

INTRODUÇÃO

A presente dissertação trata das novas tecnologias, telemática e da difícil proteção da privacidade: Uma abordagem dos aspectos penais na rede mundial de computadores.

A palavra telemática¹ foi criada em 1978 pelos franceses Simon Nora e Alain Minc com a finalidade de criar uma nova terminologia para expressar a associação de tecnologias em telecomunicações (telefonia, satélite, cabos elétricos e ópticos) e informática (computadores, softwares e sistemas de redes) que facultam o processamento, armazenamento e a comunicação de grandes quantidades de dados nos diversos formatos como texto, imagem e som. Tudo isso em interoperabilidade no menor decurso temporal possível, entre pessoas-usuários localizadas em qualquer parte do planeta.

Na atualidade, a evolução das tecnologias mencionadas pode ser representada pela rede mundial de computadores (Internet) em razão de ser a expressão da telemática no mundo fático.

Assim, os benefícios gerados pelos avanços tecnológicos são inegáveis. A interação entre os indivíduos proporciona maior integração entre eles tendo em vista que mesmo com uma comunicação virtual, em que o fator distância está presente, rompe-se o paradigma da frieza e do distanciamento entre os indivíduos. A rede pode servir como instrumento de educação e acesso a vários tipos de assuntos a qualquer hora e em diversas áreas, desde os esportes à culinária, compras de Cds/Dvds, livros, vídeos, roupas, acesso à economia mundial, cotações da Bolsa de Valores, atividades bancárias e até o que outrora seria inimaginável, possibilitando ao Judiciário obter depoimentos de presos² à distância usando uma tecnologia denominada Vídeo Conferência cujo meio de propagação é a Internet, utilizando assim, todos os recursos da telemática.

¹ O termo Telemática significa a associação de tecnologias de telecomunicações e informática utilizado pela primeira vez no "Rapport Nora-Minc": SIMON NORA e ALAIN MINC, L'Informatisation de la société, ed. La Documentation Française, Paris, 1978.

² BRASIL. **A Lei nº 11.900/2008 que altera dispositivos do Decreto-Lei nº 3.689**, de 3 de outubro de 1941 - Código de Processo Penal, para prever a possibilidade de realização de interrogatório e outros atos processuais por sistema de videoconferência, e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2009/Lei/L11900.htm> Acesso em: 18 dez. 2011.

Dentre os diversos Direitos e Garantias Fundamentais, através do critério do objeto de estudo, menciona-se o direito à informação o qual está previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal, assim como de forma consolidada na Lei nº 12.527 de 18 de novembro de 2011. Também encontramos no art. 5º, inciso XII, da Carta Máxima, a inviolabilidade do sigilo de correspondência, dados, comunicações telegráficas e telefônicas.

O direito à informação é um dos alicerces do Estado Democrático de Direito, bem como ferramenta basilar para a efetivação do exercício da cidadania. O direito de dar e receber informação se origina historicamente na liberdade de imprensa, direito este que atualmente se estende a todas as pessoas e entidades públicas ou privadas, conceituado como “*o direito público subjetivo e individual de transmitir informações a terceiros, inclusive à coletividade, respeitada a dignidade, a honra e a imagem da pessoa humana*”³.

A necessidade de análise das relações dos homens via rede mundial de computadores - Internet - foi o motivador da grande vontade de aprofundamento neste rumo que o Direito terá que administrar. Indubitavelmente, estabelecer o equilíbrio entre as tecnologias emergentes e o remédio jurídico que deverá ser aplicado será o grande desafio da atualidade, em especial na Internet.

O móvel desse trabalho é a dificuldade de tutelar direitos fundamentais à dignidade da pessoa humana nas questões pertinentes à intimidade, privacidade, inviolabilidade das comunicações pessoais e à propriedade imaterial na rede mundial de computadores – Internet e quais os remédios jurídicos na esfera penal que podem ser aplicados.

Para o adequado desenvolvimento do tema desta dissertação serão evocados o direito normatizado na Constituição Federal e todas as demais normas infraconstitucionais vinculadas ao direito da sociedade da informação, ao direito penal e diplomas extravagantes, o direito estrangeiro, abordagens doutrinárias a respeito do tema e o trato da jurisprudência dos Tribunais Superiores. Essas considerações afirmam a urgente necessidade de ação estatal no sentido de efetivar

³ WEICHERT, Marlon Alberto. **Dicionário de Direitos Humanos**. Disponível em: <<http://www.esmpu.gov.br/dicionario/tiki-index.php?page=Informa%C3%A7%C3%A3o>> Acesso em: 19 dez. 2012.

o direito em análise tendo em vista a competência dos poderes constituídos para a efetivação dos direitos fundamentais e formação da cidadania.

1. DOS DIREITOS FUNDAMENTAIS E A DIGNIDADE DA PESSOA HUMANA

1.1. Dos Direitos Fundamentais

Os Direitos Fundamentais são compreendidos como aqueles direitos inerentes à própria condição humana os quais estão previstos no ordenamento jurídico. Existe um gama de denominações de conceitos sobre esse tema, tanto que para José Afonso⁴, entre as várias denominações empregadas para os Direitos do Homem, o mais adequado é a denominação de Direitos Fundamentais do Homem:

[...] esse é o termo mais correto a ser usado, pois além de referir-se a princípios que resumem a concepção do mundo, no nível de direito positivo, com prerrogativas e instituições que ele concretiza em garantias de uma convivência digna, livre, e igual de todas as pessoas. Fundamentais, porque exprime situações jurídicas sem as quais a pessoa humana não se realiza e às vezes nem sobrevive⁵.

Segundo Manoel Ferreira Filho, a partir da Revolução de 1798 as questões pertinentes às declarações de direitos ancoram aspectos do constitucionalismo:

[...] a opressão absolutista foi a causa próxima do surgimento das Declarações. Destas a primeira foi a do Estado da Virgínia, votada em junho de 1776, que serviu de modelo para as demais na América do Norte embora a mais conhecida e influente seja a dos "Direitos do Homem e do Cidadão", editada em 1789 pela Revolução Francesa⁶.

Preconiza ainda que a Declaração dos Direitos do Homem e do Cidadão, editada em 1789, não surge com a finalidade de criar direitos fundamentais, mas para conscientizar o homem da existência dos direitos fundamentais, afirmando ainda que "*[..]proteger os Direitos do Homem contra os atos do Governo e é expressa a menção ao Poder Legislativo e ao Poder Executivo, o objetivo imediato é de caráter pedagógico: instruir os indivíduos de seus direitos fundamentais*"⁷.

⁴ SILVA, José Afonso da. **Curso de Direito Constitucional Positivo**. Ed. Malheiros, 2002. p.176.

⁵ FRANÇA, Limongi Rubens. **Instituições de Direito Civil**. 3.^a Ed. atual. São Paulo: Saraiva, 1994.

⁶ FERREIRA FILHO, Manoel Gonçalves. **Curso de Direito Constitucional**, 25 Ed., São Paulo: Saraiva, 1999, p. 281

⁷ Idem. **Direitos Humanos Fundamentais**. 4.^a Ed. revista São Paulo: Saraiva, 2000. p22.

A partir dessa data a Universalização dos Direitos do Homem toma maior proporção tornando-se o ponto inicial para a inserção de outros direitos, como o direito da personalidade. Esse avanço decorre das ações implementadas pelos homens na Constituição Mexicana de 1917, conforme registra Fábio Comparato que tal constituição foi “*a primeira a atribuir aos direitos trabalhistas a qualidade de direitos fundamentais, juntamente com as liberdades individuais e os direitos políticos*”⁸, instituindo o pioneirismo no mundo do direito laboral.

Em seguida, contribuía a nação Alemã com o projeto de república democrática o qual foi resultante dos problemas econômicos e geopolíticos vividos logo após a Primeira Guerra Mundial. Era uma fase de profunda instabilidade política e social levando-a a ser signatária do tratado de Versalhes. Dentro desse quadro incluía-se o fato de que a Alemanha tinha uma extensa classe operária organizada em sindicatos e partidos políticos com movimentos revolucionários. A burguesia buscou neutralizar através da repressão e com o projeto denominado República Democrática e Social, posteriormente chamada por República de Weimar⁹. Essa constituição apresentava dois aspectos: a regulamentação e organização do Estado, e a declaração de direitos e deveres fundamentais do homem, incluindo as liberdades individuais e alguns direitos de conteúdo social¹⁰.

A Declaração da Organização das Nações Unidas de 1948 foi o ponto culminante para o nascedouro dos remédios jurídicos que tutelam os direitos fundamentais. Uma reação em cascata ocorreu em diversas nações do mundo, a positivação dos direitos torna-se fenômeno que revolucionou a condição humana. Essas positivações surgem ao longo de todo o planeta como forma de assegurar direitos fundamentais da condição humana. Nesse sentido aduz Norberto Bobbio:

Do ponto de vista teórico, sempre defendi - e continuo a defender, fortalecido por novos argumentos - que os direitos do homem, por mais fundamentais que sejam, são direitos históricos, ou seja, nascidos em certas circunstâncias, caracterizadas por lutas em defesa de novas liberdades contra velhos poderes, e nascidos de modo gradual, não todos de uma vez e nem de uma vez por todas¹¹.

⁸ COMPARATO, Fábio Konder. **A Afirmação Histórica Dos Direitos Humanos**. São Paulo: Saraiva, 2008. 6a ed. p. 174

⁹ DIMOULIS, Dimitri; MARTINS, Leonardo. **Teoria geral dos Direitos Fundamentais**. São Paulo: Revista dos Tribunais, 2006. , p. 33

¹⁰ COMPARATO, op. cit., p. 193.

¹¹ BOBBIO, Norberto. **A Era dos Direitos**. 11. ed. Rio de Janeiro: Campus, 1992. , p. 5.

A Declaração Universal dos Direitos Humanos inicia com o texto do artigo 1º que por si só resume todas as necessidades e carências da humanidade: “*I - Todos os Homens nascem livres e iguais em dignidade e direitos. São dotados de razão e consciência e devem agir em relação uns aos outros com espírito de fraternidade*”¹².

1.2. Direitos Fundamentais e a Constituição Brasileira

Os direitos fundamentais assegurados ao homem ao serem introduzidos pelo legislador na Constituição de 1988 acabaram por consignar um dever do Estado em salvaguardar os direitos do ser humano.

O *caput* do art. 5º da Constituição Federal determina: “*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[...]*”¹³.

Para Figueiredo Ingo Wolfgang Sarlet¹⁴, a Constituição de 1988 reconhece a pessoa humana como titular dos direitos fundamentais com base no princípio da dignidade humana. As garantias referidas na Carta Magna seguem aos princípios como ordem basilar e determinante, valorando aspectos relevantes para o bem-estar social e democrático da vida individual e comum, em que pese(m) abarcar os novos e crescentes problemas surgidos no seio social, a fim de buscar solucionar os conflitos deles recorrentes e encontrar a melhor solução diante de tais questões. Para J.J. Gomes Canotilho, deve-se ressaltar que a “*consequência natural da*

¹² ONU. **Declaração Universal dos Direitos Humanos**, Disponível em: http://portal.mj.gov.br/sedh/ct/legis_intern/ddh_bib_inter_universal.htm. Acesso em 12 dez. 2012.

¹³ BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em 21 mar. 2012.

¹⁴ SARLET, Ingo Wolfgang; FIGUEIREDO, Mariana Filchtiiner. Reserva do possível, mínimo existencial e direito à saúde: algumas aproximações. In: SARLET, Ingo Wolfgang; TIMM, Luciano Benneti. (Coord.) **Direitos fundamentais, orçamento e “reserva do possível”**. 2. ed. Porto Alegre: Livraria do advogado, 2010.

*existência de princípios em uma constituição reside na existência de fenômenos de tensão*¹⁵.

Os princípios jurídicos são os pontos primários, o alicerce do Direito, servindo como seu ponto de partida. Assim lembra De Plácido¹⁶, para quem, nesta acepção, além dos fundamentos jurídicos legalmente instituídos, está também o axioma jurídico que tem origem na cultura jurídica universal.

Desta forma, os princípios constituem os fundamentos da Ciência Jurídica onde se consolidaram as normas originárias ou as leis científicas do Direito, balizadores das noções em que se fundamenta o próprio Direito, aduzindo o referido autor que *“Assim nem sempre os princípios se inscrevem nas leis, mas, porque servem de base ao Direito, são tidos como preceitos fundamentais para a prática do Direito e proteção aos direitos”*¹⁷.

Os princípios fundamentais devem ser mitigados conjuntamente à concepção do Estado e à realidade social. Eles estão inter-relacionados e interagem entre si. No caso concreto, cabe ao intérprete, em caso de colisão, privilegiar um ou outro, sempre com o juízo de ponderação¹⁸.

A Constituição de 1988 vincula-se ao movimento doutrinário pós-positivista¹⁹ que se caracteriza pela aproximação entre o Direito e a ética, pela tentativa de resgatar os valores civilizatórios dando primazia aos direitos fundamentais, no centro dos quais está o princípio da dignidade do ser humano.

¹⁵ CANOTILHO, J.J. Gomes. **Direito Constitucional e Teoria da Constituição**. Portugal: Almedina, 2003, p.36.

¹⁶ SILVA, De Plácido e. **Vocábulos jurídicos**. Rio de Janeiro: Forense, 1999, p.1090.

¹⁷ Ibidem, p.449.

¹⁸ ARAÚJO, José Henrique Mouta. Ações judiciais em defesa dos direitos fundamentais: em busca de solução para casos concretos. In: DIAS, Jean Carlos; KLAUTAU FILHO, Paulo. (Coord.) **Direitos fundamentais: teoria do direito e sustentabilidade**. Rio de Janeiro: Forense, 2009.

¹⁹ BARROSO, Luís Roberto. **Fundamentos Teóricos e Filosóficos do Novo Direito Constitucional Brasileiro (Pós-modernidade, Teoria Crítica e Pós-Positivismo)**. In *A Nova Interpretação Constitucional: Ponderação, Direitos Fundamentais e Relações Privadas*. Luís Roberto Barroso (organizador). 2ª Edição. Rio de Janeiro: Renovar, 2006, p. 27-28.

1.3 Da Dignidade da Pessoa Humana

Na busca de discorrer sobre temática de tal importância destacamos Imanuel Kant quando aduz que *“Ora digo eu: O homem, e, de uma maneira geral, todo o ser racional, existe como fim em si mesmo, não só como meio para o uso arbitrário desta ou daquela vontade”*²⁰, buscou expressar o valor do homem como ser autônomo.

Para se expressar com maior exatidão a idéia de que o homem *existe como fim em si mesmo* começa fazendo um paralelo entre os seres - racionais e irracionais:

Os seres cuja existência depende, não em verdade da nossa vontade, mas da natureza têm contudo, se são seres irracionais, apenas um valor relativo como meios e por isso se chamam coisas, ao passo que os seres racionais se chamam pessoas, porque a sua natureza os distingue já como fins em si mesmos.²¹

Para caracterizar o homem com ser especial aduz Kant: *“Mas o homem não é uma coisa; não é, portanto, um objeto que possa ser utilizado ‘simplesmente’ como um meio, mas pelo contrário deve ser considerado sempre em todas as suas ações como fim em si mesmo.”*²², complementa ao afirmar: *“Portanto não posso dispor do homem na minha pessoa para o mutilar, o degradar ou o matar.”*²³

O Destaque à dignidade da pessoa humana surge com Kant quando diferencia a finalidade, as coisas e as pessoas:

No reino dos fins tudo tem um *preço* ou uma *dignidade*. Uma coisa que tem um preço pode ser substituída por qualquer outra coisa *equivalente*; pelo contrário, o que está acima de todo preço e, por conseguinte, o que não admite equivalente, é o que tem uma dignidade²⁴.

²⁰ KANT, Immanuel. **Fundamentação da Metafísica dos Costumes**. Edições 70, Lda. 2007, Lisboa- Portugal, p.68.

²¹ Ibidem, p. 65.

²² Ibidem, p.68.

²³ Ibidem.

²⁴ Ibidem, p.77.

Kant atribui para o homem características especiais, colocando-o com ser racional especial, cujas ações têm como fim a si mesmo atribuindo-lhe dignidade, quando aduz que no mundo dos fins tudo tem um preço ou uma dignidade. Para a dignidade *“não tem somente um valor relativo, isto é um preço, mas um valor íntimo”*:

[..] aquilo porém que constitui a condição só graças à qual qualquer coisa pode ser um fim em si mesma, não tem somente um valor relativo, isto é um preço, mas um valor íntimo, isto é 'dignidade'.

Ora a moralidade é a única condição que pode fazer de um ser racional um fim em si mesmo, pois só por ela lhe é possível de moralidade, são as únicas coisas que têm dignidade. ser membro legislador no reino dos fins. Portanto a moralidade, e a humanidade enquanto capaz de moralidade, são as únicas coisas que têm dignidade²⁵.

Na visão de Ingo Wolfgang Sarlet a dignidade da pessoa humana é a qualidade intrínseca e distintiva de cada ser humano:

[..] qualidade intrínseca e distintiva de cada ser humano que o faz merecedor do mesmo respeito e consideração por parte do Estado e da comunidade, implicando, neste sentido, um complexo de direitos e deveres fundamentais que assegurem a pessoa tanto contra todo e qualquer ato de cunho degradante e desumano, como venham a lhe garantir as condições existenciais mínimas para uma vida saudável, além de propiciar e promover sua participação ativa e responsável nos destinos da própria existência e da vida em comunhão dos demais seres humanos²⁶.

Para Alexandre Morais, a dignidade da pessoa humana *"é um valor espiritual e moral intrínseco da pessoa, que se manifesta singularmente na sua autodeterminação consciente e responsável"*, partindo do pressuposto de que cabe ao Estado o *"dever de garantir a justiça e direitos de liberdade individual"*.

Ao Estado cabe o dever de garantir a justiça e direitos de liberdade individual. A dignidade da Pessoa Humana atribui unidade aos direitos e garantias fundamentais, inerente às personalidades humanas afastando a idéia de predomínio das concepções transpessoalistas de Estado e Nação, em função da liberdade

²⁵ KANT, Immanuel. **Fundamentação da Metafísica dos Costumes**. Edições 70, Lda. 2007, Lisboa-Portugal, p.77-78

²⁶ SARLET, Ingo Wolfgang. **Dignidade da Pessoa Humana e Direitos Fundamentais**. Porto Alegre: Livraria do Advogado, 2001, p. 60.

individual. A dignidade é um valor espiritual e moral intrínseco da pessoa, que se manifesta singularmente na sua autodeterminação consciente e responsável, trazendo consigo a pretensão ao respeito das demais pessoas, edificando um mínimo invulnerável que todo estatuto jurídico deve assegurar, de modo que, excepcionalmente, possam ser feitas limitações ao exercício dos direitos fundamentais, todavia sem menosprezar o merecimento das pessoas enquanto seres humanos.

[...] funcionaria como uma cláusula 'aberta' no sentido de respaldar o surgimento de 'novos direitos' não expressos na Constituição de 1988 mas nela implícitos, seja em decorrência do regime e princípios por ela adotados, ou em virtude de tratados internacionais em que o Brasil seja parte, reforçando, assim, o disposto no art. 5º, § 2º. Estreitamente relacionada com essa função, pode-se mencionar a dignidade da pessoa humana como critério interpretativo do inteiro ordenamento constitucional.²⁷

1.4. Direitos da Personalidade: Conceitos e Fundamentos

A Personalidade humana é o conjunto de características psicológicas, esse conjunto é denominado de traço, que faz a distinção de um indivíduo dos outros no meio de uma coletividade. Esses traços são definidos por Guilford²⁸ como *“algo que distingue um indivíduo de outro, de forma permanente”*.

Dessa forma, o perfil de um indivíduo é a sua personalidade cuja imagem é moldada pelos traços, o que por sua vez determina a sua forma de interagir com o mundo externo através dos pensamentos e ações na relação com a coletividade, tornando o indivíduo um ser único e especial. Complementando a ideia, manifesta-se Gordon W. Allport ao afirmar que *“a organização dinâmica dos sistemas fisiológicos e psicológicos individuais determinam a maneira pela qual cada pessoa se ajusta ao ambiente”*²⁹.

São nos traços da personalidade do indivíduo que estão relacionados os fatores fisiológicos e psicológicos que contribuem para composição da sua personalidade.

²⁷ MORAIS, Alexandre. **Direito Constitucional**. Ed. Atlas, São Paulo, 2005, p. 16.

²⁸ GUILDFORD, J., “On Personality”, in Mischel, W., **Introduction to Personality**, New York, Holt Rinehart and Wilson, 1973, pp. 22-25.

²⁹ ALLPORT, Gordon Willard. **Personalidade: Padrões e desenvolvimento**. Trd. Dante Moreira Leite, 4ª reimp., São Paulo, EPU, 1973, p. 213.

Em virtude de característica tão especial, a personalidade humana necessita de uma proteção para melhor desenvolver-se nesse vasto processo de interação com outras personalidades, necessitando do surgimento de uma especialidade do ramo do direito denominado Direito da Personalidade.

Na visão do civilista Silvio Rodrigues, esse novo direito tem caráter protetivo por surgir como forma de propiciar à vítima meios de defesa: *“Essa proteção consiste em propiciar à vítima meios de fazer cessar a ameaça, ou lesão, bem como de dar-lhe o direito de exigir reparação do prejuízo experimentado se o ato lesivo já houvesse causado dano”*³⁰.

Nesse mesmo diapasão manifesta-se o jurista Orlando Gomes no tocante aos direitos da personalidade, quando assim o define:

São direitos essenciais ao desenvolvimento da pessoa humana, que a doutrina moderna preconiza e disciplina, no corpo do Código Civil, como direitos absolutos. Destinam-se a resguardar a eminente dignidade da pessoa humana, preservando-a dos atentados que pode sofrer por parte de outros indivíduos³¹.

Na conceituação de Carlos Alberto Bittar, os direitos da personalidade visam proteger unicamente a condição humana focando em sua personalidade.

[..] os direitos reconhecidos à pessoa humana tomada em si mesma e em suas projeções na sociedade, previstos no ordenamento jurídico exatamente para a defesa de valores inatos no homem, com a vida a higidez física, a honra, a intelectualidade e outros tantos³².

Todavia, Goffredo da Silva Telles Júnior afirma ser um entendimento errado dizer-se que o homem tem direito à personalidade considerando que a personalidade é base de apoio de todos os direitos e obrigações, assim a definindo:

A personalidade consiste no conjunto de caracteres próprios da pessoa. A personalidade não é um direito, de modo que seria errôneo afirmar que o ser humano tem direito à personalidade. A personalidade é que apóia os direitos e deveres que dela irradiam, é o objeto de direito, é o primeiro bem da pessoa, que lhe pertence como primeira utilidade, para que ela possa ser o que é, para sobreviver e se adaptar às condições do ambiente em que se

³⁰ RODRIGUES, Silvio. **Direito Civil. Parte Geral**. 32^o ed. São Paulo, Saraiva, 2002, p.65

³¹ GOMES, Orlando. **Introdução ao Direito Civil**. 18. ed. Rio de Janeiro: Forense, 2001, p.47

³² BITTAR, Carlos Alberto; BITTAR, Eduardo Carlos Bianca. **Os direitos da personalidade**. 6. ed. / rev., atual. e ampl. por Eduardo C. B. Rio de Janeiro: Forense Universitária, 2003. p.164.

encontra, servindo-lhe de critério para aferir, adquirir e ordenar outros bens.³³

Voltando aos ensinamentos de Carlos Eduardo Bittar, registrando-se que a personalidade é dotada de características especiais - atributos - que necessitam ser tutelados. Esses atributos protegidos asseguram a dignidade humana como valor fundamental, "*direitos inatos (originários), absolutos, extrapatrimoniais, intransmissíveis, imprescritíveis, impenhoráveis, vitalícios, necessários e oponíveis erga omnes*"³⁴.

Na visão de Limongi França Savigny, os direitos da personalidade têm características mais extensas em virtude de tutelarem três campos: o da própria pessoa, que está intrinsecamente ligado ao direito da personalidade; como ampliação da pessoa à família, tutelado pelos direitos da família e o mundo exterior à pessoa; e vinculado aos direitos patrimoniais. Dessa forma, "*as faculdades jurídicas cujo objeto são os diversos aspectos da própria pessoa do sujeito, bem assim as suas emanações e prolongamentos*"³⁵ compõe os direitos da personalidade.

Outro aspecto que deve ser abordado está no fato de que a pessoa humana é um ser social e, por consequência, vive em comunidade, assim, lhe cabe dar atenção aos outros membros da comunidade como pares. Quando ocorre afrontamento a tal preceito é afrontar a si próprio, nesse sentido segue Ana Lúcia Leonel ao aduzir "*que deve haver uma unicidade entre ele e o grupo, como se fossem uma única pessoa, lembrando sempre, que todos são iguais em dignidade, e quando se atinge a dignidade do outro, está se atingindo a própria dignidade*"³⁶.

Peter Haberle aduz que a dignidade da pessoa humana está intrinsecamente ligada na responsabilidade que a pessoa humana tem diante de outros homens e da comunidade, como resultado de um estado da auto-responsabilidade, no sentido de autodeterminação:

³³ GOFFREDO da Silva Telles Junior, **Direito Subjetivo**, enciclopédia Saraiva do Direito, São Paulo: Saraiva, 1977 v. 28, p. 315-316.

³⁴ BITTAR, Carlos Alberto. **Os Direitos da Personalidade**. 2.^a ed. Rio de Janeiro: Forense Universitária, 1995. p.11.

³⁵ FRANÇA, Rubens Limongi. **Manual de Direito Civil**. 3. ed. rev. São Paulo: Revista dos Tribunais, 1975. v. 1, p.403.

³⁶ LEONEL, Ana Lúcia. **O Princípio da Dignidade da Pessoa Humana e a Unção Social do Contrato no Direito Privado Brasileiro**. Osasco/SP:UNIFIEO/Centro Universitário FIEO, 2007. Dissertação(Mestrado), p.21.

