UNIVERSIDADE ESTADUAL DA PARAÍBA
CAMPUS I _ CAMPINA GRANDE
CENTRO DE CIÊNCIAS JURÍDICAS
CURSO DE DIREITO

JEÍSA DOS SANTOS PEREIRA LINHARES PORDEUS

CRIMES CONTRA O PATRIMÔNIO NA SOCIEDADE DA INFORMAÇÃO

CAMPINA GRANDE
2011

JEÍSA DOS SANTOS PEREIRA LINHARES PORDEUS

CRIMES CONTRA O PATRIMÔNIO NA SOCIEDADE DA INFORMAÇÃO

Trabalho de Conclusão de Curso apresentado ao Curso de Direito da Universidade Estadual da Paraíba em cumprimento à exigência para a obtenção do título de Bacharela em Direito.

Orientador: Prof. Esp. Cláudio Simão de Lucena Neto

CAMPINA GRANDE – PB
2011

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA CENTRAL – UEPB

P835c Pordeus, Jeísa dos Santos Pereira Linhares.

Crimes contra o patrimônio na sociedade da informação [manuscrito] / Jeísa dos Santos Pereira Linhares Pordeus.– 2011.

23 f.

Digitado.

Trabalho Acadêmico Orientado (Graduação em Direito) – Universidade Estadual da Paraíba, Centro de Ciências Jurídicas, 2011.

"Orientação: Prof. Esp. Cláudio Simão de Lucena Neto, Departamento de Direito Privado".

1. Direito penal. 2. Cibercrimes. 3. Código Penal. I. Título.

21. ed. CDD 345

JEÍSA DOS SANTOS PEREIRA LINHARES PORDEUS

CRIMES CONTRA O PATRIMÔNIO NA SOCIEDADE DA INFORMAÇÃO

Trabalho de Conclusão de Curso apresentado ao Curso de Direito da Universidade Estadual da Paraíba em cumprimento à exigência para a obtenção do título de bacharela em Direito.

Aprovada em 30/ 11 /2011

Prof. Esp. Cláudio Simão de Lucena Neto/UEPB
Orientador

Profª. Esp. Marilia Daniella Freitas Oliveira Leal /UEPB
Examinador(a)

Ana Alice Ramos Tejo Salgado

Profª. Ms. Ana Alice Ramos Tejo Salgado/UEPB
Examinador (a)

CRIMES CONTRA O PATRIMÔNIO NA SOCIEDADE DA INFORMAÇÃO

PORDEUS, Jeísa dos Santos Pereira Linhares[1]

RESUMO

O presente trabalho analisa a problemática de como o direito tem tuteladoo bem jurídico patrimônio nos crimes cometidos por meio eletrônico, posto que, no Brasil não há legislação específicarelativa à prática desse tipo de delito. Ométodo utilizado para tanto foi a pesquisa bibliográfica, com a análise da doutrina acerca da repercussão dos cibercrimes no direito brasileiro.Tem como escopo analisar esse tipo de delito; comentar as características gerais e aspectos de enfrentamento, bem como, definir crimes eletrônicos, podendo sintetizá-loscomo toda açãotípica, antijurídica e culpável que seja praticada ou provida através dos meios informáticos e/ou internet.Essa tipicidade é analisada com enfoque na aplicação do Código penal às práticas delituosas, mediante a falta de legislação específica. Por meio do estudo,percebeu-se que, dentre as dificuldades de combate a tais delitos, podemos destacar a falta de denúncias, a identificação da autoria, colheita e armazenamento de provas, e o modo como se dará a pretensão punitiva do Estado. Conclui-se que apesar da inexistência de legislação penal específica, o nosso Código Penal e as leis penais posteriores, possuem plenas condições de serem aplicadas, uma vez que a Internet é apenas um novo meio para a prática delituosa e que o que necessitamos, na verdade, é de práticas efetivas de combate aos cibercrimes.

PALAVRAS-CHAVE: Cibercrimes.Direito. Patrimônio.Código Penal.

1 – A autora possui graduação e licenciatura plena em Psicologia, pela Universidade Estadual da Paraíba. É acadêmica do Curso de bacharelado em Direito nesta mesma UES_ UEPB. E-mail: jeisa.splp@hotmail.com.

1 INTRODUÇÃO

A criação e o desenvolvimento da internet foram um marco na vida do homem, ampliando as relações sociais, o conhecimento, a rapidez na circulação de informações, as possibilidades de trabalho, de realizar movimentações bancárias etc. Por meio dela temos acesso a uma gama e uma velocidade imensuráveis de informação.

A sociedade atual já introduziu a internet como algo imprescindível no seu dia a dia,as relações virtuais e seus desdobramentos são pura realidade. Assim, é muito comum, atualmente, um indivíduo realizar uma transação bancária de seu computador, notebook, ou até mesmo de seu celular, ao invés de ir a uma agência bancária.

Entretanto, a sociedade tem ficado assustada com o avanço da criminalidade por meio da rede; pois essa ferramenta tem sido utilizada para a prática de crimes; algo que tem ocorrido não só no Brasil, mas no mundo todo. O ambiente digital é apenas uma extensão da vida real. Em ambos podemos nos comunicar, compartilhar, comprar, inclusive, furtar, fraudar, entre outros.Diversos são os crimes virtuais cometidos hoje e que permanecem impunes por falta de conhecimento por parte das próprias vítimas.

Diante disso, surge a problemática da falta de legislação específica relativa a esse tipo de delito e o judiciáriose depara com a necessidade de adequação às leis já existentes.Porém, os problemas gerados pelos crimes virtuais, no campo jurídico, vão além da tipificação. A tecnologia tem avançado a passos largos, e com ela, também surgem novas formas de prática de ilícitos, surgindo assim, a necessidade de adequação do Direito a esta nova realidade.

