UNIVERSIDADE FEDERAL DE CAMPINA GRANDE
CENTRO DE CIÊNCIAS JURÍDICAS E SOCIAIS
UNIDADE ACADÊMICA DE DIREITO
CURSO DE CIÊNCIAS JURÍDICAS E SOCIAIS

PRISCILA MILENA ALBUQUERQUE DE MOURA CAVALCANTI

A TUTELA JURÍDICO-PENAL DA PRIVACIDADE NA INTERNET

SOUSA - PB
2009

PRISCILA MILENA ALBUQUERQUE DE MOURA CAVALCANTI

A TUTELA JURÍDICO-PENAL DA PRIVACIDADE NA INTERNET

Monografia apresentada ao Curso de Ciências Jurídicas e Sociais do CCJS da Universidade Federal de Campina Grande, como requisito parcial para obtenção do título de Bacharela em Ciências Jurídicas e Sociais.

Orientadora: Professora Esp. Danielle da Rocha Cruz.

SOUSA - PB
2009

PRISCILA MILENA ALBUQUERQUE DE MOURA CAVALCANTI

A TUTELA JURÍDICO-PENAL DA PRIVACIDADE NA INTERNET

Trabalho monográfico apresentado ao curso de Direito do Centro de Ciências Jurídicas e Sociais da Universidade Federal de Campina Grande, como exigência parcial da obtenção do título de Bacharel em Ciências Jurídicas e Sociais.

Orientador (a): Profª. Msc. Danielle da Rocha Cruz

Banca Examinadora: Data de aprovação:_____

_____

Profª. Msc. Danielle da Rocha Cruz
Orientadora

_____

Examinador(a) interno

_____

Examinador(a) externo

Aos meus pais.

As minhas irmãs.

Aos meus amigos.

AGRADECIMENTOS

Agradeço a Deus, por ter me amparado todos esses dias de caminhada.

Aos meus pais, por tudo que fizeram e ainda fazem por mim.

As minhas irmãs, que estão sempre comigo nos momentos de tristeza e de alegria. Em especial a minha irmã Lenira, que dividiu comigo todas as etapas da graduação, sempre com cumplicidade. Sem ela eu não teria conseguido chegar até aqui.

Ao meu amigo José Carlos, companheiro sempre presente nesta longa jornada, que quero levar para sempre comigo. Tenho-o como um verdadeiro irmão.

A minha amiga Lorenna, por toda a ajuda, companheirismo e amizade ao longo desses cinco anos.

A minha orientadora Danielle, por ter me orientado com dedicação e colaborado para a realização deste trabalho.

Por fim, agradeço a todos aqueles que torceram por mim e contribuíram de alguma maneira para a minha formação acadêmica.

"E aqueles que foram vistos dançando, foram julgados insanos por aqueles que não podiam escutar a música".

Nietzsche

RESUMO

O progresso da informática tem provocado grandes transformações na sociedade. As pessoas utilizam o computador todos os dias para alcançar as mais variadas tarefas e seu uso já se tornou essencial para a realização de alguns serviços. Essa nova realidade, a de uma sociedade informatizada, trouxe profundas modificações nas relações humanas. Atualmente, através da internet, podem-se praticar atividades como compra e venda de diversos produtos, transações bancárias ou comunicação instantânea. Inúmeros são os benefícios que a internet originou para a humanidade, no entanto algumas conseqüências negativas do seu uso também surgiram, tais como os chamados crimes informáticos. Os autores desses delitos usam da facilidade que a internet proporciona para cometer diversos crimes, os quais podem causar enormes prejuízos para suas vítimas. Dentre os delitos cometidos através da internet, os que infringem o direito à privacidade constituem um dos mais danosos à humanidade. São exemplos desses últimos, os crimes que violam a correspondência eletrônica das pessoas. Desse modo, pretende-se demonstrar o perigo que esses delitos geram para os indivíduos e a necessidade de uma regulamentação específica para a matéria. O presente trabalho utiliza-se dos métodos dedutivo e exegético-jurídico para analisar as alterações que os crimes de internet produziram na sociedade. Emprega-se também a técnica de pesquisa bibliográfica, que possibilita um melhor desenvolvimento dos assuntos discutidos. Os crimes cometidos no ambiente informático, especialmente aqueles que violam a privacidade dos cidadãos, devem ser vistos com atenção pela sociedade e pelo Poder Público. Este último deve contribuir para a diminuição dos delitos da internet através da produção de normas específicas e da informação as pessoas.

Palavras-chave: Crimes informáticos. Privacidade. Correspondência eletrônica.

ABSTRACT

The progress of computer science has provoked great transformations in the society. The people use the computer every day to reach the most varied tasks and its use already if she became essential for the accomplishment of some services. This new reality, of a computerized society, brought deep modifications in the relations human beings. Currently, through the Internet, activities can be practised as purchase and sale of diverse products, banking transactions or instantaneous communication. Innumerable they are the benefits that the Internet originated for the humanity, however some negative consequences of its use had also appeared, such as the cyber crimes. The authors of these delicts use of the easiness that the Internet provides to commit diverse crimes, which can cause enormous damages for its victims. Amongst the delicts committed through the Internet, the ones that they infringe the right to the privacy constitute one of the harmful to the humanity. They are examples of these last ones, the crimes that violate the correspondence electronic of the people. In this manner, It is intended to demonstrate the danger that these delicts generate for the individuals and the necessity of a specific regulation for the subject. The present work is used of the methods deductive and legal-exegetic to analyze the alterations that the internet crimes had produced in the society. The technique of bibliographical research is also employed, that makes possible one better development of the argued subjects. The crimes committed in the cyber environment, especially those that they violate to the privacy of the citizens, must be seen with attention for the society and the Public Power. This last one must contribute for the reduction of the internet delicts through the production of specific norms and of the information to the people.

Key-words: Digital crimes. Privacy. Electronic correspondence.

SUMÁRIO

1 INTRODUÇÃO

As profundas modificações que a humanidade vem conhecendo são decorrências do progresso por ela experimentado, intensificado no decorrer das últimas décadas. Novas invenções surgem a todo o momento em diversas áreas, provocando uma alteração na forma dos indivíduos relacionarem-se.

A internet é produto dos avanços da tecnologia e sua utilização tem provocado grandes transformações nas relações sociais e jurídicas. Sua criação na década de sessenta tinha como objetivo a proteção militar dos sistemas informáticos dos Estados. Após alguns anos, perceberam-se as vantagens que sua adaptação para a forma comercial proporcionaria. Desde então, a internet vem sendo utilizada por particulares e empresas para a realização das mais diversas atividades.

A facilidade que a internet proporciona, permitindo um intenso fluxo de dados que podem ser transmitidos em fração de segundos e diminuindo significativamente o tempo gasto na realização de tarefas, motiva cada dia mais pessoas a utilizá-la. Cada sujeito busca no ambiente informático diferentes interesses, tais como a realização de transações bancárias, compras, pesquisas, envio de mensagem eletrônica ou outros dos diversos serviços que ele proporciona.

A internet estimula o progresso da sociedade através do crescimento do número de transações comerciais e da diminuição da distância entre os indivíduos. Os inúmeros benefícios que o meio virtual gera são conhecidos pela maioria da população.

No entanto, os indivíduos desconhecem os perigos que esse mesmo meio acarreta aos que o utilizam. A intensificação do uso da internet pelos particulares traz consigo alguns malefícios, aos quais todos devem estar atentos. Determinadas pessoas aproveitam-se das facilidades do ambiente informático para a prática de atividades criminosas que podem gerar danos irreparáveis.

O crime cometido no ambiente virtual não conhece fronteiras, desse modo, o espaço físico não é um empecilho para a sua produção. Na maioria das vezes, esses delitos são de difícil identificação, fato que dificulta a punição dos criminosos. Alguns fatores obstam ainda mais a efetivação dessa punição, tais como: a falta de legislação específica nos países, a inexistência de técnicas investigativas especiais,

bem como a não integração entre as nações para o combate a criminalidade informática.

Dentre a variedade de crimes informáticos existentes um grupo merece destaque pela forma com que são praticados, bem como por sua lesividade, são os delitos que infringem o direito à privacidade. Tal direito, constitucionalmente previsto vem sendo alvo de ataques freqüentes pelos criminosos, principalmente com o auxílio da internet.

Este trabalho tem como objetivo principal estudar os crimes cometidos no meio informático com violação da privacidade das pessoas e suas peculiaridades, bem como alertar os indivíduos sobre os delitos mencionados. Além de almejar também demonstrar a insuficiência de legislação especial, sugerindo a necessidade de aprovação de normas que regulem o ambiente virtual.

Diante do exposto, destaca-se a importância desse estudo, pois a internet não pode ser considerada um local a margem do ordenamento jurídico. Ela deve ser objeto de regulamentação pelo Direito, haja vista que proporciona a efetuação de um grande número de relações diariamente. Destaca-se também a relevância do tema que irá aprofundar o estudo da proteção à privacidade no ordenamento jurídico pátrio.

Para a realização do presente trabalho será utilizado o método dedutivo, pois se buscará sempre analisar os ensinamentos e a legislação de maneira geral, para, então, se considerar os casos específicos, quais sejam os delitos informáticos que violam o direito à privacidade. Dessa maneira, será possível uma melhor avaliação desses comportamentos lesivos ao longo do estudo.

Neste estudo, será utilizado também o método exegético-jurídico, baseando-se sempre em consultas à doutrina, à jurisprudência pátria, bem como à legislação estrangeira e brasileira para melhor efetuar a análise dos assuntos propostos, possibilitando uma exposição segura da temática escolhida.

Para a produção do trabalho, será empregada a técnica de pesquisa indireta, efetivada através de consulta bibliográfica, destacando-se a utilização de livros, periódicos e artigos científicos a respeito do tema. Essa forma de pesquisa proporcionará uma vasta fonte de material a respeito dos tópicos que serão apresentados.

Destaca-se que o pressente trabalho será composto de três capítulos, cada um com conteúdo específico relacionado à temática abordada. O primeiro capítulo

versará sobre a internet, enfatizando o contexto histórico do seu surgimento, sua aplicação no mundo moderno e os efeitos por ela produzidos, tais como o aparecimento de crimes informáticos.

O segundo capítulo abordará as questões relativas ao direito à privacidade, sua interpretação no meio informático, além de demonstrar algumas condutas cometidas que infringem esse direito, tais como a interceptação de correspondência eletrônica e o acesso indevido ao correio eletrônico dos indivíduos.

O terceiro capítulo irá tratar da competência para punir os crimes informáticos que envolvem mais de um país e da identificação do lugar de sua consumação. Também será abordada a necessidade de se produzir uma legislação específica para os delitos informáticos no Brasil, analisando as leis de nações que já introduziram a tutela desses crimes em seus ordenamentos jurídicos, bem como a proposta legislativa em trâmite no país.

Por fim, reitera-se a relevância de se pesquisar sobre os crimes informáticos, haja vista que a utilização em massa da internet gera um potencial lesivo maior dessas condutas. Espera-se contribuir para o esclarecimento dos indivíduos acerca da criminalidade informática, pois a informação é essencial para a prevenção e o combate à criminalidade.

2 A FUNÇÃO DA INTERNET NA SOCIEDADE ATUAL

Grandes mudanças surgiram no cenário econômico, ao longo das últimas décadas. Entre essas mudanças está a criação da internet, a qual tem transformado o modo de viver das pessoas, afetando suas relações sociais de maneira significativa. Estudar a internet, suas peculiaridades, bem como as conseqüências que ela provocou na sociedade é de fundamental importância.

2.1 Conceito e diferenças entre as denominações utilizadas na informática

O conceito de informática encontrado nos dicionários sempre diz respeito ao tratamento automático das informações. Definida como ciência ou técnica da informação, ela tem modificado significativamente o cotidiano das pessoas. Modificando constantemente a sociedade, por um lado facilitando a realização de diversas tarefas e por outro, surpreendendo-a com o aparecimento de condutas lesivas.

É pelo grande espaço que a informática ocupa na atualidade e pelo desenvolvimento acelerado dos utensílios ligados a ela relacionados, que se faz mister definir alguns conceitos desse universo antes de aprofundar o estudo do tema.

O sistema informático é uma denominação ampla que engloba elementos tangíveis ou palpáveis, tais como o computador e seus componentes e intangíveis, como aqueles que não se pode tocar, a exemplo dos dados armazenados. De forma ampla, pode-se falar em sistemas informáticos pessoais, hospitalares, empresariais, governamentais, entre outros.

Nos dias de hoje, o mais importante tema relacionado à informática é, sem dúvida, a internet. Essa tecnologia consiste em uma rede internacional de comunicação que proporciona a transferência de dados entre computadores, sendo utilizada por milhões de pessoas no mundo contemporâneo.

De acordo com SOUZA (2006; p.53): "a internet é um conjunto de redes interligadas, de abrangência mundial, isto é, consiste em um conjunto de tecnologias para acesso, distribuição e disseminação de informação em redes de computadores". Essas várias redes unem-se para possibilitar a troca de informação, através de padrões específicos para esse fim.

Através de seu computador cada indivíduo pode ter acesso às informações oriundas de qualquer parte do planeta, quase que de forma instantânea, podendo realizar transações bancárias e comunicar-se com outras pessoas, independente da distância que os separam.

Pelo seu vasto campo e por sua enorme utilização, é necessário conceituar desde logo alguns dos assuntos relacionados à internet. O primeiro deles é o provedor de acesso ou provedor de serviço, que é a porta de entrada dos usuários para a rede mundial de computadores.

As ações dos usuários, tais como as páginas visitadas e as correspondências eletrônicas enviadas ficam armazenadas em uma espécie de banco de dados do provedor. A política de privacidade e a responsabilidade dos provedores de acesso pelo conteúdo nele publicado são temas de extrema importância que serão vistos no decorrer deste trabalho.

É o provedor de serviço que possibilita a troca de correspondência eletrônica entre os usuários, os chamados e-mails. Largamente utilizado nos dias de hoje, o e-mail é como uma carta que se envia pelo correio, no entanto, a facilidade e a agilidade que a internet proporciona fazem com que as pessoas prefiram se comunicar através de correspondência eletrônica. Afinal o envio da comunicação pode ser feito quase que de modo imediato e ficará armazenado na caixa de mensagens do destinatário e salvo na do remetente.