A dignidade humana habita, de antemão, a dimensão comunicativa social, que pode ganhar realidade tanto na esfera privada quanto na pública. Dignidade humana significa também, mas não somente, o espaço interno do homem. Sua abertura social, o momento da responsabilidade diante de outros homens e da comunidade, pertence a ela do mesmo modo e revela-se tão constituinte como o momento da autorresponsabilidade, no sentido de autodeterminação. As conexões intersubjetivas dos direitos fundamentais individualmente tomados constituem parcela da dignidade humana³⁷.

Contribuindo com as idéias de Peter Haberle, expressa-se Charles Taylor no tocante à manifestação da solidariedade como elemento da autodeterminação e atribuição de direitos, como representação da forma de integração da pessoa humana à sua comunidade:

Repare-se que a autodeterminação e a atribuição de direitos representam uma forma de integração da pessoa na comunidade, fazendo-a participar por sua própria iniciativa e alvedrio do plano de valores da ordem jurídica, e não uma forma de manter no indivíduo uma espécie de poder de veto perante os compromissos sociais. Do mesmo modo, também não faz sentido reduzir a responsabilidade e a atribuição de deveres a um activo, como querem os tradicionalistas, ou a preço global, como pensam alguns liberais, imputado a cada um para benefício das exigências de protecção da comunidade.

A autodeterminação e a responsabilidade, além de dependerem, na existência concreta de cada pessoa, da respectiva biografia jurídica, procuram inscrever a posição de cada um no contexto de uma sociedade simultaneamente livre, justa e solidária, sem se deixarem aprisionar por entendimentos exclusivamente libertários, justicialistas ou solidaristas das relações da pessoa com a comunidade. Sobre a relação da pessoa com a responsabilidade e os seus limites nos dias que correm.³⁸

Podemos concluir esse capítulo sob a síntese das afirmações de Caio Mario Pereira³⁹ para quem os direitos da personalidade são: 1) absolutos: *erga omnes*, por serem oponíveis contra todos; 2) extrapatrimoniais: por não possuírem diretamente conteúdo patrimonial; 3) gerais: por serem outorgados a todas as pessoas; 4) imprescritíveis: por não estarem vinculados aos aspectos temporais para exercício do seu direito; 5) impenhoráveis: não são passíveis de penhora os direitos da

³⁷ HABERLE, Peter. **A Dignidade Humana como Fundamento da Comunidade Estatal**. In: SARLET, Ingo Wolfgang (Org.). *Dimensões da Dignidade: ensaios de filosofia do direito e direito constitucional*. 2a ed. Porto Alegre. Livraria do Advogado. 2009. p.91.

³⁸ TAYLOR, Charles. *Responsability for self*, in AMÉLIE O. RORTY (org.), **The Identities of Persons**, Berkeley/Los Angeles/Londres, 1984, pp. 281-299.

³⁹ PEREIRA, Caio Mario da Silva. **Instruções de Direito Civil**. Rio de Janeiro, Forense 1994. 13ª ed. p.153.

personalidade; 6) vitalícios: são inatos, permanentes, surgem com o nascimento da pessoa humana acompanhando no todo da vida e sucumbindo com a sua morte; 7) indisponíveis: independem da própria vontade da pessoa a consagração desse direito, não podendo ser transferido.

2. DA REDE MUNDIAL DE COMPUTADORES

2.1 A Globalização

Milton Santos apresenta uma visão política sobre a globalização quando aduz que:

[..] globalização é, de certa forma, o ápice do processo de internacionalização do mundo capitalista. Para entendê-la, como, de resto, a qualquer fase da história, há dois elementos fundamentais a levar em conta: o estado das técnicas e o estado da política⁴⁰.

Milton Santos⁴¹ prossegue afirmando que o mundo contemporâneo impôs novos ritmos ao deslocamento dos corpos e ao transporte das idéias, acrescentando novos ritmos à história. Segundo essas palavras, a globalização requer união de forças visando à criação de uma realidade diferente da existente.

Para o autor, vivemos em um mundo confuso cuja forma qual o percebemos é ainda mais confusa em função de estarmos diante de dois grandes paradoxos: de um lado o extraordinário progresso *“das ciências e das técnicas, das quais um dos frutos são os novos materiais artificiais que autorizam a precisão e a intencionalidade”*⁴². Do outro, a existência da *“referência obrigatória à aceleração contemporânea e todas as vertigens que cria, a começar pela própria velocidade”*⁴³, como consequência do *“mundo físico fabricado pelo homem, cuja utilização, aliás, permite que o mundo se torne esse mundo confuso e confusamente percebido”*⁴⁴.

O termo globalização admite duas conotações, a primeira como um sistema de relações que se fundamenta em possibilidades reais de um determinado momento histórico visando ao benefício de muitos indivíduos. A segunda, como um

⁴⁰ SANTOS, Milton. **Por uma outra Globalização**: do pensamento único à consciência universal. 6ª ed. Rio de Janeiro: Record, 2001 p.9

⁴¹ _____, **Técnica, Espaço e Tempo**. São Paulo: Hucitec, 2000, p.17-16.

⁴² Idem. **Por uma outra globalização**: do pensamento único à consciência universal. 6ª ed. - Rio de Janeiro: Record, 2001 p.9

⁴³ Ibidem.

⁴⁴ Ibidem.

sistema de relações hierárquicas cujo objetivo é perpetuar o domínio de um subsistema sobre outros subsistemas, beneficiando apenas alguns⁴⁵.

Milton Santos ainda afirma que a globalização das últimas décadas do século XX foi um processo perverso. Mesmo diante da possibilidade da rejeição do argumento explica o autor:

[..] que esse mundo assim apresentado é verdadeiro, e não queremos admitir a permanência de sua percepção enganosa, devemos considerar a existência de pelo menos três mundos num só. O primeiro seria o mundo tal, como nos fazem vê-lo: a globalização como fábula; o segundo seria o mundo tal como ele é: a globalização como perversidade; e o terceiro o mundo como ele pode ser: uma outra globalização⁴⁶.

Para Demétrio Magnoli e Regina Araújo, a globalização pode ser conceituada como um “[..] processo pelo qual o espaço mundial adquire unidade, por meio da intensificação da rede de fluxos que conecta os lugares, as regiões, os países e o mundo⁴⁷”. Quanto à sua história, aduz o autor:

[...]remontam às grandes navegações e à configuração de uma divisão internacional do trabalho. No mundo contemporâneo, o processo de globalização é ritmado pela ação dos conglomerados transnacionais, pelos tratados econômicos e comerciais⁴⁸.

Sobre o fenômeno da globalização, ensina Jacinto Nelson M. Coutinho:

O fenômeno da globalização (ou globalizações, como querem alguns), porém, parece não ter mais retorno, sem embargo dos seus inúmeros inimigos. Bem estruturada na difusão, atinge a todos, mas só faz gozar a poucos, deixando à maioria tão-somente a esperança ou a desilusão, onde, definitivamente, coloca-se em risco.⁴⁹

Nesse fenômeno, globalização, intensificado nas últimas décadas, os Estados que detêm hegemonia definem normas de ação em detrimento de outros,

⁴⁵ SANTOS, Milton. **Técnica, espaço e tempo**, p. 17. São Paulo: Hucitec, 2000, p. 15-16.

⁴⁶ Idem. **Por uma outra globalização: do pensamento único à consciência universal**. 6ª ed. - Rio de Janeiro: Record, 2001 p.9

⁴⁷ MAGNOLI, Demétrio. **Globalização: estado nacional e espaço mundial**. São Paulo: Moderna, 2003, p.371.

⁴⁸ Ibidem.

⁴⁹ COUTINHO, Jacinto Nelson de Miranda, **O Papel do Pensamento Economicista no Direito Criminal de Hoje**. **Revista Brasileira de Ciências Criminais** nº. 32, p. 299, 2000.

que possuem como única opção a subserviência. Giovanni Arrighi conceitua a hegemonia como sendo a “*capacidade de um Estado exercer funções de liderança e governo sobre um sistema de nações soberanas*”⁵⁰.

Para Ronaldo Porto Macedo Júnior, a globalização não mais se relaciona com o processo histórico, pois ela é a descrição de uma nova fase do capitalismo mundial:

A globalização, assim entendida, não se confunde com uma etapa inexorável do processo histórico, mas descreve uma nova fase do capitalismo mundial, marcada pela transformação dos arranjos institucionais (econômicos e políticos), hábitos, cultura e apreensão teórica do mundo anteriormente existentes. Como se vê, a definição inicial era mesmo precária, devendo servir apenas como ponto inicial para a reflexão que se segue⁵¹.

Dentro da globalização a rede mundial de computadores surge como elemento da difusão desse propósito. Como pode ser visualizada, a possibilidade do uso da rede mundial de Computadores como meio de globalizar ideias e tecnologias em favor de determinado Estado ou comunidades internacionais em detrimento aos demais, está fortemente demonstrada no posicionamento de Jean-Noel Jeanneney, presidente da Biblioteca Nacional da França.

Jeanneney temeu a idéia da Google⁵² de digitalizar milhões de livros das cinco maiores bibliotecas dos Estados Unidos para disponibilizar no serviço de pesquisas *online*. Esta informação, a lógica de tal temor, é passível de observação na transcrição de trecho da matéria jornalística de Renata Mesquita publicada na revista Info da editora Abril.

“Terça-feira, 22 de fevereiro de 2005 - 18h04

SÃO PAULO - Jean-Noel Jeanneney, presidente da Biblioteca Nacional da França, detestou a idéia do Google de digitalizar milhões de livros das cinco maiores bibliotecas dos Estados Unidos para seu serviço de pesquisas *online*.

Há algumas semanas, Jeanneney escreveu um polêmico editorial no jornal *Le Monde* para dizer que está preocupado com a iniciativa da

⁵⁰ ARRIGHI, Giovanni. **O Longo Século XX: dinheiro, poder e as origens de nosso tempo**. Rio de Janeiro: Contraponto, 1996. p.27.

⁵¹ MACEDO JÚNIOR, Ronaldo Porto. **Revista de Direito do Consumidor**. vol. 32, Editora Revista dos Tribunais, Out. 1999. p.45.

⁵² Google Inc. é uma empresa multinacional de serviços online e software dos Estados Unidos. O Google hospeda e desenvolve uma série de serviços e produtos baseados na internet e gera lucro principalmente através da publicidade pelo AdWords.

pontocom, pois o processo refletirá "uma visão de mundo unilateral, dominada pelo idioma inglês e pela cultura americana" que poderá, a longo prazo, "aumentar o nível de generalização" e impedir que as pessoas "reflitam sobre a diversidade das civilizações", conta o BetaNews.com. O projeto do Google abrange a digitalização dos acervos de domínio público das bibliotecas de Nova York e das universidades de Stanford, Michigan, Havard e Oxford.

O presidente da Biblioteca Nacional insistiu que não pretende defender sentimentos anti-americanos, mas que acredita ser necessária a adoção de algumas medidas para evitar que outras culturas se percam. A saída, diz, é a digitalização de seu próprio acervo e de outras bibliotecas européias - Jeanneney já começou a levantar fundos para viabilizar sua idéia.⁵³

A partir desse contexto da globalização e de disseminação da informação, aduz Maria das Graças Targino, que a *"influência da informática nos processos de difusão da informação é decisiva. Conduz à adoção de novo modelo informacional distributivo, dinâmico e hipertextual"*⁵⁴. Conclui ainda, que tal importância está não apenas na tecnologia em si, mas *"no sentido de atender os usuários conectados em redes eletrônicas, de modo não mais linear, mas respeitando sua estrutura cognitiva, suas demandas singulares independentemente da localização geográfica"*⁵⁵.

⁵³ MESQUITA, Renata, **Biblioteca da França se volta contra o Google**, Revista Abril. Info-Online Disponível em: <http://info.abril.com.br/aberto/infonews/022005/22022005-10.sh>. Acesso em: 22 abril 2012.

⁵⁴ TARGINO, Maria das Graças. **Novas tecnologias de comunicação**: mitos, ritos ou ditos? Ciência da Informação, Brasília, v.24, n.2, p.194-203, maio/ago. 1995..

⁵⁵ Ibidem.

2.2. A Pesquisa Nacional de Amostra de Domicílios (PNAD) de 2009.

Sobre o acesso da última Pesquisa Nacional de Amostra de Domicílios (PNAD)⁵⁶ do Instituto Brasileiro de Geografia e Estatística (IBGE) realizada no ano de 2009, trouxe novidades em relação às edições anteriores. A tecnologia da informação se tornou um tema permanente e a pesquisa registrou que o número de usuários da Internet mais que dobrou, aumentando de 31,9 milhões em 2005 para 67,9 milhões em 2009, o equivalente ao aumento de 112,9%. Foi registrado que em 2009, cerca de 67,9 milhões de pessoas com 10 ou mais anos de idade declararam ter usado a Internet, o que representa um aumento de 12 milhões, equivalente a 21,5% sobre 2008.

Ainda segundo o PNAD⁵⁷ de 2009, entre 2005 e 2009 as faixas etárias dos pesquisados que estavam em uso contínuo da Internet distribuía-se da seguinte maneira: 71% dos jovens de 15 a 17 anos, em seguida vieram as pessoas de 18 a 19 anos, com 68,7%. A faixa etária que menos utilizava a Internet foi a de 50 anos ou mais, com apenas 15,2%. Contudo, esse contingente de usuários cresceu 138% no período de quatro anos.

Outro aspecto significativo do PNAD⁵⁸ 2009 está no fato de que o gênero feminino avançou mais que o masculino no que se refere ao acesso à Internet, principalmente as mulheres que se situam na faixa etária de 30 a 39 anos as quais aumentaram seu acesso em 28,2% contra 24,8% dos homens. As mulheres de 40 a 49 anos tiveram um crescimento de acesso à Internet equivalente a 31,9%, enquanto os homens avançaram em 21,8%. No grupo de 50 anos ou mais, os usuários do gênero feminino apresentaram um crescimento de 46,1% contra o 35,5% de usuários do gênero masculino⁵⁹.

⁵⁶ IBGE. Pesquisa Nacional por Amostra de Domicílios, **Em um ano, número de pessoas que acessaram a Internet aumentou em 12 milhões.** Disponível em: http://www.ibge.gov.br/home/presidencia/noticias/noticia_visualiza.php?id_noticia=1708. Acesso em: 07 Nov. 2012.

⁵⁷ Ibidem.

⁵⁸ Ibidem..

⁵⁹ Ibidem.

A análise analítica dessa amostra demonstra a necessidade do estudo mais profundo dessa temática em virtude de ter apresentado no ano de 2009 um contingente de 67,9 milhões de pessoas, pessoas essas com 10 ou mais anos de idade que se declararam como usuários da Rede Mundial de Computadores.

2.3. O surgimento da Internet

Segundo Ângelo Volpi Neto, o surgimento ocorreu no período da denominada Guerra Fria⁶⁰: "Os primórdios da rede surgiram nos anos 60, no Departamento de Defesa do governo norte-americano, que constituiu a ARPAnet (ARPA: *Advanced Research Projects Agency* - Agência de Pesquisa de Projetos Avançados)"⁶¹.

Sua finalidade era manter a comunicação das bases militares dos Estados Unidos com o objetivo de constituir uma rede de computadores para interconexão entre os principais centros militares de comando que pudessem sobreviver a um possível ataque nuclear e que atendessem às seguintes exigências: não ser vulnerável a ataque militar, pois sendo Washington atacada, outros pontos deveriam estar funcionando; não existir um centro de comando, pois no caso de um ataque o centro seria o primeiro lugar a ser atacado; possuir flexibilidade para adaptarem-se às mais diversas situações possíveis.

Os primórdios da rede surgiram nos anos 60, no Departamento de Defesa do governo norte-americano, que constituiu a ARPAnet (ARPA: *Advanced Research Projects Agency* - Agência de Pesquisa de Projetos Avançados), com a finalidade de facilitar a troca de informações pelos computadores da área militar e do governo. Por problemas de segurança, os norte-americanos decidiram criar um sistema paralelo e alternativo ao existente, de forma que fosse possível administrar informações sob condições extremas e com total segurança, como no caso de um bombardeio nuclear.

⁶⁰ Guerra fria foi a designação dada ao conflito político-ideológico entre os Estados Unidos (EUA), defensores do capitalismo e a União Soviética (URSS), defensora de uma forma de socialismo, compreendendo o período entre o final da Segunda Guerra Mundial e a extinção da União Soviética., [...]É chamada de *fria* porque não houve qualquer combate físico, embora o mundo todo temesse a vinda de um novo combate mundial. HOBBSAWN. Eric. **Era dos Extremos**. Cia. das Letras, São Paulo, 2002, p.130-137.

⁶¹ VOLPI NETO, Angelo. **Comércio Eletrônico - Direito e Segurança**. Curitiba. Juruá, 2002, p.25-26.

O sucesso em âmbito militar despertou interesse no mundo dos negócios, e o fim da Guerra Fria possibilitou a abertura dessa tecnologia ao mundo civil. Inicialmente, apenas universidades e grandes corporações usufruíram dessa maravilhosa ponte eletrônica, que hoje emprega diferentes meios de conectividade, utilizando linhas telefônicas, cabos de TV por assinatura, de fibras óticas, transmissão via satélite ou frequências de ondas de rádio como meio de transporte. [...] Desde 1990 a Internet está disponível a qualquer pessoa que tenha um computador ligado a uma linha telefônica; no Brasil, isso é possível desde 1995.⁶²

Continuando o autor, quando a ameaça da Guerra Fria passou, ARPANet⁶³ tornou-se desnecessária e naquele momento não era mais considerada importante ao ponto da manutenção sob sua guarda. Neste momento, foi permitido o acesso aos cientistas, em seguida foi estendida até as universidades as quais, sucessivamente, passaram-na para as universidades de outros países. Por último, foi concedido aos pesquisadores domésticos o acesso, até que mais de cinco milhões de pessoas já estavam conectadas com a rede e, para cada nascimento, mais 4 (quatro) se conectavam com a imensa “teia” da comunicação mundial.

A ARPANet usava uma tecnologia chamada de “*packet switching*” (troca de pacotes), que transportava informação dessa forma: quando um dos computadores da rede queria mandar informação para outro, repartia essa informação em diversos pacotes e, ao invés, de estabelecer uma ligação direta com o computador de destino, enviava para o computador mais perto de si, com a indicação, em cada pacote do computador, do remetente e do destinatário⁶⁴. Os pacotes viajavam pelos computadores que estavam ligados entre si e cada um se encarregava de remeter os pacotes pelo caminho mais curto e disponível até o destino⁶⁵.

A Internet passou a ser usada com fins comerciais desde 1987, entretanto, só a partir de 1991 ela explodiu com o aparecimento da *Word Wide Web* (Rede de

⁶² VOLPI NETO, Angelo. **Comércio Eletrônico - Direito e Segurança**. Curitiba. Juruá, 2002, p. 25-26.

⁶³ Ibidem.

⁶⁴ QUEIROZ. Regis Magalhães Soares, LUCCA, Newton De e Simão Filho. Adalberto (coordenadores) e outros de. **Direito & Internet – Aspectos Jurídicos Relevantes**. 1ª ed. , Bauru-SP, Edipro, 2001, 1ª reimpressão, pág. 379 –380.

⁶⁵ Tanenbaum, Andrew S. *Redes de Computadores* Tradução: Vandenberg D. de Souza. Rio de Janeiro: Campus, 2002, p.316.

Alcance Mundial, WWW ou Web), que usava a multimídia, concatenando palavras, sons e imagens; e a combinação de informações através do hipertexto. Na década de 90, a Internet já possuía mais de um milhão de usuários e diversas empresas montaram suas próprias redes de conexão interligando-se com a Internet e obtendo enormes lucros⁶⁶.

2.4. A Internet no Brasil

Para Eduardo Vieira, a história da Internet no Brasil começou bem atrasada, quando comparada com os países integrantes do denominado 1º mundo, com base em seus registros que marcam o ano de 1988. As primeiras conexões foram feitas pela Fundação de Amparo a Pesquisa do Estado de São Paulo (FAPESP) e pelo Laboratório Nacional de Computação Científica do Rio de Janeiro, criando, dessa forma, uma Rede Nacional de Pesquisa em 1989 patrocinada pelo Ministério da Ciência e Tecnologia. Em 1992, o Governo Federal criou a Rede Nacional de Pesquisa (RNP) através do Ministério de Ciência e Tecnologia (MCT).

O governo Federal entrou na onda em 1992, com a criação da Rede Nacional de Pesquisa (RNP) pelo Ministério da Ciência e Tecnologia (MCT). A RNP, coordenada pelo cientista Tadao Takashi, criou uma gigantesca infra-estrutura de cabos para suportar a rede mundial de computadores, chamada de espinha dorsal (ou backbone), que recebia o link internacional. Também espalhou pontos de conexão pelas principais capitais do país e começou a operar a infra-estrutura de funcionamento da Internet, distribuindo o acesso à rede para universidades, fundações de pesquisa e órgãos governamentais espalhados pelo território nacional. Paralelamente ao início das operações da RNP, surgiu no Rio de Janeiro uma organização não-governamental (ONG), chamada Instituto Brasileiro de Análises Sociais e Econômicas (Ibase), que se tornaria a primeira instituição brasileira fora do ambiente acadêmico a utilizar a Internet em 1989. O grande teste do Alternex ocorreu em 1992, durante a conferência internacional da ECO-92, qual foi montado um sistema de veiculação de informações eletrônicas para acompanhar o debate.⁶⁷

Para Eduardo Vieira, a intervenção estatal foi muito importante para impulsionar essa tecnologia que ascendia de forma muito lenta. Em “1994 o

⁶⁶ Ibidem.

⁶⁷ VIEIRA, Eduardo. **Os Bastidores da Internet no Brasil**. Barueri, Manole, 2003, p.9.

Governo Federal manifestou a intenção de investir e promover o desenvolvimento da Internet no país numa ação conjunta entre os Ministérios da Ciência e Tecnologia (MCT) e das Comunicações (MC)”⁶⁸.

Tratava-se de uma parceria fundamental para o desenvolvimento e expansão da recém-criada rede mundial de computadores. A parceria ocorria nos seguintes aspectos: *“a RNP entraria com infra-estrutura básica, enquanto a Embratel, na época a empresa do sistema Telebrás responsável pelos serviços interurbanos e internacionais, exploraria comercialmente o acesso à rede”*.⁶⁹

A efetiva utilização de forma comercial da Internet no Brasil ocorreu no ano de 1995, facultando-se às empresas denominadas provedores de acesso, comercializar o acesso à rede mundial de computadores. Na definição de Márcia Regina Sawaya, essa modalidade de provedores são denominados de ISP (*Internet Service Provider*), *“conhecidos também como Provedor de Acesso (IAP), é uma companhia que provê acesso a usuários finos, administrando a conexão de seus PCs ao resto da Internet”*⁷⁰.

2.5. Definição de Internet

Para Marcelo Xavier Freitas Crespo *“A internet é uma vastíssima rede capaz de interligar computadores de todo o mundo, possibilitando, assim, a comunicação entre eles”*⁷¹.

Guilherme Magalhães Martins define a Internet como uma rede de computadores ligados entre si cuja difusão no planeta impossibilita a identificação de fronteiras. A internet é,

[...] uma rede de computadores ligados entre si, compreendendo ainda outras redes em - escala global, perfazendo-se a conexão e comunicação por meio de um conjunto de softwares denominados

⁶⁸ VIEIRA, Eduardo. **Os Bastidores da Internet no Brasil**. Barueri, Manole, 2003, p.10.

⁶⁹ Ibidem.

⁷⁰ SAWAYA, Márcia Regina. **Dicionário de Informática e Internet**. São Paulo, Nobel, 3ª reimpressão 2010. p.242.

⁷¹ CRESPO, Marcelo Xavier de Freitas, **Crimes Digitais**. São Paulo.

TCP/IP (Transmission Control Protocol/Internet Protocol), de modo que a sua difusão no planeta acarreta a impossibilidade de identificação de fronteiras nacionais.⁷²

No mesmo diapasão, segue Gustavo Correa quando conceitua a Internet como:

[...] um sistema global de rede de computadores que possibilita a comunicação e a transferência de arquivos de uma máquina à outra máquina conectada na rede possibilitando, assim, um intercâmbio de informações sem precedentes na história, de maneira rápida, eficiente e sem limitação de fronteiras, culminando na criação de novos mecanismos de relacionamento.⁷³

2.6. Natureza Jurídica da Internet

Quanto à natureza jurídica, não existe uma definição segura que possa ser tomada por parâmetro, entretanto, todas elas apresentam as mesmas afirmações e dúvidas quanto ao lugar e ou meio.

Para Luis Henrique Ventura, a internet é simplesmente um meio que permite aos indivíduos acesso direto a diversas informações constantes nos inúmeros computadores espalhados pelo mundo:

Se entendermos que a Internet é um lugar, muitas das questões já previamente definidas pelo Direito, tais como o foro competente, deveriam ser redesenhadas. Imagine um contrato celebrado entre uma empresa alemã e outra brasileira. Se a Internet é um lugar, onde seria assinado o contrato? A resposta, então, é nem no Brasil e nem na Alemanha, mas na Internet. A proposta e a aceitação também seriam realizadas na Internet. E, nesse caso, como definir o foro?. De fato, a internet é simplesmente um meio que nos permite ter acesso direto a diversas informações constantes nos sem-número de computadores espalhados por todo o mundo. Não se trata, portanto, de um lugar, mas de um veículo de comunicação que nos propicia lidar com milhões e milhões de dados de forma rápida, prática, cômoda e eficiente.⁷⁴

⁷² MARTINS, Guilherme Magalhães. **Formação dos contratos eletrônicos de consumo via internet**. 1. ed. Rio de Janeiro: Forense, 2003, p.94.

⁷³ CORRÊA, Gustavo Testa. **Aspectos jurídicos da Internet**. São Paulo: Saraiva, 2000, p. 08.

⁷⁴ VENTURA, Luis Henrique. **Comércio e contratos eletrônicos: aspectos jurídicos**. São Paulo: EDIPRO, 2001, p. 63-68.