Há diversos delitos cometidos através da Internet. De maneira geral, esses delitos são cometidos contra a pessoa e contra o patrimônio. Estes últimos englobam os crimes referentes a ataques a redes ou a computadores; o envio de *vírus*; a invasão de computadores de terceiros; a alteração de dados armazenados em computadores; a quebra de privacidade de banco de dados; furto; os crimes de natureza bancária e financeira, incluindo a transferência ilegal de fundos de uma conta bancária para outra; fraudes envolvendo o uso de cartões de crédito de terceiros etc.

O prejuízo causado pelos golpes cometidos por meio eletrônico crescem a cada ano, em contrapartida a quase nenhuma medida tomada pelas autoridades para coibir essa prática criminosa.

Conforme a Folha onLine de 07 de janeiro de 2006, as fraudes virtuais causaram, em 2005, um prejuízo recorde de R$ 300 milhões a

instituições financeiras (bancos e administradoras de cartões) no Brasil; a perda de 2005 representa 12% dos R$ 2,5 bilhões faturados pelo comércio eletrônico brasileiro no período; conforme estimativas do Instituto de Peritos em Tecnologias Digitais e Telecomunicações (IPDI).

Em 2009, o Centro de Estudos, Resposta e Tratamento de Incidentes no Brasil registrou no segundo trimestre de 2008 um aumento de 96% de tentativas de fraudes virtuais em relação ao primeiro trimestre de 2009 e de 114% em comparação ao segundo trimestre de 2007, demonstrando o avanço da criminalidade por esse meio.

Neste ano de 2011, dos incidentes reportados ao CERT.br , nos meses de abril a junho, 48,35% foram de tentativas de fraude com objetivos financeiros envolvendo o uso de cavalos de tróia; 47,10% tentativas de fraude com objetivos financeiros envolvendo o uso de páginas falsas; 1,56% de notificações de eventuais violações de direitos autorais e 3% de outras tentativas de fraude.

Os criminosos têm demonstrado “criatividade”, inteligência e versatilidade, e vêm, paulatinamente, aprimorando suas práticas; fazendo-se urgente a contrapartida da sociedade por meio de ações policiais, jurídicas, políticas e de segurança de dados eletrônicos. Ainda há uma grande caminhada a ser percorrida, tanto no sentido de embasamento legal quanto em relação aos recursos a serem utilizados nesse combate.

Desse modo, reveste de grande importância traçar a noção jurídica do crimes ocorridos por meio eletrônico; analisar os crimes contra o patrimônio à luz do Código Penal brasileiro, e comentar as características gerais e aspectos de enfrentamento destas modalidades de crime.

2 **A noção jurídica de crime eletrônico**

Os crimes eletrônicos são também conhecidos como cybercrimes, crimes virtuais, crimes de informática, crimes cometidos por meio da internet, entre outros e referem-se a qualquer tipo de crime que seja praticado ou provido através dos meios informáticos e/ou internet. Não se tratam de uma nova modalidade de crimes, mas, de uma nova ferramenta utilizada por criminosos para fazerem mais vítimas e praticarem ilícitos.

A Prof.ª Ivete Senise Ferreira*apud*Silva (2000) em artigo intitulado “Os Crimes da Informática”, define os crimes eletrônicos como “toda ação

típica, antijurídica e culpável contra ou pela utilização de processamento automático de dados ou sua transmissão".

Rocha (1994, p. 38) concebe esse tipo de criminalidade como “aqueles que têm por instrumento ou por objeto sistema de processamento eletrônico de dados, apresentando-se em múltiplas modalidades de execução e de lesão de bens jurídicos”.Carlos M. Correa e outros,*apud*Silva (2000) cita que conforme a definição da Organização para a Cooperação e Desenvolvimento Econômico (OECD), “delito informático é qualquer conduta ilegal, não ética e não autorizada que envolva o processamento automático de dados ou a transmissão de dados”.

Neil Barret*apud* Corrêa (2008, p.44), os crimes digitais são “a utilização de computadores para ajuda em atividades ilegais, subvertendo a segurança de sistemas, ou usando a internet ou redes bancárias de maneira ilícita”.

Já na opinião de Corrêa (2008, p.44), “os crimes digitais seriam todos aqueles relacionados às informações arquivadas ou em trânsito por computadores, sendo esses dados, acessados ilicitamente, usados para ameaçar ou fraudar”.

Na década dos anos 70, o principal criminoso era o técnico da informática. Na década seguinte, nos anos 80,tanto os técnicos de informática quanto os funcionários de instituições financeiras eram os principais criminosos. Já na atual década, qualquer pessoa física pode praticar os crimes da informática, pelas inúmeras oportunidades que as novas tecnologias e os novos ambientes organizacionais proporcionam.

Assim, é que Pinheiro (2009) afirma que, à exceção dos crimes cometidos por hackers, os crimes ocorridos na internet não correspondem a um crime de fim, mas um crime de meio, por utilizar-se do meio virtual.

É interessante ressaltar que é por meio do computador que indivíduos mal intencionados encontram vítimas para aplicarem seus golpes, porém, mediante o avanço da tecnologia, têm sido também utilizados os notebooks, laptops, palmtops, e até mesmo, o telefone celular.

Apesar de “o meio de materialização de a conduta criminosa ser virtual; contudo, em certos casos, o crime não” (PINHEIRO, 2009, p. 226), tendo em vista que há vítimas, pessoas são ofendidas em sua honra, seu patrimônio.

Constitui um atrativo para os criminosos o fato da possibilidade de sua não identificação, ou, ao menos, a dificuldade de identificar um agente que comete crime por meio eletrônico. Entretanto, o anonimato na rede é relativo,

pois temos o IP como uma forma de identificação virtual. Mesmo assim, essa identidade virtual pode também não possuir um correspondente de identidade real, tal como o chamado “laranja”.

É importante observar que aquele que comete crimes por meio da internet visa obter lucro de forma fácil. “Hoje, o cybercrime visa resultados financeiros e se mostra mais como uma ramificação do crime organizado (PINHEIRO, 2009, p. 227). Tanto no mundo ‘real’ quanto no ‘virtual’, o Direito Penal deve assegurar que haja sanção para aqueles que cometem delitos.