É impossível abordar o assunto da internet sem mencionar as figuras dos hackers e dos crackers. Tipos por diversas vezes confundidos, ambos são pessoas com alto conhecimento em informática que conseguem invadir sistemas informáticos, aproveitando-se de falhas de segurança desses. A diferença entre eles é que o hacker não planeja invadir um determinado sistema com a finalidade de deteriorá-lo ou inutilizá-lo, ele pode apenas observar o conteúdo alheio e não fazer qualquer alteração. Na verdade, os hackers, muitas vezes, trabalham na área de informática e produzem ou aperfeiçoam sistemas de segurança. O cracker, por sua vez, é o indivíduo que entra em um sistema informático para causar um prejuízo ao

seu proprietário, apagando arquivos, destruindo equipamentos ou, mesmo, conseguindo identificar qualquer tipo de senhas privadas, tais como de correio eletrônico ou de acesso a contas bancárias.

Uma das atividades mais comuns dos crackers é a de capturar números de cartões de créditos. O prejuízo que essa conduta pode trazer é imensurável, sendo muito mais vantajosa do que assaltar uma instituição financeira pessoalmente, pois pode lesar um ou milhares de indivíduos, além da sensação de impunidade que ela proporciona.

Vários exemplos de invasões por hackers e crackers ganharam notoriedade mundial, tais como a invasão à página da CIA ou a sistemas de gigantes da internet como os grupos Yahoo e Hotmail. Quanto maior a influência e o poder econômico das empresas, maior o fascínio que seus sistemas informáticos exercem sobre os também chamados de "piratas da internet". É por esse motivo que as empresas devem constantemente aperfeiçoar seu sistema de segurança, pois os invasores trabalham a uma velocidade sem igual a fim de descobrir falhas e acessar sistemas alheios.

Os hackers e crackers podem agir sozinhos, visto que, muitas vezes, seu instrumento é apenas um computador pessoal, ou podem se unir a outros, formando grupos. Esses sujeitos, possuindo um vasto conhecimento na área de informática podem trocar informações entre si, tornando-se uma ameaça muito perigosa até para os mais seguros sistemas informáticos.

Eles, geralmente, são jovens que começam suas atividades como forma de diversão e terminam por se especializarem nisso, podendo ser contratados por empresas para prestar assistência em seus sistemas de segurança ou para ingressar no sistema de suas concorrentes e descobrir projetos novos, por exemplo.

Uma invasão na área da informática pode ser extremamente rápida, levando segundos ou, ao contrário, demorando dias e até meses para se concretizar. Os meios para realizá-la podem ser os mais diversos, o mais divulgado é o vírus. As vítimas geralmente são induzidas a clicar em e-mails contendo o vírus, o qual pode reproduzir-se e danificar o computador.

O vírus pode, também, deixar uma abertura para que o invasor tenha livre acesso ao sistema, podendo visualizar todas as informações armazenadas e até mesmo aquelas que foram utilizadas de forma transitória. Um exemplo bastante comum é o vírus Cavalo de Tróia, ele pode fazer com que o computador invadido

fique inteiramente acessível ao invasor, que poderá ver todas as informações pessoais da vítima.

A facilidade com que esses vírus podem se espalhar pelo mundo é o que amplia demasiadamente os danos causados. Um exemplo recente de vírus mundialmente conhecido foi o denominado "*I love you*", que se disseminou através de mensagens de e-mails, durante dias, para milhares de pessoas em toda parte do planeta.

2.2 Histórico: surgimento, evolução e importância da internet

Não há um consenso quanto à data exata do surgimento da internet. no entanto, para SILVA (2000), sua origem remonta a década de sessenta, quando os Estados Unidos desenvolviam tecnologias avançadas para utilizar na Guerra Fria. Após o lançamento, em 1957, do primeiro satélite artificial, pela antiga União Soviética, os americanos passaram a temer ainda mais um ataque nuclear e, conseqüentemente, aumentaram os investimentos em tecnologia.

Naquela época, as redes de comunicação não eram confiáveis e, no caso de uma guerra real, o sistema pararia de funcionar. Por isso, surgiu a necessidade de criar uma rede de computadores mais segura e descentralizada, a qual conseguisse permanecer funcionando, mesmo que parcialmente, após um ataque nuclear.

O Ministério da Defesa Americano passou a financiar e desenvolver projetos pioneiros para coordenar e interligar os sistemas informáticos militares. A internet surge, portanto, com uma finalidade de proteção militar, posteriormente, seria utilizada nas Universidades, possibilitando a troca de informações, de dados e de pesquisas entre os professores e os cientistas.

Só após décadas, depois de certa resistência do governo americano, a internet ganha uma destinação comercial, sendo disponibilizada para empresas e usuários individuais. Essa utilização deu-se de forma peculiar, haja vista que a internet não foi lançada com essa finalidade. Novas formas de exploração dos recursos foram sendo criadas e adaptadas em uma velocidade impressionante. No Brasil, há relatos da utilização da internet no final da década de oitenta, entretanto sua utilização comercial no país só ocorreu em meados dos anos noventa.

Tecnologias foram sendo desenvolvidas para aperfeiçoar a interligação entre as redes e possibilitar o intercâmbio de dados. Foi criado o Protocolo de Controle de Transmissão (TCP), que posteriormente foi adaptado e associado ao Protocolo Internet (IP), surgindo, assim, o TCP/IP, protocolo padrão utilizado até hoje. Essa estrutura faz com que os dados transmitidos sejam gravados tanto no remetente, quanto no destinatário, o que gera uma segurança aos usuários.

Em 1990, foi criada a *World Wide Web* (www), conjunto de dados em hipertexto, que possibilitou a transferência de dados, figuras, links, entre computadores conectados de forma mais fácil e rápida. A *World Wide Web* de fato acelerou a expansão da internet pelo mundo. Como revistas eletrônicas, as *webpages* se popularizaram e permitem o acesso de usuários de qualquer parte do planeta, bastando conhecer o endereço eletrônico da página procurada ou digitar algumas palavras relacionadas em um site de busca. Hoje, essa é a forma mais utilizada pelos usuários da internet, devido à facilidade que ela proporciona.

Esse acesso rápido e fácil modificou bastante a comunicação e a prestação de serviços no mundo, não apenas na esfera privada, como também, na pública. O próprio governo utiliza as facilidades que a internet oferece, ao criar páginas oficiais e disponibilizar vários serviços que, anteriormente, os cidadãos só teriam acesso comparecendo pessoalmente às repartições públicas.

De fato, a internet está provocando uma revolução na sociedade, o acesso a ela não é mais privilégio das camadas financeiramente abastadas. Ao contrário, as *lan houses*, casas comerciais que proporcionam ingressar na rede por um período de tempo, estão proliferadas pela periferia a um preço acessível a todos. E, cada vez mais, o governo vem dando incentivos para a população de baixa renda possuir um computador com acesso à internet, além de disponibilizá-la em bibliotecas públicas e centros culturais.

Pela gama de possibilidades que a internet proporciona, as pessoas buscam nela interesses diversos, tais como ler livros, divulgar produtos, serviços ou fazer compras de forma cômoda e rápida. A visibilidade de um serviço disponibilizado na rede é muito maior do que se, esse mesmo serviço, fosse oferecido em uma rádio ou jornal local, pois a divulgação da página da internet é mundial.

O número de pessoas que usam a internet vem crescendo de forma veloz, recente pesquisa do Ibope Nielsen Online demonstra o crescimento do uso em residências ou no trabalho, no Brasil:

> Em agosto de 2009, 37,3 milhões de pessoas usaram a internet no trabalho ou em residências, crescimento de 2,3% sobre os 36,5 milhões registrados no mês de julho. A quantidade de pessoas com acesso no trabalho ou em residências, que era de 44,5
> milhões, cresceu 5% e chegou a 46,7 milhões.

O Ibope Nielsen Online estima, também, o número de brasileiros que têm acesso à internet, de alguma forma, considerando o mês de agosto do corrente ano:

> O IBOPE Nielsen Online projeta a existência de 64,8 milhões de pessoas com acesso à internet em qualquer ambiente (residências, trabalho, escolas, lan-houses, bibliotecas e telecentros), considerando os brasileiros de 16 anos ou mais de idade com posse de telefone fixo ou móvel.

Segundo dados do próprio Ibope, no primeiro trimestre de 2008, o número de usuários que de alguma forma tinham acesso à internet era de 41,565 milhões de pessoas com dezesseis anos ou mais. Percebe-se um aumento considerável em relação à pesquisa de agosto de 2009.

O estudo apresenta, também, o número de brasileiros que possuem internet em suas residências, bem como o tempo médio de utilização nos meses de julho e agosto de 2009.

Tempo de uso, número de usuários ativos e número de pessoas com acesso – Internet em domicílios, Brasil – julho e agosto/2009

	julho/2009	agosto/2009
Tempo de navegação por usuário (hh:mm)	30:13	30:33
Número de usuários ativos (000)	27.501	28.977
Número de pessoas com acesso (000)	40.164	42.209

Fonte: IBOPE Nielsen Online

Os dados de maio de 2008 revelam que o Brasil possuía 23,1 milhões de internautas ativos com acesso à internet em suas residências e o tempo de navegação por usuário, nesse período, era de 23 (vinte e três) horas e 48 (quarenta e oito) minutos. Pesquisa realizada entre dez países demonstrou que, já nessa

época, o brasileiro estava no topo da lista de usuários residenciais que passavam mais tempo na internet.

Por toda essa ampla propagação, é importante examinar os fenômenos do mundo virtual. O Direito, portanto, não pode quedar-se anacrônico, visto que ele tem a função de regular condutas e as chamadas condutas virtuais estão cada vez mais presentes na realidade da população. É por isso que o chamado Direito de Informática tem ganhado espaço nas Universidades, tentando estabelecer normas de convivência dentro do universo virtual.

2.3 Crimes cometidos através da internet

O aparecimento e, principalmente, o espaço que a internet ganhou na sociedade atual não trouxeram apenas benefícios para facilitar a vida dos indivíduos, trouxeram novos problemas, com os quais o mundo jurídico deve se preocupar em regular.

Diariamente, milhares de atividades são realizadas pela internet, como exemplo tem-se a compra de produtos, que serão pagos por boleto bancário, cartões de crédito ou outra forma. Ressalvada as peculiaridades do meio utilizado, trata-se de um contrato de compra e venda, no qual a expectativa é a do comprador receber o produto desejado, através de uma contraprestação pecuniária devida ao vendedor.

Se o contrato não produzir os efeitos esperados, a parte lesada deve procurar ressarcir-se do prejuízo, mas para isso, é necessário conhecer, de forma clara, os comportamentos e as soluções adequadas ao caso.

A internet possibilitou o aparecimento dos chamados crimes informáticos. Relatos da ocorrência desses crimes apontam seu surgimento logo em seguida à criação da própria internet. A princípio, as finalidades eram as de obter vantagem exclusivamente econômica ou militar, como exemplo da primeira, tem-se invasões a sistemas bancários ou a bolsas de valores e da segunda, a sistemas informáticos governamentais.

Atualmente, os objetivos dos delitos informáticos podem ser os mais diversos, existem relatos de invasões a sistemas hospitalares, com a modificação na

quantidade de remédio ministrado aos pacientes, o que configura verdadeira tentativa de homicídio.

Ainda não há um consenso a respeito da definição de crime informático. Novas condutas lesivas só passaram a existir por causa dos recursos fornecidos pela internet, ao mesmo tempo em que crimes antigos ganharam maneiras modernas de serem cometidos. Portanto, o crime informático pode ser uma espécie nova de delito, surgida com o advento da técnica da informática ou um delito tradicional, praticado de uma forma moderna e simplificada.

Sobre esse tema, o *Coucil of Europe* (apud Albuquerque, 2006, p. 40):

> Tem-se tentado definir "crime informático" de várias maneiras. Por exemplo, como qualquer conduta ilícita na qual um sistema informático constituir um instrumento ou objeto de um crime. Noutras palavras, qualquer crime cujo meio ou objetivo for influenciado por um computador, qualquer atividade ilícita associada a um sistema informático na qual o sujeito passivo perca ou possa ter perdido algo, e o sujeito ativo tenha, deliberadamente, ganhado ou possa ter ganhado algo.

Segundo ensinamentos de SOUZA (2005, p. 70), algumas classificações foram criadas em se tratando de crimes informáticos, uma das mais utilizadas, é a que os divide em crimes puros e impuros. O crime informático puro é aquele em que a finalidade é ter acesso a sistemas ou aos dados de um computador. Já o crime informático impuro é o que utiliza os meios que a informática oferece para praticar uma conduta ilícita tipificada, como o furto, o estelionato, entre outros.

Os "criminosos cibernéticos", como são chamados aqueles que se utilizam desse meio para praticar crimes, aproveitando-se da aparentemente impunidade, cometem os mais diversos delitos. É certo que o anonimato, provocado pela sensação de esconder-se atrás de um computador e a distância física que separa vítima de criminoso, muitas vezes, aumenta o anseio de cometer o crime.

A gravidade desse problema é evidenciada pela dimensão mundial que a internet proporciona. Apenas um computador é suficiente para uma pessoa praticar, de uma só vez e em países diferentes, as infrações mais diversas à lei.

Alguns exemplos de delitos pré-existentes à revolução da informática, mas que ganharam novas formas de serem cometidos são os de estelionato, fraude, pedofilia e terrorismo. Entre os mais praticados estão os crimes contra a honra e a imagem, pois a internet é ainda um espaço muito livre, onde qualquer pessoa pode depositar informações, fotos, documentos. Tal acontecimento, apesar de ser uma

democratização dos meios de comunicação, é extremamente perigoso, haja vista que, utilizando-se de má fé, o indivíduo pode facilmente provocar um arrasamento na vida social de outrem, ao expor a intimidade alheia ou divulgar fatos falsos, de uma forma que serão propagados em segundos pela rede.

Crimes novos também vêm surgindo com freqüência, entre eles os de invasão de privacidade tornam-se cada vez mais comuns, podendo ser cometidos de diferentes formas. Através das novas tecnologias, pode alguém ter acesso ao computador de outrem, observando o correio eletrônico e todas as páginas visitadas pelo usuário, sem que esse tenha condição alguma de saber que está sendo espionado. Essa conduta se torna mais gravosa quando empresas utilizam-se desse meio para controlar funcionários, ou quando governos passam a se utilizar dessa forma ilegal para investigar cidadãos.