Na visão de David S. Willing a *"Internet é uma rede mundial, não regulamentada, de sistemas de computadores conectados por comunicações de alta velocidade e compartilhando um protocolo comum que lhes permite comunicar-se"*.⁷⁵

As definições acima podem ser diluídas em pequenos tópicos para observar a sua abrangência: a formação de uma rede rompe o paradigma da territorialidade, as suas ramificações podem chegar a todas as nações; as suas informações podem estar em conformidade com os ordenamentos jurídicos de outros Estados quando, ao passar, rompe as suas fronteiras; e vários são os objetivos para os quais a internet é utilizada, a exemplo de meio de propagação, entretenimento aos negócios, da religião e solidariedade ao crime.

O acesso pode ocorrer de maneira bastante diversificada a partir de um computador pessoal, servidor de arquivos de alto porte, laptop, terminais públicos, entre outros.

3.7 Privacidade na Internet

A tutela direta da privacidade está definida no artigo 5º, inciso X da Constituição Federal que trata sobre o direito à inviolabilidade da privacidade e da intimidade:

Art. 5º - 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*⁷⁶. [Grifo nosso]

Em seguida o referido direito é recepcionado pelo Código Civil através do Art. 21 que define que a “vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma”.

⁷⁵ WILLING, David S. **A internet e a Constituição dos Estados Unidos**. São Paulo: Consulex, ano 1, n.4, abr. 1997. p.30.

⁷⁶ BRASIL. **Constituição da República Federativa do Brasil de 1988**. op. cit.

Para Celso Lafer, a privacidade consiste “*no direito do indivíduo de estar só e a possibilidade que deve ter toda pessoa de excluir do conhecimento de terceiros aquilo que a ela só se refere, e que diz respeito ao seu modo de ser no âmbito da vida privada*”.⁷⁷

Para Celso Bastos, o direito à privacidade é:

[...] a faculdade que tem cada indivíduo de obstar a intromissão de estranhos em sua vida privada e familiar, assim como de impedir-lhes o acesso a informações sobre a privacidade de cada um, e também impedir que sejam divulgadas informações sobre esta área da manifestação existencial do ser humano⁷⁸.

O conceito trabalhado tem o cunho da subjetividade, pois compete a cada indivíduo delimitar quais fatos ou informações ele considera como sigilosos. O direito à privacidade, entretanto, não é absoluto. Atualmente, muito se questiona a respeito de seus limites os quais são também subjetivos e variam segundo o tempo e o espaço.

Marcel Leonardi⁷⁹ destaca que a privacidade está estreitamente ligada à intimidade, pois depende do próprio indivíduo guardar informações a seu respeito de algo que é seu, não havendo motivos para outras pessoas tomarem conhecimento. A privacidade pode ser considerada como o direito de ficar só, assim como o resguardo contra interferências de terceiros e o segredo; ou como o sigilo das informações e o controle das informações pessoais.

No tocante à privacidade no âmbito da Internet, aduz Marcel Leonardi que a amplitude e complexidade dessa rede dificultam o controle da privacidade dos seus usuários e a sua regulamentação. Diante desta magnitude, destacam-se organizações que abordam o tema de regulamentação da Internet, algumas entidades de prestígio global como a ONU – Organização das Nações Unidas e a Comissão das Nações Unidas para o Direito Comercial Internacional. Todavia, esses órgãos limitam-se a estabelecer diretrizes para aprimorar a ética e a função do uso

⁷⁷ LAFER, Celso. **A Reconstrução dos Direitos Humanos**. São Paulo, Companhia das Letras, 1998, p. 63.

⁷⁸ BASTOS, Celso Ribeiro. **Comentários à Constituição do Brasil**. Editora Saraiva, 1989, volume 2, p.63.

⁷⁹ LEONARDI, Marcel. **Tutela e Privacidade na Internet**. São Paulo: Saraiva, 2012. p.297.

da rede. A ausência de coercitividade dificulta o controle eficaz do uso da Internet, afinal, sem a potencial aplicação de sanções não é possível vincular as condutas dos indivíduos visando a diminuição de práticas lesivas pela rede.⁸⁰

Na visão de Ana Paula Gambogi Carvalho,

Os sofisticados recursos informáticos disponíveis na atualidade facilitam sobremaneira a devassa da esfera íntima do homem, seja na forma da espionagem e monitoração de hábitos, da quebra do sigilo da correspondência e das comunicações³ ou da criação e manutenção de bancos de dados contendo as mais variadas informações sobre o indivíduo. Todas essas práticas lesivas à privacidade encontram um espaço propício na internet, devido à sua arquitetura aberta e à insuficiência de dispositivos de segurança. Para se justificar as invasões à intimidade do usuário, que se tornaram corriqueiras e muitas vezes sequer são percebidas pela vítima, tem-se levantado o argumento de que a rede seria um ambiente público, em que incontáveis informações e mensagens circulam por muitos lugares e se cruzam o tempo todo, se expondo aos olhos de todos.⁸¹

Continua aduzindo Ana P. Carvalho que o grande problema da privacidade no âmbito da rede mundial de computadores está na falta de regulamentação em virtude de que *“o uso da informática de forma lesiva a direitos fundamentais do homem nos leva a buscar meios para controlar o acesso às informações sobre o indivíduo e o uso que se faz delas, visando a coibir práticas ilícitas e a proteger o cidadão”*⁸². Para a autora, há escassez de leis específicas no Brasil com finalidade de resguardar a *“privacidade do usuário da internet ou regulamentar a criação e a utilização de bancos de dados eletrônicos”*⁸³, para a conclusão da sua ideia, concebe que *“o ordenamento jurídico brasileiro oferece as bases principiológicas e normativas para se assegurar a proteção da intimidade contra os diversos tipos de ataques que podem ocorrer, inclusive em ambiente virtual”*⁸⁴.

⁸⁰ LEONARDI, Marcel. **Tutela e Privacidade na Internet**. São Paulo: Saraiva, 2012. p.297-305.

⁸¹ CARVALHO, Ana Paula Gambogi. **O consumidor e o Direito à Autodeterminação Informacional: considerações sobre os bancos de dados eletrônicos**. Revista de Direito do Consumidor | vol. 46 | p. 77 | Abr / 2003.

⁸² Ibidem.

⁸³ Ibidem.

⁸⁴ Ibidem.

Para Carlos Roberto Fornes Mateucci, a questão que envolve o tema não é puramente técnica em função de que:

A quantidade de dados, fotografias, informações transmitidos pela rede dificulta, em determinadas situações, precisar a natureza do ambiente e conceituá-lo como privado ou público. A curiosidade sobre a privacidade alheia toma ainda conta dos meios de transmissão eletrônica, como revistas, jornais e de programas de televisão especializados, que exibem o dia a dia de pessoas famosas, ou até mesmo da população em geral.⁸⁵

Para o autor, devem ser analisados dois aspectos, o primeiro reside no fato de que *“a tecnologia facilita a vulneração de nossa intimidade”*⁸⁶; no outro aspecto *“a Internet foi concebida e se desenvolveu como local onde as pessoas, anônima e livremente, expressam-se das mais diferentes formas, sem qualquer barreira e até mesmo controle legal”*⁸⁷. Nesse ambiente favorável à insegurança que a tecnologia representa, a privacidade é comprometida, fazendo com que algumas nações como *“EUA, por exemplo, promulgaram lei que limita garantias individuais dos cidadãos, autorizando, por exemplo, rastreamento de e-mails. Idêntica iniciativa foi tomada pela Comunidade Européia e alguns de seus países membros”*⁸⁸.

Segundo Laura Schertel Mendes a restrição da liberdade do cidadão é uma possibilidade concreta que não pode ser descartada em virtude da estrutura da Internet que *“ao mesmo tempo em que possibilitou a sua difusão e o aperfeiçoamento da tecnologia, propiciou também o desenvolvimento de tecnologias de controle e monitoramento”*⁸⁹. Justifica a sua concepção ao aduzir que:

Nesse contexto, destaca-se o surgimento da Internet como uma estrutura aberta de rede de computadores que radicalizou as possibilidades de fluxos de informação de forma inédita. A principal característica da Internet é a sua abertura, tanto em sua arquitetura técnica, como em sua organização social/institucional⁹⁰.

⁸⁵ MATEUCCI, Carlos Roberto Fornes. **Privacidade e internet**, revista de Direito Privado | vol. 19 | p. 46 | Jul / 2004, Doutrinas Essenciais de Responsabilidade Civil | vol. 8 | p. 931 | Out / 2011DTR\2004\427

⁸⁶ Ibidem.

⁸⁷ Ibidem.

⁸⁸ Ibidem.

⁸⁹ Mendes, Laura Schertel. **O Direito Fundamental à Proteção de Dados Pessoais**, Revista de Direito do Consumidor | vol. 79 | p. 45 | Jul / 2011DTR\2011\2474.

⁹⁰ Ibidem.

Dentro dessa temática, aduz ainda a autora que os riscos de afronta aos direitos inerentes à personalidade do homem, se expandem de forma geométrica, exponencialmente. Tal risco de violação está ligado diretamente aos efeitos da tecnologia na denominada sociedade da informação que, para o autor, a:

[...]violação da privacidade na sociedade da informação passa a significar, por exemplo, o risco do uso indevido de dados pessoais, da classificação dos indivíduos, de imposição de comportamentos padronizados e da discriminação dos cidadãos⁹¹.

Marco Antônio Zanellato ao discorrer sobre privacidade e internet aduz sobre a difícil privacidade nesse meio:

[...] podemos afirmar que em nenhum lugar do mundo é tão difícil ter vida privada quanto na Internet. A cada clique do *mouse*, as pessoas são marcadas, seguidas, encaixadas em estatísticas anônimas - ou nem tanto - graças a tecnologias cada vez mais invasoras e onipresentes⁹².

O grande ponto para o autor é a discussão sobre o desafio de definir linhas, parâmetros e limites para marcar esta altura, “o que é aceitável e o que é abuso de privacidade na Internet”⁹³. Ao dar sequência à afirmação Zanellato argúi que, o “*virtual passa a ter valor próprio, independente do seu suporte físico:*”

O 'virtual' passa a ter valor próprio, independente do seu suporte físico, a mensagem ou a informação têm valor independente de um suporte em que se apóia ou de um meio para sua transmissão. Os interesses jurídicos e, conseqüentemente, os direitos e deveres daí decorrentes passam a ter como objeto a própria mensagem ou informação e não mais o meio em que se apresentam (não interessa o disquete, mas sim o *software* que nele se encontra). A mensagem em si passa a ter um valor próprio, independente dos átomos do seu meio físico.⁹⁴

Zanellato prossegue sua abordagem afirmando que a grande mudança está no fato de que “*o valor não está mais atrelado necessariamente às*

⁹¹ Mendes, Laura Schertel. **O Direito Fundamental à Proteção de Dados Pessoais**, Revista de Direito do Consumidor | vol. 79 | p. 45 | Jul / 2011DTR\2011\2474.

⁹² ZANELLATO, Marco Antonio, **Condutas Ilícitas na Sociedade Digital**. Revista de Direito do Consumidor | vol. 44 | p. 206 | Out / 2002DTR\2002\757

⁹³ Ibidem.

⁹⁴ Ibidem.

*características físicas das coisas. As informações, mensagens, dados, instruções, softwares etc. adquiriram valor próprio, independente dos átomos de que é formado seu meio físico*⁹⁵. As mudanças de valores são extremamente significativas, “*mesmo objetos que originalmente tinham natureza física, passaram a ter feição virtual*”⁹⁶, à título de exemplo, cita o caso das “*ações de sociedades anônimas que até certo tempo atrás eram apresentadas em papel, geralmente coloridas, numeradas, assinadas etc.*”⁹⁷, sendo agora substituídas por simples registro na memória do computador, meros *bits*.

Aduz ainda o autor, nessa temática da privacidade na rede mundial de computadores, destacando espécies de ilícitos informáticos, como os *cookies*, conjuntamente com os *arquivos de log*, em virtude de “*registrar ou monitorar as atitudes de usuários em visita a websites, para quaisquer finalidades*”.

Para uma melhor compreensão da abordagem, Marcia Regina Sawaya define *cookies* como sendo:

[...] “biscoito”, um arquivo que é reemitido, automaticamente, pelo servidor de rede ao disco rígido do usuário quando este entra em certos sites WWW(world wide web) alojados no servidor. Este arquivo chamado de *cookie*, é usado pelos servidores para manter rastro dos padrões e preferencias dos usuários, deste modo, em uma visita posterior ao mesmo site, os servidores reconhecem o *cookie* e torna-se aptos a usar a informação nele armazenada para personalizar o que será enviado ao usuário.⁹⁸

Quanto aos *arquivos log*, para Marcia Regina Sawaya, trazem todo o histórico operacional dos dados referente a um determinado software utilizado:

Um arquivo contendo todos os dados pertinentes a uma rodada na máquina (corrida de um programa na máquina). O log possuem a identificação da rodada, arquivo de alteração por meio de classes, identificação de disco e de entrada e de saídas, identificação das paradas e decisões tomadas na ocorrência das mesmas.⁹⁹

⁹⁵ Ibidem.

⁹⁶ Ibidem.

⁹⁷ Ibidem.

⁹⁸ SAWAYA, Márcia Regina. **Dicionário de Informática e Internet**. São Paulo, Nobel, 3ª Reimpressão. 2010, p.101

⁹⁹ Ibidem.

Os *cookies* além das definições apresentadas, também “*têm por escopo guardar alguns dados, como nomes e senhas, para que, quando o usuário retorne a determinados sites, não precise digitar tudo novamente.*”¹⁰⁰.

A grande questão nesse momento é discorrer sobre a finalidade de tais informações que estão armazenadas no computador do usuário, questiona-se se o simples fato de que os sites comerciais utilizam usuários da Internet para, de forma automática, “*direcionar os anúncios com base nos interesses e no comportamento do usuário*”¹⁰¹, como também, as informações coletadas pelos *cookies* são denominadas de *sequência de cliques*, “*podem descrever quais páginas o usuário visitou em cada loja do vendedor*”¹⁰², possa atentar a privacidade.

Da mesma maneira, os *arquivos log* deixam registrados no computador do usuário os rastros das suas operações. E, seguindo o mesmo questionamento de Zanellato, se faz presente a busca da resposta, “*os cookies e arquivos log são benéficos ou maléficos?*”¹⁰³.

O entendimento para esse questionamento cuja resposta é a de que é maléfico, é encontrado na própria definição de Zanellato ao considerar “*que os cookies só devem ser usados com autorização explícita dos usuários*” em função de deixar o usuário da Internet com a sua privacidade exposta.

Nesse mesmo diapasão manifesta-se Luciana Antonini Ribeiro, quando aduz:

Não há dúvidas, pois, da necessidade de adequação das empresas virtuais às regras de proteção ao consumidor, sendo-lhes exigida a comunicação ao consumidor quanto à criação de bancos de dados. Dados privados do indivíduo, entretanto, somente poderão figurar em bancos de dados caso haja prévia autorização do consumidor, sendo vedada utilização para fins diversos do que os autorizados¹⁰⁴.

¹⁰⁰ ZANELLATO, Marco Antônio. op. cit.

¹⁰¹ Ibidem.

¹⁰² Ibidem.

¹⁰³ Ibidem.

¹⁰⁴ RIBEIRO, Luciana Antonini. **A privacidade e os Arquivos de Consumo na Internet - Uma Primeira Reflexão**. Revista de Direito do Consumidor | vol. 41 | p. 151 | Jan / 2002.

Dessa forma pode-se observar que o Direito deve ser dinâmico para acompanhar os avanços da tecnologia, que no mundo fático, nada mais são que a intervenção do homem no mundo conhecido como natural.

3. DELITOS INFORMÁTICOS: OS AGENTES DELITUOSOS NO AMBIENTE CIBERNÉTICO E APLICAÇÃO DA NORMA JURÍDICA PENAL

3.1. Os agentes.

Tomando por base o conceito de crime da Organização para Cooperação Econômica e Desenvolvimento da ONU, quando atribui que "*delito do computador é qualquer comportamento ilegal aéctico ou não autorizado envolvendo processamento automático de dados ou transmissão de dados*"¹⁰⁵. Nessa definição, presume-se que o agente tenha a necessidade mínima de conhecimento de informática, nível técnico para manipular o sistema, nesse tema sempre surgem às figuras do *Hacker* e do *Crackers*¹⁰⁶.

Segundo Túlio Lima Vianna o termo Hacker:

[..]de origem inglesa derivado do verbo *to hack* (cortar, cavar) que originalmente significava alguém que fabrica móveis utilizando um machado. No jargão da informática, pode ser traduzido livremente por "fuçador". É o indivíduo que se dedica a explorar os detalhes de sistemas programáveis. Profundo conhecedor de computadores, o hacker em geral domina muito bem o uso de sistemas operacionais como o Linux e o Windows e programa em linguagens como C e Assembly, entre outras. A especialidade dos hackers, no entanto, são as redes de computadores, em especial, a Internet¹⁰⁷.

Para Assis Medeiro o termo Cracker:

"[...] usado para designar quem quebra um sistema de segurança de forma ilegal ou sem ética. Este termo foi criado em 1985 pelos hackers em defesa contra o uso jornalístico do termo hacker. O uso deste termo reflete a forte revolução contra o roubo e vandalismo praticado pelo cracking" [...] "fora do contexto especializado, o termo encontra-se geralmente associado à prática de atividades maliciosas e criminosas, como invasão de computadores, furto de informações, depredação de sites, entre outros. Esta associação é frequentemente criticada por várias comunidades (notavelmente

¹⁰⁵ ROSSINI, Augusto Eduardo de Souza. **Brevíssimas considerações sobre delitos informáticos**. Caderno Jurídico, São Paulo, n. 4, ano 2, jul. 2002, p. 04..

¹⁰⁶ MEDEIRO, Assis. **Livro Hackers: entre a ética e a criminalização**, São Paulo: Visual Books, jul, 2002.

¹⁰⁷ Vianna, Túlio Lima. **Dos Crimes por Computador**. Revista dos Tribunais | vol. 801 | p. 405 | Jul / 2002DTR\2002\382

pelos grupos desenvolvedores de software livre), que re-significam o termo designando-o às pessoas que tem entendimento avançado de informática e redes, disseminam a prática do conhecimento livre e se auto-organizam conectados em rede para a criação de eventos, estruturas e disseminação da cultura livre. Não estando estes ligados a atividades ilícitas, impõe-se uma distinção¹⁰⁸.

Márcia Regina Sawaya corrobora com a definição de Medeiro ao aduzir que o Cracker é:

[...] um indivíduo que usa o computador, maliciosamente, como hobby, e obtém acesso não autorizado a sistemas de computador, com o objetivo de derrotá-los. Pode roubar informações sobre contas bancárias e cartões de crédito ou destruir dados¹⁰⁹.

Quanto à definição de Hacker "*são programadores tecnicamente sofisticados, que dedicam boa parte de seu tempo a conhecer, dominar e modificar programas equipamentos*"¹¹⁰.

Para Tulio Lima Viana:

Cracker é o indivíduo que se utiliza de seus conhecimentos técnicos para "quebrar" todo e qualquer tipo de barreira de segurança. Numa definição simplista poderíamos dizer que é o hacker "do mal". Os crackers podem ter como objeto de seus crimes a quebra do sistema de segurança de programas ou o acesso ilícito a informações armazenadas em computadores. Limitaremos, no entanto, nosso estudo ao acesso não autorizado a e-mails, que é uma das modalidades do acesso ilícito a computadores¹¹¹..

Dessa maneira para melhor entendimento da denominação dos termos *Hacker* e *Cracker*, definiremos Hacker como toda a pessoa que tenha alto nível de conhecimento em ciência da computação - informática, na especialidade de rede de computadores e segurança dela. O *hacker* "*em geral domina muito bem o uso de*

¹⁰⁸ MEDEIRO, Assis. Livro Hackers - **Entre a Ética e a Criminalização**, Visual Books, São Paulo, jul, 2002. p. 17-22

¹⁰⁹ SAWAYA, Márcia Regina. **Dicionário de Informática e Internet**. São Paulo, Nobel, 3ª Reimpressão. 2010. p105.

¹¹⁰ Ibidem, p.208.

¹¹¹ Vianna ,Túlio Lima. **Dos crimes por computador**. Revista dos Tribunais | vol. 801 | p. 405 | Jul / 2002DTR\2002\382

sistemas operacionais como o Linux e o Windows, bem como programas em linguagens como C e Assembly, entre outras”¹¹².

Em publicação da matéria da Revista *Veja online*, registrou-se que no ano 2001 o Brasil abrigava cinco dos dez grupos mais ativos de vândalos cibernéticos no mundo. Em primeiro e terceiro lugar estavam os grupos autodenominados ‘*Silver Lords*’ e *Brasil ‘Hackers Sabotage*’¹¹³, estimando-se que consolidaram juntos 1911 ataques bem sucedidos, com a cifra de 1.172 ataques às páginas da Internet para os silver-lords, e entre seus feitos, registram-se invasões contra a Meca militar americana, o Pentágono, a própria Microsoft e a IBM americana. Os outros grupos brasileiros eram *prime suspectz*, *tty0* e *demônios*.

Embora tenha se passado mais de dez anos não houve mudanças positivas no quadro dos vândalos cibernéticos brasileiros, ao contrario, houve aumento na quantidade e no desempenho tecnológico desses vândalos. Esse aumento atinge tal proporção que obrigou a Polícia Federal a inaugurar um centro contra ataques cibernéticos o qual, segundo o portal G1 da Rede Globo de Televisão, registra que “*pelo menos 250 hackers já foram identificados e estão sendo monitorados. Redes do governo federal são alvo de dois mil ataques por hora, diz PF*”. Os relatórios da Polícia Federal registram ainda que “*as 320 redes de informação governo atualmente recebem mais de dois mil ataques por hora. Em junho de 2011, hackers atacaram e tiraram do ar sites de ministérios e da Presidência*”¹¹⁴.

¹¹² MEDEIRO, Assis. Livro Hackers - **Entre a Ética e a Criminalização**, Visual Books, São Paulo, jul, 2002. p. 17-22

¹¹³ HACKERS: os nossos são campeões. **Brasil abriga cinco dos dez grupos mais ativos de vândalos cibernéticos**. Geral Tecnologia. Revista Veja on-line. Edição 1716. 5 set. 2001. Disponível em: http://veja.abril.com.br/050901/p_076.html. Acesso em 15 maio. 2012.

¹¹⁴ Polícia Federal inaugura centro contra ataques cibernéticos. **Pelo menos HACKERS: os nossos são campeões. Brasil abriga cinco dos dez grupos mais ativos de vândalos cibernéticos**. Geral Tecnologia. Revista Veja on-line. Edição 1716. 5 set. 2001. Disponível em: http://veja.abril.com.br/050901/p_076.html. Acesso em 15 maio. 2012. **250 hackers já foram identificados e estão sendo monitorados. Redes do governo federal são alvo de 2 mil ataques por hora, diz PF**. “A Polícia Federal inaugurou na manhã desta segunda-feira (4), em Brasília, o Centro de Monitoramento do Serviço de Repressão a Crimes Cibernéticos. Segundo o diretor do centro, delegado Carlos Eduardo Sobral, a ideia é que a PF possa acompanhar suspeitos, identificar os ataques às redes do governo e prevenir maiores danos. A PF informou que o órgão será usado para prevenção e investigação a ataques cibernéticos contra sistemas de informação e infraestruturas críticas do governo federal. As 320 redes de informação governo atualmente recebem mais de 2 mil ataques por hora. Em junho de 2011, hackers atacaram e tiraram do ar sites de ministérios e da Presidência”. Portal G1 Brasil – Rede Globo de Televisão.

O ordenamento jurídico penal do Brasil é o maior estimulador dessa seara de desordeiros virtuais. A facilidade de atuação e a impunidade por parte de nossas leis são os combustíveis necessários para o desenvolvimento de tal classe de pessoas. Dentro deste quadro é que a sociedade brasileira reclama ao Direito, esperando dele um novo posicionamento que promova meios coibitivos, implantando sanções a toda gama de atos aéticos e condenáveis pela sociedade como um todo, cometidos no ambiente cibernético.

3.2 Delitos informáticos ou condutas aéticas

Nesse trabalho adota-se a denominação delitos informáticos com a finalidade de abranger todas as denominações que são compreendidas como sinônimos de crimes informáticos, pois essa terminologia não é consensual. Esses delitos são denominados de várias maneiras diferentes como: delitos computacionais, crimes de informática, crimes de computador, crimes eletrônicos, crimes telemáticos, crimes informacionais, ciberdelitos, cibercrimes. Adotamos o termo delito e iremos analisar as demais como expressões sinônimas. Quanto ao termo condutas aéticas, referimo-nos ao fato da sua nocividade à sociedade, mas, ainda, sem o enquadramento legal em norma penal incriminadora.

Augusto Eduardo de Souza Rossini aduz que "*delito do computador é qualquer comportamento ilegal, aético ou não autorizado envolvendo processamento automático de dados e/ou transmissão de dados*"¹¹⁵. Essa definição não se trata da mais adequada em virtude de não contemplar aspectos formais.

Os delitos informáticos são definidos por Manuel Lopes Rocha como "*aqueles que têm por instrumento ou por objeto sistema de processamento*

Atualizado em 04/06/2012, 13h32. Disponível em: <<http://g1.globo.com/brasil/noticia/2012/06/policia-federal-inaugura-centro-contra-ataques-ciberneticos.html>>. Acesso em 10 maio. 2012.

¹¹⁵ ROSSINI, Augusto Eduardo de Souza. **Brevíssimas considerações sobre delitos informáticos**. Caderno Jurídico, São Paulo, n. 4, ano 2, jul. 2002, p. 3.

eletrônico de dados, apresentando-se em múltiplas modalidades de execução e de lesão de bens jurídicos".¹¹⁶

Klaus Tiedemann¹¹⁷ conceitua o crime de informática como "*Criminalidade mediante computadores*", utilizando ainda como definição para todas as condutas por meio do computador que sejam ilegais, ou prejudiciais à sociedade¹¹⁸.