3 **Dos crimes contra o patrimônio na sociedade da informação**

A internet passou expressivo crescimento na última década, tanto em número de usuários como em portabilidade aos serviços multimídias e aumento na velocidade de transmissão de dados, de acordo com NEVES (2009). Ao mesmo passo, os crimes eletrônicos aumentaram o seu poder de lesão, levando facilmente o usuário ao erro, dando credibilidade e aparente idoneidade à fraude.

Neil Barret*apud* Corrêa (2008, p.45) afirma que “a era da informação não afeta apenas as nossas empresas ou o nosso correio eletrônico, mas também toda a infra-estrutura nacional, como a economia”.

Corrêa ainda analisa:

> [...] a estrutura e a capacidade oferecida pelo computador e pelas “novas tecnologias’ serão diretamente utilizadas por criminosos e terroristas, seja para lavar dinheiro, esconder arquivos que versem sobre material ilegal, ou até mesmo armar uma conspiração contra determinada ordem. O ‘palco’ da maior parte desses crimes digitais está dentro das facilidades oferecidas pela internet. Isso é lógico, visto que toda uma comunidade está se desenvolvendo por meio da implementação dessa tecnologia. Além disso, a popularidade da WWW, aliada à possibilidade do anonimato que é dada aos seus usuários, vem fazendo dela um desafio para as autoridades mundiais.(CORRÊA, 2008, P.45)

Defende Heleno Fragoso *apud* Bitencourt (2010, p. 38) que não há possibilidade de haver crime patrimonial sem lesão a interesse jurídico economicamente apreciável, aplicando-se, nesses casos, a noção do direito civil de que é elementar ao conceito de patrimônio a avaliação econômica dos bens e, ou suas relações.

Bitencourt (2010, p. 38) cita ainda a observação de Hungria de que “também são patrimoniais aquelas coisas que, embora sem valor venal, representam uma utilidade, ainda que simplesmente moral”. Desse modo, o valor patrimonial não corresponde apenas ao valor econômico, contudo, deve-se levar em consideração o valor da coisa para a vítima, que sofrerá um dano em seu patrimônio.

Para que um dano patrimonial por meio da internet seja um cibercrime, deve ser classificado como fato típico, e, assim, será relevante juridicamente. Não há uma grande necessidade de serem criadas mais leis, especialmente, com relação aos crimes cometidos por meio eletrônico, já que, com base no próprio Código Penal Brasileiro pode ser feito o enquadramento desses crimes.

Embora não haja uma legislação específica que trate sobre os crimes eletrônicos, os mesmos são passíveis de qualificação penal perante a legislação vigente, uma vez que a título de exemplo, um crime de estelionato não deixa de ser estelionato por ter sido praticado por meio da internet.

Apesar da possibilidade de enquadramento penal, o crescimento dos crimes informáticos é notório. Este crescimento pode ser atribuído em parte à sensação de impunidade por parte dos autores, à baixa necessidade de conhecimento informático para aplicar certos tipos de golpes e a facilidade para encontrar vítimas; em parte ao usuário, por motivos de falta de informação, falta de cuidados na navegação pela internet, não adoção de medidas e ferramentas de segurança e demora em relatar as denúncias às autoridades.

Tramita no Legislativo Nacional, um polêmico projeto de lei que visa combater os cibercrimes, proposto pelo Senador Eduardo Azeredo, o qual, foivotado no Senado no mês de outubro do corrente ano de 2011, e tenta regulamentar a identificação de usuários em todo o país. O citado projeto tem sido bastante criticado, principalmente no que diz respeito à redação de alguns artigos.

Conforme seu proponente, o Senador citado, o mesmo visa a tipificar determinadas condutas cibernéticas, em consonância com as recomendações da Convenção de Budapeste, estando, nesse sentido, em harmonia com a mesma. No entanto, face ao desrespeito evidente aos direitos fundamentais e às liberdades civis que aquele acarreta, é explícita a dissonância entre esses instrumentos normativos, bem como a inconstitucionalidade de dispositivos do projeto em análise.

Azeredo (2011, p. 29) afirma que os crimes eletrônicos não respeitam fronteiras; por isso, o Brasil precisa ser signatário de um tratado que

permita a colaboração externa, e considera a adesão do Brasil à Convenção Internacional do Cibercrime (o Tratado de Budapeste) bastante importante para o país.

Criada em 2001, na Hungria, pelo Conselho da Europa, e em vigor desde 2004, após a ratificação de cinco países, a Convenção de Budapeste, em seu Preâmbulo, 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 reconhece a necessidade de uma cooperação entre os Estados e a indústria privada.

O Tratado possui quatro Capítulos (Terminologia, Medidas a Tomar a Nível Nacional, Cooperação Internacional e Disposições Finais, respectivamente). Traz definição acerca dos cibercrimes(Capítulo I), tipificando-os como infrações contra sistemas e dados informáticos (Capítulo II, Título 1), infrações relacionadas com computadores (Capítulo II, Título 2), infrações relacionadas com o conteúdo,pornografia infantil (Capítulo II, Título 3), infrações relacionadas com a violação de direitos autorais (Capítulo II, Título 4).

Com relação às matérias do Direito Processual, trata de: âmbito das disposições processuais, condições e salvaguardas, conservação expedita de dados informáticos armazenados, injunção,busca e apreensão de dados informáticos armazenados, recolha em tempo real de dados informáticos e interceptação de dados relativos ao conteúdo.

Nesse sentido, a Convenção mencionada, eminentemente flexível e respeitosa à soberania dos Estados Parte, incumbe-os, consoante explicitado, de estabelecer leis internas de combate ao cibercrime, recomendando que as infrações tipificadas relacionem-se a condutas em que se rompam, intencionalmente, medidas de segurança, com vistas à usurpação de dados, instituindo,assim, o elemento subjetivo do dolo específico, o qual restringe a abrangência do tipo penal. Ao contrário, o PLS em questão impõe tal prática como infração indiscriminadamente, sem definir,como ressalta Corrêa(2008), se a modalidade do tipo seria dolosa ou não, recaindo em imprecisão legislativa e podendo criminalizar muitos usuários honestos.