Ainda dentro da linha de invasão de privacidade, existem as condutas de interceptação de correspondência eletrônica e de violação de segredo informático. A primeira consiste em interceptar a mensagem antes que ela chegue ao seu destino. A segunda conduta apresenta como vítimas, geralmente, empresas, que têm seus projetos revelados antes da hora. Em geral, essa violação de segredo é cometida por um funcionário ou ex-funcionário que sabe manusear o sistema da empresa e seu objetivo pode ser o de obter lucro, vendendo uma informação sigilosa para a concorrência ou o de vingar-se do empregador por algo que não o agradou.

Os relatos de usuários individuais e empresas que foram vítimas de algum tipo de crime informático são crescentes. Dados do *Federal Bureau of Investigation* (FBI) apontaram que 64% (sessenta e quatro por cento) das empresas já foram vítimas de algum crime informático (GERMAN, apud Albuquerque, 2006, p. 23). Um exemplo famoso foi a invasão do sistema informático do Citibank, por dois indivíduos, os quais desviaram a quantia de dez milhões e setecentos mil dólares sem sair de suas casas.

Ainda assim, estima-se que o problema tenha uma extensão muito maior do que aquilo que se pensa, pois, muitos desses crimes nem são descobertos pelas vítimas e outros não são sequer tipificados no ordenamento jurídico atual. Portanto, a produção de uma estatística real resta prejudicada.

Também se deve levar em conta, que as vítimas, principalmente quando são empresas, preferem não divulgar a ocorrência de tais crimes, pois a polícia judiciária ainda não possui um método adequado para investigar os delitos informáticos.

No curso da averiguação, a apreensão de objetos da empresa pode ocasionar um prejuízo considerável ou mesmo uma paralisação de suas atividades. Além disso, o sigilo e a agilidade durante a investigação são essenciais, porque se o investigado suspeitar dessa ação, ele poderá apagar qualquer vestígio do crime, impossibilitando que a polícia o descubra.

Existe ainda, em se tratando de investigação de crimes cometidos pelos meios informáticos, a questão da necessidade desenvolver uma maneira de perquirir o criminoso sem expor a vítima. O prejuízo que uma divulgação desse tipo pode causar é amplo, pois expõe os problemas com a segurança de sistemas informáticos da empresa vitimizada, fato que provocaria a perda de confiança por parte dos investidores e clientes.

Muitas vezes, as empresas preferem sofrer os danos gerados pelo crime informático, do que levar a frente uma investigação policial, tentando evitar um prejuízo duplo, primeiro por conta do ato ilícito; segundo por provocar uma diminuição na credibilidade e, conseqüentemente, nos lucros da instituição.

Apesar das dificuldades citadas, o Brasil vem caminhando para um melhoramento do seu sistema de investigação, haja vista que estão sendo criadas delegacias especializadas em crimes informáticos e já se tem um departamento específico na Polícia Federal só para a investigação desses crimes.

2.4 Sistemas de segurança

Relatadas algumas das inúmeras formas de cometer um crime através da internet, os usuários dessa rede precisam ficar atentos a maneiras de prevenirem-se de um ataque virtual. Da mesma forma, o legislador deve tipificar algumas condutas para que os cidadãos sintam-se protegidos ao enviarem suas correspondências, realizarem suas transações bancárias ou adquirirem algum produto pela internet.

Alguns dos cuidados básicos que todo usuário deve ter foram resumidos por NUNES (2000):

> Os ataques pela rede, por exemplo, podem ser impedidos se você não utilizar computadores públicos e mantiver sempre um antivírus atualizado

> em sua máquina pessoal para que programas que extraem informações não a infectem. Ao realizar transações financeiras e enviar dados confidenciais, certifique-se sempre de que a operação é segura (a exigência de assinatura eletrônica, por exemplo, indica maior confiabilidade). Nunca forneça sua senha a ninguém, não aceite ajuda de estranhos em caixas eletrônicos e tenha certeza de que nenhuma pessoa pode ver os números que você digita. Troque a senha frequentemente. E, sempre, ao primeiro sinal de problema, avise ao banco e registre queixa na polícia.

Além de estarem atentas às medidas acima, as pessoas devem atentar para outras, tais como: não abrir e-mail de indivíduos que não reconhecem, principalmente, se contiver arquivos anexados; nunca fornecer informações pessoais, tais como senhas ou dados a desconhecidos, nem preencher cadastros em sites que não sejam seguros; não salvar senhas no computador, principalmente se não estiver usando sua máquina pessoal; não utilizar páginas não confiáveis, nem *softwares* falsificados.

Todas as medidas de vigilância acima citadas são de extrema importância para o usuário individual prevenir-se de um possível crime informático. É certo que sozinhas elas não evitam completamente a ocorrência do delito, porém se utilizadas em conjunto, e permanentemente, diminuem de modo considerável as chances de ele acontecer.

No entanto, as empresas necessitam de outras medidas para protegerem-se. A maioria de suas atividades pode ser controlada por meio de computadores, além do que, dados importantes neles são armazenados, tais como, informações sobre suas contas, clientes ou projetos que estão sendo ou possam vir a ser desenvolvidos.

Diante do exposto, é essencial ter um sistema informático confiável. Os investimentos na segurança desses sistemas devem ser permanentes, pois os indivíduos estão sempre desenvolvendo novas maneiras de quebrar essa proteção, forçando as empresas a encontrarem novas formas de segurança.

É certo que um sistema informático nunca será totalmente seguro, por isso, que grande parte das empresas tem ou já tiveram problemas com seus sistemas. Ocorre que um suporte técnico adequado, realizado através de profissionais confiáveis, impede uma maior vulnerabilidade em relação a ataques virtuais. Por isso, as empresas devem reservar parte de seu orçamento para investir em medidas preventivas, evitando, assim, prejuízos no futuro.

Para proteger os cidadãos, os governos devem adotar algumas práticas, a começar por adequar o sistema penal às novas condutas. Não devem existir comportamentos lesivos sem serem passíveis de punição, de alguma forma. Além de atualizar a legislação, deve ser estimulada a elaboração de normas de coexistência na rede mundial de computadores, incluindo regras éticas a serem seguidas pelos indivíduos.

Uma fiscalização constante deve ser feita para que possa existir uma punição efetiva aos que desrespeitarem as regras e infringirem a lei. Além de tudo, o fornecimento de informações adequadas às pessoas é de relevante importância, pois muitas ainda não se acostumaram com as novidades que o meio informático introduziu na sociedade e necessitam de maiores esclarecimentos sobre como se prevenir de comportamentos danosos.

2.4.1 A Criptografia

Um recurso de proteção que vem ganhando espaço no mundo virtual, sendo usado principalmente por empresas, é a criptografia. Sua origem remonta ao Império Romano, quando o imperador passou a enviar mensagens codificadas, contendo estratégias de guerra, a seus generais. Dessa forma, evitava-se que o conteúdo da correspondência fosse revelado, se capturada pelo inimigo.

Utilizada no meio informático, a criptografia mantém sua função originária, pois mensagens codificadas são enviadas de maneira que só o remetente e o destinatário tenham conhecimento do código utilizado. Assim, evita-se que o conteúdo de um e-mail, por exemplo, seja descoberto por alguém que o interceptou ou o desviou do seu destino original, pois apesar de ter acesso ao conteúdo da mensagem, o indivíduo não entenderá a linguagem utilizada.

A criptografia é um recurso que possibilita maior segurança ao documento inserido no meio virtual. No entanto, críticas freqüentes vêm sendo elaboradas, sobretudo pelos governos. Os Estados Unidos, por exemplo, mantém uma resistência aos programas que utilizam a criptografia, pois temem que grupos terroristas ou outras organizações criminosas possam esconder-se através dela.

Um exemplo da resistência americana terminou no judiciário, quando os Estados Unidos proibiram a utilização do programa *Pretty Good Privacy* (PGP). Segundo PODESTÁ (2000, p.162):

> O PGP é um programa de encriptação que permite a leitura de mensagens somente com o emprego de um sistema de duas chaves, ou seja, a idéia é que uma pessoa possua uma 'chave secreta' que não deve ser revelada, e uma 'chave pública' disponível para quem quer que seja. As mensagens são encriptadas com a 'chave pública', e, isto feito, somente quem possui a 'chave secreta' pode decriptá-las. (sic)

O governo americano considerou que o PGP punha em risco a segurança nacional, já que a codificação utilizada fugia do conhecimento dos órgãos de segurança americanos. No entanto, o judiciário não apoiou essa tese[1].

[1] A questão da observação pelos governos dos procedimentos realizados pelos usuários de internet será melhor abordada no segundo capítulo do presente trabalho.

3 DIREITO À PRIVACIDADE E DIREITO À PRIVACIDADE NA INTERNET

O Direito à Privacidade é amplamente conhecido no mundo jurídico moderno, estando consagrado no ordenamento jurídico brasileiro. No entanto, é preciso conhecer o sentido desse direito no ambiente virtual. Dessa forma, os comportamentos que infringem a privacidade, nesse meio, podem ser melhor estudados.

3.1 Surgimento do direito à privacidade

Desde a antiguidade, algumas manifestações apontavam a origem de direitos individuais. Tratava-se de demonstrações isoladas e de formas ainda muito tímidas de amparar o indivíduo, que vinham quase sempre confundidas com a religião. Na Grécia, por exemplo, surgiram importantes conceitos como o de democracia e com ele idéias de liberdade do indivíduo.

O nascimento de alguns dos direitos e garantias que se tem atualmente encontra-se no Direito Romano, muitos deles incitados pelas insatisfações da plebe com um governo opressor. Essa foi sem dúvida a demonstração mais completa até então de tutela de direitos do homem, em detrimento dos caprichos dos governantes.

No século XIX, com a Revolução Francesa e as idéias liberais do período, muitos dos direitos que se encontram amplamente difundidos nos dias de hoje surgiram ou foram ampliados, dentre eles o direito à privacidade. Naquela época, os direitos da personalidade enfloravam como novas garantias para defender os indivíduos do próprio Estado.

O contexto histórico era o da existência de um Estado soberano, absoluto, personificado na figura de um rei, que oprimia o indivíduo, e não deixava espaço algum para os direitos da pessoa. As mais diversas arbitrariedades eram cometidas em nome de um poder que se dizia legítimo. O direito, em geral, não era escrito, era produzido no momento em que o monarca necessitava tomar alguma decisão. O

que o tornava mutável, adequando-se aos desejos de um déspota e gerando grande insegurança para a população.

De acordo com o que leciona SOUZA (2005, p. 24), pode-se inferir que para a gradativa modificação desse pensamento, foram importantes também as idéias cristãs de fraternidade, incluindo a de dignidade da pessoa, e a chamada Escola do Direito Natural, a qual acreditava na existência de direitos inerentes ao homem, sobrepondo-se a outros direitos.

Nessa ocasião surge a Declaração dos Direitos do Homem e do Cidadão (1789), reunindo em um documento os pensamentos inovadores da época. A declaração logo ganhou abrangência mundial e os direitos nela contidos foram sendo reproduzidos em tratados internacionais e nas Cartas dos Estados.

Inicialmente, os direitos individuais surgem como forma de limitar o poder dos déspotas, ou seja, vêm defender o indivíduo dos excessos praticados pelo próprio Estado. Ganhou mais força a idéia de que o governante não possuía poderes ilimitados e que ele não era o próprio poder, tendo em vista que sua função equivale a de um preposto da sociedade.

Posteriormente, com o desenvolvimento desses direitos e o surgimento do Constitucionalismo em sua forma social, eles passaram a ser uma garantia não apenas contra o Estado, mas também, contra atos arbitrários das demais pessoas.

Uma discussão se trava quanto ao nascimento do direito à privacidade. Parte dos doutrinadores entende que ele só surgiu após a criação da propriedade, como uma regulamentação a aquele direito. No entanto, a maioria acredita que o direito à privacidade aparece como uma valorização da personalidade, não estando limitado à propriedade por ser bem mais amplo que essa, e também por abarcar diversos âmbitos da vida dos cidadãos.

Ao longo do século XX, vários tratados ou convenções internacionais preocuparam-se em inserir o direito à privacidade em seu conteúdo. Um dos mais importantes foi a "Declaração Universal dos Direitos do Homem" (1948), que assim dispôs em seu artigo 12:

"Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da lei".

O contexto histórico exigia uma proteção escrita, pois com o fim da 2ª Guerra Mundial era necessário tomar todas as providências para que jamais ocorressem

novas violações à dignidade humana. Surgiu, então, a Declaração Universal dos Direitos do Homem, retomando idéias da declaração francesa do século XIX.

Após tal declaração, uma série de instrumentos internacionais confirmou em seus textos a proteção ao direito à privacidade. Um exemplo é a Convenção Americana dos Direitos do Homem, de 1969, mais conhecida como Pacto de são José da Costa Rica, da qual o Brasil é signatário:

> Artigo 11 - Proteção da honra e da dignidade
> 1. Toda pessoa tem direito ao respeito da sua honra e ao reconhecimento de sua dignidade.
> **2. Ninguém pode ser objeto de ingerências arbitrárias ou abusivas em sua vida privada, em sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais à sua honra ou reputação.**
> 3. Toda pessoa tem direito à proteção da lei contra tais ingerências ou tais ofensas.
>
> **(grifo nosso)**

Vários países também passaram a incluir em suas constituições a proteção à privacidade. No Brasil, via-se uma proteção tímida, tendo em vista que todas as Constituições anteriores apenas faziam menção à inviolabilidade de domicílio. Era a primeira delimitação expressa de um espaço particular do cidadão, onde nem mesmo o Estado poderia adentrar, ressalvados os casos previstos em lei.

3.2 O direito à privacidade na Constituição Federal

A Constituição Federal de 1988 foi a primeira a proteger de forma expressa o direito à privacidade. As Constituições anteriores não traziam essa previsão, o que não significa que a vida privada não tivesse proteção constitucional antes de 1988, haja vista ela estar presente de forma implícita e, em parte, quando se previa a inviolabilidade domiciliar.

Ocorre que à época da elaboração da atual Constituição a imprensa estava cada vez mais presente na vida dos brasileiros e surgiam novas formas de comunicação e difusão de informação, necessitando, portanto de uma proteção maior ao indivíduo. Esses fatos contribuíram para o legislador inserir expressamente o direito à privacidade na Carta Magna.

Determina o artigo 5º, X, da Constituição Federal (1988):

> Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: [...]
> **X - são invioláveis a intimidade, a vida privada**, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;
>
> **(grifo nosso)**

Antes de adentrar no tema da proteção constitucional, faz-se necessário traçar algumas diferenças entre direito à privacidade e direito à intimidade. Parte da doutrina não faz essa distinção, abordando ambos os temas como se fossem um único direito. Do mesmo modo, a jurisprudência pátria também não vem distinguindo esses conceitos.