Ivete Senise Ferreira concebe que o crime de informática é o resultado da "[...] *informatização crescente das várias atividades desenvolvidas individual ou coletivamente na sociedade veio colocar novos instrumentos nas mãos dos criminosos*", complementa:

[...] cujo alcance ainda não foi corretamente avaliado, pois surgem a cada dia novas modalidades de lesões aos mais variados bens e interesses que incumbe ao Estado tutelar, propiciando a formação de uma criminalidade específica da informática, cuja tendência é aumentar quantitativamente e, qualitativamente, aperfeiçoar os seus métodos de execução¹¹⁹.

Na definição de Damásio de Jesus sobre a divisão dos delitos informáticos: "*Os crimes serão puros ou próprios, aqueles que sejam praticados por computador e se realizem ou se consumem também em meio eletrônico*"¹²⁰. Além disso, o autor complementa a definição incluindo a proteção ao ambiente:

Neles, o bem juridicamente protegido é o próprio ambiente informático, compreendendo os sistemas computacionais, sistemas operacionais, software de conexão entre os sistemas a informática, de conexão dos periféricos, segurança dos sistemas, titularidade das informações, integridade dos dados.

¹¹⁶ ROCHA, Manuel Lopes. **Direito da Informática Legislação e Deontologia** – Lisboa: ed. Cosmos, 1994, p.38.

¹¹⁷ TIEDMANN Klaus. **Poder Econômico e Delito**. Traduzido por Amélia Mantilla Villegas, Barcelona, 1985, apud LUIZ GUILHERME MOREIRA PORTO - "Fraude Informática", ob. coletiva Comércio Eletrônico, coordenadores: Ronaldo Lemos da Silva Júnior e Ivo Waisberg, co-edição IASP e Ed. RT. S. Paulo

¹¹⁸ Ibidem.

¹¹⁹ FERREIRA, Ivete Senise. **A Criminalidade Informática**, in **Direito e Internet - Aspectos Jurídicos Relevantes**, Bauru (SP), Edipro, 2000, p. 207..

¹²⁰ JESUS, Damásio E. de. **Comentários em Palestra Proferida no I Congresso Internacional do Direito na era da Tecnologia Informação**, realizado pelo Instituto Brasileiro de Política e Direito da Informática — IBDI, em novembro de 2000, no auditório do TRF da 5ª Região, em Recife-PE., Op. Cit *apud* ARAS, Vladimir. **Crimes de informática. Uma nova criminalidade**. Brasília. UFSC. Portal de e-governo, inclusão digital e sociedade do conhecimento. Disponível em: <http://www.egov.ufsc.br/portal/conteudo/crimes-de-informatica-uma-nova-criminalidade>. Acesso em: 12 dez. 2011.

Nesse posicionamento, continua aduzindo Damásio de Jesus:

Quanto aos delitos informáticos serão puros ou próprios: Constituem-se naqueles em que o sujeito ativo visa especificamente ao sistema de informática. O computador é o meio utilizado e o fim a ser alcançado pelo agente. Portanto, é crime de informática puro toda e qualquer conduta ilícita que tenha por objetivo exclusivo o sistema de computador.

Quanto aos delitos eletrônicos impuros, impróprios ou mistos: São aqueles em que o agente se vale do computador como meio para produzir resultado naturalístico, que ofenda o mundo físico ou o espaço "real", ameaçando ou lesando outros bens, não-computacionais ou diversos da informática.

Qualquer ação em que o agente tem por objetivo um bem juridicamente protegido diverso da informática, porém, o sistema de informática se constitui em ferramenta, em meio imprescindível à sua consumação¹²¹. [grifos nossos]

Nesse tocante da divisão dos delitos informáticos, Marcelo Xavier de Freitas Crespo apresenta uma classificação e tomada de posição qual corrobora com Damásio de Jesus, ao aduzir que “*as condutas praticadas contra um sistema informático ou dado são o que se pode chamar de delito de risco informático, ao passo que as demais podem ser denominadas delitos vinculados à informática*”¹²². Classificando assim, como crimes digitais próprios e crimes digitais impróprios:

Para os crimes digitais próprios, “*Conforme a classificação adotada, passamos agora a discorrer sobre os delitos, cujos bens jurídicos atingidos são primordialmente os sistemas informatizados ou de telecomunicações ou dados*”¹²³.

Para firmar um melhor entendimento dessa divisão, destacamos a definição ao Crespo para os crimes digitais impróprios:

[...]os crimes digitais impróprios nada mais são que aqueles já tradicionalmente tipificados no ordenamento, mas agora praticados com auxílio de modernas tecnologias. Assim, essa denominação apenas representa que os ilícitos penais tradicionais podem ser cometidos por meio de novos *modus operandi*¹²⁴.

¹²¹ JESUS, Damásio E. Op. Cit.

¹²² CRESPO, Marcelo Xavier de Freitas, **Crimes Digitais**. São Paulo: Saraiva, 2011, p.63.

¹²³ Ibidem, p.44.

¹²⁴ Ibidem, p.63

A doutrina apresenta uma visão analítica de crime com o seguinte conceito “*ação humana típica, antijurídica e culpável*”¹²⁵.

A **ação humana típica**, segundo Damásio de Jesus, consiste na “*é o comportamento humano (positivo ou negativo) que provoca um resultado (em regra) e é previsto na lei penal como infração.*”¹²⁶

Quanto à **antijuridicidade** ou **ilicitude**, para Guilherme de Souza Nucci:

[...] trata-se de um juízo de reprovação social, incidente sobre o fato e seu autor, devendo o agente ser imputável, atuar com consciência potencial de ilicitude, bem como ter a possibilidade e a exigibilidade de atuar de outro modo, seguindo regras impostas pelo direito (teoria normativa pura, proveniente do finalismo)¹²⁷.

A **antijuridicidade** é todo comportamento humano que descumpre, desrespeita, infringe uma lei penal e, conseqüentemente, fere o interesse social protegido pela norma jurídica. Retornando a Damásio de Jesus encontramos: “*É a relação de contrariedade entre o fato típico e o ordenamento jurídico.*”¹²⁸ o fato contradizendo a norma jurídica Pena. Contata-se que há antijuridicidade quando a conduta se opõe ao ordenamento jurídico. O fato típico, até que se prove o contrário, é um fato que, ajustando-se ao tipo penal, caracteriza-se como antijurídico. Todavia, há causas excludentes da antijuridicidade do fato típico, como por exemplo, matar em legítima defesa.

No tocante à **culpabilidade** aduz Damásio de Jesus que é a “*reprovação da ordem jurídica em face de estar ligado o homem a um fato típico e antijurídico.*”¹²⁹ Diz-se que há culpabilidade quando o agente poderia ter agido em consonância com o ordenamento jurídico, mas não o fez¹³⁰.

¹²⁵ LEAL, João José. **Direito Penal Geral**. São Paulo: Atlas, 1998, p.167.

¹²⁶ JESUS, Damásio Evangelista de, **Direito Penal**, parte geral, 34ª ed., São Paulo, Saraiva, 2013, p.196.

¹²⁷ NUCCI, Guilherme de Souza. **Código Penal Comentado**, 9ª ed. São Paulo. Revista dos Tribunais, 2009, p.227.

¹²⁸ JESUS, Damásio Evangelista de, op. cit. p.197.

¹²⁹ Ibidem.

¹³⁰ Ibidem.

3.3 Formas de atuação do agente

O agente usará todas as técnicas e métodos que lhe permita obter informações já que essas informações são os elementos necessários para a sua prática espúria e delituosa. Para Marcelo de Luca Marzochi, “o *modus operandi* é o resultado das leis do mundo hacker”¹³¹, dividindo a conduta em cinco etapas: 1 - Use sempre a inteligência ao invés da força bruta; 2 - Nunca faça nada de sua casa; 3 - Guarde seu material de *Hacking* fora do alcance de *Lammers*; 4 - Seja cauteloso e não confie em ninguém; 5 - Cuidado com os Governos e órgãos corruptos; 6 - Não seja pego, por nada neste mundo Hacker.

Segundo Marzochi o *modus operandi* do agente com melhor resultado é a Engenharia Social:

A técnica mais usada dispensa conhecimento de computação. É a ‘Engenharia Social’. É simples: a maneira mais fácil de se conseguir uma informação é perguntando! Fazer as perguntas certas na hora certa. Essa foi a “técnica” utilizada por Kevin Mitnick no ataque a algumas empresas. Ele telefonava se fazendo passar por funcionário e com isso obtinha as informações necessárias. Mas há ainda outros pontos.

[...]

A segurança física dos computadores e também do local onde estes se encontram. As técnicas nesse caso são: vasculhar o lixo (trashing), escuta telefônica (wiretapping), negação de serviço (denial of service) e a monitoração de emanações eletrônicas. Vasculhar o lixo consiste em procurar por papéis que tenha sido jogados fora por funcionários das empresas e que tenham informações importantes (essa técnica é mostrada no filme “Hackers - Piratas de Computador”). Escuta telefônica é o famoso grampo. Monitoração de emanações eletrônicas é a mais interessante. Consiste na monitoração das ondas eletromagnéticas emitidas pelo monitor do computador. Essas ondas podem ser decodificadas e pode-se ter acesso a tudo o que é feito na tela do monitor. Em instalações militares os monitores são revestidos de chumbo para evitar esse tipo de ataque. A negação de serviço consiste na não disponibilização do serviço ao usuário. São exemplos desse tipo de ataque o corte da energia, o flooding (muito utilizado no programa de bate-papo mIRC) e o mail-bomb.¹³²

¹³¹ MARZOCHI, Marcelo de Luca. **Aspectos Jurídicos da Internet no Brasil**, São Paulo, LTR, 2000.

¹³² Ibidem.

Contudo, o forte do hacker são as armas tecnológicas que são softwares computacionais com finalidades específicas, como: Vírus, Trojans, Mail-bomb, Anonymai Backdoor, Worms.

Devemos ainda ressaltar que todas as *armas tecnológicas* utilizadas em conjunto com o *modus operandi* do agente podem afetar direitos inerentes à privacidade do homem, direitos esses consubstanciados na dignidade da pessoa humana.

3.4 As Armas Tecnológicas.

3.4.1 As Armas Tecnológicas: Os Vírus

Na definição de Marcelo Xavier de Freiras Crespo, os vírus:

Segmentos de códigos de computação que se anexam a programas ou sistemas de modo a se propagar pelas máquinas e contaminar outros sistemas em contato com esta, através de e-mail remetidos automaticamente e até mesmo por transmissão de dados maliciosos por outros métodos.¹³³

Quanto à forma de infectar os sistemas informáticos aduzem Marco Antonio de Barros, Daniella D'Arco Garbossa e Christiany Pegorari Conte, que:

Já os "vírus", podem ser espalhados de diversas maneiras, a partir da instalação de programas de procedência duvidosa, com a utilização de disquetes ou CDs infectados, com a abertura de arquivos, entre outros. Os vírus podem destruir totalmente os programas e arquivos do computador, podendo exercer controle total sobre a máquina.¹³⁴

A atuação do vírus de computador é semelhante a um vírus biológico, infecta sistemas de computadores multiplicando-se através de cópias de si mesmo e

¹³³ Crespo. Marcelo Xavier de Freiras, **Crimes Digitais**, Saraiva, São Pulo, 2011. p.74.

¹³⁴ Barros. Marco Antônio de, Garbossa. Daniella D'Arco, Conte, Christiany Pegorari. **Crimes informáticos e a Proposição Legislativa: considerações para uma reflexão preliminar**. Revista dos Tribunais | vol. 865 | p. 399 | Nov / 2007.

tenta se espalhar para outros computadores utilizando todos os meios, inclusive as conexões das redes de computadores.

4.4.2 As Armas Tecnológicas: Cavalo de Tróia (Trojans)

Trojan ou Cavalo de Tróia é um pequeno programa que quando instalado no computador tem a ação semelhante à lenda do cavalo de Tróia, abrindo uma porta de acesso para que seu invasor possa manipular à distância. Trata-se de um programa espião na definição de Marco Antonio de Barros, Daniella D'Arco Garbossa e Christiany Pegorari Conte:

O "cavalo de tróia" também é um programa espião e, uma vez instalado no computador, permite o "roubo" de informações, arquivos e senhas do usuário. Normalmente o usuário recebe e-mails com um arquivo anexado e, quando abre esse arquivo, instala-se o cavalo de tróia no computador do usuário. Na maioria das vezes, tal programa ilícito vai possibilitar aos *crackers* o controle total de sua máquina. Poderá ver e copiar todos os arquivos do usuário, descobrir todas as senhas que ele digitar, formatar seu disco rígido, ver a sua tela e até mesmo ouvir sua voz se o computador tiver um microfone instalado. É um verdadeiro procedimento de invasão informática.¹³⁵

O conceito foi resultante de programas que se faziam passar por esquemas de segurança de autenticação em que o operador inseria logins e senhas pensando que estas operações eram legítimas.

Para Valdir Carlos Pereira Filho o *cavalo de tróia*:

[...]é um programa que fica instalado em um computador e, através dele, as proteções que impediriam transferências de dados ficam desabilitadas. Logo, a captura de informações e dados colocados e digitados é facilitada, o computador fica vulnerável a invasões de terceiros¹³⁶.

¹³⁵ BARROS, Marco Antonio de, Garbossa. Daniella D'Arco, Conte, Christiany Pegorari. **Crimes Informáticos e a Proposição Legislativa: considerações para uma reflexão preliminar**. Revista dos Tribunais | vol. 865 | p. 399 | Nov / 2007.

¹³⁶ PEREIRA FILHO, Valdir Carlos. **Responsabilidade Civil dos Bancos em Operações Financeiras Realizadas pela Internet**, Revista de Direito Bancário e do Mercado de Capitais | vol. 42 | p. 163 | Out / 2008 | DTR\2011\1538.

3.4.3 As Armas Tecnológicas: Mail-bomb

Segundo Marcelo de Luca Marzochi, o Mail-bomb é nocivo aos sistemas computacionais cuja função está diretamente associada à própria designação do seu nome cuja finalidade é sobrecarregar um servidor de e-mail:

O problema do mail-bomb geralmente não é seu, mas sim do seu provedor. [...] cada usuário de um provedor de Internet possui um espaço limitado na caixa postal para receber mensagens. O bomb se refere à "estourar" o espaço que lhe destina no seu provedor, e assim o provedor, com sua caixa postal entupida de mensagens, começa a rejeitar mensagens novas destinadas a você, até que você retire suas mensagens e esvazie sua caixa postal.

O processo de mail-bomb é exatamente isso: várias mensagens repetidas, geralmente contendo um texto malcriado, que abarrotam seu e-mail e impede que você receba mais mensagens, o que pode ser muito prejudicial para algumas pessoas com negócios importantes que dependem de correio eletrônico.¹³⁷

Percebe-se que a intensão do agente é congestionar o servidor de e-mail. Com as contas dos usuários atingindo o máximo da capacidade, o resultado será a suspensão do funcionamento do servidor de e-mail.

3.4.4 As Armas Tecnológicas: Anonymail (e-mail anônimo)

Segundo Marcelo de Luca Marzochi, *Anonymail* é uma modalidade de software nocivo aos sistemas computacionais cuja finalidade é gerar uma fraude, de forma mais específica, uma falsidade ideológica, pois nesse programa não existe o preenchimento automático do campo *from* dos e-mails:

Existem alguns programas de e-mail (como o próprio Anonymail) onde, além de preencher todos os campos normais de uma mensagem, eles permitem que você preencha também o campo "from:", ou seja, ele deixa você se passar por quem você quiser. E também em que servidor de e-mail você deseja mandar a mensagem¹³⁸.

¹³⁷ MARZOCHI, Marcelo de Luca. op. cit.

¹³⁸ Idem.

3.4.5 As Armas Tecnológicas: Backdoor

Explica Marco Antonio Zanellato, que a palavra é a união de duas palavras da língua inglesa back e door. O Backdoor é um pequeno software nocivo aos sistemas computacionais desenvolvido para acessar remotamente sistemas de computação. No primeiro momento, ocorre a invasão para que o Backdoor seja instalado. Instalado e em funcionamento, abre-se uma porta ou rompe-se uma segurança para permitir o ataque.

[...]..que existe uma confusão entre o que é um Backdoor e um Cavalo de Tróia, principalmente porque o estrago provocado por ambos é semelhante. Para deixar claro, um Cavalo de Tróia é um programa que cria deliberadamente um Backdoor em seu computador. Programas que usam a Internet e que são de uso corriqueiro, como Browsers, programas de e-mail, ICQ ou IRC podem possuir Backdoors.

[..]os Backdoors são abertos devido a defeitos de fabricação ou falhas no projeto dos programas. Isto pode acontecer tanto acidentalmente quanto pode ser introduzido ao programa propositadamente. Exemplo: versões antigas do ICQ possuem defeito que abre um Backdoor que permite ao hacker derrubar a conexão do programa com o servidor, fazendo com que ele pare de funcionar. Por isso, é aconselhável sempre atualizar as versões dos programas instalados no computador. O fabricante do software com defeito tem o dever de avisar aos usuários sobre a sua existência e promover a substituição do programa por outro em perfeitas condições (CDC (LGL\1990\40), art. 10, § 1.º).¹³⁹

Essa é uma das características dos Trojans, que, quando associado ao Backdoor podem se utilizar desta característica para monitorar todas as informações.

3.4.5 As Armas Tecnológicas: Worms (vermes)

Para Carla Rodrigues Araújo de Castro os *Worms* “são programas que se propagam de um sistema para o outro sem a interferência do usuário infectado,

¹³⁹ ZANELATO. Marco Antônio. op. cit..

dividem-se em: “worm” de Internet e “worm” de IRC. O worm destrói diversos arquivos do computador”¹⁴⁰.

Quanto à forma de infestação explica Marcelo de Luca Marzochi:

Da mesma forma que os biológicos, esse verme informático se instala nos hospedeiros para a realização de determinada tarefa. Um exemplo de worm é um programa que desvia pequenas quantias de cada conta de um banco, de modo que nem o correntista nem o banco percebam, para uma determinada conta que o autor do ataque tenha acesso¹⁴¹.

3.5 Aplicação da Norma Jurídica Penal

Segundo Fernando Capez a aplicação da norma penal incriminadora deve estar sustentada e ser dirigida à dignidade da pessoa humana, aduz que “*tipos penais que se limitam a descrever formalmente infrações penais, independente de sua efetiva potencialidade lesiva, atentam contra a dignidade humana*”¹⁴². A dignidade da pessoa humana é o elemento que emana dos princípios estruturadores e limitadores do Direito, devendo estar alicerçado nos Princípios Básicos do Direito Penal.

Para Nilo Batista¹⁴³, são cinco os princípios básicos para a tutela do Direito Penal: a) **Princípio da Legalidade ou da reserva legal**: Amparado pela Carta Máxima de 88, no art. 5º, XXXIX, conjuntamente com o Código Penal no art. 1º que assegura que “*não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal*”; b) **Princípio da intervenção mínima**: Dispõe limite à atuação Estatal através do Direito Penal, apenas havendo sua manifestação apenas “*quando os outros ramos do Direito não conseguirem prevenir a conduta ilícita*”¹⁴⁴; c) **Princípio da lesividade**: Para Nilo Batista e Zaffaroni esse princípio exige que a

¹⁴⁰ CASTRO, Carla Rodrigues Araújo de. **Crimes de Informática e seus Aspectos Processuais**. 2 ed. rev., ampl. E atualizada. Rio de Janeiro: Lumen Juris, 2003. p.27-28.

¹⁴¹ MARZOCHI, Marcelo de Luca. op.cit.

¹⁴² CAPEZ, Fernando. **Curso de Direito Penal: Parte geral**. Vol. 1. 7.ed. rev. e atual. São Paulo: Saraiva, 2004. p.14.

¹⁴³ Batista, Nilo, **Introdução Crítica ao Direito Penal Brasileiro**, 4ª edição, Rio de Janeiro. Ed. Revan, 1999.

¹⁴⁴ JESUS, Damásio E. de, **Direito Penal - Parte Geral**, vol. 1/10, item n. 11, "h", 26ª ed., 2003, São Paulo, Saraiva.p.10.

conduta do agente lesione ou exponha à lesão um bem jurídico penalmente tutelado e deve ainda afetar interesses de outrem¹⁴⁵; d) **Princípio da Humanidade**: já prevista no ordenamento pátrio quando na máxima carta no Art. 5º, inciso III, assegura que "*ninguém será submetido à tortura nem a tratamento desumano ou degradante*" e d) **Princípio da Culpabilidade**: propõe Nilo Batista que, como premissa, qualquer espécie de responsabilidade pelo resultado na denominada responsabilidade objetiva, seja rejeitada. Verificando-se sempre que a pena seja aplicada unicamente quando a conduta do agente esteja associada causalmente a um resultado reprovável¹⁴⁶.

A interpretação

A exegese é o primeiro passo a ser dado na busca da descoberta da vontade do legislador ao criar a norma jurídica com a finalidade de ajustar às situações fáticas, aos casos concretos da vida. Segundo Celso D. de Albuquerque Mello, "*.. a arte de bem interpretar a norma jurídica é a grande virtude do verdadeiro jurista: conhecer as leis não é considerar seu texto, mas, sim, sua força e majestade (seire leges non hoc est verba earum tenere, sed vim ac potestatem)*"¹⁴⁷.

No processo da interpretação das normas jurídicas para melhor focar o nosso estudo destacamos a interpretação *analógica* e a interpretação *extensiva*.

¹⁴⁵ Nilo Batista e Zaffaroni aduzem que o "princípio da lesividade, segundo o qual nenhum direito pode legitimar uma intervenção punitiva quando não medeie, pelo menos, um conflito jurídico, entendido como a afetação de um bem jurídico total ou parcialmente alheio, individual ou coletivo. [...] Para elaborar esse princípio no direito penal, o conceito de bem jurídico é essencial, embora habitualmente se proceda logo a uma indevida equiparação entre bem jurídico lesionado ou exposto a perigo e bem jurídico tutelado, identificando noções substancialmente diferentes, pois nada prova que a lei penal efetivamente tutele um bem jurídico: a única coisa suscetível de verificação é que ela confisca um conflito que atinge ou coloca em perigo o bem jurídico". ZAFFARONI, Eugênio Raul; BATISTA, Nilo. **Direito Penal Brasileiro I**. Rio de Janeiro: Editora Revan, 2006, pp. 226-227.

¹⁴⁶ "O princípio da culpabilidade deve ser entendido, em primeiro lugar, como repúdio a qualquer espécie de responsabilidade pelo resultado, ou responsabilidade objetiva. Mas deve igualmente ser entendido como exigência de que a pena não seja infligida senão quando a conduta do sujeito, mesmo associada causalmente a um resultado, seja-lhe reprovável." BATISTA, Nilo. **Introdução Crítica ao Direito Penal Brasileiro**, 9ª ed. Rio de Janeiro: Editora Revan, 2004. p. 103.

¹⁴⁷ MELLO, Celso D. de Albuquerque. **Curso de Direito Internacional Público**. 10. ed. Rio de Janeiro: Editora Renovar, 1994.

A interpretação analógica na visão do escritor Mirabete é estar “*Diante do princípio da legalidade do crime e da pena, pelo qual não se pode impor sanção penal a fato não previsto em lei, é inadmissível o emprego da analogia para criar ilícitos penais ou estabelecer sanções criminais*”¹⁴⁸, continua Mirabete:.

Nada impede, entretanto, a aplicação da analogia às normas não incriminadoras quando se vise, na lacuna evidente da lei, favorecer a situação do réu por um princípio de equidade. Há, no caso, a chamada analogia *in bonam partem*, que não contraria o princípio da reserva legal, podendo ser utilizada diante do disposto no já citado artigo 4º da LICC. Ressalte-se, porém, que só podem ser supridas as lacunas legais involuntárias: onde uma regra legal tenha caráter definitivo não há lugar para a analogia, ou seja não há possibilidade de sua aplicação *contra-legem*.¹⁴⁹

Para Heleno Cláudio Fragoso a analogia:

[...]distingue-se da interpretação, porque constitui um processo de integração da ordem legal, e não meio de esclarecer o conteúdo da norma. Através da analogia aplica-se a lei a hipótese por ela não prevista, invocando-se substancialmente o chamado argumento a *pari ratione*”¹⁵⁰.

Sendo uma forma de integração, o exegeta investe tentando fechar uma lacuna resultante da inexistência da norma específica sobre determinada matéria. No entanto, na esfera penal tal procedimento não é passível da utilização pelo exegeta simplesmente porque seu uso foi vedado pelas normas e artigos já mencionados, exceto para benefício do réu.

A Interpretação Extensiva é ensinada por Damásio de Jesus como forma de ampliar o alcance das palavras da Lei:

Diz-se extensiva a interpretação quando o caso requer que seja ampliado o alcance das palavras da lei para que a letra corresponda à vontade do texto. Ocorre quando texto legal não expressa a sua vontade em toda a extensão desejada. Diz menos do que pretendia dizer. *Lex minus dixit quam voluit ou Lex minus scripsit, plus voluit*¹⁵¹

¹⁴⁸ MIRABETE, Julio Fabrini. **Manual de Direito Penal**. São Paulo: Atlas, 1991. p.48.

¹⁴⁹ Ibidem.

¹⁵⁰ FRAGOSO, Heleno Cláudio. **Lições de Direito Penal: a nova parte geral**. 8ª ed. Rio de Janeiro: Forense, 1985. p. 87

¹⁵¹ JESUS, Damásio Evangelista de, **Direito Penal – Parte Geral**, 34ª ed., São Paulo, Saraiva, 2013, p.83

Segundo Heleno Cláudio Fragoso é plenamente admissível a interpretação extensiva em relação à lei penal em função de que a interpretação mostra a vontade do legislador já existente:

A interpretação extensiva é perfeitamente admissível em relação à lei penal, ao contrário do que afirmavam autores antigos. Nestes casos não falta a disciplina normativa do fato, mas, apenas, uma correta expressão verbal. Há interpretação extensiva quando se aplica o chamado argumento *a fortiori*, que são casos nos quais a vontade da lei se aplica com maior razão. É a hipótese do argumento *a maiori ad minus* (o que é válido para o mais, deve necessariamente prevalecer para o menos) e do argumento *a minori ad maius* (o que é vedado ao menos é necessariamente no mais). Exemplo deste último argumento: se o Código Penal incrimina a bigamia, logicamente também pune o fato de contrair alguém mais de dois casamentos (Manzini)¹⁵².

