Salvo. **Direito civil: responsabilidade civil**/Sílvio de Salvo Venosa - 9. ed. - São Paulo: Atlas, 2009. - (Coleção direito civil; v. 4)

WIKIPÉDIA. **Lan house**. Disponível em: <http://pt.wikipedia.org/wiki/LAN_house>. Acesso em 21 nov. 2011.

WIKIPÉDIA. **Endereço de IP**. Disponível em: <http://pt.wikipedia.org/wiki/Endere%C3%A7o_IP>. Acesso em 21 nov. 2011.

WIKIPÉDIA. **Crime informático**. Disponível em: <http://pt.wikipedia.org/wiki/Crime_inform%C3%A1tico#Hist.C3.B3rico>. Acesso em: 22 nov. 2011.