Não se pode não abordar uma questão de tanta relevância, pois a diferença entre ambos revela-se uma linha tênue, quase imperceptível, que pode dar margens a algumas dúvidas quando da leitura da legislação ou de textos sobre o tema.

Os conceitos de privacidade e de intimidade não são estáticos, eles se transformam ao longo do tempo para adequarem-se à evolução da sociedade e apresentam algumas variações entre os Estados. No Brasil, o direito à privacidade, tal qual se conhece hoje, é mais amplo e comporta o direito à intimidade. Este último versa sobre as relações mais íntimas do indivíduo e está abrangido pelo primeiro.

De acordo com MENDES (2008, pág. 377):

> O direito à privacidade teria por objeto os comportamentos e acontecimentos atinentes aos relacionamentos pessoais em geral, às relações comerciais e profissionais que o indivíduo não deseja que se espalhem ao conhecimento público. O objeto do direito à intimidade seriam as conversações e os episódios ainda mais íntimos, envolvendo relações familiares e amizades mais próximas.

Em sentido amplo, tem-se a privacidade como direito do indivíduo quedar-se isolado, sem os constantes olhares de terceiros, possuindo o direito de manter suas relações em sigilo e de perseguir judicialmente aqueles que violarem esse direito.

É a privacidade para Tércio Sampaio (2006):

> Um direito subjetivo fundamental, cujo titular é toda pessoa, física ou jurídica, brasileira ou estrangeira, residente ou em trânsito no país; cujo conteúdo é a faculdade de constranger os outros ao respeito e de resistir à violação do que lhe é próprio, isto é, das situações vitais que, por só a ele

> lhe dizerem respeito, deseja manter para si, ao abrigo de sua única e discricionária decisão; e cujo objeto é a integridade moral do titular.

A proteção à vida privada, tal qual está na Carta Magna, segundo ROLIN apud Mendes (2008, pág. 378), ampararia contra:

> Ataques à integridade física, moral e sobre a liberdade intelectual e moral [do indivíduo] e contra o uso impróprio do nome e da imagem de alguém, contra atividades de espionagem ou de controle ou de perturbação da tranqüilidade da pessoa e contra a divulgação de informações cobertas pelo segredo profissional.

Com uma menor abrangência, a intimidade visa resguardar os assuntos mais pessoais, as peculiares de cada ser, para que essas não possam ser divulgadas a um grupo, muito menos publicamente. Cada um tem garantido ver seus assuntos íntimos resguardados do público, em uma esfera em que nem o Estado poderia interferir[2].

3.3 Peculiaridades do meio informático

A revolução provocada pela internet na sociedade contemporânea causou também mudanças na maneira de interpretar alguns direitos fundamentais. Essas mudanças são geradas pelas peculiaridades desse meio de comunicação.

O direito à informação e a livre manifestação do pensamento são direitos fundamentais constitucionalmente previstos, artigo 5º, IX e artigo 220, ambos da Carta Magna. Portanto, o direito de manifestar seus pensamentos, de obter informações, bem como o de informar estão indiscutivelmente previstos na legislação pátria. Ocorre que muitas vezes eles esbarram no direito à privacidade das pessoas, nesse momento, deve entrar em cena o princípio da ponderação. Através desse princípio busca-se descobrir até onde a liberdade de expressão deve ser exercida e quando essa encontra limite nos direitos da personalidade.

---

[2] Neste trabalho, a abordagem ao direito à privacidade irá considerá-lo em um sentido amplo, abrangendo também o direito à intimidade, compreendendo-se as relações profissionais, familiares, de amizade, entre outras.

A livre manifestação do pensamento e o direito à informação não podem servir de escudo para indivíduos praticarem abusos contra a privacidade das pessoas. Aqueles que forem prejudicados têm o direito de procurar o judiciário e valer-se dos meios adequados para punir os responsáveis. Dessa maneira futuras condutas lesivas também podem ser coibidas.

No meio informático as informações são transmitidas aparentemente de forma livre, sem nenhuma restrição, essa impressão é ocasionada pela velocidade com que elas são lançadas e pelo seu amplo alcance. Através do acesso à rede mundial de computadores, qualquer cidadão pode disponibilizar uma informação que poderá ser visualizada por pessoas em diferentes partes do planeta.

Utilizando-se da rede, o direito à privacidade é violado não apenas com condutas correspondentes a lançar uma informação pessoal sobre alguém em uma página da internet. Várias outras maneiras podem ser utilizadas, tais como a interceptação de correspondências eletrônicas por terceiros, o armazenamento de dados de um usuário e a venda desses dados às empresas[3].

A comunicação em tempo real e a facilidade de acesso aos meios informáticos podem gerar uma ampla possibilidade de violações ao direito à privacidade. No entanto, também nesse meio é preciso buscar um parâmetro para se limitar as manifestações de pensamento e esse parâmetro são os direitos fundamentais, como o da privacidade.

A figura do intermediário, responsável por fiscalizar o que se está transmitindo, praticamente não existe quando se utiliza a internet, o que torna a atividade ainda mais perigosa aos direitos individuais. Os provedores de serviço, que poderiam enquadrar-se como intermediários e fiscalizadores dos conteúdos veiculados por seus usuários, aproveitam-se das lacunas na legislação para escusarem-se de suas responsabilidades.

3.4 Correspondência eletrônica: armazenamento, transmissão e formas de violação

[3] Esses e outros comportamentos atentatórios à vida privada serão tratados ainda neste capítulo.

Correspondência eletrônica, correio eletrônico ou *e-mail* são formas de nomear mensagens eletrônicas trocadas pelos usuários da internet. Essas mensagens são enviadas de maneira similar às cartas escritas em papel, sendo necessário para tanto que o destinatário e o remetente possuam um endereço eletrônico, onde a correspondência ficará armazenada.

Um *e-mail* pode ter conteúdos diversos, pode apresentar-se na forma de texto, imagens, vídeos, sons, ou qualquer outra que se possa reproduzir em um documento eletrônico, a depender da vontade do usuário.

A correspondência eletrônica é transmitida da caixa de mensagens do remetente para a do destinatário com o auxilio do provedor de serviço. Ele possibilita que a mensagem chegue ao destino correto de forma imediata, sem a demora de uma correspondência escrita. É essa agilidade que o universo virtual proporciona que atrai um número cada vez maior de adeptos.

Atualmente, milhares de pessoas utilizam o correio eletrônico como forma de comunicação, são indivíduos, empresas, entidades governamentais e até mesmo o poder judiciário vem usando essa ferramenta como alternativa para diminuir a morosidade dos seus julgamentos. Essa crescente utilização da correspondência eletrônica implica na necessidade de ampliar as formas de segurança, impedindo sua violação e possibilitando uma proteção especial para os dados nela armazenados e transmitidos

As informações contidas no e-mail podem ser transmitidas de uma pessoa para outra e ficam armazenadas na própria caixa de mensagens do usuário. Essa distinção entre os dados armazenados e os transmitidos é essencial para distinguirem-se as formas de invasão à privacidade.

Uma terceira pessoa pode interceptar a correspondência no momento em que ela está sendo enviada do remetente ao destinatário, fazendo com que ela vá para destino diverso do pretendido. Com isso, esse terceiro tem acesso aos dados que seriam transmitidos, podendo utilizá-los como quiser.

A interceptação é demasiadamente perigosa, haja vista que empresas se utilizam de correspondência eletrônica para comunicar-se com seus clientes, fornecedores, ou funcionários e empresas concorrentes podem aproveitar essa ação para lucrar de forma ilícita, através de espionagem.

Pode ocorrer também de alguém acessar a caixa de mensagens de outrem, sem que o seu titular sequer suspeite, com a finalidade de visualizar os dados armazenados e fazer uso deles de alguma maneira.

A importância dessa distinção entre dados armazenados e aqueles que estão sendo transmitidos tem em vista estabelecer quando esses dados estão protegidos pelo sigilo das correspondências. Esse sigilo está previsto na Constituição Federal (1988):

> Artigo 5º [...] XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;

Para MENDES (2008, p. 392): "o sigilo das comunicações é não só um corolário da garantia da livre expressão de pensamento; exprime também aspecto tradicional do direito à privacidade e à intimidade".

Em que pesem as opiniões em contrário, o sigilo das comunicações eletrônicas está abrangido no inciso citado. Não havia a possibilidade de uma previsão expressa das mensagens eletrônicas porque à época da elaboração da Carta Magna, a internet ainda ocupava um pequeno espaço e sua utilização era incomum. Não podendo exigir-se do legislador, na ocasião, a inserção desse tipo de correspondência no texto constitucional.

A Lei nº 9296/1996, que regulamentou o artigo 5º, XII, parte final, da Constituição Federal, estabelece a necessidade de autorização judicial para a realização de interceptação telefônica. O artigo 1º, parágrafo único, estende a aplicação da referida lei à interceptação do fluxo de comunicações em sistemas de informática e telemática.

E o artigo 10º da referida lei assim dispõe: "constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei". Portanto, os dados transmitidos através de correio eletrônico só são passíveis de interceptação mediante autorização do juiz competente e seguindo as determinações da Lei nº 9296/1996.

No caso de correio eletrônico, o preceito constitucional assegura a proteção contra a interceptação dos dados que estão sendo transportados de uma caixa de

mensagens para outra, além das disposições da Lei nº 9296/1996. Deve, portanto, ser inviolável o sigilo dessa comunicação particular transmitida através da internet.

Ressalta-se que os dados armazenados nas caixas de mensagens, são considerados dados estáticos, assim como os contidos no disco rígido do computador, em CDs ou outras formas de armazenamento. Esses não estão protegidos pelo sigilo das correspondências e das comunicações, previsto no artigo 5º, XII da Constituição Federal, por não serem passíveis de interceptação.

No entanto, sua visualização sem o conhecimento do titular fere o direito à privacidade, por tratar-se de mensagens particulares, protegidas por uma senha pessoal de acesso. Se houver a necessidade de apreender esses dados, a autoridade judicial deve aprovar sua busca e apreensão, como visto não há a possibilidade de interceptação judicial de dados armazenados pela forma que se encontram.

Foi esse o entendimento do Supremo Tribunal Federal no julgado a seguir colacionado:

> **EMENTA:** I. Decisão judicial: fundamentação: alegação de omissão de análise de teses relevantes da Defesa: recurso extraordinário: descabimento. Além da falta do indispensável prequestionamento (Súmulas 282 e 356), não há violação dos art. 5º, LIV e LV, nem do art. 93, IX, da Constituição, que não exige o exame pormenorizado de cada uma das alegações ou provas apresentadas pelas partes, nem que sejam corretos os fundamentos da decisão; exige, apenas, que a decisão esteja motivada, e a sentença e o acórdão recorrido não descumpriram esse requisito (v.g., RE 140.370, 1ª T., 20.4.93, Pertence, DJ 21.5.93; AI 242.237 - AgR, 1ª T., 27.6.00, Pertence, DJ 22.9.00).
> II. Quebra de sigilo bancário: prejudicadas as alegações referentes ao decreto que a determinou, dado que a sentença e o acórdão não se referiram a qualquer prova resultante da quebra do sigilo bancário, tanto mais que, dado o deferimento parcial de mandado de segurança, houve a devolução da documentação respectiva.
> III. Decreto de busca e apreensão: validade. 1. Decreto específico, que somente permitiu que as autoridades encarregadas da diligência selecionassem objetos, dentre aqueles especificados na decisão e na sede das duas empresas nela indicadas, e que fossem "interessantes à investigação" que, no caso, tinha pertinência com a prática do crime pelo qual foi efetivamente condenado o recorrente. 2. Ademais não se demonstrou que as instâncias de mérito tenham invocado prova não contida no objeto da medida judicial, nem tenham valorado qualquer dado resultante da extensão dos efeitos da decisão determinante da busca e apreensão, para que a Receita Federal e a "Fiscalização do INSS" também tivessem acesso aos documentos apreendidos, para fins de investigação e cooperação na persecução criminal, "observado o sigilo imposto ao feito".
> **IV - Proteção constitucional ao sigilo das comunicações de dados - art. 5º, XVII, da CF: ausência de violação, no caso. 1. Impertinência à hipótese da invocação da AP 307 (Pleno, 13.12.94, Galvão, DJU 13.10.95), em que a tese da inviolabilidade absoluta de dados de computador não pode ser tomada como consagrada pelo Colegiado,**

> **dada a interferência, naquele caso, de outra razão suficiente para a exclusão da prova questionada - o ter sido o microcomputador apreendido sem ordem judicial e a conseqüente ofensa da garantia da inviolabilidade do domicílio da empresa - este segundo fundamento bastante, sim, aceito por votação unânime, à luz do art. 5º, XI, da Lei Fundamental. 2. Na espécie, ao contrário, não se questiona que a apreensão dos computadores da empresa do recorrente se fez regularmente, na conformidade e em cumprimento de mandado judicial. 3. Não há violação do art. 5º. XII, da Constituição que, conforme se acentuou na sentença, não se aplica ao caso, pois não houve "quebra de sigilo das comunicações de dados (interceptação das comunicações), mas sim apreensão de base física na qual se encontravam os dados, mediante prévia e fundamentada decisão judicial". 4. A proteção a que se refere o art.5º, XII, da Constituição, é da comunicação 'de dados' e não dos 'dados em si mesmos', ainda quando armazenados em computador. (cf. voto no MS 21.729, Pleno, 5.10.95, red. Néri da Silveira - RTJ 179/225, 270).**
> V - Prescrição pela pena concretizada: declaração, de ofício, da prescrição da pretensão punitiva do fato quanto ao delito de frustração de direito assegurado por lei trabalhista (C. Penal, arts. 203; 107, IV; 109, VI; 110, § 2º e 114, II; e Súmula 497 do Supremo Tribunal).
> *(RE 418416 / SC, Relator Min. sepúlveda pertence, TRIBUNAL PLENO, julgado em 10/05/2006, publicado em19-12-2006).*
>
> ***(grifo nosso)***

3.4.1 Controle da correspondência eletrônica dos empregados pelas empresas

Uma prática cada vez mais freqüente é a observação da correspondência do empregado pela empresa na qual esse trabalha, sem o seu conhecimento. Algumas empresas julgam possuir o direito de visualizar as correspondências recebidas e enviadas pelos seus empregados nos computadores dos locais de trabalho. Outras vão mais além, recuperando e visualizando as mensagens instantâneas em programas como MSN e todas as páginas acessadas pelos trabalhadores.