Assim, concluímos a total impossibilidade da adequação de tais interpretações, seja o método analógico ou extensivo, sem que previamente esteja contida na própria norma tal possibilidade.

¹⁵² FRAGOSO, Heleno Cláudio. **Lições de Direito Penal**: a nova parte geral. 8ª ed. Rio de Janeiro: Forense, 1985. p.86.

4. DELITOS INFORMÁTICOS TIPIFICADOS POR NORMA PENAL INCRIMINADORA QUE TUTELA OS DIREITOS DA PERSONALIDADE.

Nesse tópico abordaremos sobre os tipos penais enquadrados como delitos informáticos e inseridos em nosso ordenamento jurídico no Código Penal ou em Legislação Especial, que buscam tutelar os direitos da personalidade.

Como definido anteriormente, esses delitos podem ser classificados como próprios quando contra sistemas telemáticos ou impróprios quando a via de consecução seja sistemas informáticos.

4.1. Inserção de dados falsos em sistema de informações.

Foi introduzida pela Lei Federal nº. 9.983/2000 que criou o Art. 313-A do CP:

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.

4.2. Modificação ou alteração não autorizada de sistema de informações.

Foi Introduzido pela Lei Federal nº. 9.983/2000 que criou o Art. 313-B do CP: *“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 administrador”*.

4.3. Interceptação de comunicações telefônicas.

Foi introduzido pelo Art. 10 da Lei Federal nº 9.296/96. “*Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei*”. Pena -reclusão, de dois a quatro anos, e multa.

4.4 Divulgação de segredo.

Redação dada pela Lei Federal nº 9.983/2000 que criou no Art. 153, o § 1º-A do CP. “*Divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública*”. Pena – detenção, de 1 (um) a 4 (quatro) anos, e multa.

4.5 Violação de sigilo funcional.

Encontra-se descrito no Art. 325, § 1º, inciso I do CP: “*Permite ou facilita, mediante atribuição, fornecimento e empréstimo de senha ou qualquer outra forma, o acesso de pessoas não autorizadas a sistemas de informações ou banco de dados da Administração Pública.*” Pena - detenção, de 6 (seis) meses a 2 (dois) anos, ou multa, se o fato não constitui crime mais grave, Tendo ainda, uma qualificadora da pena de 2 (dois) a 6 (seis) anos, e multa no § 2º “*Se da ação ou omissão resulta dano à Administração Pública ou a outrem.*”

4.6. Fraude no serviço eleitoral através de computador.

Encontra-se descrito no art. 72 da Lei Federal nº 9.504/97, no inciso I: “*Obter acesso a sistema de tratamento automático de dados usado pelo serviço eleitoral, a fim de alterar a apuração ou a contagem de votos*”; no inciso II registra:

Desenvolver ou introduzir comando, instrução, ou programa de computador capaz de destruir, apagar, eliminar, alterar, gravar ou transmitir dado, instrução ou programa ou provocar qualquer outro resultado diverso do esperado em sistema de tratamento automático de dados usados pelo serviço eleitoral”; “Causar, propositadamente, dano físico ao equipamento usado na votação ou na totalização de votos ou a suas partes.

4.7 Impedir ou dificultar o acesso do consumidor às informações.

Encontra-se descrito no CDC (Código de Defesa do Consumidor), Lei Federal nº 8.078/90, Art. 72, “*Impedir ou dificultar o acesso do consumidor às informações que sobre ele constem em cadastros, banco de dados, fichas e registros*”. Pena: detenção de seis meses a um ano ou multa.

4.8 Informação desatualizada sobre o consumidor.

Encontra-se descrito no CDC, Art. 73, “*Deixar de corrigir imediatamente informação sobre consumidor constante de cadastro, banco de dados, fichas ou registros que sabe ou deveria saber ser inexata*”. Pena - detenção de um a seis meses ou multa.

4.9 Sigilo dos dados.

Encontra-se descrito no Art. 5º, inciso XII, Constituição Federal ao definir que “*É inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas*”, tendo como exceção, exclusivamente “*por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal*”.

4.10 Delito de acesso não autorizado a sistemas computacionais

Este tipo penal requer um estudo mais detalhado em relação aos demais tipos penais mencionados, em virtude de ser uma inovação no ordenamento jurídico penal pátrio.

Com o advento da recém-criada Lei nº 12.737 de 30 de novembro de 2012 em vigor desde a data de 30 de março de 2013, foi criado o tipo penal de *Invasão de dispositivo informático* que passou a ser inserido no Código Penal pátrio através dos artigos 154-A e 154-B com a seguinte redação:

Invasão de dispositivo informático

Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:

Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.

§ 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no *caput*.

§ 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.

[...]

Ação penal

Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos.

Segundo o editorial do site G1 da Rede Globo de televisão, a lei foi denominada pela mídia como Lei Carolina Dieckmann em função do ocorrido no “começo de maio de 2012, 36 fotos íntimas da atriz Carolina Dieckmann foram furtadas do computador dela e postadas na internet. O advogado da atriz chegou a dizer que, em cinco dias, as fotos foram acessadas oito milhões de vezes”¹⁵³. Continua a reportagem narrando que “o episódio serviu para desengavetar, no

¹⁵³ Globo *online*, BOM DIA BRASIL. **Senado aprova Lei Carolina Dieckmann sobre crimes de internet**. Disponível em: <<http://g1.globo.com/bom-dia-brasil/noticia/2012/11/senado-aprova-lei-carolina-dieckmann-sobre-crimes-de-internet.html>>, Acesso em: 10 dez. 2012.

*mesmo mês, a discussão no Congresso sobre como punir esses criminosos cibernéticos - já que o Código Penal, de 1940, não trata do assunto”*¹⁵⁴.

O que estimulou o destaque da mídia no ocorrido residia na falta de proteção de privacidade. A simples discussão dos direitos da personalidade em esfera cível não satisfaz a vítima, àquele que teve o seu direito vilipendiado. A vítima requer uma resposta do Estado com rapidez e na proporção da violação do bem valorado, que é a sua privacidade.

Para Victor Haikal no dispositivo legal há um requisito imperioso para enquadramento da conduta humana ao tipo penal, a exigência da necessidade de “*ultrapassar um mecanismo de segurança, mas o texto não define exatamente qual*”¹⁵⁵, o que questiona-se no caso dos computadores que já existe uma senha para acesso se “*ela já terá um ‘mecanismo de segurança’ a ser quebrado*”¹⁵⁶.

Contudo, cabe esclarecer que o acesso não autorizado somente se caracteriza em sistemas computacionais de *ambiente fechado*, ou seja, aquele que possui regras severas de segurança. Não se aplicando nos casos de simples utilização de sistemas computacionais abertos que encontram-se disponíveis para que qualquer um que queira conhecer o seu conteúdo possa acessar. Essa tese é defendida por Lóren Formiga de Pinto Ferreira e José Carlos Macedo de Pinto Ferreira Júnior quando aduzem:

O acesso não autorizado a um sistema computadorizado ou rede de computadores pela violação de regras de segurança. [...] Já o uso não autorizado pode ser realizado aceitando o risco de causar prejuízo ou dano ao sistema, ao seu proprietário ou a quem tenha autorização para acessá-lo, no intuito de causar tal prejuízo ou efetivamente o causando.¹⁵⁷

¹⁵⁴ Globo *online*, BOM DIA BRASIL. Op. Cit.

¹⁵⁵ Globo *online*, TECNOLOGIA E GAME.. Victor Haikal, advogado especialista em direito digital e sócio do Patrícia Peck Advogados. **Lei 'Carolina Dieckmann' só vale para PCs protegidos, diz advogado**. Disponível em: <<http://g1.globo.com/tecnologia/noticia/2012/12/lei-carolina-dieckmann-so-vale-para-pcs-protegidos-diz-advogado.html>> Acesso em 10 dez. 2012.

¹⁵⁶ Ibidem.

¹⁵⁷ FERREIRA, Lóren Formiga de Pinto. FERREIRA JÚNIOR, José Carlos Macedo de Pinto, **Os "Crimes de Informática" e seu enquadramento no direito penal pátrio**. Revista dos Tribunais | vol. 893 | p. 407 | Mar / 2010 | DTR\2010\137.

Fabrcio Rosa apresenta a mesma argumentaçaõ da necessidade de seguranga redigida para configurar o acesso nãõ autorizado quando aduz que:

[...]concerne especificamente à conduta daquele que ilegalmente penetra em um sistema informático ou telemático protegido por medidas de seguranga, ou, ainda, ali se mantenha contra a vontade expressa ou tácita de quem tem o direito de excluí-lo.¹⁵⁸.

Em uma análise mais profunda, Vãlter Kenji Ishida expõe que a objetividade jurídica da norma recém-criada foi proteger “a liberdade individual, particularmente o direito à intimidade, já que o objetivo é tutelar dados e informações pertencentes a determinada pessoa”¹⁵⁹. A norma traz abertura à sua adequaçãõ ao avanço da tecnologia ao referir que o “tipo penal fala em ‘invadir’ que significa acessar de forma indevida dispositivo informático alheio”¹⁶⁰.

O termo *dispositivo informático* é denominaçaõ moderna, bem contemporânea, podendo contemplar quaisquer equipamentos informáticos, ou que venha a ser criado, na visãõ de Ishida:

O termo hodierno é mais abrangente, já que tal dispositivo nãõ mais se limita a computadores, abrangendo aparelhos celulares, smartphones, tablets, ipads etc. Nãõ há necessidade do dispositivo estar conectado à internet, podendo ser outro o acesso (p. ex. através de bluetooth)¹⁶¹.

A norma também busca contemplar o *modus operandi* do agente que, para Ishida, deve contemplar a violaçaõ de vulnerabilidades:

[...]deve incluir violaçaõ indevida de mecanismo de seguranga ou ainda através da instalaçaõ de vulnerabilidades. O modo mais comum é a instalaçaõ de programa através de e-mail falso, onde o *hacker* (pessoa que invade o sistema) passa a ter acesso ao conteúdo do seu computador ou de outro dispositivo similar¹⁶².

¹⁵⁸ ROSA, Fabrcio. **Crimes de Informática**. 2. ed. Campinas: CookSeller, 2005.

¹⁵⁹ ISHIDA, Vãlter Kenji. **As modificações promovidas pela Lei Carolina Dieckmann no Código Penal**. Jornal Carta Forense. Artigos Penal, Disponível em: <<http://www.cartaforense.com.br/conteudo/artigos/as-modificacoes-promovidas-pela-lei-carolina-dieckmann-no-codigo-penal/9986>>, Acesso em: 12 dez 2012.

¹⁶⁰ Ibidem.

¹⁶¹ Ibidem.

¹⁶² Ibidem.

Para Ishida, ainda há a necessidade da observação dos elementos tipo subjetivo e objetivo do tipo por serem elementos integrantes da culpabilidade, quando aduz:

Tipo subjetivo. É o dolo de invadir, acrescido do elemento subjetivo do tipo consistente na vontade de obter, adulterar, ou destruir dados ou informações. Os dados podem ser entendidos como números ou valores. São a unidade básica da informação. Já informação significa interpretação destes dados ou o processamento destes dados. Consumação¹⁶³.

Na mesma vertente da necessidade do preenchimento dos requisitos subjetivos como elementos integradores da culpabilidade, aduzem Rebeca de Paula S. Andrade e Roberta D'Ángeles S. Andrade, que “o crime não é formal, é material, para a sua configuração requer que a ação humana do agente se ajuste na descrição da conduta do tipo e que o resultado se materialize”¹⁶⁴. A simples adequação da conduta humana ao tipo penal, ao “núcleo do verbo invadir não exauri o delito, é necessário adicionar o ‘animus nocend’ do agente quando deliberadamente quer obter, adulterar, ou destruir dados ou informações”¹⁶⁵.

Para as autoras, o simples enquadramento da conduta do agente à primeira proposição do caput do Art.154-A, não satisfaz á consumação do tipo penal, É necessário que haja forma de comprovar o elemento subjetivo da culpabilidade, que é: “com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita”¹⁶⁶. Como já mencionado, o tipo penal requer a existência de no mínimo duas proposições verdadeiras, dessa forma não haverá a configuração do tipo penal, por conseguinte não há crime.

¹⁶³ ISHIDA, Válter Kenji. **As modificações promovidas pela Lei Carolina Dieckmann no Código Penal.** Jornal Carta Forense. Artigos Penal, Disponível em: <<http://www.cartaforense.com.br/conteudo/artigos/as-modificacoes-promovidas-pela-lei-carolina-dieckmann-no-codigo-penal/9986>>, Acesso em: 12 dez 2012.

¹⁶⁴ ANDRADE. Rebeca Silva, ANDRADE. Roberta D'Ángeles Silva, **Breves Comentários Sobre a Lei nº 12.737.** Instituto Universitário Paulista. Publicações. Disponível em: <http://www.iunip.com.br/portal/publicacoes/breves_comentarios_lei_12-737.pdf>, Acesso em: 12 dez 2012.

¹⁶⁵ Ibidem.

¹⁶⁶ ISHIDA. Válter Kenji, op. cit.

4.11. Sabotagem de Computadores

Para João Araújo Monteiro Neto:

A Sabotagem Informática é um dos mais danosos delitos praticados por meio de um sistema informático e tem como objeto o próprio sistema. Efetua-se principalmente por dois meios. O primeiro é a destruição do programa ou dos dados por meio de elementos criados pelos sabotadores como vírus ou mini-programas que, quando ativados, inutilizam os programas principais destruindo-os ou distorcendo o seu funcionamento, tornando o sistema inapto a processar. O segundo ocorre quando estes mecanismos desfiguram os dados já armazenados, o que acarreta inúmeros prejuízos aos programas principais¹⁶⁷.

Passou a vigorar a partir do dia 30 de março de 2013, através da Lei nº 12.737, que alterou o caput do Art. 266, com a seguinte redação: “*Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública*”, com pena de “*detenção, de um a três anos, e multa.*” e criando o § 1º onde está descrito que “*incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento*”¹⁶⁸.

Segundo Rebeca de Paula S. Andrade e Roberta D’Angeles S. Andrade, a definição do tipo não prevê a possibilidade da sabotagem parcial, isto é, quando o agente intervém nos sistemas de processamento de dados e informações não para interromper, mas para reduzir o fluxo processamento ao ponto mínimo. Assim aduzem as autoras:

[...] nesse caso, o restabelecimento total do sistema é mais complexo, em virtude que esse “gargalo” pode estar em qualquer um dos itens que compõe o sistema do processamento do serviço, como: as redes físicas, as redes *wifi*, o próprio computador principal, os computadores auxiliares, cabos elétricos, cabos óticos e outros dispositivos que esteja em interoperabilidade com sistema de processamento de dados ou informações da rede telemática.¹⁶⁹

¹⁶⁷ MONTEIRO, João Araújo Neto, **Crimes informáticos uma abordagem dinâmica ao direito penal informático**, Revista Pensar, Fortaleza, v. 8, n. 8, p. 39-54, fev. 2003.

¹⁶⁸ BRASIL. **Lei nº 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12737.htm#art2. Acesso em: 12 dez 2012.

¹⁶⁹ ANDRADE, Rebeca Silva; ANDRADE, Roberta D’Angeles Silva. op. cit.

Conclui-se que no caso da situação problema abordado o resultado fático é tão desastroso quanto à interrupção do serviço, em função da dificuldade do pronto restabelecimento, e ainda mais, o agente mesmo descoberto não poderá ser incriminado por essa norma.

4.12. Criação de Vírus.

Passou a vigorar a partir dia 30 de março de 2013, através da Lei nº 12.737, que criou o § 1º do Art. 154 “*Invadir dispositivo informático alheio*”, do Código Penal pátrio com a seguinte redação: “*Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no ‘caput’*”. A pena referencia é de detenção, de 3 (três) meses a 1 (um) ano, e multa.

No tópico 6.0 desse trabalho, intitulado direito estrangeiro, podemos verificar que a pena aplicada ao agente delituoso desse tipo penal, que a legislação penal brasileira é a mais branda em relação aos demais países estudados.

5. CONDUTAS AÉTICAS NÃO TIPIFICADAS POR NORMA PENAL INCRIMINADORA, MAS QUE AFETAM DIREITOS DA PERSONALIDADE.

5.1 O delito de dano e os dados computacionais

O que buscaremos abordar nesse estudo é compreender com maior clareza o delito de dano e a possibilidade da sua adequação à conduta aética de dano a dados ou informações computacionais. O crime de dano está previsto no artigo 163 do Código Penal brasileiro “*Destruir, inutilizar ou deteriorar coisa alheia*”.

Nelson Hungria aduz que: “*o objeto material do crime de dano é a coisa imóvel ou móvel, devendo tratar-se obviamente, de coisa corpórea ou no sentido realístico, pois somente pode ser danificada por ação física*”¹⁷⁰.

Para Heleno Fragoso, “*dano é a alteração prejudicial de um bem; a destruição ou diminuição de um bem; o sacrifício ou restrição de um interesse jurídico*”¹⁷¹.

Para Damásio Evangelista de Jesus: “[...] *o elemento subjetivo do crime de dano é simplesmente o dolo, a vontade de destruir, inutilizar ou deteriorar coisa alheia*”¹⁷².

No tocante à Natureza jurídica, crime comum por não requerer característica especial do sujeito ativo; é unissubjetivo¹⁷³, em função de que para a sua consecução basta a conduta de um só agente; os sujeitos ativo e passivo: qualquer pessoa humana dispõe de capacidade para praticar o delito¹⁷⁴, quanto na condição de vítima qualquer pessoa física ou jurídica; tipo objetivo: o bem jurídico protegido, a coisa, móvel ou imóvel, pública ou privada e quanto ao tipo subjetivo: no

¹⁷⁰ HUNGRIA, Nelson. **Comentários ao Código Penal**, 1967, v. VII, Rio de Janeiro, Forense. p.106.

¹⁷¹ FRAGOSO, Heleno Cláudio. **Lições de direito penal: a nova parte geral**, 7ª ed. Rio de Janeiro: Forense. 1985. p.173.

¹⁷² JESUS, Damásio E. de. **Código Penal Anotado**, 13ª Ed. São Paulo. Saraiva, p.608.

¹⁷³ Idem. **Direito Penal – Parte Geral**, 34ª ed., São Paulo, Saraiva, 2013.

¹⁷⁴ BITENCOURT, Cezar Roberto. **Tratado de Direito Penal, Parte Geral 1**. 10ª ed. São Paulo. Saraiva. 2006. p.268.

Código Penal o dano só existe na forma dolosa¹⁷⁵. Já no Código Penal Militar¹⁷⁶, contempla a forma culposa para certos bens de maior importância ou relevo.

5.1.1 A conduta de dano a dados ou informações computacionais

Nesse primeiro momento nos cabe analisar ao *caput* da *norma agendi*, “*Destruir, inutilizar ou deteriorar coisa alheia*”, temos que entender com maior propriedade: a) o que são dados computacionais; b) qual o seu valor econômico; e c) compatibilidade ao verbo do tipo penal: “*da possibilidade de ser destruída, inutilizada ou deteriorada*”.

a. O que são dados computacionais:

O termo *dado* computacional é definido por Ricardo Miranda como um “*conjunto de registros qualitativos ou quantitativos conhecido que organizado, agrupado, categorizado e padronizado adequadamente transforma-se em informação*”¹⁷⁷. Já o termo *informação* é conceituado por Richard Wurman como “*aquilo que leva à compreensão [...] O que constitui informação para uma pessoa pode não passar de dados para outra*”¹⁷⁸. Para Miranda, *informação* são “*dados organizados de modo significativo, sendo subsídio útil à tomada de decisão*”¹⁷⁹.

¹⁷⁵ BRASIL, **Decreto-Lei nº 2.848 Código Penal**. “Art. 163 - Destruir, inutilizar ou deteriorar coisa alheia”, “Art. 18 - Diz-se o crime: Crime doloso, I - doloso, quando o agente quis o resultado ou assumiu o risco de produzi-lo”. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em 05 mai 2012.

¹⁷⁶ BRASIL, **Decreto-Lei nº 1001 - Código Penal Militar**, Art. 266. “Se o crime dos arts. 262, 263, 264 e 265 é culposos, a pena é de detenção de seis meses a dois anos; ou, se o agente é oficial, suspensão do exercício do posto de um a três anos, ou reforma; se resulta lesão corporal ou morte, aplica-se também a pena cominada ao crime culposos contra a pessoa, podendo ainda, se o agente é oficial, ser imposta a pena de reforma.” Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del1001.htm. Acesso em 05 mai 2012.

¹⁷⁷ MIRANDA, Roberto Campos da Rocha. “**O uso da informação na formulação de ações estratégicas pelas empresas**”. Ciência da Informação, Brasília, v.28, n.3, p.284-290, set./dez. p.285.

¹⁷⁸ WURMAN, Ricardo S. **Ansiedade de informação: como transformar informação em compreensão**. 5.ed. São Paulo: Cultura Editores, 1995. p.43.

¹⁷⁹ MIRANDA, Roberto Campos da Rocha. op. cit. p.285.

Para Carlos Caruso e Flavio Deny Steffen, o “bem mais valioso de uma empresa pode não ser o produzido pela sua linha de produção ou o serviço prestado, mas as ‘informações relacionadas’ com esse bem de consumo ou serviço”, continuando:

Acima de tudo, o bem mais valioso de uma empresa pode não ser o produzido pela sua linha de produção ou o serviço prestado, mas as informações relacionadas com esse bem de consumo ou serviço. É importante que os executivos em geral se conscientizem de que todas as informações têm algum tipo de valor para alguém e/ou para algo; o que ocorre é que ainda não se descobriu para quem ou para quê.

Ao longo da história, o ser humano sempre buscou o controle sobre as informações que lhe eram importantes de alguma forma; isso é verdadeiro mesmo na mais remota Antiguidade. O que mudou desde então foram as formas de registro e armazenamento das informações; se na Pré-história e até mesmo nos primeiros milênios da Idade Antiga o principal meio de armazenamento e registro de informações era a memória humana, com o advento dos primeiros alfabetos isso começou a mudar. Mas foi somente nos últimos dois séculos que as informações passaram a ter importância crucial para as organizações humanas”¹⁸⁰.

b. Da possibilidade de ser destruída, inutilizada ou deteriorada:

Esse é o momento de maior importância quando se coteja o objeto da pesquisa, *dado*, ao núcleo do verbo nos termos do *caput* do artigo 163 do CP, nesse caso, a questão raiz é se *dado* é coisa móvel?

Se *dado* tem valor econômico então é um bem. Assim conceitua Cezar Fiúza quando aduz que “bem é tudo aquilo que é útil às pessoas”¹⁸¹. Resta-nos agora diferenciar entre coisa e bem, que segundo Silvio Rodrigues “coisa é tudo que existe objetivamente, com exclusão do homem”¹⁸², enquanto os bens “são coisas que, por serem úteis e raras, são suscetíveis de apropriação e contêm valor

¹⁸⁰ Caruso, Carlos A. A., Steffen, Flavio Deny, **Segurança em Informática**, 3a Edição Revista e Ampliada, 3a ed. rev. ampl. - São Paulo, 2006.p.23

¹⁸¹ FIÚZA, Cezar. **Direito Civil: Curso Completo**. Belo Horizonte: Del Rey, 2004, p. 171..

¹⁸² RODRIGUES, Silvio. **Direito Civil – Parte Geral**. v 1. 32 ed. Saraiva. São Paulo: 2002. p. 116.

*econômico*¹⁸³. Tendo com distinção a seguinte distinção: “*coisa é o gênero do qual bem é espécie*”.

Os dados Informáticos ou de computador não podem ser classificados e/ou incluso entre coisas físicas ou corpóreas em função da intangibilidade, são incorpóreos equiparando-se à propriedade intelectual, constituindo-se numa nova forma de propriedade.

Para Carlos María Romeo Casabona:

Uma das características mais peculiares é a da natureza incorpórea da informação, sua intangibilidade. Do ponto de vista jurídico, isto significa que não se deve pretender proteger esta informação aplicando critérios semelhantes aos utilizados para a proteção dos objetos materiais. Assim, é necessário identificar o proprietário dos dados, seu detentor, a pessoa a que se referem esses dados, a própria sociedade. Ao mesmo tempo, deve-se prestar atenção aos sujeitos do delito, pois em alguns casos existem especificidades que requerem um cuidadoso exame dogmático e político-criminal¹⁸⁴.

Ao cotejar a norma do Código Penal e a interpretação da doutrina, mesmo sendo muito discutida a forma da sua aplicação na proteção dos dados informáticos, verifica-se a da impossibilidade da sua equiparação ao mundo das coisas móveis por falta de definição legal e doutrinária. Contudo, poderia resolver-se de forma bastante simples o problema através da alteração normativa, equiparando-se à coisa móvel a dados computacionais.

À título informativo, em situação semelhante, o furto de energia elétrica, não poderia ser contemplado pelo artigo 155 do CP: “*Subtrair, para si ou para outrem, coisa alheia móvel*”, em função que a energia elétrica na figura no mundo das coisas moveis, semelhante aos dados computacionais. Para suplantar o obstáculo, o legislador buscou equipará-la através da criação do § 3º: “*Equipara-se à coisa móvel a energia elétrica ou qualquer outra que tenha valor econômico*”, assim a conduta antes aética tornar-se conduta delituosa.

¹⁸³ RODRIGUES, Silvio. **Direito Civil – Parte Geral**. v 1. 32 ed. Saraiva. São Paulo: 2002. p. 116.

¹⁸⁴ CASABONA. Carlos María Romeo. **Dos delitos informáticos ao crime cibernético**: uma aproximação conceitual e político-criminal. Ed: RT. Ciências penais | vol. 4 | p. 83 | jan / 2006.