O Tratado de Budapeste - "*ConventiononCybercrime*", de 2001, foi assinado por 46 países. O Brasil não é signatário, e apesar de existirem leis específicas sobre assuntos correlatos (pirataria, invasão de bancos de dados do governo, lei geral das telecomunicações etc.), até o momento, o projeto mais importante, PL 84/99, continua em trâmite e sem previsão de virar lei.

Outro desafio para proteger a privacidade no mundo virtual é que a internet é global e a lei, brasileira. De acordo com Patrícia Peck *apud* SCHIAVON (2009), se um site internacional, que não possui representação ou servidor no Brasil, ofender um internauta de alguma maneira e se recusar a tirar a informação do ar, o juiz pode emitir uma carta rogatória — que possibilita ações entre os Judiciários de diferentes países. No entanto, isso gera um ônus de tempo que nem sempre a vítima está disposta a pagar e acaba não fazendo nada.

As ações internacionais são complicadas, mas são possíveis. Os sites ditos 'internacionais' devem saber que a exposição mundial gera um custo que é a possibilidade de responsabilização perante diversos ordenamentos jurídicos. Os termos de uso e de privacidade dos sites são como qualquer contrato de adesão. Tratando-se de relação de consumo, prevalece a hipossuficiência do consumidor e a aplicação da Lei 8.078/90.

3.1 **Do furto**

Muitos dos crimes de furto são cometidos por hackers e crackers, que invadem computadores alheios sem autorização, obtém inicialmente informações e senhas pessoais, para, então praticarem transferência ilegal de fundos de uma conta bancária para outra, compras indevidas realizadas por meio do cartão de crédito, clonagem de página pessoal de site de relacionamento, cópia ilícita de dados e programas etc.

Corrêa suscita que:

> Mais preocupante é saber que os mesmos artifícios utilizados por hackers para ocultar material pedófilo ou pornográfico em sistemas externos sem deixar vestígios podem ser usados para ‘furtar’ espaço em disco, por meio de arquivos ocultos e mascarados.(CORRÊA, 2008, P.45)

Conforme já explanado, na ausência de legislação específica, ocorre o enquadramento nos crimes já tipificados no nosso Código Penal. Temos nesse último, em seu artigo 155, *caput*, que furto é “subtrair para si ou para outrem, coisa alheia móvel”; com pena de 1 a 4 anos de reclusão e multa.

O Direito Penal tutela prioritariamente a posse, e de forma secundária, a propriedade. A perda do bem atinge não só o proprietário, que muitas vezes possui apenas a posse indireta, mas aquele que tem a posse direta do bem furtado.

Afirma Bitencourt (2010, p. 32) que a propriedade constitui “o direito complexo de usar, gozar e dispor de seus bens _ *jus utendi, fruendiet abutendi*”; enquanto a posse é a relação de fato estabelecida entre o indivíduo e a coisa, pelo fim de sua utilização econômica.

A necessidade de proteção do judiciário não pode basear toda e qualquer pretensão, e penalmente, não autoriza interpretação extensiva para admitir a tipificação de condutas que não encontram correspondência típica em nenhum dispositivo penal, devendo assim, nesse caso, o sujeito com legitimidade ativa, procurar amparo no âmbito cível.

O sujeito ativo do crime de furto pode ser qualquer pessoa, exceto o proprietário, mediante o fato de que o elemento normativo requer que a coisa seja alheia, não se enquadrando a proprietário, posto que para este, a coisa é própria. “Sujeitos passivos são o proprietário, o possuidor e, eventualmente, até mesmo o detentor da coisa alheia móvel, desde que tenha algum interesse legítimo sobre a coisa subtraída” (BITENCOURT, 2010, p. 33). Ambos sofrerão dano e sentir-se-ão lesados com a perda da coisa.

No tocante á adequação típica, para a ocorrência do crime, deve haver subtração da coisa. Subtrair significa tirar, retirar; desta feita, afirma Bitencourt (2010, p. 33) que “subtrair não é a simples retirada da coisa do lugar em que se encontrava; é necessário, a *posteriori*, sujeitá-la ao poder de disposição do agente”; de forma que, deve haver por parte do agente o *animus* definitivo de possuir o bem ou entregá-lo à possessão de um terceiro.

Coisa, para fins penais, é todo e qualquer objeto passível da ação de subtração, de deslocamento, remoção, apreensão ou transporte de um lugar para o outro. Conforme Capez (2010, p.427), coisas imóveis não podem ser objeto do delito de furto, especialmente por meio eletrônico, pois faltará ao agente a possibilidade de transporte e assenhoramento do bem. Bitencourt (2010, p. 34) faz pertinente observação concernente ao fato de que eventual intangibilidade da coisa não gera afastamento de sua idoneidade para ser objeto de subtração.

A condição de ser alheia a *res furtiva* é elemento normativo exigido para a tipificação do crime em questão, do contrário, a conduta será atípica. É importante a ocorrência de efetiva diminuição do patrimônio alheio. Além disso, é necessário que o agente subtraia a coisa para si ou para outrem. Pressupõe dissenso da vítima.

O crime de furto consuma-se com a retirada da coisa da esfera de disponibilidade da vítima, de modo que esta não tenha meios para exercer os atos relativos à posse. Com base nisso, pode ser suscitado o seguinte

questionamento: a simples colheita dos dados da vítima, como por exemplo, uma senha de home banking, que não é retirada da posse daquela, será considerada furto?

Enquadrando a situação de o agente obter a senha da vítima dentro do tipo penal, não poderemos afirmar a ocorrência de furto, posto que, apesar de constituir coisa alheia móvel, não há a subtração, mas apenas a cópia da coisa, e em regra, a vítima continua com a posse da senha.