Não se está analisando aqui a observação pela empresa de e-mail fornecido por essa para que o empregado possa realizar suas atividades laborais, mas sim, na espionagem de e-mails pessoais dos trabalhadores, bem como na interceptação de correspondência eletrônica entre funcionários.

Há quem considere que os e-mails pessoais dos empregados acessados a partir do servidor da empresa podem ser observados por essa, pois tudo aquilo feito no local de trabalho deveria ser considerado algo em função da atividade empresarial.

Outras opiniões há no sentido de que a empresa que pratica a investigação do correio dos empregados deve deixar claro que adota essa política, seja no contrato de trabalho ou de alguma outra forma. Essa conduta dispensaria a ordem judicial necessária mencionada na Lei nº 9296/1996. Nesse sentido é o entendimento de ALMEIDA (2001):

> Isso porque o poder disciplinar do empregador, reconhecido pela CLT, deve ser conciliado com o direito à privacidade, conferido a todo indivíduo, e previsto na Constituição Federal (art. 5º, X) [...] Portanto, o funcionário tem o direito de ser alertado previamente. Note-se, não é necessário obter assinaturas de concordância com a "monitoração", basta guardar a prova de que os funcionários foram avisados, seja por e-mail, notícia no quadro de avisos etc. Manter-se, assim, dentro dos limites do poder disciplinar e de fiscalização é garantir o amparo da CLT para a prática da monitoração. Isso gera uma outra conseqüência. É que existe uma lei (Lei n. 9.296) que trata especificamente das interceptações telefônicas e de dados, admitindo-as, para fins de investigação criminal, quando haja prévia aprovação judicial ou um "objetivo autorizado por lei". Como é inviável obter a ordem do juiz a todo instante, a primeira condição é imprestável para justificar "monitoração" permanente.

Em que pesem os entendimentos acima mencionados, não é possível conceber que o empregado deve ser monitorado desta maneira. O melhor entendimento é o que considera verdadeira ofensa à privacidade do empregado a visualização de suas correspondências eletrônicas pela empresa em que trabalha e a violação de correspondência no caso da prática de interceptação. Não se pode acessar informações pessoais ou interceptar correspondências eletrônicas sem uma autorização judicial.

Na esteira de inadmitir a observação das mensagens eletrônicas do empregado, entende SOUZA (2005, p. 83):

> O trabalhador é acima de tudo um indivíduo que tem sua intimidade. A privacidade não pode ser desmembrada do ser humano enquanto ele trabalha. Isso não é possível. No máximo ela é restringida, em face do próprio local de trabalho e da atividade realizada. Não almejamos a privacidade do lar, mas apenas o mínimo possível para se trabalhar confortavelmente sem se sentir parte de um terreno de espionagem.

Algumas empresas já estabelecem restrições à privacidade do trabalhador, como o monitoramento por câmeras de seguranças, as revistas periódicas, ligações telefônicas gravadas para garantir a segurança da empresa, no entanto as restrições à privacidade não podem ser total, englobando o monitoramento de correspondência

eletrônica particular. Deve- se ter em vista a aplicação do princípio da dignidade da pessoa humana, previsto no artigo da Carta Magna, nas relações de trabalho.

Vários podem ser os motivos que levam uma empresa a praticar esse tipo de espionagem, são alguns deles: controlar o tempo que empregado gasta com assuntos particulares no horário de trabalho; verificar se o empregado está a procura de novo emprego; evitar condutas racistas ou pornográficas por parte de seus prepostos; evitar que esses se comuniquem com empresas concorrentes, revelando algum dado sigiloso, entre outros.

Essa invasão praticada pela empresa pode resultar em várias condutas malévolas ao empregado, tais como a demissão por justa causa, por exemplo, se o empregador entender que houve incontinência de conduta, violação de sigilo ou outros comportamentos atentatórios nas mensagens eletrônicas do empregado.

As empresas se utilizam de uma espécie de grampo eletrônico para poder visualizar tudo aquilo que foi feito pelo empregado em seu computador. As informações são obtidas de maneira simples, pois essa tecnologia já é encontrada facilmente no mercado. Uma alternativa para evitar a espionagem do correio eletrônico dos empregados é a utilização pelas empresas dos chamados filtros. Eles impedem que certas *webpages* previamente selecionadas sejam acessadas nos computadores da empresa, bem como que alguns arquivos com conteúdo de sexo, racismo, dentre outros sejam identificados através de palavras-chaves e não possam ser baixados.

No mundo, as legislações dos países divergem quanto à tolerância ou não desse comportamento. O ideal é que os Estados possuam leis específicas com o fim de proibir esse tipo de invasão de privacidade pelas empresas. O Brasil ainda não possui essa normatização, no entanto, as leis já existentes (Constituição Federal, Lei nº 9296) devem ser usadas para coibir o controle da correspondência dos empregados pelas empresas.

3.4.2 Necessidade de controle do correio eletrônico pelo poder público

A liberdade que a internet proporciona na transmissão de dados, através do correio eletrônico, faz surgir uma preocupação por parte do poder público a respeito dos conteúdos nela transmitidos.

Qualquer pessoa com acesso à internet pode divulgar informações que violam a privacidade de outrem, ou veicular pornografia, ou exaltar a pedofilia, o racismo, entre outras condutas atentatórias. Discute-se se os governos devem manter um controle sobre os conteúdos particulares das mensagens eletrônicas ou se a difusão de informações nesse meio deve ser ilimitada, bem como se esse controle é ou não uma nova forma de censura.

Alguns países tentam controlar as informações pessoais dos usuários da internet como forma de coibir algumas práticas, como terrorismo, racismo e homofobia. Ocorre que esses países terminam por violar o direito à privacidade, acima especificado. A doutrina discute incessantemente até que ponto o interesse público deve ser sobreposto aos direitos individuais, fundamentais. É necessária uma ponderação para descobrir a resposta e, acima de tudo, é preciso analisar cada caso isoladamente.

Logo após o atentado terrorista de 11 de setembro de 2001, os Estados Unidos criaram a "Lei Antiterrorismo". Após sancionar a lei, o presidente americano, George W. Bush comentou sobre as mudanças, inclusive sobre o monitoramente de mensagens e a interceptação de dados pelo serviço de inteligência americano:

> A vigilância das comunicações é outra ferramenta essencial para perseguir e deter os terroristas. As leis existentes foram escritas na era dos telefones de disco. Esta nova lei que assino hoje permitirá um controle de todas as formas de comunicação usadas pelos terroristas, incluindo e-mails, internet e os telefones celulares.

As instituições de proteção da segurança nacional dos Estados Unidos passaram a ter acesso de maneira ampla a correspondências eletrônicas particulares, inclusive de cidadãos não americanos, com a finalidade de descobrir possíveis ataques terroristas. Além de visualizar o conteúdo armazenado, elas contam com modernas técnicas que permitem a recuperação de todos os dados apagados que um dia pertenceram a um usuário.

Espionar caixas de mensagens ou interceptar e-mails de indivíduos indiscriminadamente, sem uma ordem judicial e sob o pretexto de proteger a segurança nacional americana é uma afronta ao direito à privacidade das pessoas.

Esse comportamento se torna inadmissível quando as mensagens vasculhadas são de cidadãos de qualquer parte do mundo, haja vista que a internet dá margem a esta extraterritorialidade, porém deve haver uma delimitação da competência jurisdicional nesse meio.

Após a iniciativa americana, outros países criaram também suas legislações antiterrorismo, a exemplo da França que em 2005 aprovou uma das leis de combate ao terrorismo mais rígidas da Europa. O então ministro Nicolas Sarkozy chegou a comentar o seguinte: "Quem voa, viaja de trem, vai a um cyber café ou telefona, deve ter em mente que seus dados poderão ser armazenados por um ano e enviados para investigadores".

Seguindo a mesma linha, a Inglaterra, que já possuía uma lei permitindo a observação pelo governo de correspondência eletrônica de particulares, sancionou novas leis que limitaram ainda mais os direitos civis dos cidadãos.

A espionagem de correspondência eletrônica e o armazenamento de dados pessoais em bancos de dados foram práticas que alguns países resolveram tornar lícitas, outras, porém, existem que eles conservam de maneira camuflada ou mesmo mantêm no desconhecimento das pessoas comuns.

O livre acesso aos e-mails dos particulares permite que mensagens criptografadas[4] sejam decodificadas para possibilitar a leitura do seu conteúdo, independente de quem seja o remetente ou o destinatário delas. Chegando os governos a tentar proibir a criação e circulação de programas de criptografia de difícil interpretação, tudo em nome da segurança nacional.

Todas essas medidas que permitem o controle indiscriminado das comunicações transmitidas através da internet, sem a necessidade de autorização do judiciário, violam o direito à privacidade, além de transformar todas as pessoas em suspeitos, passíveis de terem suas correspondências vasculhadas.

O acesso a dados particulares não deixa de ser invasivo à privacidade das pessoas, apenas porque não é praticado por indivíduos comuns, e sim, pelos sistemas de segurança dos Estados, sob a aparência da legalidade. A pretexto da proteção ao interesse público, não podem ser esquecidos os direitos individuais conquistados ao longo de séculos pelos cidadãos. O direito à privacidade, apesar de

[4] Informações transmitidas através de códigos, como explicado no primeiro capítulo deste trabalho.

não ser considerado um direito absoluto, é um dos mais relevantes e deve ser oponível *erga omnes*.

4 PROTEÇÃO PENAL DA PRIVACIDADE NO ÂMBITO VIRTUAL

É essencial que os crimes informáticos sejam regulamentados pelos ordenamentos jurídicos. Em especial, os delitos que violam à privacidade dos indivíduos, haja vista que são de difícil percepção e provocam grandes conseqüências danosas às vítimas. O Brasil necessita adaptar sua legislação penal, para inserir os delitos citados e proporcionar uma maior segurança à população.

4.1 Lugar do crime informático e jurisdição competente

A liberdade que a internet proporcionou na transmissão de dados provocou um "desaparecimento" das fronteiras nacionais, tendo em vista que uma pessoa no Brasil pode comunicar-se com outras em diversas partes do planeta.

Os crimes informáticos também quebram fronteiras e se propagam pelo mundo. A título de exemplo, uma pessoa nos Estados Unidos pode invadir um sistema bancário no Brasil e desviar um determinado valor em dinheiro para uma conta localizada em um terceiro país. Da mesma maneira, um vírus pode ser criado em um país e causar prejuízos em inúmeros outros.

No caso específico dos delitos que atentam contra a privacidade, mais especificamente os de interceptação de correspondência eletrônica e de invasão ao correio eletrônico, cidadãos de diversos países podem estar envolvidos, sejam como vítimas, autores ou beneficiários.

A primeira questão importante é saber se a vítima teve conhecimento do crime, pois diariamente essas invasões à privacidade acontecem sem que a pessoa lesada tenha ciência delas. Superado esse ponto e tendo conhecimento do delito e da forma de agir do criminoso, a pergunta que emerge é qual o local competente para processar e julgar tal crime?

No Brasil, punem-se os crimes cometidos no âmbito do seu território nacional. Este é o chamado princípio da territorialidade e está previsto no artigo 5º do Código Penal Brasileiro. Imprescindível é analisar as teorias penais sobre o lugar do crime, são elas: teoria da ação, teoria do resultado e teoria mista ou da ubiqüidade. De acordo com as elucidações de GRECO (2008, p. 136):

> Pela teoria da atividade, lugar do crime seria o da ação ou da omissão, ainda que outro fosse o da ocorrência do resultado. Já a teoria do resultado despreza o lugar da conduta e defende a tese de que lugar do crime será, tão-somente aquele em que ocorrer o resultado. A teoria da ubiquidade ou mista adota as duas posições anteriores e aduz que lugar do crime será o da ação ou da omissão, bem como onde se produz ou deveria produzir-se o resultado. (sic)

O Código Penal Brasileiro, ao identificar o local do crime, em seu artigo 6º, adota a teoria da ubiqüidade. Essa teoria é importante para demarcar a competência na esfera internacional. Veja-se o que dispõe o artigo mencionado:

> Lugar do Crime
> Artigo 6º: Considera-se praticado o crime no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado.

Vários outros países adotam a teoria mista ou da ubiqüidade. Essa teoria surgiu para delimitar a competência nos crimes em que a conduta ocorre em um país e o resultado em outro ou, mesmo, quando partes da ação ocorrem em lugares diferentes e o resultado se dá em outro local.

Nos crimes informáticos a questão é um pouco mais complexa. Existem dificuldades até mesmo para identificar o local onde o autor do delito se localizava fisicamente no momento do crime, bem como o lugar onde os dados, objeto do delito, encontravam-se naquele momento. Há a necessidade de técnicos em sistemas de informática para desvendar esses pontos.

Pode ocorrer de mais de um país entender-se competente para processar e julgar o delito, com base na teoria da ubiqüidade ou em outra eventualmente adotada, bem como no princípio da extraterritorialidade[5], o que poderia ocasionar que alguém fosse processado em mais de um país pela prática do mesmo delito.

Além disso, ainda não há uma definição a respeito dos limites da investigação policial ou judicial. A interceptação de correspondência eletrônica ou a busca e apreensão *on line* de dados judicialmente autorizados, ainda assim podem ser consideradas uma afronta à soberania de outro país, no caso dos dados ou partes dele estarem localizados em outro país.

---

[5] Artigo 7º do Código Penal Brasileiro.