5.2 Delito acessório de dano a dados informáticos.

A recém-criada Lei de nº 12.735¹⁸⁵ alterou o Código Penal Brasileiro com o *caput* do Art. 154-A criando o tipo penal de Invasão de dispositivo informático, assim como o crime acessório de dano inserido no *caput*, com o seguinte texto:

Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de *obter, adulterar ou destruir dados ou informações* sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita

¹⁸⁶

Surge a figura do partícipe¹⁸⁷ e o crime acessório de receptação¹⁸⁸ na definição do § 1º “*Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput*”.

Contudo, para a configuração do crime de dano de dados ou informações a Lei condiciona a existência da conduta humana ao núcleo do verbo *Invadir* dispositivo informático alheio, conectado ou não à rede de computadores, *mediante*

¹⁸⁵ A **Lei de nº 12.737** é objeto de estudo nesse trabalho no Capítulo 4 - Delitos Informáticos: Tipificados por Norma Penal incriminadora que tutela os direitos da personalidade, item 4.10 Acesso não autorizado a sistemas computacionais.

¹⁸⁶ **Crime acessório** é aquele que para sua configuração, decorre de outros crimes cometidos. O crime acessório pressupõe a prática de outro crime que lhe dá conteúdo e justificativa. “*Assim, no furto e posterior receptação, o primeiro é o principal e o segundo é acessório*”. JESUS, Damásio Evangelista de, **Direito Penal – Parte Geral**, 34ª ed., São Paulo, Saraiva, 2013, p.236.

¹⁸⁷ A **participação** é “a atividade acessória daquele que colabora para a conduta do autor com a prática de uma ação que, em si mesma, não é penalmente relevante”. MIRABETE, Júlio Fabbrini. **Manual de Direito Penal**, Ed: Atlas, 1990, p.232.

BRASIL. **Código Penal**. Art. 29 – “Quem, de qualquer modo, concorre para o crime incide nas penas a este cominadas, na medida de sua culpabilidade”. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>, Acesso em: 13 dez 2012.

¹⁸⁸ **Receptação**: Art. 180 – “Adquirir, receber, transportar, conduzir ou ocultar, em proveito próprio ou alheio, coisa que sabe ser produto de crime, ou influir para que terceiro, de boa-fé, a adquira, receba ou oculte”. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>, Acesso em: 13 dez 2012.

*violação indevida de mecanismo de segurança*¹⁸⁹ em virtude de ser um crime acessório e não principal.

O questionamento nesse momento é: um proprietário de um dispositivo informático desprovido de senha de acesso, em relação aos seus dados e informações, perde a condição da pessoa humana detentora dos direitos inerentes à personalidade?

Para melhor resposta ao questionamento apresentado, nesse contexto, Rebeca de Paula Silva Andrade e Roberta D'Angeles Silva Andrade aduzem: “*Por certo que a resposta é não! Em virtude de que os direitos da personalidade são próprios, únicos, irrenunciáveis*”, complementam aduzindo: “*O simples fato do esquecimento de ativar ou de criar uma senha de acesso, para um determinado dispositivo informático não poderá ruir direitos irrenunciáveis. de forma mais clara é explicado*”:

No que tange ao acesso não autorizado, podemos nesse momento criar uma situação hipotética para melhor verificar a eficácia da norma recém-criada que passa a compor o direito informático. Nesse aspecto específico, a norma busca tutelar a privacidade ao proteger os dados e informações, assim, hipoteticamente se um usuário / proprietário de um dispositivo informático, que a título de atender uma solicitação do seu superior hierárquico, ausenta-se do ambiente de trabalho por aproximadamente uma hora esquecendo-se de ativar a senha de acesso. Ao retornar, toma conhecimento que um colega de trabalho o qual é seu desafeto, realiza acesso ao dispositivo efetivando uma ou algumas operações como:

a) adultera conteúdo de arquivos de dados, de trabalho de pesquisa transcorrido em um lapso temporal de dois anos ininterruptos; b) apaga todos os dados de *backup* do referido trabalho de pesquisa; c) formata do disco rígido eliminando todos os dados e informações contidas e reinstalando apenas os softwares básicos e necessários (editores de texto e planilha eletrônica); d) copia os arquivos com as fotos íntimas do proprietário do dispositivo informático, para posterior divulgação na Internet.

[..]questiona-se: É justo que o dispositivo informático tenha sido acessado e por consequência os dados e informações modificadas, corrompidas ou eliminadas por terceiro, em função da falta de senha de acesso, sem que esse agente sofra a coerção da norma penal incriminadora? Os direitos inerentes à personalidade poderiam ser

¹⁸⁹ ARDIZZONE, Salvatore, **A legislação penal italiana em matéria de computer crimes entre direito e política criminal**. Universidade Federal de São Carlos. Portal de e-governo, inclusão digital e sociedade do conhecimento. Disponível em: <<http://www.egov.ufsc.br/portal/sites/default/files/anexos/10685-10685-1-PB.html>>. Acesso em 12 dez 2012.

desrespeitados pela simples falta da senha de acesso ao dispositivo informático?

Por certo que a resposta é não! Em virtude de que os direitos da personalidade são próprios, únicos, irrenunciáveis. O simples esquecimento de ativar ou de criar uma senha de acesso para um determinado disposto informático não poderá ruir direitos inalienáveis.

[...]

Na criação do texto do Art. 154-A o legislador inseriu uma vez a letra “e” como conjunção aditiva, e três vezes o termo “ou” como conjunção alternativa, criando assim vários elementos lógicos, passíveis de serem explicadas utilizando uma *tabela verdade* da Lógica Matemática. Quando é utilizado o conectivo *e* ou *and* (em inglês) cria-se proposições, onde todas as proposições são juntadas, na qual somente resultará como verdadeiro se todas elas forem verdadeiras. Quando é utilizada a conjunção *ou* (or em inglês) sua finalidade é unir as proposições que, bastando que apenas uma delas seja verdadeira para que toda a expressão também seja.

Dessa forma, para a configuração do crime descrito, é necessário que a primeira proposição seja verdadeira: a) “**Invadir dispositivo informático[...] mediante violação indevida de mecanismo de segurança**” conjuntamente com qualquer outra proposição, podendo ser a segunda conjunção aditiva ou qualquer uma das conjunções alternativas, como: b) “**com o fim de obter, adulterar**”; c) ou “**destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo**”, ou d) “**instalar vulnerabilidades para obter vantagem ilícita**”¹⁹⁰. [grifos do autor]

Verifica-se que o legislador buscou contemplar no Art. 154-A várias condutas aéticas prejudiciais à sociedade e agressora aos direitos da personalidade, transformando-as em delito as quais destacaremos: a) “*crime de furto: na descrição fim de obter*”¹⁹¹; b) “*crime de dano: na descrição adulterar ou destruir dados ou informações*”¹⁹²; c) “*crime de perigo concreto: da descrição oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.*”¹⁹³

¹⁹⁰ ANDRADE. Rebeca de Paula Silva, ANDRADE. Roberta D’Angeles Silva, **Breves Comentários sobre a Lei nº 12.737**. Instituto Universitário Paulista. Publicações. Disponível em: <http://www.iunip.com.br/portal/publicacoes/breves_comentarios_lei_12-735.pdf>, Acesso em: 12 dez 2012.

¹⁹¹ Ibidem.

¹⁹² Ibidem.

¹⁹³ “No direito penal brasileiro, os crimes de perigo concreto têm sido tradicionalmente definidos como uma categoria típica que se particulariza por exigir a comprovação de que o bem jurídico tutelado tenha estado efetivamente em perigo”. D’AVILA, Fabio Roberto e DARCIE, Stephan

Como já mencionado, todas as definições dos tipos penais requer como premissa para o enquadramento do agente que a conduta humana esteja de acordo com a definição na primeira proposição¹⁹⁴ do Art. 148-A: “*Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança*”. Assim, não haverá os crimes de furto, dano ou perigo concreto.

5.3 Violação de correspondência.

No art. 5º, inciso XII da Constituição Federal, encontra-se que é “*inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas*”, essa mesma proteção, da inviolabilidade da correspondência encontramos também Código Penal, no *caput* do Art. 151:

Devassar indevidamente o conteúdo de correspondência fechada, dirigida a outrem”, no inciso II Violação de comunicação telegráfica, radioelétrica ou telefônica – “quem indevidamente divulga, transmite a outrem ou utiliza abusivamente comunicação telegráfica ou radioelétrica dirigida a terceiro, ou conversação telefônica entre outras pessoas.

Encontra-se como criminoso o ato de qualquer pessoa que, indevidamente, divulga, transmite a outrem ou utiliza abusivamente a comunicação telegráfica ou radioelétrica dirigida à terceiro, bem como conversação telefônica entre outras pessoas cuja pena é de detenção, de um a seis meses, ou multa.

Para poder compreender o tipo penal quando se tenta equiparar aos crimes informáticos, surge o problema da definição o que é correspondência?

A Lei 6.538/78 dispõe sobre os Serviços Postais da União. A definição está registrada no artigo 7º, parágrafo 1º, do que é o serviço postal: “*Constitui serviço*

Doering. **Algumas Reflexões sobre os Crimes de Perigo Concreto.** In Boletim IBCCRIM. São Paulo : IBCCRIM, ano 18, n. 218, p. 08-09, jan., 2011.

¹⁹⁴ ISHIDA. Válder Kenji, **As modificações promovidas pela Lei Carolina Dieckmann no Código Penal.** Jornal Carta Forense. Artigos Penal, Disponível em: <<http://www.cartaforense.com.br/conteudo/artigos/as-modificacoes-promovidas-pela-lei-carolina-dieckmann-no-codigo-penal/9986>>, Acesso em: 12 dez 2012.

postal o recebimento, expedição, transporte e entrega de objetos de correspondência, valores e encomendas, conforme definido em regulamento", nos itens do parágrafo 1º do mencionado diploma, são definidos os objetos que possam ser enquadrados como correspondência, que são: as cartas, cartões postais, impressos, cecograma e pequena-encomenda, conforme abaixo transcrevemos:

TÍTULO II - DO SERVIÇO POSTAL

Art. 7º - Constitui serviço postal o recebimento, expedição, transporte e entrega de objetos de correspondência, valores e encomendas, conforme definido em regulamento.

§ 1º - São objetos de correspondência:

- a) carta;
- b) cartão-postal;
- c) impresso;
- d) cecograma;
- e) pequena - encomenda.

§ 2º - Constitui serviço postal relativo a valores:

- a) remessa de dinheiro através de carta com valor declarado;
- b) remessa de ordem de pagamento por meio de vale-postal;
- c) recebimento de tributos, prestações, contribuições e obrigações pagáveis à vista, por via postal.

§ 3º - Constitui serviço postal relativo a encomendas a remessa e entrega de objetos, com ou sem valor mercantil, por via postal.¹⁹⁵

Na Rede Mundial de computadores o que de forma fática substitui ou assemelha-se com os serviços postais da União é o correio eletrônico. Desta maneira, iremos estudar a possibilidade da adequação da proteção legal concedida à correspondência ao correio eletrônico, popularizado com a denominação de *e-mail* ou *email*.

5.3.1 O correio eletrônico (e-mail)

O correio eletrônico, denominado como correio-e, ou *e-mail* "*é um termo usado para designar toda mensagem enviada através de uma rede de computadores para uma caixa postal eletrônica*"¹⁹⁶.

¹⁹⁵ BRASIL, **Lei nº 6.538, de 22 jul.1978. (Dispõe sobre os Serviços Postais.)** Regula os direitos e obrigações concernentes ao serviço postal e ao serviço de telegrama em todo o território nacional. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L6538.htm/>. Acesso em 22 jun. 2011.

Para Patrícia Peck Pinheiro, o “*e-mail ou correio eletrônico é uma aplicação de redes de computadores, muito utilizado na Internet, que possibilita a troca de mensagens e arquivos entre os usuários. A palavra tem o significado literal de ‘electronic mail’ ou correio eletrônico*”¹⁹⁷.

Segundo Vânia Siciliano Aieta:

O correio eletrônico pode ser concebido como um mecanismo disposto por meio eletrônico que tem como finalidade principal a transmissão de conteúdo à distância. O e-mail nada mais é do que um recurso tecnológico auxiliar na transmissão de informações. Trata-se de um sistema mediante o qual se pode enviar e receber mensagens de uma caixa de correio de uma pessoa até a caixa de correio de outra, permitindo a emissão e recepção de mensagens¹⁹⁸.

Podemos resumir como sendo o e-mail um sistema de computação que permite a troca de mensagens eletrônicas na rede Mundial de Computadores.

O que importa para o momento à título de verificação da existência da tutela constitucional e de lei ordinária para o e-mail, equivalente a deferida para a correspondência, é questionar se as mensagens trafegadas no correio eletrônico podem ser assemelhadas aos serviços regulares desenvolvidos pelas Empresas de Correios e Telégrafos, ente público detentor exclusivo dos serviços, como telegrama, cartas, cartão postal?

Aduzem Valkíria Aparecida Lopes Ferraro, Rogério Martins de Paula e Renata Silveira Paiva, que “*o e-mail constitui hoje uma das formas mais comuns de liberdade de expressão e de pensamento, devendo, portanto, ser resguardado afim de que se proteja a intimidade do remetente e a do destinatário*”¹⁹⁹, indo além ao discorrerem, entende-se que deve ser dada a proteção da tutela constitucional

¹⁹⁶ Vianna, Túlio Lima. **Dos crimes por computador**. Revista dos Tribunais | vol. 801 | p. 405 | Jul / 2002DTR\2002\382

¹⁹⁷ PINHEIRO, Patrícia Peck. **Direito digital**. 4. ed. rev., atual. e ampl. São Paulo: Saraiva, 2010, p.164.

¹⁹⁸ AIETA Vânia Siciliano. **A violação da intimidade no ambiente de trabalho e o monitoramento eletrônico dos empregados**. São Paulo: RT, Revista de direito constitucional e internacional | vol. 55 | p. 60 | abr / 2006

¹⁹⁹ Ferraro. Valkíria Aparecida Lopes ; DE PAULA, Rogério Martins; PAIVA. Renata Silveira de. Semina: **A Sociedade da Informação na Economia Globalizada: Alguns Aspectos do Direito Cibernético**. Ciências Sociais e Humanas, Londrina, v. 25, set. 2004, p.26.

deferida para a correspondência convencional para as mensagens eletrônicas, o e-mail, equiparando-as:

Não se poderia, dessa forma, permitir a inspeção sobre o conteúdo das mensagens enviadas, já que o dispositivo constitucional não faz distinção entre o correio postal e o eletrônico e mesmo porque, a Internet representa apenas uma evolução na forma com que as correspondências são transmitidas. Por essa razão, seria perfeitamente possível a aplicação das regras pertinentes a outros meios de comunicação como, por exemplo, o art. 151 do Código Penal brasileiro. A inviolabilidade das informações transmitidas é a mesma, pouco importando o meio pelo qual sua transmissão se dá.²⁰⁰

5.3.2 Natureza Jurídica do correio eletrônico (e-mail)

Observamos as enumeras interrogações acerca da definição da natureza jurídica do e-mail e na busca da melhor compreensão destacamos a posicionamento de Ana Amélia Menna Barreto de Castro Pereira a qual aduz que “a correspondência fechada corresponde a uma mensagem eletrônica que trafega sem qualquer mecanismo de segurança que impossibilite o acesso por terceiros não autorizados”²⁰¹

Dessa maneira, poderia ser analisado “traçando-se um paralelo, a correspondência eletrônica encontraria alguma semelhança com a definição de cartão postal, uma vez que a mensagem circula na rede despojada de qualquer envoltório ou lacre, vale dizer em termos tecnológicos, sem proteção de segurança”²⁰².

Para Kildare Gonçalves Carvalho, a interceptação dos e-mails somente é possível nos casos de prática delituosa e de forma indireta equipara à correspondência ao aduzir que “Quanto à inviolabilidade de correspondência,

²⁰⁰ Ferraro. Valkíria Aparecida Lopes ; DE PAULA, Rogério Martins; PAIVA. Renata Silveira de. Semina: **A Sociedade da Informação na Economia Globalizada: Alguns Aspectos do Direito Cibernético**. Ciências Sociais e Humanas, Londrina, v. 25, set. 2004, p.26.

²⁰¹ PEREIRA, Ana Amélia Menna Barreto de Castro, **Correio Eletrônico Corporativo – aspectos jurídicos**, in revista de Direito do Trabalho, n.110, abril/junho de 2003, p.12.

²⁰² Ibidem.

embora não haja, quanto a ela, previsão expressa no texto constitucional permitindo que seja interceptada, deve-se entender possa ser quebrada naqueles casos em que venha a ser utilizada como instrumento de práticas ilícitas”²⁰³.

De maneira mais abrangente manifesta-se Euler Sinoir de Oliveira ao conceber que as contas de e-mail pessoal que de traz a privacidade absoluta de seu titular:

[...]pessoal insere-se em inquestionável ambiente de privacidade absoluta de seu titular, uma vez que as informações trafegadas são de natureza pessoal, confidencial e de seu interesse específico. Por esse motivo, se sujeitam ao agasalho das garantias constitucionais de proteção à intimidade, da vida privada, assim como a inviolabilidade do sigilo de correspondência”.

[...]

Nas condições apontadas, o endereço eletrônico de titularidade pessoal não comporta a incidência de qualquer acesso ou interferência de terceiros, nem mesmo do provedor de serviço de conexão à internet contratada, que não está autorizado a fornecer informações sobre o usuário, ressalvadas a hipótese de cumprimento judicial”²⁰⁴.

Em função da inexistência de uma construção doutrinária ou jurisprudencial sobre o tema não permite que, de forma sólida, coloque-se o e-mail em paralelo com a correspondência ou comunicação de dados, sendo necessário, primeiramente, a abordagem de alguns aspectos: a) O e-mail é uma correspondência? Se for verdadeira a afirmativa, sua natureza Jurídica é de correspondência! Nesse caso questiona-se: É uma correspondência aberta ou uma correspondência fechada? b) Caso seja falsa a afirmativa, a natureza jurídica será concebida como transmissão de dados.

5.3.3 Correio eletrônico no ambiente de trabalho.

Para Alexandre Agra Belmonte “*Pesquisar a natureza jurídica da violação do conteúdo das mensagens eletrônicas é enfrentar e responder a seguinte*

²⁰³ CARVALHO, Kildare Gonçalves. **Direito constitucional** 10ª ed.. Belo Horizonte: Del Rey, 2004. p 390.

²⁰⁴ OLIVEIRA, Euler Sinoir de. A Inconstitucionalidade da Violação de E-mail do Empregado pelo Empregador. **Revista Justiça do Trabalho**, Porto Alegre, ano 22, nº 261, p. 47, setembro 2005.

*pergunta: o que impede a violação de mensagens*²⁰⁵. A resposta ao questionamento está em escolher qual o inciso do Art. 5º que fará a proteção: Se a tutela constitucional virá da inviolabilidade das comunicações pessoais contido no inciso XII - “*é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas...*”, ou da proteção à intimidade provinda do inciso 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*” do mesmo diploma legal?²⁰⁶

Para o autor, de acordo com a tutela legal, a doutrina manifesta-se de forma própria no tópico em pauta e por se tratar das comunicações no ambiente laboral exclui-se a violação da intimidade, incluindo-se de forma exclusiva a comunicação em si.

Para Ana Amélia M. C. Pereira não há que se falar em preceito constitucional do sigilo da correspondência por não se aplicar ao ambiente corporativo em virtude de ser um ambiente próprio com finalidade exclusiva, assim, aduz:

As características específicas que envolvem a mensagem eletrônica corporativa não se enquadram do preceito constitucional garantidor da inviolabilidade da correspondência (CRFB, art. 5º, XII), da intimidade e da vida privada de obreiro que se utiliza de sistema operacional na qualidade de usuário autorizado²⁰⁷.

Segundo Euler Sinoir de Oliveira os e-mails corporativos trafegam na rede privada do empregador, cabendo-lhe unicamente a titularidade:

A correspondência eletrônica corporativa trafega através de rede privada de computadores da empresa, suportando o empregador, na qualidade de proprietário dos equipamentos e titular da caixa postal, com os custos do registro e outros relativos à prestação de serviços de provimento de acesso a conexão à internet²⁰⁸.

²⁰⁵ BELMONTE, Alexandre Agra. **Monitoramento da Correspondência Eletrônica nas Relações do Trabalho**. LTR, São Paulo, 2004, p.64.

²⁰⁶ Ibidem.

²⁰⁷ PEREIRA, Ana Amélia Menna Barreto de Castro, **Correio Eletrônico Corporativo – aspectos jurídicos**, in revista de Direito do Trabalho, n.110, abril/junho de 2003, p.12.

²⁰⁸ OLIVEIRA, Euler Sinoir de. **A Inconstitucionalidade da Violação de E-mail do Empregado pelo Empregador**. Revista Justiça do Trabalho, Porto Alegre, ano 22, nº 261, p. 47-48, setembro 2005.

A idéia central está no objeto do correio eletrônico que é exclusivamente para serviço de *correio interno e privativo da empresa*, voltado exclusivamente para o exercício de sua atividade comercial.

Portanto, o endereço eletrônico pertencente à conta corporativa atua como um veículo de comunicação privada do empregador e integra seu ambiente privado. O correio eletrônico corporativo traduz-se em um serviço de correio interno e privativo da empresa, voltado exclusivamente para o exercício de sua atividade comercial. Esse meio de comunicação remota, largamente utilizado no tráfego de informação, destaca-se por propiciar sensível economia de tempo, rapidez na condução de problemas, elevando em consequência a produtividade e reduzindo custos operacionais.²⁰⁹

Retornando ao posicionamento de Patrícia Peck Pinheiro, aduz: “[...]apesar de muito semelhante à correspondência, é um meio de comunicação com características próprias”²¹⁰. Essas características devem ser analisadas, como: “*número de receptores da mensagem variável e do uso para o qual está sendo submetido, se pessoal, comercial ou publicitário*”²¹¹.

A maior distinção que a autora identifica no momento da comparação está no fato de que “*seu conteúdo é disponibilizado na rede para que seus dados sejam enviados no sistema de pacotes aleatórios, utilizando vários caminhos*”²¹².

A inexistência de uma construção doutrinária ou jurisprudencial sobre o tema não permite que, de forma sólida, venha-se a colocar em paralelo com a correspondência ou comunicação de dados. Contudo, encontramos na doutrina todos os elementos para a efetiva realização da tutela da privacidade das informações que nele circula como a tutela Constitucional do art. 5º, inciso XII, quando assegura a inviolabilidade excetuando-se: “[...]no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal.”, devendo, por ser fonte mediata, ser

²⁰⁹ OLIVEIRA, Euler Sinoir de. **A Inconstitucionalidade da Violação de E-mail do Empregado pelo Empregador**. Revista Justiça do Trabalho, Porto Alegre, ano 22, nº 261, p. 47-48, setembro 2005.

²¹⁰ PINHEIRO, Patrícia Peck. **Direito digital**. 4. ed. rev., atual. e ampl. São Paulo: Saraiva, 2010, p.164.

²¹¹ Ibidem.

²¹² Ibidem.

elemento suficiente para realizar a tutela do e-mail por apresentar uma correspondência do mundo real no mundo virtual.

Segundo Amaro Moraes e Silva Neto, é impossível a equiparação do correio eletrônico os serviços convencionais de correspondência em consequência do próprio processo tecnológico da rede por onde os dados que compõe o e-mail trafega:

Entrementes, a par dessas vantagens, o correio eletrônico é um meio de comunicação bastante inseguro, eis que antes de uma mensagem eletrônica chegar a seu destino ela realiza uma longa e tortuosa viagem. Parte do computador remetente para o computador de seu provedor de acesso à Internet (ISP) e, na sequência, passa por incontáveis outros servidores até alcançar seu destinatário. Portanto, em primeiro lugar, constata-se que os administradores (*webmasters*) dos provedores de acesso podem, facilmente, vasculhar o conteúdo dos *e-mails* que retransmitem, que neles aportam durante a transmissão ou que simplesmente recebem.

Além dos provedores que têm acesso direto às mensagens eletrônicas, outros podem interceptá-las em seu curso porque tais mensagens enviadas chegam a passar por centenas de pontos no Planeta – aleatórios e sempre novos – antes de alcançarem seus destinatários.

Daí a facilidade de serem adulteradas, acrescentando-se-lhes ou excluindo-se-lhes texto. Também podem ser interceptadas e sumariamente excluídas, apagadas. Afinal os *bits* (aquelas ‘coisas’ que não são ‘coisas’) se misturam sem qualquer esforço e os rastros que deixam não são tão facilmente identificáveis ou descobertos.

Enfim, a transmissão de *e-mails*, no que diz respeito à privacidade, não difere muito das transmissões através de sinais de fumaça dos índios da América nortista (na época em que eram devastados) ou dos sons dos tambores de muitas tribos africanas (que ainda resistem à devastação). Ninguém se responsabiliza pela integridade dos *e-mails* remetidos²¹³.

5.3.4 Da manifestação judiciária.

No âmbito judicial, os posicionamentos dos tribunais que ocorreram confrontam-se com algumas teorias doutrinárias, a exemplo do Tribunal de Justiça de Goiás que se pronunciou sobre o tema de forma favorável a não equiparação do

²¹³ MORAES, Amaro. NETO, Silva. **E-mails Indesejados à Luz do Direito: spam**. São Paulo: Quartier Latin, 2002. p. 55-56.

e-mail à correspondência, através da rejeição da denúncia oferecida pelo Ministério Público de Goiás contra a juíza Ana Cláudia Veloso Magalhães de Itapuranga:

Por maioria de votos, o Órgão Especial do Tribunal de Justiça de Goiás rejeitou [...] denúncia oferecida pelo Ministério Público de Goiás contra a juíza Ana Cláudia Veloso Magalhães, de Itapuranga. Ela foi acusada de praticar os crimes de prevaricação (retardar ou deixar de praticar, indevidamente, ato de ofício, ou praticá-lo contra disposição expressa de lei, para satisfazer interesse ou sentimento pessoal) e interceptação de comunicação telemática, sem autorização judicial (Lei nº 9.296/96), por ter obtido junto à Bol On Line Ltda endereço e telefone de internauta que havia enviado mensagens ofensivas à sua honra à Corregedoria-Geral da Justiça e à jornal de grande circulação local²¹⁴.