Na opinião de Siqueira (2011) por tratar-se de ambiente virtual, há inversão da posse, entretanto, esta ocorre dentro de poucos segundos. Acrescenta ainda:

> A informação da senha autoriza a entrada virtual a sua conta corrente. O momento em que o agente captura sua senha por um programa no ciberespaço e realiza a subtração sucessiva de dinheiro, configura o furto porque a informação foi o meio para alcançar o dinheiro, então, a informação sigilosa e personalíssima reveste-se de valor, então, é passível de ser furtada.(SIQUEIRA, 2011)

Nesse mesmo sentido, Capezdemonstra:

> É indispensável que o agente tenha a intenção de possuí-la, submetendo-a ao seu poder, isto é, de não devolver o bem de forma alguma. Assim, se ele o subtrai apenas para uso transitório e depois o devolve no mesmo estado, não haverá a configuração do tipo penal. Cuida-se na hipótese de mero furto de uso, que não constitui crime[...]. (Capez, 2010, p.429)

O furto será duplamente qualificado na maioria dos delitos cibernéticos, uma vez que, incidem duas qualificadoras no delito, quais sejam o rompimento de obstáculo à subtração da coisa, e abuso de confiança, ou mediante fraude ou destreza (artigo 155, § 2º, I e II, Código Penal). O obstáculo seria a senha, que é rompida por trojans e crackers; configura o inciso II, o uso de sites ou propagandas aparentemente confiáveis, que, quando acessados, permitem obtenção do banco de dados da vítima.

3.2 **Da extorsão**

Ocorreu em João Pessoa, estado da Paraíba, o caso de um menino de 11 (onze anos) que costumava ficar nas redes sociais conversando. Um certo indivíduo, fazendo passar-se por uma menina da idade daquele_

após algumas conversas_ convenceu-o a mostrar seu corpo por meio da webcan.

Conseguido seu intento, revelou ao menino que era um adulto e que, caso aquele não conseguisse R$ 10.000,00 (dez mil reais) com seu pai, suas imagens seriam divulgadas na internet, passando assim, à ameaça psicológica.

O pai do garoto contatou os policiais de João Pessoa que, fazendo as vezes do menino, conversaram com o extorsionário, negociaram e combinaram local e data para entrega do valor requerido, que deveria ser entregue pelo próprio garoto; ocasião na qual, foi preso por policiais sem fardamento, que circulavam no ambiente combinado: o Manaíra Shopping. (Este caso foi relatado verbalmente pelo coronel João da Matta Medeiros Neto no“I Seminário Internacional De Análises Criminais:Crimes Sexuais Contra Vulneráveis”, realizado no auditório da Justiça Federal da cidade campina Grande-PB nos dias 31 de agosto e 01 e 02 de setembro de 2011).

O caso relatado acima é apenas um dos vários casos de extorsão ocorridos por meio da internet, que tem feito muitas vítimas em todo o mundo. O Código Penal Brasileiro em seu artigo 158, *caput*, refere-se à extorsão como o ato de “constranger alguém, mediante violência ou grave ameaça, e com o intuito de obter para si ou para outrem indevida vantagem econômica, a fazer, tolerar que se faça ou deixar de fazer alguma coisa: pena- reclusão, de quatro a dez anos, e multa”.

A extorsão tutela prioritariamente o patrimônio e secundariamente, a vida, a integridade física, a tranquilidade e a liberdade pessoal. Nesse tipo de delito, o agente visa auferir vantagem patrimonial, utilizando-se como meio para tanto, a violência ou grave ameaça à pessoa.

O sujeito ativo do crime em comento é aquele que constrange a vítima a agir ativa ou passivamente contribuindo para que aquele realize seu intento em obter vantagem econômica ilícita. O sujeito passivo também pode ser qualquer pessoa, inclusive pessoa diversa da que sofre a perda patrimonial, pois uma das vítimas pode sofrer a violência ou ameaça, e outra, o dano patrimonial, havendo, no caso, dois sujeitos passivos.

Diferentemente do furto, que tem como objeto coisas móveis, podem ser objeto do delito da extorsão tanto bens móveis quanto imóveis. Capez (2010, p.489) assegura que “o agente pode obrigar a vítima a assinar uma escritura pública, por meio da qual ela lhe transfere uma propriedade imóvel”.

O verbo constranger constitui a ação nuclear do tipo, e pode significar coagir, compelir com força, sujeitar, entre outros. Os meios deconstrangimento citados na lei são o uso de violência ou grave ameaça, direcionada ao titular do patrimônio ou pessoa ligada a ele (por exemplo, filhos, pai, mãe etc.), tal como no caso supracitado. “A ameaça é o meio mais comum utilizado pelo agente para constranger a vítima a agir ou se abster de determinado comportamento” (CAPEZ, 2010, p.490). Ela (a ameaça) pode ser física ou psicológica, contudo, em meio virtual se dará da segunda forma, mediante a impossibilidade da primeira.

O elemento subjetivo é o dolo de constranger outrem, utilizando-se da violência ou grave ameaça para que faça, tolere que se faça ou deixe de fazer alguma coisa; além disso, exige o tipo penal o fim especial de agir no intuito de o agente obter vantagem econômica.

Para a consumação da extorsão, não é necessário que o agente obtenha a vantagem econômica indevida, mas que consiga constranger a vítima utilizando-se da violência ou ameaça. Nesse sentido, é o entendimento do Superior Tribunal de Justiça em sua súmula 96: “O crime de extorsão consuma-se independentemente de obtenção da vantagem indevida”.

A tentativa é possível na medida em que o meio coativo empregado seja idôneo a intimidar, a constranger a vítima, mesmo que esta não venha a realizar o intento do agente por circunstâncias alheias à vontade do mesmo. Não será considerada a tentativa, caso o meio empregado pelo agente não seja idôneo.