Convênios internacionais sobre o assunto podem ser firmados com o intuito de tornar lícitos certos procedimentos no momento da investigação, sem que isso viole a soberania dos Estados. Já existem exemplos de cooperação internacional para esse fim, é o caso da Decisão-Quadro 2005/222/JAI, de 2005, do Conselho da União Européia, que versou sobre ataques contra os sistemas de informação, tratando de competência internacional, intercâmbio de informações e procedimentos de investigação. Observem-se alguns dos termos mais importantes dessa decisão:

> (1) A presente decisão-quadro tem por objetivo reforçar a cooperação entre as autoridades judiciárias e outras autoridades competentes, nomeadamente as autoridades policiais e outros serviços especializados responsáveis pela aplicação da lei nos Estados-Membros, mediante uma aproximação das suas disposições de direito penal em matéria dos ataques contra os sistemas de informação. (...)
> (5) As consideráveis lacunas e diferenças entre as legislações dos Estados-Membros neste domínio podem entravar a luta contra a criminalidade organizada e o terrorismo e podem dificultar uma cooperação policial e judiciária eficaz no âmbito de ataques contra os sistemas de informação. A natureza transnacional e sem fronteiras dos modernos sistemas de informação implica que os ataques contra esses sistemas têm frequentemente uma dimensão transfronteiriça, evidenciando assim a necessidade urgente de prosseguir a harmonização das legislações penais neste domínio. (...)
> (16) Deverão ser igualmente adotadas medidas de cooperação entre os Estados-Membros, a fim de assegurar uma ação eficaz contra os ataques que visem os sistemas de informação. Os Estados-Membros devem, pois, recorrer à atual rede de pontos de contacto operacionais referida na Recomendação do Conselho, de 25 de Junho de 2001, relativa a um serviço de 24 horas por dia de combate ao crime de alta tecnologia [5], para efeitos de troca de informações.
> **Artigo 10º**
> **Competência**
> 1. Cada Estado-Membro deve definir a sua competência relativamente às infrações referidas nos artigos 2.o, 3.o, 4.o e 5.o, sempre que a infração tiver sido praticada:
> a) Total ou parcialmente no seu território; ou
> b) Por um nacional seu; ou
> c) Em benefício de uma pessoa colectiva com sede no seu território.
> 2. Ao definir a sua competência em conformidade com a alínea a) do n.o 1, cada Estado-Membro deve assegurar que sejam incluídos os casos em que:
> a) O autor praticou a infracção quando se encontrava fisicamente presente no território desse Estado-Membro, independentemente de a infracção visar ou não um sistema de informação situado no seu território; ou
> b) A infracção foi praticada contra um sistema de informação situado no território desse Estado-Membro, independentemente de o autor da infracção se encontrar ou não fisicamente presente no seu território.
> **Artigo 11º**
> **Intercâmbio de informações**
> 1. Para efeitos da troca de informações relativa às infracções referidas nos artigos 2.o, 3.o, 4.o. e 5.o e de acordo com as normas em matéria de protecção de dados, os Estados-Membros devem recorrer à rede existente de pontos de contacto operacionais, disponíveis 24 horas por dia e sete dias por semana.

> 2. Cada Estado-Membro deve notificar ao Secretariado-Geral do Conselho e à Comissão o ponto de contacto designado para efeitos de troca de informações sobre infracções relacionadas com ataques contra sistemas de informação. O Secretariado-Geral transmite essa informação aos restantes Estados-Membros.
>
> **(grifo nosso)**

Ainda não há uma solução capaz de resolver todas as questões anteriormente mencionadas. Pois alguns Estados não possuem legislação sobre os crimes cometidos através da internet, também não há uma uniformidade na normatização da matéria, o que faz com que condutas previstas como crimes em alguns países não o sejam em outros.

Todos esses problemas, além de obstarem a aquisição de provas, dificultam a punição aos criminosos informáticos, deixando-os, muitas vezes, impunes condutas extremamente lesivas não só ao particular, como aos países, como os ataques ao sistema financeiro e à segurança nacional.

O ideal é que os países busquem normas de combate aos delitos informáticos, porém, não de forma isolada, e sim com o apoio de instrumentos de cooperação internacional nessa área. Não se está propondo aqui a criação de um Código Internacional sobre o tema, mas uma maior consonância nas legislações acerca desse assunto através de tratados internacionais.

Os mecanismos de cooperação internacional que versam sobre procedimentos de investigação penal também são importantes, pois, apesar de não tipificarem condutas, procuram oferecer uniformidade aos métodos de investigação, além de proporcionarem uma maior segurança ao país que a desempenha.

É importante também agir com cautela para não ultrapassar a competência territorial do país onde a investigação está ocorrendo, não transformar a prova em ilícita, bem como não transgredir o direito à privacidade das pessoas.

4.2 Evolução histórica da legislação estrangeira e brasileira

A sociedade está em constante transformação e o Direito deve tentar acompanhá-la, sob pena de quedar-se retrógrado. Novas formas de criminalidade surgem a todo o tempo, os Códigos tentam preservar os bens e valores da época

em que foram criados. No entanto, circunstâncias outras aparecem fazendo com que eles não sejam mais capazes de abarcar os comportamentos lesivos, nem de defender a totalidade dos bens jurídicos relevantes.

Hoje, o computador faz parte das vidas das pessoas de uma maneira quase que fundamental, utilizar a internet para realizar pesquisas, fazer compras, enviar um e-mail, são ações rotineiras para milhares de indivíduos. Dados, titulados objetos intangíveis, passaram a ser utilizados com muito mais freqüência, integrando a rotina dos indivíduos e necessitando de uma normatização jurídica.

Essa comunidade completamente informatizada em que se vive fez surgir a já mencionada criminalidade informática, comportando novas formas de cometimento de ilícitos conhecidos, bem como delitos inteiramente novos. E é por causa dessas condutas acima mencionadas que o Direito deve buscar renovar-se, da maneira que sempre aconteceu ao longo dos tempos.

Em se tratando de crime cometido com o auxílio da internet, aconteceram algumas transformações no universo jurídico importantes para sua disciplina. No entanto, até hoje os Estados não concluíram as reformas necessárias em seus ordenamentos jurídicos que pudessem disciplinar de maneira completa essa questão. De acordo com o que ensina Albuquerque (2006, p. 31), dentre as modificações que ocorreram ao longo da história recente dos delitos informáticos, três delas são importantes, as quais serão analisadas nos parágrafos que se seguem.

A primeira delas diz respeito ao direito à privacidade. Esse direito, amplamente conhecido no mundo jurídico, teve que ser analisado sob uma nova perspectiva, a de que dados pessoais devem ser considerados objetos de proteção desse direito. A internet obrigou alguns países a encarar a necessidade de atualizar suas leis a fim de protegerem os dados dos cidadãos, que circulam no ambiente informático.

Em seguida, vieram as alterações nas legislações para acrescentar os crimes de internet de natureza econômica, motivados pela preocupação dos governos com as novas formas de infringir as normas relativas à tributação e à previdência. Por último, surgiram novas concepções referentes aos ilícitos que atentam sobre o direito autoral.

Detendo-se a esfera do direito à privacidade, a legislação estrangeira evoluiu ao longo das últimas décadas para reprimir a espionagem de dados e outros comportamentos similares. Como exemplo, inclui-se o direito alemão, a Carta Magna

da Alemanha, semelhante a do Brasil, faz previsão para o sigilo das telecomunicações, incluindo proteção as transferências de dados pelo meio informático.

O legislador alemão optou por tipificar condutas relativas ao acesso não permitido de dados, inserindo-as dentro do próprio Código Penal Alemão. Na seção 202 deste diploma, já era previsto o delito de violação de correspondência, com aplicação apenas aos dados escritos, e não à violação de correspondência eletrônica.

A grande inovação do Código Penal alemão foi a inserção do artigo 202a, que aborda a espionagem de dados. Incriminando a obtenção não autorizada de dados protegidos através de senhas de acesso ou similar, o conteúdo dos e-mails foi, dessa maneira, abarcado, tenham sido eles enviados ou não. O tipo prevê pena privativa de liberdade de até três anos ou multa para quem comete essa espécie de espionagem.

O diploma incriminador alemão prevê a possibilidade de busca e apreensão de sistemas informáticos, possibilitando também a captação dos dados existentes nesses sistemas, bem como a interceptação de dados que estejam sendo transmitidos, sempre com a devida autorização da autoridade competente. Além disso, há a punição para a modificação de dados (artigo 303a, §1º) e para os crimes de estelionato informático (artigo 263ª e parágrafos) e de sabotagem informática (seção 303b, §1º). É oportuno destacar o teor de alguns dos artigos, mencionados, trazidos por ALBUQUERQUE (2006; p. 195):

> **Art. 202a Espionagem de dados**
> §1º Quem obtém sem autorização para si mesmo ou para outrem dados que não lhe são destinados e que são especialmente protegidos contra acesso não autorizado, será punido com pena privativa de liberdade de até três anos ou com pena de multa.
> §2º Dados no sentido do parágrafo 1º são apenas aqueles que são armazenados ou transmitidos eletrônica ou magneticamente, ou de outra maneira que não seja diretamente perceptível.
> **Art. 263a Estelionato Informático**
> §1º Quem, com a intenção de obter pára si mesmo ou para terceiros uma vantagem patrimonial ilícita, assim prejudica o patrimônio de outrem, ao influenciar o resultado de um procedimento de processamento de dados através da configuração incorreta do programa, através da utilização de dados incorretos ou incompletos, através da utilização não autorizada de dados ou através da intromissão não autorizada sobre o fluxo de dados, será punido com pena privativa de liberdade de até cinco anos ou com pena de multa. [...]
> **Art. 303a Modificação de dados**

> §1° Quem, ilicitamente, apaga, suprime, inutiliza ou modifica dados (art. 202ª, §2°), será punido com pena privativa de liberdade de até dois anos ou com pena de multa.
> §2° A tentativa é punível.
> **Art. 303b Sabotagem informática**
> §1° Quem pertuba um processamento de dados que é de significado essencial para uma firma alheia, para uma empresa alheia ou para um órgão público, ao:
> 1. Praticar um to de acordo com o art. 303ª, §1° ; ou
> 2. Destruir, danificar, inutilizar, eliminar ou modificar uma instalação de processamento de dados ou um suporte de dados;
>
> Será punido com pena privativa de liberdade de até cinco anos ou com pena de multa.
> §2° A tentativa é punível.

Todas essas modificações na legislação alemã inspiraram outros países a legislar sobre o assunto. Algumas das leis estrangeiras foram apresentadas por Silva (2000, págs. 14/15) e serão analisadas nos parágrafos que seguem.

O Código Penal Austríaco foi modificado, primeiro para inserir os crimes de destruição de dados e fraude informática e apenas, posteriormente, a semelhança do Alemão, foi alterado para abarcar a interceptação abusiva de dados (artigo 119a), o acesso ilícito a sistemas de dados (artigo 118a) o dano informático (artigo 119a) e outras práticas com relação a dados informáticos.

A Bélgica também resolveu inserir em seu Código Penal alguns crimes como o estelionato informático, a falsificação informática e os crimes contra a confidencialidade dos sistemas informáticos, bem como dos dados armazenados e transmitidos por eles.

A Holanda adaptou seu Código Penal e introduziu os delitos de dano informático, sabotagem informática e violação de domicílio informático (artigo 138a), além de prever expressamente a busca e apreensão on-line de dados.

Alguns Estados optaram por não modificar seus Códigos Penais, criando leis específicas sobre os delitos informáticos. Assim fizeram Portugal, ao criar as Leis nº 109/91 e 167/98, o Reino Unido, com a promulgação do Ato de Abuso do Computador em 1990, o Chile, que aprovou a Lei nº 19.223/93, entre outros países.

A exemplo dos mencionados, ao longo da década de noventa, outros países adaptaram suas legislações com o intuito de acrescentar a tutela dos delitos informáticos, se não diretamente em seus Códigos Penais, aprovando legislações específicas sobre o tema.

Existem ainda acordos internacionais visando a cooperação e integração dos países no combate aos crimes informáticos. Iniciativas como a Decisão-Quadro

2005/222/JAI, de 2005 do Conselho da União Européia que criam normas comuns para prevenir, investigar e fixar a competência dos ilícitos informáticos são de extrema importância para garantir a punição desses crimes e proporcionar um controle mínimo das ações cometidas através do ambiente virtual.

Comparados com os países citados acima, o Brasil encontra-se atrasado em matéria de legislação para os crimes informáticos. Como já mencionado, a proteção à privacidade é resguardada pela Constituição Federal, em seu artigo 5º, X. O Código Penal Brasileiro prevê em seu artigo 151 o delito de violação de correspondência, porém só se enquadram nesse tipo, a correspondência fechada, instrumento tangível, conhecido à época da elaboração desse diploma repressivo. Apesar de se poder invocar uma violação ao princípio consagrado, não há, portanto, previsão da prática de acesso não autorizados de dados particulares, protegidos através de medidas de segurança.

A interceptação de comunicação informática é proibida pela Lei nº 9296/1996, porém essa norma não é suficiente para proteger o sigilo dos dados transmitidos através de sistemas informáticos no ordenamento jurídico brasileiro.

O Brasil não dispõe de nenhuma legislação específica em matéria de crimes informáticos, e apenas uma pequena alteração foi realizada no Código Penal pátrio, através da Lei nº 9983/2000, para incluir no título XI, que disciplina os crimes contra a administração pública, os artigos 313-A e 313-B, os quais assim dispõem:

> **Inserção de dados falsos em sistema de informações**
> Art. 313-A. Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano:
> Pena - reclusão, de 2 (dois) a 12 (doze) anos, e multa.
> **Modificação ou alteração não autorizada de sistema de informações**
> Art. 313-B. Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente: Pena - detenção, de 3 (três) meses a 2 (dois) anos, e multa.
> Parágrafo único. As penas são aumentadas de um terço até a metade se da modificação ou alteração resulta dano para a Administração Pública ou para o administrado.

Ambos os crimes estão entre os delitos praticados por funcionário público em detrimento da administração pública, sendo o primeiro, o do artigo 313-A chamado de "peculato eletrônico".

Realizando uma pesquisa na legislação penal extravagante do país, observa-se a presença de algumas leis que apesar de não abordarem os delitos informáticos,

indiretamente servem para a proteção dos indivíduos que sofram algum ilícito cometido através de um computador. São exemplos: a lei nº 9610/1998, que versa sobre os direitos autorais; a lei nº 8.137/90, que define crimes contra a ordem tributária, econômica e contra as relações de consumo; a lei nº 9.609/98, que dispõe sobre a proteção da propriedade intelectual de programa de computador e sua comercialização no País.

Como já mencionado, as leis apresentadas não dispõem especificamente sobre delitos cometidos através de computadores, no entanto, algumas dessas condutas ilícitas podem ser protegidas por elas, apenas nas matérias objeto das leis e vedada a analogia *in malam partem* no Direito Penal.

Ainda assim, questões importantes como o acesso ilícito à correspondência eletrônica e aos sistemas informáticos permanecem sem normatização no ordenamento jurídico brasileiro.

4.3 Necessidade de alteração da legislação penal brasileira

A legislação penal vigente não é suficiente para a disciplina dos delitos informáticos, o que gera uma insegurança na sociedade, bem como uma dúvida em que tipos de comportamentos seriam considerados ilegais. Além disso, as normas penais não permitem a aplicação da analogia, salvo a analogia *in bonam partem*, aquela que visa beneficiar o réu. Além disso, a interpretação de leis penais deve ser feita de maneira restritiva.