No primeiro momento, o desembargador Floriano Gomes votou pelo recebimento da denúncia, porém o desembargador Paulo Teles Antunes divergiu, argumentando que “[...]que não existe nenhuma legislação específica que normatize a privacidade e proteção de dados na internet, pois a interceptação do fluxo não é o mesmo que quebra o sigilo de dados telemáticos”²¹⁵, tendo sido acompanhado pela maioria, passando a redator do acórdão o qual iremos transcrever em parte:

[...]a natureza jurídica do e-mail (correio eletrônico) é decorrente do fato de que ele não circula através de serviço postal, já que seu tráfego ocorre através de sistema operacional e não tem finalidade pessoal ou expectativa de privacidade”. Ainda, “Convém lembrar que a internet é um dos grandes nichos das telecomunicações e transmissões de dados e informações em qualquer lugar do mundo, gerando comunicação remota entre equipamentos”, ainda, ressalta o magistrado.

[...]que não existe nenhuma legislação específica que normatize a privacidade e proteção de dados na internet, pois a interceptação do fluxo não é o mesmo que quebra o sigilo de dados telemáticos. “Não há disposição penal específica a reger o sigilo de dados em se tratando de correio eletrônico, evidente que fica vedada a aplicação extensiva da norma penal prevista no artigo 10 da Lei 9.296/96”

Ao analisar os fatos e os personagens jurídicos, o magistrado afirmou ainda que como Bruno Cali Fonseca não existia no contexto investigatório até o momento em que a denunciada tentou localizar a pessoa que enviou as mensagens, já que naquela ocasião, procurava evadecastro@bol.com.br, não há que se falar em quebra de sigilo telemático. “Se não existe no mundo civil a pessoa de Eva

²¹⁴ JORNAL JURID. **Órgão Especial Rejeita Denúncia Contra Juíza**. Disponível em: <http://jornal.jurid.com.br/materias/noticias/orgao-especial-rejeita-denuncia-contra-juiza>, Acesso em 10 Jun. 2010.

²¹⁵ Idem. **Órgão Especial rejeita denúncia contra juíza**. Disponível em: <http://jornal.jurid.com.br/materias/noticias/orgao-especial-rejeita-denuncia-contra-juiza>, Acesso em 10 Jun. 2010.

de Castro não existe motivo para se falar em quebra de sigilo telemático. A mensagem anônima não tem rosto, nem personalidade. E neste caso, tanto não tem, que Bruno Calil Fonseca se identificava como "evadecastro", ressaltou. Para ele, o fato de Bruno Calil ter se ocultado no anonimato, utilizando do correio eletrônico para expelir suas opiniões depreciativas, denota que ele agiu de má-fé, pois a seu ver, a atitude do internauta estava impregnada do sentimento de covardia e da expectativa de impunidade.²¹⁶

Ante ao exposto, o Tribunal de Justiça do Estado de Goiás concebe como natureza jurídica do e-mail como transmissão de dados.

O Tribunal Superior do Trabalho (TST)²¹⁷ reconheceu pela primeira vez no ano de 2005 o direito do empregador em monitorar os e-mails dos seus funcionários, até como forma de obter provas para justa causa. No caso concreto, o procedimento foi adotado pelo HSBC Seguros Brasil S.A. depois de tomar ciência da utilização do e-mail, por um funcionário, para envio de fotos pornográficas para os seus colegas.

Em julgamento de um tema inédito no TST, a Primeira Turma decidiu, por unanimidade, que não houve violação à intimidade e à privacidade do empregado e que a prova assim obtida é legal. Para o embasamento da decisão, o Ministro Relator Dr. João Oreste Dalazen aduziu:

Os sacrossantos direitos do cidadão à privacidade e ao sigilo de correspondência, constitucionalmente assegurados, concernem à comunicação estritamente pessoal, ainda que virtual ("e-mail" particular). Assim, apenas o e-mail pessoal ou particular do empregado, socorrendo-se de provedor próprio, desfruta da proteção constitucional e legal de inviolabilidade²¹⁸.

Argumentou ainda o Ministro, que na relação empregatícia, quando se utiliza o e-mail corporativo perde-se o condão da tutela constitucional, tornando-se necessária outra interpretação: "[...]e-mail" corporativo, instrumento de comunicação

²¹⁶ JORNAL JURID. **Órgão Especial rejeita denúncia contra juíza**. Disponível em: <http://jornal.jurid.com.br/materias/noticias/orgao-especial-rejeita-denuncia-contra-juiza>, Acesso em 10 Jun. 2010.

²¹⁷ JUSBRASIL, Jurisprudências. **TST - Recurso de Revista: RR 613002320005100013 61300-23.2000.5.10.0013**. Disponível em: <http://www.jusbrasil.com.br/jurisprudencia/3487039/recurso-de-revista-rr-613002320005100013-61300-2320005100013-tst>, Acesso em: 13 nov 2011.

²¹⁸ JUSBRASIL, Jurisprudência. **TST - Agravo de instrumento em recurso de revista: airr 1542402420055020055** Disponível em: <http://www.jusbrasil.com.br/jurisprudencia/3157228/agravo-de-instrumento-em-recurso-de-revista-airr-1542-1542-2005-055-02-404-tst/inteiro-teor>, Acesso em 05 nov 2012.

virtual mediante o qual o empregado louva-se de terminal de computador e de provedor da empresa, bem assim do próprio endereço eletrônico que lhe é disponibilizado igualmente pela empresa”²¹⁹.

Complementa o ministro, definindo a natureza jurídica do correio eletrônico: *“Ostenta, pois, natureza jurídica equivalente à de uma ferramenta de trabalho proporcionada pelo empregador ao empregado para a consecução do serviço”*:

PROVA ILÍCITA. -E-MAIL- CORPORATIVO. JUSTA CAUSA. DIVULGAÇÃO DE MATERIAL PORNOGRÁFICO.

1. Os sacrossantos direitos do cidadão à privacidade e ao sigilo de correspondência, constitucionalmente assegurados, concernem à comunicação estritamente pessoal, ainda que virtual (email-particular). Assim, apenas o e-mail pessoal ou particular do empregado, socorrendo-se de provedor próprio, desfruta da proteção constitucional e legal de inviolabilidade.

[...]

4. Se se cuida de email- corporativo, declaradamente destinado somente para assuntos e matérias afetas ao serviço, o que está em jogo, antes de tudo, é o exercício do direito de propriedade do empregador sobre o computador capaz de acessar à INTERNET e sobre o próprio provedor. Insta ter presente também a responsabilidade do empregador, perante terceiros, pelos atos de seus empregados em serviço (Código Civil, art. 932, inc. III), bem como que está em xeque o direito à imagem do empregador, igualmente merecedor de tutela constitucional. Sobretudo, imperativo considerar que o empregado, ao receber uma caixa de email de seu empregador para uso corporativo, mediante ciência prévia de que nele somente podem transitar mensagens profissionais, não tem razoável expectativa de privacidade quanto a esta, como se vem entendendo no Direito Comparado (EUA e Reino Unido).

5. Pode o empregador monitorar e rastrear a atividade do empregado no ambiente de trabalho, em email- corporativo, isto é, checar suas mensagens, tanto do ponto de vista formal quanto sob o ângulo material ou de conteúdo. Não é ilícita a prova assim obtida, visando a demonstrar justa causa para a despedida decorrente do envio de material pornográfico a colega de trabalho. Inexistência de afronta ao art. 5º, incisos X, XII e LVI, da Constituição Federal.

6. Agravo de Instrumento do Reclamante a que se nega provimento.
²²⁰

²¹⁹ JUSBRASIL, Jurisprudência. **TST - Agravo de instrumento em recurso de revista**: airr 1542402420055020055 Disponível em: <<http://www.jusbrasil.com.br/jurisprudencia/3157228/agravo-de-instrumento-em-recurso-de-revista-airr-1542-1542-2005-055-02-404-tst/inteiro-teor>>, Acesso em 05 nov 2012.

²²⁰ Idem. Jurisprudência. **TST - Agravo de instrumento em recurso de revista**: airr 1542402420055020055 Disponível em: <<http://www.jusbrasil.com.br/jurisprudencia/3157228/agravo-de-instrumento-em-recurso-de-revista-airr-1542-1542-2005-055-02-404-tst/inteiro-teor>>, Acesso em 05 nov 2012.

Em outro julgado, no processo sob o nº 1.542/2005-055-02-40.4, o Ministro do TST Ives Gandra Martins Filho, relator do processo, ao se manifestar sobre o acesso pelo empregador à caixa de e-mail corporativo fornecida ao empregado, reitera posicionamento anterior do Tribunal. Também, concebe que existe um distanciamento da tutela constitucional em virtude de que a “concessão, por parte do empregador, de caixa de e-mail a seus empregados em suas dependências tem por finalidade potencializar a agilização e eficiência de suas funções para o alcance do objeto social da empresa”.

1.542/2005-055-02-40.4 - PRELIMINAR DE NULIDADE DO JULGADO POR CERCEAMENTO DE DEFESA. PROVA ILÍCITA. ACESSO PELO EMPREGADOR À CAIXA DE E-MAIL CORPORATIVO FORNECIDA AO EMPREGADO. ÓBICE DA SÚMULA 126 DO TST.

1. Consoante a diretriz da Súmula 126 do TST, é incabível o recurso de revista para reexame de fatos e provas.

2. *In casu*, pretende o Reclamante modificar a decisão vergastada, ao argumento de que a prova acostada aos autos é ilícita, porquanto consubstanciada no acesso à sua conta de e-mail pessoal, quando o Regional, ao enfrentar a questão, entendeu que a prova era lícita, porque se tratava de acesso, pela Reclamada, ao conteúdo do e-mail corporativo fornecido ao Reclamante para o exercício de suas atividades funcionais, do qual se utilizava de forma imprópria, recebendo fotos com conteúdo que estimulava e reforçava comportamentos preconceituosos. Além disso, os e-mails continham conversas fúteis que se traduziam em desperdício de tempo.

3. Com efeito, as alegações obreiras esbarram no óbice do referido verbete sumulado, porquanto pretendem o revolvimento do conjunto fático-probatório dos autos.

4. Por outro lado, ainda que o presente recurso não ultrapasse a barreira do conhecimento, a controvérsia em torno da licitude ou não da *prova acostada pela Reclamada, consubstanciada no acesso à caixa de e-mail corporativo utilizado pelo Reclamante, é matéria que merece algumas considerações.*

5. O artigo 5º, X e XII, da CF garante ao cidadão a inviolabilidade da intimidade, da vida privada, da honra, da imagem das pessoas, bem como o sigilo de suas correspondências, dados e comunicações telegráficas e telefônicas.

6. A concessão, por parte do empregador, de caixa de e-mail a seus empregados em suas dependências tem por finalidade potencializar a agilização e eficiência de suas funções para o alcance do objeto social da empresa, o qual justifica a sua própria existência e deve estar no centro do interesse de todos aqueles que dela fazem parte, inclusive por meio do contrato de trabalho.

7. Dessa forma, como instrumento de alcance desses objetivos, a caixa do e-mail corporativo não se equipara às hipóteses previstas

nos incisos X e XII do artigo 5º da CF, tratando-se, pois, de ferramenta de trabalho que deve ser utilizada com a mesma diligência emprestada a qualquer outra de natureza diversa. Deve o empregado zelar pela sua manutenção, utilizando-a de forma segura e adequada e respeitando os fins para que se destinam. Mesmo porque, como assinante do provedor de acesso à Internet, a empresa é responsável pela sua utilização com observância da lei.

8. Assim, se o empregado eventualmente se utiliza da caixa de e-mail corporativo para assuntos particulares, deve fazê-lo consciente de que o seu acesso pelo empregador não representa violação de suas correspondências pessoais, tampouco violação de sua privacidade ou intimidade, porque se trata de equipamento e tecnologia fornecidos pelo empregador para utilização no trabalho e para alcance das finalidades da empresa.

9. Nessa esteira, **entendo que não se configura o cerceamento de defesa a utilização de prova consubstanciada no acesso à caixa de e-mail fornecido pelo empregador aos seus empregados. [grifos nossos]**

Agravo de instrumento desprovido.

Vistos, relatados e discutidos estes autos de Agravo de Instrumento em Recurso de Revista TST-AIRR 1.542/2005-055-02-40.4, em que é Agravante GUSTAVO FRANCISCO BASTOS e Agravada MBM RECUPERAÇÕES DE ATIVOS FINANCEIROS S/C LTDA.

Dessa forma, o posicionamento é pacífico para compreender que a natureza jurídica do correio eletrônico corporativo, segundo o Tribunal Superior do Trabalho (TST), é de ser instrumento de trabalho.

Ao cotejar a norma do Código Penal e a interpretação da doutrina, mesmo sendo muito discutida a forma da sua aplicação na proteção do correio eletrônico nos termos da Carta Constitucional, verifica-se a sua total inviabilidade em função da falta de previsão legal, executando-se no caso da inclusão do correio eletrônico (e-mail) no rol do artigo 7º da Lei 6.538/78 que dispõe sobre os Serviços Postais da União. Por consequência, seria possível receber a proteção deferida ao sigilo da correspondência e das comunicações telegráficas.

6.0 O DIREITO ESTRANGEIRO E PROJETOS DE LEI.

6.1 Direito Estrangeiro

6.1 1 Estados Unidos da América

A Lei Federal conhecida como Fraud and Related Activity in Connection with, com a finalidade de coibir as fraudes e atividade relacionada em conexão com a Internet, Lei 18 U.S.C. 1030²²¹, instituída desde outubro de 2001, buscou refrear os crimes de furto através de dispositivos informáticos. Essa norma se refere ao crime de furto, previstos nos incisos 1, 2 e 4 do item A:

O inciso I, protege os computadores dos órgãos públicos governamentais norte-americanos, tendo em vista os riscos que uma invasão hacker e coleta de informações destes computadores poderiam significar um risco, comprometendo a segurança nacional. A pena para estas condutas é de até 20 anos e multa, tendo em vista a gravidade desta para a segurança do país.

O inciso II, protege a cópia de informações de computadores de instituições financeiras e de departamentos ou agências não governamentais, e sua pena é de até 10 anos, mais multa.

O inciso IV protege os computadores privados, e condena a até 5 anos de prisão mais multa, se o hacker conseguir, com a invasão, obter qualquer vantagem econômica

Em função da autonomia dos Estados – unidades federativas – norte-americano em matéria penal, muitos Estados têm legislação própria. Destacaremos aqui algumas das normas de alguns Estados americanos que incluem normas penais incriminadoras que buscam tutelar os direitos da personalidade, qual sejam, a privacidade e a propriedade.

No Estado de Kansas foi criado o Kansas Criminal Code @ 21-3755²²², que inclui como propriedade a informação e os dados eletrônicos, especificando que qualquer conduta com o intuito de obter acesso e danificar, modificar, alterar, copiar ou obter posse de um computador, sistema de computador, rede de computador ou

²²¹ UNITED STATES, **Low 18 U.S.C. 1030**, October 24, 2001. Disponível em: <http://www.law.cornell.edu/uscode/text/18/1030>. Acesso em: 10 jan. 2012.

²²² Idem. **Low Code@21-3755**. Disponível em: http://kansasstatutes.lesterama.org/Chapter_21/Article_37/21-3755.html. Acesso em: 10 jan. 2011.

qualquer outra propriedade, como crime. Qualifica como objeto material a informação e os dados de computador, assim, tornam-se passíveis de sofrer lesão.

A conduta está descrita no Kansas Statutes Annotated, no capítulo 21, em seu artigo 37, que define também o crime de dano cometido com o acesso autorizado de a um sistema informático, e, com o dano, modificação ou destruição de dados.

No Estado da Califórnia a legislação segue os mesmos critérios adotados em Kansas e admite como objeto material deste crime os dados de computador, a propriedade e dinheiro, passíveis de serem lesionadas recebendo a proteção que o Estado defere à propriedade e aos bens:

1 - Idaho Code @ 18-2201²²³, em seu título 18, Capítulo 22, define, no artigo 2º a conduta de dano a sistemas informáticas, baseado em três condutas típicas: alterar, danificar ou destruir dados de computadores.

2 - O Código Penal Californiano, em sua seção 502 define a pena, entretanto, pode chegar à multa de US\$ 5.000,00 (cinco milhões de dólares) e o tempo de prisão é de 16 meses. Além disso, caso um menor cometa a infração, deve um de seus pais ou representante legal responder por sua atitude.

No Estado de Wisconsin a Computer Law²²⁴, define de forma similar o crime de dano uma vez que este pode ser produzido também com a alteração ou destruição de dados. A pena, entretanto, chega a 20 anos de prisão, e a multa a US\$ 10.000,00 (dez milhões de dólares)

O Estado da Florida tem a legislação mais rigorosa do mundo para os que usam o computador como instrumento ou como finalidade do seu ato criminoso, servindo de modelo para os demais Estados americanos. Entrou em vigor no ano de 1985, quando os norte-americanos querendo coibir crimes praticados contra os sistemas informáticos ou com o auxílio do computador.

O objetivo primário foi a proteção dos dados e informações, chegando até a fixação pena de prisão perpétua através da norma Florida Computers Crime Act, S.

²²³ UNITED ESTATES. **Low Code@21-3755**, Disponível em: **Erro! A referência de hiperlink não é válida.** <http://legislature.idaho.gov/idstat/Title18/T18CH22SECT18-2201.htm>>. Acesso em: 10 jan. 2010.

²²⁴ Idem **Computer Law - State of Wisconsin Statute**. Disponível em: <http://courses.cs.vt.edu/cs3604/lib/Crime/wisconsin.law.html>. Acesso em: 20 jun 2011.

755084²²⁵ para o indivíduo que viola habitualmente sistemas de proteção de dados de terceiros em 1º grau, causando-lhe prejuízos.

6.1.2 Portugal

A nação portuguesa aprovou na data de 11 de Junho de 1991 a. Lei nº 109/91²²⁶, que define normas sobre os crimes informáticos. Destacamos os tipos penais mínimos e necessários para equilibrar as relações dos homens através dos sistemas informáticos computacionais, os quais podem ser concentrados em apenas seis artigos que tratam dos crimes contra os sistemas computacionais.

O crime de Falsidade informática está definido no Art. 4º:

Quem, com intenção de provocar engano nas relações jurídicas, introduzir, modificar, apagar ou suprimir dados ou programas informáticos ou, por qualquer outra forma, interferir num tratamento informático de dados, quando esses dados ou programas sejam susceptíveis de servirem como meio de prova, de tal modo que a sua visualização produza os mesmos efeitos de um documento falsificado, ou, bem assim, os utilize para os fins descritos, *será punido com pena de prisão até cinco anos ou multa de 120 a 600 dias.*[grifo nosso]

O crime de dano relativo a dados ou programas informáticos definido no artigo 5º:

Quem, sem para tanto estar autorizado, e atuando com intenção de causar prejuízo a outrem ou de obter um benefício ilegítimo para si ou para terceiros, apagar, destruir, no todo ou em parte, danificar, suprimir ou tornar não utilizáveis dados ou programas informáticos alheios ou, por qualquer forma, lhes afectar a capacidade de uso será punido com a pena de prisão até três anos ou pena de multa. A tentativa é punível. Se o dano causado for de valor elevado, a pena será a de prisão até *5 anos ou de multa até 600 dias ou 1 a 10 anos* [grifo nosso].

²²⁵ Assembléia Legislativa do Estado de São Paulo. **Informativo DDI 45**. p.8. Disponível em: http://www.al.sp.gov.br/StaticFile/documentacao/manual_proclis_2.pdf. Acesso em: 12 mar. 2012.

²²⁶ PORTUGAL. **Lei n.º 109/91, 13 de agosto de 1991. Lei da Criminalidade Informática**. Disponível em: https://ciist.ist.utl.pt/docs_da/Lei_109-91_Lei_da_Criminalidade_Informatica.pdf. Acesso 15 jan. 2011.

O crime de Sabotagem informática está definido no Art. 6º:

Quem introduzir, alterar, apagar ou suprimir dados ou programas informáticos ou, por qualquer outra forma, interferir em sistema informático, actuando com intenção de entrar ou perturbar o funcionamento de um sistema informático ou de comunicação de dados à distância, será punido com pena de prisão até 5 anos ou com pena de multa até 600 dias, se o dano for de valor elevado de 1 a 10 anos. [grifo nosso]

O crime de Acesso ilegítimo está definido no Art. 7º:

Quem, não estando para tanto autorizado e com a intenção de alcançar, para si ou para outrem, um benefício ou vantagem ilegítimos, de qualquer modo aceder a um sistema ou rede informáticos será punido com pena de prisão até 1 ano ou com pena de multa até 120 dias ou até 3 anos se o acesso for conseguido através de violação de regras de segurança até 5 anos de prisão.

O crime de Interceptação ilegítima está definido artigo 8º:

Quem, sem para tanto estar autorizado, e através de meios técnicos, interceptar comunicações que se processam no interior de um sistema ou rede informáticos, a eles destinadas ou deles provenientes, será punido com pena de prisão até três anos ou com pena de multa. A tentativa é punível.

O crime de Reprodução ilegítima de programa protegido definido no Art. 9º:

Quem, não estando para tanto autorizado, reproduzir, divulgar ou comunicar ao público um programa informático protegido por lei será punido com pena de prisão até três anos ou com pena de multa. .
OBS: Em todos os artigos acima descritos a tentativa é punível

6.1.3 Paraguai

Um dos menores países da América Latina que compõe a denominada tríplice fronteira²²⁷, o Paraguai, em seu código Penal de 1997²²⁸ inclui quatro artigos

²²⁷ **A tríplice fronteira ou tripla fronteira** é o lugar comum que une os limites territoriais e políticos de três países diferentes, no caso em pauta é formado pelos países: Brasil, Argentina e Paraguai.

que conseguem albergar inúmeras condutas aéticas prejudiciais à sociedade como um todo, transformando-as em condutas delituosas que tem o computador como instrumento ou como fim do ato penalmente ilícito que afronta os direitos da personalidade.

Proteção aos dados computacionais.

Está tutelado pelo artigo 174 quando define no § 1º que “lesando o direito de disposição de outro sobre dados os apagasse, suprimisse, inutilizasse ou mudasse, será castigado com pena privativa de liberdade de até dois anos ou com multa”, também prevê a punição por tentativa no § 2º. Já o § 3º faz a definição de dados computacionais ao aduzir que “*se entenderão só aqueles que sejam armazenados ou se transmitam eletrônica ou magneticamente, ou em outra forma não imediatamente visível*”.

Proteção contra sabotagem de computadores.

A sabotagem de computadores integra os delitos contra os sistemas informáticos definindo a conduta no artigo 174 como “*toda pessoa que atrapalha um processamento de dados de importância em estabelecimento alheio ou em uma entidade da administração pública mediante um ato, será punido com privação de liberdade até dois anos*”. Na atualidade, em plena época do domínio da Tecnologia da Informação o conhecimento é o maior bem que a humanidade possui e dessa forma, esse artigo busca proteger a informação como um bem, razão pela qual merece ser juridicamente protegido.

As operações fraudulentas são coibidas pelos artigos 187 e 188 cujo primeiro artigo busca punir o simples ato da fraude de forma semelhante ao artigo 171 *estelionato* do nosso CP, senão vejamos:

§ 1º O que com a intenção de obter para si ou para um terceiro um benefício patrimonial indevido, e mediante declaração falsa sobre um fato, produzisse em outro um erro que lhe induzisse a dispor de tudo ou parte de seu patrimônio ou o de um terceiro a quem represente, e

²²⁸ PARAGUAY. **Ley nº 1.160/97, Código Penal.** Asunción. 1997. Disponível em: http://www.leyes.com.py/todas_disposiciones/1997/leyes/ley_1160_97.htm. Acesso em 10 jan. 2009.

com isso causasse um prejuízo patrimonial para si mesmo ou para este, será castigado com pena privativa de liberdade de até cinco anos ou com multa.

Nesse tipo penal o efeito não precisa ser concretizado, o agente responderá pela simples tentativa e o seu patrimônio responderá por todo o prejuízo causado, além da pena privativa de liberdade de até cinco anos ou multa. O Art. 188 enfoca as operações fraudulentas e visa completar as possíveis lacunas que ficam em aberto quando o agente com a intenção de obter benefício próprio ou para terceiros, altera o processamento de dados com programação falsa, utiliza dados falsos, dados indevidos ou qualquer outro meio que altere o processamento e venha a afetar o patrimônio de outro, responderá com pena de privativa de liberdade de até cinco anos ou multa, vejamos:

1º O que com a intenção de obter para si ou para outro um benefício patrimonial indevido, influísse sobre o resultado de um processamento de dados mediante: 1. programação falsa; 2. utilização de dados falsos ou incompletos; 3. utilização indevida de dados; ou 4. outras influências indevidas sobre o processamento, e com isso, prejudicasse o patrimônio de outro, será castigado com pena privativa de liberdade de até cinco anos ou com multa. 2º Nestes casos, se aplicará também o disposto no artigo 187, incisos 2º ao 4º.

6.1.4 Argentina

Na Argentina a Lei 26.388²²⁹ promulgada em 24 de junho de 2008, alterou o Código Penal criando tipos penais que buscam coibir os delitos humanos contra os sistemas de computação ou aqueles que utilizem os sistemas computacionais como meio, trazendo grandes modificações na tutela penal dos direitos da personalidade para a qual destacaremos alguns, como a proteção da imagem, publicidade e patrimônio.

²²⁹ ARGENTINA. **CODIGO PENAL - Ley 26.388 - Modificación.** Disponível em: http://www.oas.org/juridico/PDFs/arg_ley26388.pdf. Acesso em: 12 dez 2013.

Proteção da Imagem dos menores de dezoito anos ante a sexualidade.

A tutela vem no artigo 128: Será reprimido com prisão de 6 (seis) meses a 4 (quatro) anos o que produzir, financiar, oferecer, comerciar, publicar, facilitar, divulgar ou distribuir, por qualquer meio, toda representação de um menor de dezoito (18) anos dedicado a atividades sexuais explícitas ou toda representação de suas partes genitais com fins predominantemente sexuais, ao igual que o que organizar espetáculos ao vivo de representações sexuais explícitas em que participarem ditos menores.