As causas especiais de aumento, a extorsão qualificada e a extorsão mediante sequestro não são cabíveis pela impossibilidade do meio. A extorsão distingue-se do constrangimento ilegal porque nela há a finalidade especial do agente consubstanciada no dolo de auferir vantagem econômica indevida.

Também cumpre destacar a diferença entre extorsão e estelionato, que reside no fato de que na extorsão a entrega da coisa se dá mediante o emprego de violência ou grave ameaça; enquanto no estelionato, a entrega do bem se dá em virtude de fraude empregada pelo agente que leva a vítima a entregar o bem voluntariamente.

3.3 **Do dano**

Podemos citar como crimes de dano a sabotagem de computador, destruição de sites, adulteração de dados em sistema de informações,o e-mail bombing, e-mail contaminado por vírus, spam, entre outros.

O direito civil resolve a questão dos danos por intermédio da responsabilidade civil; o direito penal comina sanção ao agente causador do dano. Aduz o artigo 163 do Código Penal referente ao dano: “destruir, inutilizar ou deteriorar coisa alheia: pena- detenção, de um a seis meses, ou multa”.

O art. 163 considera crime de dano a destruição, inutilização ou deterioração de coisa alheia. Ora, um arquivo de dados armazenado no computador e que o vírus destrói, trata-se de coisa, restando configurado o crime.

Sujeito ativo trata-se daquele que destrói, inutiliza ou deteriora a coisa. “Só pode ser pessoa física, exceto o proprietário, uma vez que o tipo penal exige que a coisa seja alheia”(Capez, 2010, p.526). O sujeito passivo é o proprietário da coisa danificada, como também o possuidor, afirma Bitencourt que o elemento normativo ‘alheia’ significa tanto a coisa que pertence a outrem como a que se encontra na posse de terceiro.

‘Destruir’ dá a ideia de exterminar, desfazer, demolir; ‘inutilizar’ torna a coisa inútil, inservível, inadequada à sua finalidade; ‘deteriorar’ reduz o valor da coisa, e configuram as ações nucleares o tipo penal. Afirma Capez (2010, p.526) que o dano pode ser praticado tanto por ação quanto por omissão; e que os meios de execução podem ser imediatos ou mediatos. Para que seja configurando o dano, não é necessário que seja total, podendo também ser parcial.

Há divergência na doutrina quanto à exigência ou não do *animus nocendi*, isto é, do dolo, quanto à configuração do delito em comento. Capez (2010, p.527) cita o exemplo de Nelson Hungria para justificar a necessidade da presença do dolo, que se refere ao caso de um amigo que causa um dano ao outro por brincadeira, não podendo, assim, ser considerado agente do crime de dano. Para Damásio de Jesus, Magalhães Noronha e Capez (2010, p.527), não é exigível o fim especial de causar prejuízo ao ofendido, pois a figura penal não faz referência expressa a nenhum elemento subjetivo do tipo.

3.4 **Do estelionato**

Alguns dos casos mais comuns de estelionato englobam a fraude em sistemas financeiros (home banking); uso ilegal de sistemas; criação de

empresas virtuais falsas; inserção de dados falsos em sistema de informações; uso de dados de outras pessoas.

Outro exemplo é o caso do indivíduo que tem problemas na internet e recorre a um atendimento virtual de suporte ao usuário ou em uma sala de chat, onde um hacker invade o sistema da empresa e simula o atendimento para tanto obtendo acesso ao dado.

Para acautelar-se, o internauta nunca deve fornecer tais dados ou acesso aos mesmos, pois, toda empresa séria tem como política mercadológica ética não requerer aos clientes o fornecimento virtual de senhas a atendentes, o que ocorre atualmente em algumas salas de chat.

O estelionato encontra-se encartado no artigo 171 e ss. do Código Penal, que prevê: “Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento: Pena _ reclusão, de um a cinco anos, e multa.”

Tanto o sujeito ativo quanto o sujeito passivo do crime de estelionato, pode ser qualquer pessoa, não se exigindo nenhuma condição especial. Bitencourt (2010, p. 267) afirma que pode haver dois sujeitos passivos, quando a pessoa enganada for diversa da que sofre o prejuízo e cita o exemplo de um empregado que sofre uma fraude, mas seu empregador é quem suportará o prejuízo.

É importante ressaltar que o bem jurídico protegido é o patrimônio, de forma que o sujeito passivo é quem sofre a lesão patrimonial, embora a fraude e a lesão nem sempre recaiam sobre a mesma pessoa, conforme resta demonstrado. Nessa esteira, é que Paulo José da Costa Jr. apud Bitencourt explica:

> No estelionato, há dupla relação causal: primeiro, a vítima é enganada mediante fraude, sendo esta a causa e o engano o efeito; segundo, nova relação causal entre o erro, como causa, e a obtenção de vantagem ilícita e o respectivo prejuízo, como efeito.(Bitencourt, 2010, p. 270)

Para a tipificação do crime de estelionato, é indispensável a existência da fraude, quando um sujeito ativo induz um sujeito passivo a erro. Para tanto, este deve possuir discernimento, do contrário, não será enganado; como no caso de criança e deficientes mentais que não possuírem capacidade de entender, levando à impropriedade absoluta do objeto.

Segundo Bitencourt (2010, p. 268), se a vítima não possuir capacidade de autodeterminação, como a criança e o débil mental, o delito será abuso de incapaz, presente no artigo 173 do Código Penal.

A descrição do fato típico requer a obtenção de vantagem ilícita, em prejuízo alheio, que é alcançada por meio de artifício, ardil ou outro meio fraudulento de forma a induzir ou manter a vítima em erro; o legislador deixa claro que a vantagem indevida pode ser para si ou para outrem.

No estelionato a entrega da coisa é voluntária pelo agente, por via do meio obtuso que eiva de vícios à vontade da vítima. No ciberespaço, a indução a erro se dá no sistema que tutela a integridade e sigilo dos dados ali inseridos, que concede o acesso aos dados. Há a manipulação de um comando que normalmente autorizaria os titulares do mesmo a este acessar. Em nenhum momento, foi voluntária a entrega da vantagem, que se torna ilícita. O emprego de um meio ilícito é necessário para desviar a atenção da proteção que a informática concedeu ao documento, induzindo-o a erro e indiretamente atingindo a pessoa.