Logo após o surgimento dos crimes cometidos através de um computador, eles foram sendo enquadrados no delito de estelionato, previsto no artigo 171 do Código Penal pátrio. Ocorre que muitos deles não são nem semelhantes ao estelionato e outros, apesar da similaridade, não poderiam ser tidos como estelionato. De acordo com a proibição da *analogia in malam partem* no direito penal, não pode haver o enquadramento de novas condutas, não previstas pelo legislador, em prejuízo do réu.

Alguns projetos de lei tramitam no Congresso Nacional, propondo a disciplina de alguns crimes informáticos, primeiramente surgiu o Projeto de Lei (PL) nº 84/99 de autoria do deputado Luiz Piauhylino, do PSDB-PE. Em seguida, dois Projetos de

Lei que tramitavam no Senado Federal foram incorporados ao PL nº 84/99, foram o PL nº 76 e o PL nº 137, ambos do ano 2000.

Segundo informações retiradas do sítio eletrônico da Câmara dos Deputados, no início, o Projeto de Lei n nº 84/99 apresentava algumas definições sobre o processamento e a disseminação de informações pelas redes de computadores. Em seu capítulo terceiro, o projeto previa apenas os delitos de dano a dado ou programa de computador (artigo 8º) e de acesso indevido ou não autorizado (artigo 9º) que seriam inseridos no ordenamento jurídico brasileiro através de lei específica. Destaca-se o conteúdo dos artigos mencionados:

> **Dano a dado ou programa de computador**
> Artigo 8º: Apagar, destruir, modificar ou de qualquer forma inutilizar, total ou parcialmente, dado ou programa de computador, de forma indevida ou não autorizada.
> Pena: detenção, de uma a três anos e multa.
> *Parágrafo único:* Se o crime é cometido:
> I - contra o interesse da União, Estado, Distrito Federal, Município, órgão ou entidade da administração direta ou indireta ou de empresas concessionárias de serviços públicos;
> II - com considerável prejuízo para a vítima;
> III - com intuito de lucro ou vantagem de qualquer espécie, própria ou de terceiro;
> IV – com abuso de confiança;
> V – por motivo fútil;
> VI – com o uso indevido de senha ou processo de identificação de terceiro; ou
> VII – com a utilização de qualquer outro meio fraudulento.
> Pena: detenção, de dois a quatro anos e multa.
> **Acesso indevido ou não autorizado**
> Artigo 9º: Obter aceso, indevido ou não autorizado, a computador ou rede de computadores.
> Pena: detenção, de seis meses a um ano e multa.
> *Parágrafo primeiro:* Na mesma pena incorre quem, sem autorização ou indevidamente, obtém, mantém ou fornece a terceiro qualquer meio de identificação ou acesso a computador ou rede de computadores.
> *Parágrafo segundo:* Se o crime é cometido:
> I – com acesso a computador ou redes de computadores da União, Estado, Distrito Federal, Município, órgão ou entidade da administração direta ou indireta ou de empresas concessionárias de serviços públicos;
> II - com considerável prejuízo para a vítima;
> III - com intuito de lucro ou vantagem de qualquer espécie, própria ou de terceiro;
> IV – com abuso de confiança;
> V – por motivo fútil; **(sic)**

Apesar de ser uma iniciativa louvável a regulamentação dos crimes na área de informática, o referido Projeto de Lei demonstrava ser insuficiente, pois só tipificava duas condutas lesivas em seus já citados artigos oitavo e nono.

Atualmente, após substitutivo do Senado Federal, que aguarda aprovação pela Câmara dos Deputados (já tendo obtido parecer favorável na Comissão de Constituição e Justiça e de Cidadania - CCJC), o Projeto 84/99 regula um número bem maior de crimes no âmbito informático e visa modificar o Código Penal Brasileiro. Seriam incluídos nesse Código, entre outros, os seguintes crimes: acesso não autorizado a rede de computadores, dispositivo de comunicação ou sistema informatizado (art. 285-A); obtenção, transferência ou fornecimento não autorizado de dado ou informação (art. 285-B); estelionato eletrônico (art. 171, §2°, VII); dano eletrônico (art. 163); falsificação de dado eletrônico ou documento público (art. 297); inserção ou difusão de código malicioso (art. 163-A)[6].

Portanto, se o Projeto de Lei mencionado restar aprovado pelo Congresso Nacional, com o substitutivo do Senado Federal, e sancionado pelo Presidente da República o Brasil terá uma das legislações mais atualizadas e eficientes em matéria de crimes cometidos na esfera virtual, tipificando várias condutas lesivas.

Ressalta-se a importância de uma reforma como esta para a Legislação Brasileira, no tópico anterior restou demonstrado vários exemplos de transformações na legislação estrangeira que resultaram na introdução de espécies de crimes informáticos, assegurando proteção ao cidadão contra as novas modalidades de delitos que o avanço da tecnologia indiretamente proporcionou.

É certo que nenhuma norma será completa a ponto de abarcar todas as condutas ilegítimas existentes e, ainda que assim fosse novos comportamentos surgem em uma velocidade tal que a legislação estaria sempre atrás, a procura de atualizar-se das transformações provocadas pelo desenvolvimento da humanidade.

Ainda assim, faz-se necessário que o Direito se mobilize a fim de alterar a legislação vigente para que ela possa contemplar as novas maneiras de criminalidade e, sobretudo, no âmbito da criminalidade informática, que possui reflexos "transfronteiriços", a integração entre os Estados é fundamental. Essa cooperação internacional pode garantir uma normatização mínima, similar entre os países, além de maiores possibilidades de combate e punição aos delitos informáticos.

---

[6] O Substitutivo do Senado Federal ao Projeto de Lei 84/99 da Câmaa dos Deputados encontra-se em anexo.

5 CONCLUSÃO

Ao final do presente estudo restou evidenciado que a presença dos computadores no cotidiano das pessoas, bem como o aparecimento da internet e sua crescente utilização para as mais variadas tarefas provocaram enormes transformações na sociedade, algumas delas de caráter negativo.

A internet passou a ser um local onde relações jurídicas acontecem de uma maneira simples e muito veloz. Isso ocorre em decorrência da velocidade proporcionada por esse meio, haja vista que dados são transmitidos instantaneamente para qualquer parte do planeta. A desnecessidade do uso de documentos tangíveis também contribue para a rapidez com que são realizadas as ações no meio eletrônco.

Todas essas mudanças na forma dos indivíduos relacionarem-se fizeram surgir delitos associados à internet. Delitos que a utilizam para suas práticas e que são muito perigosos, haja vista que a internet proporciona uma intercâmbio mundial de informações que ultrapassa as fronteiras nacionais.

Os delitos informáticos podem ter os mais variados objetivos, sejam eles econômicos, militares, entre outros. E a escolha do ambiente eletrônico para sua prática, na maioria dos casos, ocorre pela sua facilidade de utilização, pela sua característica trasfronteiriça, bem como pela sensação de impunidade que ele proporciona aos criminosos.

Restou esclarecido que dos diversos crimes cometidos através da internet, alguns já eram conhecidos e apenas a forma de cometimento foi modificada, outros eram totalmente novos. Em ambos os casos mencionados, há a necessidade de alteração na legislação para compreender os delitos informáticos.

É necessário também uma conscientização da população a respeito dos cuidados que se deve ter ao utilizar um computador, principalmente ao acessar a internet. Através da prática de simples condutas as pessoas podem se proteger de uma "ataque virtual". Essas medidas de vigilância possuem baixo custo se comparadas aos dos danos que elas podem evitar.

Também foi destacada a relevância do direito à privacidade, o qual passou por processos históricos de transformações e atualmente resta amplamente consagrado na doutrina nacional e estrangeira. Esse direito deve ser observado também no meio

informático, haja vista estar previsto na Constituição Federal e ser um corolário da própria dignidade da pessoa humana.

Apesar de a internet ser um local onde as informações circulam com maior liberdade e aparentemente sem controle algum, não se pode ferir um direito individual constitucionalmente resguardado sem provocar uma punição por parte do Estado.

Os crimes informáticos que violam o direito à privacidade devem ter uma atenção maior do legislador e do aplicador do direito. É o caso da violação de correspondência eletrônica, seja em seu momento de armazenamento ou de transmissão. Esse comportamento é de difícil visualização até mesmo pela vítima, pois novas formas de tecnologia aparecem a cada dia, possibilitando a prática de condutas que não deixam vestígios.

Foi explanado que mesmo quando a interceptação de correspondência eletrônica e o acesso não permitido ao correio eletrônico têm como agentes empresas que desejam ter um controle das atividades de seus empregados essas condutas são ilegítimas. Por isso, devem ser punidas da mesma forma que se figurasse no pólo ativo do delito um particular.

De igual modo, a espionagem indiscriminada do correio eletrônico pelo poder público, visando prevenir e combater a prática de crimes fere o direito à privacidade dos indivíduos, necessitando ser combatida e punida.

Foi demonstrada a dificuldade de se determinar o local onde o crime informático foi praticado, tendo em vista sua natureza transfronteiriça e a facilidade de fracionar o *iter criminis*. Além disso, precisar qual país é competente para processar e julgar o criminoso não é tarefa dais mais fáceis. A legislação interna dos países envolvidos deve ser observada para verificar-se se, no que diz respeito ao lugar do crime, a teoria aplicada é a da ação, do resultado ou da ubiquidade. No Brasil, como demonstrado, é adotada a teoria da ubiquidade.

O ambiente virtual não pode ser deixado à margem do ordenamento jurídico, haja vista que milhares de relações são nele efetuadas por dia. Os delitos cometidos nesse meio precisam estar regulamentados até para que não restem dúvidas de quais condutas lesivas constituem crime.

Ficou patente a necessidade dos Estados alterarem suas legislações a fim de introduzirem os delitos informáticos, principalmente os que infingem o direito à privacidade pela sua importância, bem como pela dificuldade de se enquadrarem

nos tipos já existentes. Essa alteração pode se dar de duas maneiras: pela inserção de novos artigos no Código Penal ou pela aprovação de lei específica, ambas visando regulamentar esses crimes.

Alguns países já fizeram algumas modificações em suas leis penais, visando incluir os delitos informáticos, é o caso da Alemanhã, Bélgica, Holanda, entre outros. Resta evidente que o Brasil deve seguir os exemplos mencionados e regulamentar os delitos informáticos.

No país, existe hoje um Projeto de Lei, em tramitação no Congresso Nacional, que disciplina alguns crimes informáticos, inclusive os relativos à violação de privacidade. É de fundamental importância a aprovação desse projeto para amparar o cidadão brasileiro dos chamados criminosos informáticos e de suas condutas lesivas.

Ressaltou-se, que não basta a reforma da legislação interna de cada Estado, necessário se faz firmar instrumentos de cooperação internacional. Já existem alguns exemplos desses instrumentos, os quais sugestionam os delitos que se visa punir, bem como os bem jurídicos a serem tutelados. Eles proporcionam ainda uma uniformidade nos meios de investigação a serem utilizados e aumentam a possibilidade de punição dos criminosos.

REFERÊNCIAS

ALBUQUERQUE, Roberto Chacon de. **A criminalidade informática.** 2. ed. São Paulo: Juarez de Oliveira, 2006.

ALMEIDA, Gilberto. **Grampo eletrônico de funcionários: permitido ou ilegal?** Disponível em: http://www.crasp.com.br/index.asp?secao=438. Acesso em: 04 nov. 2009.

CÂMARA DOS DEPUTADOS. Projeto de Lei nº 84/99. Disponível em: http://www2.camara.gov.br/proposicoes. Acesso em: 04 out. 2009.

DEUTSCHE WELLE. **França: vigilância cerrada e papel "positivo" do colonialismo.** Disponível em: http://www.dw-world.de/dw/article/0,,1796175,00.html. Acesso em: 04 nov. de 2009.

EMBAIXADA DOS ESTADO UNIDOS DA AMÉRICA. **Bush Comenta Sobre a Assinatura da Nova Lei Antiterrorismo.** Disponível em: http://terrorismo.embaixada-americana.org.br/?action=artigo&idartigo=215. Acesso em: 04 nov. 2009.

IBOPE NIELSEN ONLINE. **Ranking da internet no Brasil.** Disponível em: http://www.ibope.com.br/calandraWeb/servlet/CalandraRedirect?temp=6&proj=PortalIBOPE&pub=T&nome=home_materia&db=caldb&docid=E37C727B59300DFE83257639004D478C. Acesso em: 10 out. 2009.

IBOPE NIELSEN ONLINE. **Brasil superou o número de 40 milhões de pessoas com acesso à internet.** Disponível em: http://www.ibope.com.br/calandraWeb/servlet/CalandraRedirect?temp=5&proj=PortalIBOPE&pub=T&db=caldb&comp=Internet&docid=F0BA65FF8A513A48832574750050527E. Acesso em: 10 out. 2009.

JÚNIOR. Tércio Sampaio Ferraz. **Sigilo de Dados: o direito à privacidade e os limites à função fiscalizadora do Estado.** Disponível em: ttp://www.terciosampaioferrazjr.com.br/?q= /publicacoes-cientificas/49. Acesso em: 27 out. 2009.

MENDES, Ferreira Gilmar; COELHO, Inocênico Mártires; BRANCO, Paulo Gustavo Gonet. **Curso de Direito Constitucional.** 2. ed. rev. e atual. São Paulo: Saraiva, 2008.

MORAES, Alexandre de. **Direito Constitucional.** 18 ed. São Paulo: Atlas, 2005.

NUNES, Ângela. **Como evitar larápios da era digital.** Disponível em: http://veja.abril.com.br/181000/p_140.html. Acesso em: 25 set. 2009.

PODESTÁ, Fábio Henrique. **Direito à intimidade em Ambiente de Internet. Direito e Internet – Aspectos Jurídicos Relevantes.** São Paulo: EDIPRO, 2000.

SOUSA, Camila Maria Brito de. **Privacidade e internet**. Recife: Nossa Livraria, 2005.

GRECO, Rogério. **Direito Penal.** 3. ed. rev. e atual.Niterói, Rio de Janeiro: Saraiva, 2007. 2. v.

SILVA. Remy Gama. **Crimes da Informática.** CopyMarket.com, 2000.

ANEXO

Substitutivo do Senado ao Projeto de Lei da Câmara nº 89, de 2003 (PL nº 84, de 1999, na Casa de origem), que "Altera o Decreto- Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal e a Lei nº 9.296, de 24 de julho de 1996, e dá outras providências".