Consuma-se o estelionato no momento em que o agente obtém a vantagem indevida, ressaltando que essa vantagem deve ser decorrente do erro produzido pelo agente e deve resultar em prejuízo patrimonial alheio. Bitencourt (2010, p. 278) destaca que “não se pode falar em consumação sem a presença do binômio *proveito ilícito- prejuízo alheio*”.

4 Características gerais e aspectos de enfrentamento destas modalidades de crime

Diferentemente dos crimes que decorrem de um encontro “físico” e pessoal entre o agente de um crime e sua vítima, no crime informático, a vítima não vê um rosto, não sabe dizer o local do fato delituoso, e, muitas vezes até, nem percebe que foi vítimade uma fraude ou sofreu um dano em seu computador.

É possível que decorra um lapso temporal do momento em que um agente tome conhecimento de dados da vítima até o momento em que se utiliza desses dados para furtar, por exemplo, valores de sua conta. Da mesma forma, um indivíduo pode sofrer danos na sua conta de e-mail, e não associá-los a um cracker. Essas situações citadas são exemplos de motivos que levam as vítimas dos cibercrimes a não prestarem a *notitia criminis*. Além de serem

situações que dificultam os investigadores à busca da autoria delitiva; a passagem do tempo também faz com que vestígios e possíveis provas sejam perdidas ou alteradas, visto sua efemeridade.

Esses mesmos fatores levam Côrrea a afirmar:

> O grande problema relacionado aos crimes digitais é a quase-ausência de evidências que provem contra o autor, a inexistência da arma no local do crime. Uma gloriosa invasão a sistema alheio não deixaria nenhum vestígio, arquivos seriam alterados e copiados, e nenhum dano seria prontamente identificado.(Côrrea, 2008, p. 73 e 74)

Os registros dos usuários conectados à rede são mantidos pelos provedores, gozam de proteção à privacidade e ao sigilo das comunicações; só podem ser requeridos pela autoridade judicial competente. Geralmente, a testemunha do crime cometido pela internet é aquele que detém os protocolos IP, posto que é responsável pelo armazenamento dos dados sobre as transações ocorridas eletronicamente.

É possível encontrar a autoria de diversos delitos praticados por meio eletrônico, utilizando de técnicas de investigação adequadas à realidade digital.

Em razão de o sistema processual brasileiro permitir provas não especificadas em lei, é possível admitir o documento eletrônico para tal fim; entretanto, muitas vezes não são bem aceitas por serem vistas como facilmente adulteráveis, mediante a possibilidade de sua alteração e reprodução.

5 **CONCLUSÃO**

Um dos fatores que contribuem para a ocorrência dos crimes eletrônicos é a crença da impunidade, é a ideia de que aquele ilícito praticado não constitui um crime real ou algo tão grave como se fosse “ao vivo”, portanto não será tratado como tal.

Em diversas páginas da internet, estão disponibilizadas informações sobre como evitar cair em uma fraude eletrônica, cuidados a serem tomados no acesso à internet e cuidados quanto à divulgação de informações pessoais, principalmente em sites de relacionamentos; mas dada

a falta de interesse por parte dos usuários e a correria da vida moderna, a grande maioria dos internautas arriscam-se no mundo virtual sem um mínimo de informações ou segurança necessárias, ficando vulneráveis à criatividade de pessoas mal intencionadas.

Dentre as organizações que trabalham acerca da segurança na internet, podemos citar o Comitê Gestor de Internet no Brasil (http://www.cgi.br/), que se tornou referência neste quesito e disponibiliza em seu site, vídeos e cartilhas com informações e procedimentos à segurança dos usuários de internet, assim como a SaferNet(http://www.safernet.org.br), que, em parceria com a Polícia Federal possui informações sobre navegação segura, disponibiliza um canal para denúncias sobre crimes de internet.

Em que pese a latente necessidade da legislação penal específica para os crimes praticados pela Internet, o nosso Código Penal de 1940 e as leis penais posteriores, possuem plenas condições de serem aplicadas, uma vez que a Internet é apenas um novo meio, um novo veículo. Entre os crimes que ocorrem no computador e os que ocorrem fora dele, o que muda é o *modus operandi* do criminoso, ou seja, o modo de execução do crime. Por exemplo, há a substituição da arma de fogo pelo click do mouse.

Um grande problema encontra-se na crença de que somente criminalizando condutas é que se pode reprimí-las, o que evidentemente é um erro. Na verdade, são necessárias práticas que coíbam a conduta delituosa, a utilização dos meios técnicos adequados para a construção de provas contundentes, além da efetividade na aplicação das normas.

A ausência de uma lei específica não pode avalizar o "anarquismo virtual".Apesar de a maior bandeira da globalização e do avanço tecnológico estar fincado na Internet, é nela que se vislumbra, um terreno convidativo para a prática de delitos e fraudes. Controlar a Internet passou a ser uma necessidade social e é no Direito e na Justiça que podemos encontrar a melhor forma de controle do mundo virtual, que aflora e cresce a passos largos.

ABSTRACT

Thisassignment analyzesthe problem of howthe law hasprotectedthe legalheritagein the crimes committedby electronic means,putthat in Brazilthere is nospecific legislationconcerningthe commission of suchoffense.The methodwasused for boththe researchliterature, with areview of the literatureabout theimpact ofcybercrimein Brazilian law.Itsscopeanalyze thistype of crime; comment on thegeneral characteristicsand aspectsof coping,as well asdefiningelectronic crimes, cansynthesize themlike anytypical action, and culpableantilegalthat iscommitted orprovided throughelectronic meansand /or internet.Thistypicalityis analyzedwith a focus onapplication ofthepenal codecriminal practicesbythe lack ofspecific legislation.Through the study, it was noted that among thedifficulties ofcombatingsuchcrimes, we can highlight the lack ofcomplaints, identification of authorship, harvesting and storage of evidence,and how theywillclaimthepunitive state. We conclude thatdespite the lack ofspecific criminal legislation, our Criminal Codeand thesubsequentcriminal laws,arefully capableof beingapplied, since the Internet is justanew mediumfor thecriminal actandwhat we needinindeed, it isof effective practicesto combatcybercrime.

KEYWORDS: Cybercrime.Right.Property.Criminal Code.

6 REFERÊNCIAS BIBLIOGRÁFICAS

AZEREDO, Eduardo. Uma lei para combater delitos digitais. Revista Jurídica Consulex. Ano XV, Nº 343, 1º de maio de 2011, p. 29.

BITENCOURT, Cezar Roberto. Tratado de Direito Penal: Parte especial, vol. 3. 6ª Ed. São Paulo: Saraiva, 2010.

BLUM, R. O. Crimes eletrônicos: o impacto da futura lei sobre os processos e mecanismos digitais. Fecomercio, 2011. Disponível em: <http://www.opiceblum.com.br/download/Fecomercio_CrimesEletronicos-renatoopiceblum.pdf>. Acesso em: 12 de março de 2011.

BRASIL. Código Penal. In: PINTO, A. L. de T.; WINDT, M.C.V.S.; CÉSPEDES, L. VADE MECUM. 3ª ed. São Paulo: Saraiva, 2010.

BRASIL. Constituição da República Federativa do Brasil. In: PINTO, A. L. de T.; WINDT, M.C.V.S.; CÉSPEDES, L. VADE MECUM. 3ª ed. São Paulo: Saraiva, 2010.

CAPEZ, Fernando. Curso de Direito Penal- Parte especial. Vol.2. São Paulo: Saraiva, 2008.

CARPANEZ, J. Piratas dão prejuízo recorde de R$ 300 mi a bancos. São Paulo: Folha online, 07 de janeiro de 2006. Disponível em :<http://www1.folha.uol.com.br/folha/informatica/ult124u19449.shtml>. Acesso em: 09 de fevereiro de 2011.

CLEMENTINO, E. B. Processo Judicial Eletrônico. 1ª Ed. Curitiba: Juruá, 2007.

Centro de Estudos, Resposta e Tratamento de Incidentes no Brasil. Incidentes Reportados ao CERT.br. <http://www.cert.br/stats/incidentes/2011-apr-jun/fraude.html>. Acesso em: 12/08/2001.

CORRÊA, Gustavo testa. Aspectos jurídicos da internet. 4ª Ed. Saõ Pulo: saraiva, 2008.

COSTA, M. A. S. L. Computação Forense.3ª ed. Campinas, SP: Millennium Editora, 2011.

D'URSO, Luiz F. Borges. As múltiplas faces dos crimes eletrônicos e dos fenômenos tecnológicos e seus reflexos no mundo jurídico. São Paulo, 2009. Disponível em :<http://pt.scribd.com/doc/24156044/I-Livro-sobre-Crimes-Eletronicos-da-OAB-SP>. Acesso em: 11 de fevereiro de 2011.

GRECO FILHO, Vicente. Direito Processual Civil Brasileiro. 14 ed. São Paulo: Saraiva, 2000.

_____. Direito Processual Civil Brasileiro. Vol. 2. 20 ed. São Paulo: Saraiva, 2009.

LORENZENTTI, R. L. Comércio Eletrônico. São Paulo: Ed. Revista dos Tribunais, 2004.

LUNA FILHO, Eury Pereira. Internet no Brasil e o Direito no ciberespaço. Jus Navigandi, Teresina, ano 4, n. 32, 1 jun. 1999. Disponível em: <http://jus.com.br/revista/texto/1773>. Acesso em: 23 set. 2011.

MIRABETE, Julio Fabbrini. Manual de Direito Penal.vol.II; 17ª Ed. São Paulo: Altas; 2002.

MONTENEGRO FILHO, Misael. Curso de Direito Processual Civil- Teoria Geral do Processo de Conhecimento. 4ª Ed. São Paulo: Ed.Atlas S.A., 2008.

NEVES, Michel Weiler. Crimes eletrônicos: a responsabilidade do usuário. SafernetBrasil, 2009. Disponível em: <http://www.safernet.org.br/site/noticias/crimes-eletr%C3%B4nicos-responsabilidade-usu%C3%A1rio>. Acesso em: 01 de outubro de 2011.

OTONI, M. B. Certificação Digital *in* Manual de Direito Eletrônico e Internet. Coordenadores BLUM, R. M. S. O.; BRUNO, M. G. S.; ABRUSIO, J. C. 1ª ED. SãoPaulo: Ed. Lex, 2006, p. 245.

PINHEIRO, Patrícia Peck. Direito Digital. 3ª Ed. São Paulo: Saraiva, 2009.

QUEIROZ, Claudemir; VARGAS, Raffael. Investigação e Perícia Forense Computacional- Certificações, leis processuais, estudos de caso. Rio de Janeiro: Brasport, 2010.

ROCHA, M. L.Direito da Informática, Legislação e Deontologia. Lisboa: ed. Cosmos,1994.

SCHIAVON, Fabiana. Crimes eletrônicos deixam rastros que ajudam punição. Revista Consultor Jurídico, 25 de julho de 2009. Disponível em: <http://www.conjur.com.br/2009-jul-25/identificar-autores-crimes-eletronicos-cada-vez-possivel>. Acesso em: 15 de agosto de 2011.

SILVA, Remy Gama. Crimes de Informática. CopyMarket.com, 2000.

SIQUEIRA, Flávio Augusto MarettiSgrilli. Furto, supressão de dados sigilosos consignados em sites na internet de acesso restrito e o estelionato virtual. Revista Jus Vigilantibus, Domingo, 21 de setembro de 2003. Disponível em: <http://jusvi.com/artigos/500>. Acessoem: 20 de outubro de 2011.