Substitua-se o Projeto pelo seguinte:

Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), o Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), a Lei nº 7.716, de 5 de janeiro de 1989, a Lei nº 8.069, de 13 de julho de 1990, e a Lei nº 10.446, de 8 de maio de 2002, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, de rede de computadores, ou que sejam praticadas contra dispositivos de comunicação ou sistemas informatizados e similares, e dá outras providências.

O **Congresso Nacional** decreta:

Art. 1º Esta Lei altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), o Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), a Lei nº 7.716, de 5 de janeiro de 1989, a Lei nº 8.069, de 13 de julho de1990, e a Lei nº 10.446, de 8 de maio de 2002, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, de rede de computadores, ou que sejam praticadas contra dispositivos de comunicação ou sistemas informatizados e similares, e dá outras providências.

Art. 2º O Título VIII da Parte Especial do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) fica acrescido do Capítulo IV, com a seguinte redação:

CAPÍTULO IV

DOS CRIMES CONTRA A SEGURANÇA

DOS SISTEMAS INFORMATIZADOS

Acesso não autorizado a rede de computadores, dispositivo de comunicação ou sistema informatizado

Art. 285-A. Acessar, mediante violação de segurança, rede de computadores, dispositivo de comunicação ou sistema informatizado, protegidos por expressa restrição de acesso:

Pena - reclusão, de 1 (um) a 3 (três) anos, e multa.

Parágrafo único. Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada de sexta parte.

Obtenção, transferência ou fornecimento não autorizado de dado ou informação

Art. 285-B. Obter ou transferir, sem autorização ou em desconformidade com autorização do legítimo titular da rede de computadores, dispositivo de comunicação ou sistema informatizado, protegidos por expressa restrição de acesso, dado ou informação neles disponível:

Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.

Parágrafo único. Se o dado ou informação obtida desautorizadamente é fornecida a terceiros, a pena é aumentada de um terço.

Ação Penal

Art. 285-C. Nos crimes definidos neste Capítulo somente se procede mediante representação, salvo se o crime é cometido contra a União, Estado, Município, empresa concessionária de serviços públicos, agências, fundações, autarquias, empresas públicas ou sociedade de economia mista e subsidiárias."

Art. 3º O Título I da Parte Especial do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) fica acrescido do seguinte artigo, com a seguinte redação:

"**Divulgação ou utilização indevida de informações e dados pessoais**

Art. 154-A. Divulgar, utilizar, comercializar ou disponibilizar dados e informações pessoais contidas em sistema informatizado com finalidade distinta da que motivou seu registro, salvo nos casos previstos em lei ou mediante expressa anuência da pessoa a que se referem, ou de seu representante legal:

Pena – detenção, de 1 (um) a 2 (dois) anos, e multa.

Parágrafo único. Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada de sexta parte."

Art. 4º O **caput** do art. 163 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) passa a vigorar com a seguinte redação:

"**Dano**

Art. 163. Destruir, inutilizar ou deteriorar coisa alheia ou dado eletrônico alheio:

....." (NR)

Art. 5º O Capítulo IV do Título II da Parte Especial do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) fica acrescido do art. 163-A, assim redigido:

"Inserção ou difusão de código malicioso

Art. 163-A. Inserir ou difundir código malicioso em dispositivo de comunicação, rede de computadores, ou sistema informatizado: Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.

Inserção ou difusão de código malicioso seguido de dano

§ 1º Se do crime resulta destruição, inutilização, deterioração, alteração, dificultação do funcionamento, ou funcionamento desautorizado pelo legítimo titular, de dispositivo de comunicação, de rede de computadores, ou de sistema informatizado: Pena – reclusão, de 2 (dois) a 4 (quatro) anos, e multa.

§ 2º Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada de sexta parte."

Art. 6º O art. 171 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) passa a vigorar acrescido dos seguintes dispositivos:

"Art. 171. .....

.....

§ 2º Nas mesmas penas incorre quem:

.....

Estelionato Eletrônico

VII – difunde, por qualquer meio, código malicioso com intuito de facilitar ou permitir acesso indevido à rede de computadores, dispositivo de comunicação ou sistema informatizado.

§ 3º Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime previsto no inciso VII do § 2º, a pena é aumentada de sexta parte." (NR)

Art. 7º Os arts. 265 e 266 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) passam a vigorar com as seguintes redações:

"**Atentado contra a segurança de serviço de utilidade pública**

Art. 265. Atentar contra a segurança ou o funcionamento de serviço de água, luz, força, calor, informação ou telecomunicação, ou qualquer outro de utilidade pública:

....." (NR)

"**Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático, dispositivo de comunicação, rede de computadores ou sistema informatizado**

Art. 266. Interromper ou perturbar serviço telegráfico, radiotelegráfico, telefônico, telemático, informático, de dispositivo de comunicação, de rede de computadores, de sistema informatizado ou de telecomunicação, assim como impedir ou dificultar-lhe o restabelecimento:

....." (NR)

Art. 8º O **caput** do art. 297 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) passa a vigorar com a seguinte redação:

"**Falsificação de dado eletrônico ou documento público**

Art. 297. Falsificar, no todo ou em parte, dado eletrônico ou documento público, ou alterar documento público verdadeiro:

....." (NR)

Art. 9º O **caput** do art. 298 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) passa a vigorar com a seguinte redação:

"**Falsificação de dado eletrônico ou documento particular**

Art. 298. Falsificar, no todo ou em parte, dado eletrônico ou documento particular ou alterar documento particular verdadeiro:

....." (NR)

Art. 10. O art. 251 do Capítulo IV do Título V da Parte Especial do Livro I do Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), passa a vigorar acrescido do inciso VI ao seu § 1º, e do § 4º, com a seguinte redação:

"Art. 251. .....

§ 1º Nas mesmas penas incorre quem:

.....

Estelionato Eletrônico

VI - Difunde, por qualquer meio, código malicioso com o intuito de facilitar ou permitir o acesso indevido a rede de computadores, dispositivo de comunicação ou a sistema informatizado, em prejuízo da administração militar.

.....

§ 4º Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada de sexta parte." (NR)

Art. 11. O **caput** do art. 259 e o **caput** do art. 262 do Capítulo VII do Título V da Parte Especial do Livro I do Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), passam a vigorar com a seguinte redação:

"**Dano Simples**

Art. 259. Destruir, inutilizar, deteriorar ou fazer desaparecer coisa alheia ou dado eletrônico alheio, desde que este esteja sob administração militar: ....." (NR)

"**Dano em material ou aparelhamento de guerra ou dado eletrônico**

Art. 262. Praticar dano em material ou aparelhamento de guerra ou dado eletrônico de utilidade militar, ainda que em construção ou fabricação, ou em efeitos recolhidos a depósito, pertencentes ou não às forças armadas: ....." (NR)

Art. 12. O Capítulo VII do Título V da Parte Especial do Livro I do Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), fica acrescido do art. 262-A, com a seguinte redação:

"**Inserção ou difusão de código malicioso**

Art. 262-A. Inserir ou difundir código malicioso em dispositivo de comunicação, rede de computadores, ou sistema informatizado, desde que o fato atente contra a administração militar:

Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.

Inserção ou difusão de código malicioso seguido de dano

§ 1º Se do crime resulta destruição, inutilização, deterioração, alteração, dificultação do funcionamento, ou funcionamento não autorizado pelo titular, de dispositivo de comunicação, de rede de computadores, ou de sistema informatizado:

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

§ 2º Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada de sexta parte."

Art. 13. O Título VII da Parte Especial do Livro I do Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), fica acrescido do Capítulo VIII, com a seguinte redação:

"CAPÍTULO VIII

DOS CRIMES CONTRA A SEGURANÇA DOS SISTEMAS

INFORMATIZADOS

Acesso não autorizado a rede de computadores, dispositivo de comunicação ou sistema informatizado

Art. 339-A. Acessar, mediante violação de segurança, rede de computadores, dispositivo de comunicação ou sistema informatizado, protegidos por expressa restrição de acesso, desde que o fato atente contra a administração militar:

Pena - reclusão, de 1 (um) a 3 (três) anos, e multa.

Parágrafo único. Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada de sexta parte.

Obtenção, transferência ou fornecimento não autorizado de dado ou informação

Art. 339-B. Obter ou transferir, sem autorização ou em desconformidade com autorização do legítimo titular da rede de computadores, dispositivo de comunicação ou sistema informatizado, protegidos por expressa restrição de acesso, dado ou informação neles disponível, desde que o fato atente contra a administração militar:

Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.

Parágrafo único. Se o dado ou informação obtida desautorizadamente é fornecida a terceiros, a pena é aumentada de um terço.

Divulgação ou utilização indevida de informações e dados pessoais

Art. 339-C. Divulgar, utilizar, comercializar ou disponibilizar dados e informações pessoais contidas em sistema informatizado sob administração militar com finalidade distinta da que motivou seu registro, salvo nos casos previstos em lei ou mediante expressa anuência da pessoa a que se referem, ou de seu representante legal:

Pena – detenção, de 1 (um) a 2 (dois) anos, e multa.

Parágrafo único. Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada de sexta parte."

Art. 14. O **caput** do art. 311 do Capítulo V do Título VII do Livro I da Parte Especial do Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), passa a vigorar com a seguinte redação:

"**Falsificação de documento**

Art. 311. Falsificar, no todo ou em parte, documento público ou particular, ou dado eletrônico ou alterar documento verdadeiro, desde que o fato atente contra a administração **ou** **o** serviço militar:

....." (NR)

Art. 15. Os incisos II e III do art. 356 do Capítulo I do Título I do Livro II da Parte Especial do Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), passam a vigorar com a seguinte redação:

"CAPÍTULO I

DA TRAIÇÃO

Favor ao inimigo

Art. 356. .....

.....

II - entregando ao inimigo ou expondo a perigo dessa conseqüência navio, aeronave, força ou posição, engenho de guerra motomecanizado, provisões, dado eletrônico ou qualquer outro elemento de ação militar;

III - perdendo, destruindo, inutilizando, deteriorando ou expondo a perigo de perda, destruição, inutilização ou deterioração, navio, aeronave, engenho de guerra motomecanizado, provisões, dado eletrônico ou qualquer outro elemento de ação militar.

....." (NR)

Art. 16. Para os efeitos penais considera-se, dentre outros: I – dispositivo de comunicação: qualquer meio capaz de processar, armazenar, capturar ou transmitir dados utilizando-se de tecnologias magnéticas, óticas ou qualquer outra tecnologia;

II – sistema informatizado: qualquer sistema capaz de processar, capturar, armazenar ou transmitir dados eletrônica ou digitalmente ou de forma equivalente;

III – rede de computadores: o conjunto de computadores, dispositivos de comunicação e sistemas informatizados, que obedecem a um conjunto de regras, parâmetros, códigos, formatos e outras informações agrupadas em protocolos, em nível topológico local, regional, nacional ou mundial através dos quais é possível trocar dados e informações;

IV – código malicioso: o conjunto de instruções e tabelas de informações ou qualquer outro sistema desenvolvido para executar ações danosas ou obter dados ou informações de forma indevida;

V – dados informáticos: qualquer representação de fatos, de informações ou de conceitos sob forma suscetível de processamento numa rede de computadores ou dispositivo de comunicação ou sistema informatizado;

VI – dados de tráfego: todos os dados informáticos relacionados com sua comunicação efetuada por meio de uma rede de computadores, sistema

informatizado ou dispositivo de comunicação, gerados por eles como elemento de uma cadeia de comunicação, indicando origem da comunicação, o destino, o trajeto, a hora, a data, o tamanho, a duração ou o tipo do serviço subjacente.

Art. 17. Para efeitos penais consideram-se também como bens protegidos o dado, o dispositivo de comunicação, a rede de computadores, o sistema informatizado.

Art. 18. Os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado.

Art. 19. O inciso II do § 3º do art. 20 da Lei nº 7.716, de 5 de janeiro de 1989, passa a vigorar com a seguinte redação:

"Art. 20 .....

.....

§ 3º.....

.....

II – a cessação das respectivas transmissões radiofônicas, televisivas, eletrônicas, ou da publicação por qualquer meio.

....." (NR)

Art. 20. O **caput** do art. 241 da Lei nº 8.069, de 13 de julho de 1990, passa a vigorar com a seguinte redação:

"Art. 241. Apresentar, produzir, vender, receptar, fornecer, divulgar, publicar ou armazenar consigo, por qualquer meio de comunicação, inclusive rede mundial de computadores ou Internet, fotografias, imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente:

....." (NR)

Art. 21. O art. 1º da Lei nº 10.446, de 8 de maio de 2002, passa a vigorar com a seguinte redação:

"Art. 1º .....

.....

V – os delitos praticados contra ou mediante rede de computadores, dispositivo de comunicação ou sistema informatizado.

....." (NR)

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

I – manter em ambiente controlado e de segurança, pelo prazo de 3 (três) anos, com o objetivo de provimento de investigação pública formalizada, os dados de endereçamento eletrônico da origem, hora, data e a referência GMT da conexão efetuada por meio de rede de computadores e fornecê-los exclusivamente à autoridade investigatória mediante prévia requisição judicial;

II – preservar imediatamente, após requisição judicial, outras informações requisitadas em curso de investigação, respondendo civil e penalmente pela sua absoluta confidencialidade e inviolabilidade;

III – informar, de maneira sigilosa, à autoridade competente, denúncia que tenha recebido e que contenha indícios da prática de crime sujeito a acionamento penal público incondicionado, cuja perpetração haja ocorrido no âmbito da rede de computadores sob sua responsabilidade.

§ 1º Os dados de que cuida o inciso I deste artigo, as condições de segurança de sua guarda, a auditoria à qual serão submetidos e a autoridade competente responsável pela auditoria, serão definidos nos termos de regulamento.

§ 2º O responsável citado no **caput** deste artigo, independentemente do ressarcimento por perdas e danos ao lesado, estará sujeito ao pagamento de multa variável de R$ 2.000,00 (dois mil reais) a R$ 100.000,00 (cem mil reais) a cada requisição, aplicada em dobro em caso de reincidência, que será imposta pela autoridade judicial desatendida, considerando-se a natureza, a gravidade e o prejuízo resultante da infração, assegurada a oportunidade de ampla defesa e contraditório.

§ 3º Os recursos financeiros resultantes do recolhimento das multas estabelecidas neste artigo serão destinados ao Fundo Nacional de Segurança Pública, de que trata a Lei nº 10.201, de 14 de fevereiro de 2001.

Art. 23. Esta Lei entra em vigor 120 (cento e vinte) dias após a data de sua publicação.

Senado Federal, em de julho de 2008

Senador Garibaldi Alves Filho

Presidente do Senado Federal