Proteção da privacidade

Acesso indevido à comunicação eletrônica está tutelado no artigo 153. Será reprimido com prisão de 15 (quinze) dias a 6 (seis) meses o que abrir ou acessar indevidamente a uma comunicação eletrônica, uma carta, um caderno fechado, um despacho telegráfico, telefônico ou de outra natureza, que não lhe esteja dirigido; ou se apoderar indevidamente de uma comunicação eletrônica, uma carta, um caderno, um despacho ou outro papel privado, ainda que não esteja fechado; ou indevidamente suprimir ou desviar de seu destino uma correspondência ou uma comunicação eletrônica que não lhe esteja dirigida. Na mesma pena incorrerá o que indevidamente interceptar ou captar comunicações eletrônicas ou telecomunicações provenientes de qualquer sistema de caráter privado ou de acesso restringido

A publicação do conteúdo acessado indevidamente, a pena será de prisão de 1 (um) mês a 1 (um) ano, se o autor comunicar a outro ou publicar o conteúdo da carta, escrito, despacho ou comunicação eletrônica. Se o fato o cometer um servidor público que abusar de suas funções, sofrerá ademais, inabilitação especial pelo dobro do tempo da condenação.

Acesso indevido ou acesso além da restrição está definido no artigo 153. Será reprimido com prisão de 15 (quinze) dias a 6 (seis) meses se não resultar em delito mais severamente penado, o que acessar intencionalmente por qualquer meio, sem a devida autorização ou excedendo a que possua, a um sistema ou dado informático de acesso restringido. A pena será de 1 (um) mês a 1 (um) ano de prisão quando o acesso for em prejuízo de um sistema ou dado informático de um

organismo público estatal ou de um provedor de serviços públicos ou de serviços financeiros.

No artigo 155 encontramos que será reprimido com multa de \$1.500,00 (mil quinhentos) a \$ 100.000 (cem mil) pesos o que achando-se em posse de uma correspondência, comunicação eletrônica, caderno fechado, despacho telegráfico, telefônico ou de outra natureza, não destinados à publicidade, fazer publicar indevidamente, se o fato causar ou puder causar prejuízos a terceiros. Está isento de responsabilidade penal o que tiver feito com o propósito inequívoco de proteger um interesse público.

A Divulgação de Documentos ou Dados pelo servidor público está definida no artigo 157 de forma que será reprimido com prisão de um (1) mês a dois (2) anos e inabilitação especial de um (1) a quatro (4) anos, o servidor público que revelar fatos, atuações, documentos ou dados, que por lei devem ser secretos.

Também será reprimido com a pena de prisão de 1 (um) mês a 2 (dois) anos, o que: 1. Intencionalmente e ilegitimamente, ou violando sistemas de confidencialidade e segurança de dados, acessar, de qualquer forma, a um banco de dados pessoais; 2. Ilegitimamente proporcionar ou revelar a outrem informação registrada num arquivo ou num banco de dados pessoais cujo segredo estiver obrigado a preservar por disposição da lei. 3. Ilegitimamente inserir ou fazer inserir dados num arquivo de dados pessoais. Quando o autor for servidor público sofrerá, ademais, pena de inabilitação especial de um (1) a quatro (4) anos.

Delitos contra a propriedade

Delito de defraudação definido no artigo 173 inciso 16: “O que defraudar a outro mediante qualquer técnica de manipulação informática que altere o normal funcionamento de um sistema informático ou a transmissão de dados”.

No artigo 183 do Código Penal, incorre no *delito de dano* “Na mesma pena incorrerá o que alterar, destruir ou inutilizar dados, documentos, programas ou sistemas informáticos; ou vender, distribuir, fazer circular ou introduzir num sistema informático, qualquer programa destinado a causar danos”.

O artigo 184 do Código Penal vem como qualificador do artigo antecedente, elevando “[...] a pena de 3 (três) meses a 4 (quatro) anos de prisão se mediar qualquer das circunstâncias seguintes:

inciso 5: Executá-lo em arquivos, registros, bibliotecas, museus ou em pontes, caminhos, passeios ou outros bens de uso público; ou em tumbas, signos comemorativos, monumentos, estátuas, quadros ou outros objetos de arte colocados em edifícios ou lugares públicos; ou em dados, documentos, programas ou sistemas informáticos públicos;

Inciso 6: Executá-lo em sistemas informáticos destinados à prestação de serviços de saúde, de comunicações, de provisão ou transporte de energia, de meios de transporte ou outro serviço público.

Os Delitos contra as comunicações

Está tutelado pelo artigo 197 e *“Será reprimido com prisão de 6 (seis) meses a 2 (dois) anos, o que interromper ou entorpecer a comunicação telegráfica, telefônica ou de outra natureza ou resistir violentamente o restabelecimento da comunicação interrompida”*.

Os Delitos contra a administração de justiça

Está tutelado pelo artigo 255 e será reprimido com prisão de 1 (um) mês a 4 (quatro) anos aquele que subtrair, alterar, ocultar, destruir ou inutilizar em tudo ou em parte objetos destinados a servir de prova ante a autoridade competente, registros ou documentos confiados à custódia de um servidor público ou de outra pessoa no interesse do serviço público.

Se o autor for o mesmo depositário, sofrerá ademais inabilitação especial por duplo tempo. Se o fato for cometido por imprudência ou negligência do depositário, este será reprimido com multa de \$750,00 (setecentos cinquenta) a \$2.500,00 (doze mil quinhentos) pesos.

6.1.5 Inglaterra

Encontra-se em vigência a Lei Computer Misuse Act 1990 com finalidade de prever e garantir a integridade dos equipamentos e sistemas de informática contra acesso não autorizado ou alteração e para fins ligados. Foi promulgada em 29 de junho de 1990 pela Excelentíssima Majestade Rainha da Inglaterra após a aprovação do Parlamento, formado pelos Lordes espirituais e temporais, e *Commons*, reunidos²³⁰.

Acesso não autorizado a material informático.

O tipo penal está definido no artigo 1º, caracterizando a conduta delituosa quando: a) quem usa o computador para executar qualquer função com a intenção de garantir o acesso a qualquer programa ou dados contidos em qualquer computador, ou para permitir que qualquer acesso seja garantido; b) o acesso pretendido ou que se pretenda garantir seja protegido e não autorizado; c) o usuário tem consciência no momento da operação o que está sendo realizado ou que virá realizar. A ação do agente pode ser dirigida a) incluindo qualquer programa ou dados; b) a um programa ou dados de qualquer tipo, inclusive ou c) um programa ou dados realizada em todos os proprietários de computador.

Tendo como punição: a) na condenação sumária na Inglaterra e no País de Gales, com pena de prisão não superior a 12 meses ou a uma multa não superior ao máximo legal ou a ambos; b) na condenação sumária, na Escócia, com pena de prisão não superior a seis meses ou a uma multa não superior ao máximo legal ou a ambos; c) em caso de condenação na acusação, com pena de prisão não superior a dois anos ou a uma multa ou a ambos.

Acesso não autorizado com a intenção de praticar ou facilitar a prática de delitos.

²³⁰ INGLATERRA. **Computer Misuse Act 1990**: 1990 CHAPTER 18 An Act to make provision for securing computer material against unauthorised access or modification; and for connected purposes. Disponível em: <http://www.legislation.gov.uk/ukpga/1990/18/contents>. Acesso em 12 dez de 2012.

A conduta está tipificada no artigo 2º, caracterizando a conduta delituosa quando o agente comete o *delito de acesso não autorizado* com intenção de: a) cometer um delito a que se aplica esta seção, ou b) facilitar a prática de uma infração por ela ou qualquer outra pessoa.

A pena fixada é: a) na condenação sumária na Inglaterra e no País de Gales, com pena de prisão não superior a 12 meses ou a uma multa não superior ao máximo legal ou a ambos; b) na condenação sumária, na Escócia, com pena de prisão não superior a seis meses ou a uma multa não superior ao máximo legal ou a ambos; c) em caso de condenação na acusação, com pena de prisão não superior a cinco anos ou a uma multa ou a ambos.

Sabotagem de computador.

A conduta esta definida no artigo 3º, como ações não autorizadas com a intenção de prejudicar, ou com imprudência com o mesmo objetivo, de prejudicar determinada operação de computador. A culpa do agente está caracterizada se: a) faz qualquer ato em relação a um computador não autorizado; b) no momento do ato, a agente sabe que não é autorizado. Sendo a pessoa que faz o pretende pelo seu ato: a) afetar o funcionamento de qualquer computador; b) impedir ou dificultar o acesso a qualquer programa ou dados, realizado em qualquer computador; c) afetar o funcionamento de qualquer programa ou a fiabilidade de quaisquer dados.

A pena imposta na condenação: a) na condenação sumária na Inglaterra e no País de Gales, com pena de prisão não superior a 12 meses ou a uma multa não superior ao máximo legal ou a ambos; b) na condenação sumária, na Escócia, com pena de prisão não superior a seis meses ou a uma multa não superior ao máximo legal ou a ambos; c) em caso de condenação na acusação, com pena de prisão não superior a 10 anos ou a uma multa ou a ambos.

Possuir dispositivo para o acesso não autorizado

Definido ano artigo 3ºA, como uma pessoa é culpada do delito se faz se adaptar ou fornecer qualquer meio ou dispositivo para ser usado para cometer, ou para auxiliar na prática de uma infração nos termos dos artigos 1º ou 3º. O agente

será penalizado: a) na condenação sumária na Inglaterra e no País de Gales, com pena de prisão não superior a 12 meses ou a uma multa não superior ao máximo legal ou a ambos; b) na condenação sumária, na Escócia, com pena de prisão não superior a seis meses ou a uma multa não superior ao máximo legal ou a ambos; c) em caso de condenação na acusação, com pena de prisão não superior a dois anos ou a uma multa ou a ambos.

6.1.6 Espanha

Lei Orgânica de nº 5/1992

O Grande destaque na legislação espanhola está na Lei Orgânica de nº 5/1992²³¹, de 29 de outubro de 1992, que surge para definir critérios da regulação do tratamento automático de dados de carácter pessoal, com a máxima demonstração da proteção à privacidade.

Na busca de assegurar a inviolabilidade dos direito da personalidade, no foco à privacidade, diante da insegurança perante aos sistemas informáticos envolvendo a Rede Mundial de Computadores é que foi o motivador da referida Lei a qual destaca-se, nas palavras de sua Majestade Juan Carlos rei da Espanha:

“[...]Constituição espanhola, em seu artigo 18.4, convoca ao legislador a limitar o uso da informática para garantir a honra, a intimidade pessoal e familiar dos cidadãos e o legítimo exercício de seus direitos. A ainda recente aprovação Constituição e, por tanto seu moderno carácter, permitiu-lhe expressamente a articulação de garantias contra a possível utilização imprópria desse fenômeno da contemporaneidade que é a informática.”²³²

Destacaremos alguns artigos em função da sua importância como medida protetora, por ser uma Lei Federal com a finalidade única de “*garantir a honra, a*

²³¹ ESPANHA. **Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal.** Disponível em: <http://civil.udg.es/normacivil/estatal/persona/pf/Lo5-92.htm>. Acesso em: 12 dez 2012..

²³² Texto registrado no item I dos motivos justificadores para Rei Juan Carlos I sancionar a Lei Orgânica 5/1992. ESPANHA. **Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal.** Disponível em: <http://civil.udg.es/normacivil/estatal/persona/pf/Lo5-92.htm>. Acesso em: 12 dez 2012..

intimidade pessoal e familiar dos cidadãos e o legítimo exercício de seus direitos”

233

Qualidade dos dados está definido com a redação do artigo 4º, inciso 1:

Somente se poderá recolher dados de caráter pessoal para seu tratamento automatizado, bem como submetê-los a dito tratamento, quando tais dados sejam adequados, pertinentes e não excessivos em relação com o âmbito e as finalidades legítimas para as que se tenham obtido²³⁴.

O *Direito de informação* está definido no artigo 5º, sob a denominação do *caput* “na recolhida de dados”, inciso 1: a) “*As pessoas aos quais se solicitem dados pessoais deverão ser previamente informados de modo expresso, preciso e inequívoco*”; b) Do caráter obrigatório ou facultativo de sua resposta às perguntas que lhes sejam propostas.; c) Das consequências da obtenção dos dados ou da negativa a fornecê-los; d) Da possibilidade de exercitar os direitos de acesso, retificação e cancelamento; e) Da identidade e direção do responsável do arquivo.

Do *consentimento ao fornecimento dos dados* está definido no artigo 6º, sob a denominação do *caput* “*Do consentimento do afetado*”, inciso 1: “*O tratamento automático de dados de caráter pessoal requer o consentimento da pessoa atingida, salvo se a lei disponha de outra coisa*”.

Os *dados especialmente protegidos* estão definidos no artigo 7º, inciso I, assegurando que pessoa alguma será obrigada a declarar sobre sua ideologia, religião ou crenças.

A *segurança dos dados* está definida no artigo 9º, definindo que o responsável pelo arquivo de dados adotará as medidas de índole técnica e organizacionais necessárias que garantam a segurança dos dados de caráter pessoal, evitando a alteração, perda e o acesso não autorizado.

²³³ Texto registrado no item I dos motivos justificadores para Rei Juan Carlos I sancionar a Lei Orgânica 5/1992. ESPANHA. **Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal**. Disponível em: <http://civil.udg.es/normacivil/estatal/persona/pf/Lo5-92.htm>. Acesso em: 12 dez 2012..

²³⁴ ESPANHA. **Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal**. Disponível em: <http://civil.udg.es/normacivil/estatal/persona/pf/Lo5-92.htm>. Acesso em: 12 dez 2012..

O *dever de segredo sobre os dados pessoais* está definido no artigo 10, que assegura aos dados automatizados e a quem intervenha em qualquer fase do tratamento dos dados de carácter pessoal, estando obrigados ao segredo profissional, ao respeito dos mesmos e ao dever de guardá-los.

Lei Orgânica 10/1995²³⁵, de 23 de novembro de 1995 - Código Penal.

A *proteção penal à inviolabilidade do Correio eletrónico* está definida no artigo 197, inciso I, que assegura uma pena de prisão de um a quatro anos e multa de doze a vinte e quatro meses, como podemos verificar mais nitidamente a seguir:

Quem, para descobrir os segredos ou vulnerar a intimidade de outro, sem seu consentimento, ***apodere-se de seus papéis, cartas, mensagens de correio eletrónico*** ou quaisquer outros documentos ou efeitos pessoais ou intercepte suas telecomunicações ou utilize artifícios técnicos de escuta, transmissão, gravação ou reprodução do som ou da imagem, ou de qualquer outro sinal de comunicação, será castigado com as penas de prisão de um a quatro anos e multa de doze a vinte e quatro meses. [grifo nosso]

A *Proteção aos dados e Segredo* está definida no inciso II do artigo 197, que atribui a mesma pena aplicada no inciso I, com a seguinte redação:

ao que, sem estar autorizado, apodere-se, utilize ou modifique, em prejuízo de terceiro, dados reservados de carácter pessoal ou familiar de outro que se achem registrados em ficheiros ou suportes informáticos, eletrónicos ou telemáticos, ou em qualquer outro tipo de arquivo ou registro público ou privado.

Também no artigo 278 está definida a pena de dois a quatro anos de prisão para àqueles que se apoderem escritos ou eletrónicos – dados - suporte informáticos que permitam acesso aos segredos da empresa.

Para complementar a proteção aos dados, o inciso VI define a pena de dois a cinco anos de prisão para àqueles que difundem, revelem ou cedam para terceiros

²³⁵ ESPANHA. **Ley Orgánica 10/1995, de 23 de noviembre de 1995, del Código Penal.** Disponível em: <http://www.juecesdemocracia.es/legislacionvigente/penal/general/codigopenal.pdf>. Acesso em 12 dez 2012.

os dados descobertos ou as imagens captadas. Existindo ainda a qualificadora no inciso VII, no caso da pessoa afetada ser menor idade ou se envolver questões pertinentes a ideologia, religião, crenças, saúde, origem racial ou vida sexual, aumentando a pena em 50%.

O *Estelionato* está definido no artigo 248 a 250 e de forma clara é mencionada a utilização de sistemas informáticos / internet como meio para a consecução do crime, incluindo a todos aqueles que se envolveram, facilitaram ou desenvolveram softwares para tal fim, com pena de prisão de um a oito anos.

6.2 Futuras Condutas a serem tipificadas.

Alguns comportamentos não podem mais ser aceitos ou tolerados, principalmente as condutas compatíveis com os delitos próprios, delitos estes praticados por intermédio da informática ou dos computadores com objetivo de gerar um dano ao próprio ambiente informatizado.

Verifica-se nesse estudo que a sabotagem parcial em sistemas informatizados ainda não está tipificada de forma adequada, e como foi estudado, as consequências poderão ser tão desastrosas quanto a paralisação total do sistema.

Como também, verifica-se que mesmo os *dados computacionais* tem uma proteção relativa, proteção essa condicionada ao rompimento da segurança – senhas – pelo agente infrator, tornando-se crime acessório.

O desenvolvimento de softwares nocivos aos sistemas informáticos como, por exemplo: Os *vírus* e *trojans*, que tanto afetam os dados computacionais e aos sistemas informatizados em si, penalizados de com no máximo 1 (um) ano e multa, independente do malefício causado, tem uma pena muito branda, tornando-se incipiente e ineficaz.

Esses são os que têm mais urgência na busca de remédio jurídico, pois os sistemas informáticos não se adaptam às figuras penais existentes na nossa legislação, sejam as que constituem crimes de informática como *crimes próprios*, sejam as que se constituem como crimes da legislação comum ou especial

praticados por intermédio da informática ou dos computadores como crimes impróprios, como é o caso do delito de dano, interceptação e-mail, criação de software com objetivos prejudiciais à tecnologia da informação e outros, cujos aspectos pertinentes ao assunto já foram analisados nessa pesquisa com as suas conclusões e ponderações.

A proteção do e-mail com a mesma conotação da Carta Máxima deferida à correspondência convencional é mais que necessária em virtude que em função da evolução da tecnologia as correspondências nos moldes convencionais – físicos – estão sendo substituídos pela comunicação *virtual*.

6.3 Anteprojetos e Projetos de Lei

Atualmente existe diversos projetos de Lei que movimentam-se pelas Câmaras de Constituição e Justiça sendo estudadas que buscam tutelar a proteção dos direitos da personalidade no ambiente telemático, quais destacaremos:

1. O Projeto de Lei 2793/11 de autoria do deputado Paulo Teixeira, Dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências.
2. Anteprojeto de Lei da Ordem dos Advogados do Brasil - Seção São Paulo Dispõe sobre o comércio eletrônico, a validade jurídica do documento eletrônico e a assinatura digital, e dá outras providências.
3. Projeto de Lei nº 1.589, de 1999 - O Projeto de Lei é de autoria do Deputado Luciano Pizzatto e outros que dispõe sobre o comércio eletrônico, a validade jurídica do documento eletrônico e a assinatura digital, e dá outras providências.
4. Projeto de lei nº 3.016, de 2000 - O Projeto de Lei do Deputado Antônio Carlos Pannunzio dispõe sobre a conduta e responsabilidade dos Provedores de Acesso.
5. Projeto de lei nº 84, de 1999 - Dispõe sobre os crimes cometidos na área de informática, suas penalidades e outras providências.
6. Projeto de Lei Nº 1713 - Dispõe sobre os crimes de informática - Deputado Décio Braga.

7. Substituto ao Projeto de Lei nº 84, de 1999 - 7. Projeto de Lei Nº 1.483, de 1999 (Apensado Projeto de Lei nº 1.589, DE 1999) e Parecer Institui a fatura eletrônica e a assinatura digital nas transações de comércio eletrônico
8. Projeto de Lei do Senado 672/99 - dispõe sobre a regulamentação do comércio eletrônico em todo o território nacional, aplica-se a qualquer tipo de informação na forma de mensagem de dados usada no contexto de atividades comerciais.
9. Parecer nº, de 2000 - Da Comissão de Constituição, Justiça e Cidadania - CCJ, em caráter terminativo, sobre o Projeto de Lei do Senado nº 672, de 1999, que "dispõe sobre o comércio eletrônico."
10. PROJETO DE LEI Nº 3891, DE 2000- (Do Sr. Júlio Semeghini) - Dispõe sobre o registro de usuários pelos provedores de serviços de acesso a redes de computadores, inclusive à Internet.
11. Projeto de Lei nº 3.360, de 2000 - Dispõe sobre a privacidade de dados e a relação entre usuários, provedores e portais em redes eletrônicas.
12. Projeto de Lei nº 2.358, de 2000 - Altera a Lei nº 9.504, de 30 de setembro de 1997, dispondo sobre a propaganda eleitoral por meio de Serviços de Valor Adicionado, inclusive Internet, e dá outras providências.
13. Projeto de Lei nº 4.906, de 2001 - Projeto de Lei do Deputado Júlio Semeghini que dispõe sobre comércio eletrônico.
14. Projeto de Lei nº 4.906 de 2001 sobre comércio eletrônico aprovado pela Comissão Especial da Câmara dos Deputados
15. Projeto de Lei Complementar Nº 208, de 2001 - Inclui item na Lista de Serviços a que se refere o art. 1º da Lei Complementar nº 56, de 15 de dezembro de 1987 (provimento de acesso à Internet)
16. Projeto de Lei Complementar Nº 209, de 2001 - Dá nova redação ao item 24 da Lista de Serviços a que se refere o art. 1º da Lei Complementar nº 56, de 15 de dezembro de 1987.
17. Projeto de Lei nº 6.210, de 2002 - Limita o envio de mensagem eletrônica não solicitada ("spam"), por meio da Internet.

18. Projeto de Lei nº 268, de 1999 - Dispõe sobre a estruturação e o uso de banco de dados sobre a pessoa e disciplina o rito processual de habeas data.
19. Projeto de Lei nº 5.165 de 2001 (dispõe sobre crimes na Internet - criança e adolescente) Modifica a Lei nº 8069, de 13 de julho de 1990, que estabelece o Estatuto da Criança e do Adolescente, e dá outras providências.
20. Projeto de Lei nº 1.806-A, de 1999 - Altera dispositivo do Código Penal para incluir no crime de furto o acesso aos serviços de comunicação e acesso aos sistemas de armazenamento, manipulação ou transferência de dados eletrônicos; tendo parecer da Comissão de Constituição e Justiça e de Redação, pela constitucional idade, juridicidade, técnica legislativa e, no mérito, pela rejeição (Dep. José Roberto Batochio)

6.4 O PROJETO DE LEI N.º 84/99

Breve comentário

Entre os vários Projetos de Lei acima mencionados, destacaremos o Projeto de Lei nº 84/99 o qual representa a iniciativa mais completa que dispõe sobre os crimes cometidos na área de informática, suas penalidades e dá outras providências. Apresenta uma pauta muito extensa porque insere o que há de mais atual no panorama internacional. A sua elaboração é o resultado da colaboração de inúmeros juristas especializados de várias unidades federativas.

O aspecto positivo é o de que tenderá a se fundir com outros projetos lei que versam sobre o mesmo assunto, em tese, crimes informáticos. Entretanto a morosidade na aprovação das leis em nosso País representa um grande entrave. Esse anteprojeto iniciou o processo da tramitação nos órgãos competentes em 1999, completando no ano de 2013, 14 (quatorze) longuíssimos anos que a sociedade espera por parte do legislativo leis melhores, atuais e que atendam o anseio da sociedade. Leis que abracem com maior profundidade a dinâmica de um

mundo globalizado, que seja capaz de gerar uma redução das distorções das relações dos homens.

O Capítulo I e II

- Define regras gerais de funcionamento e os princípios que norteiam a prestação de serviços da rede de computadores e proteção à sociedade, respeitados os critérios de garantia dos direitos individuais e coletivos e de privacidade e segurança de pessoas físicas e jurídicas.

Seção I

- Define as normas incriminadoras a quem gerar dano a dado ou programa de computador, garante a privacidade dos dados e sua inviolabilidade.

Seção II

- Trata do acesso indevido ou não autorizado, como invasão, protege os sistemas computacionais como um todo, incluindo software e hardware.

Seção III

- Protege os mecanismos de acesso, como senhas, programa de dados e o seu uso indevido.

Seção IV

- Busca proteger os dados e códigos computacionais da obtenção indevida ou não autorizada de dados ou instrução de computador. Protege o próprio software.

Seção V,

- Trata da violação de segredo armazenado em computador ou qualquer outro meio, seja magnético, de natureza magnética, óptica ou similar.

Seção VI,

- Busca combater os programadores nocivos, criadores de “software do mal”, como vírus, Trojan, vermes e outros. “criação, desenvolvimento ou inserção em computador de dados ou programa de computador com fins nocivos”.

Seção VII,

- Protege o usuário dos sítios pornográficos sem a prévia e devida identificação e veiculação de pornografia.

CONCLUSÃO

Existe um paralelo entre o desenvolvimento das tecnologias computacionais com ênfase na Rede Mundial de Computadores - como expressão máxima da telemática - e o crescimento dos crimes que as utilizam como meio da sua consecução. Em contrapartida, surge a necessidade de ruptura da norma legal para criar novos tipos penalmente condenáveis, tipos esses que devem surgir como resultado do anseio de uma sociedade que não concebe, não aceita, e tampouco suporta ver os seus direitos serem preteridos para aqueles que os desrespeitam.

Fala-se dos elementos básicos que compõem a Dignidade da Pessoa Humana tornando um ato lícito penal, porém aético, em ilícito penal condenável pela antijuridicidade e com dupla missão: a primeira, desestimular a prática comportamental daqueles que acham que a Internet, o mundo cibernético seja um espaço desprovido de regra, em que seja possível prevenir a expressão de comportamentos delituosos, em função da existência de norma penal; a segunda, punir àqueles que venham a desrespeitar a norma objetiva, servindo de exemplo aos demais, pois já estarão cientes das consequências da similitude comportamental.

A partir dessa necessidade, decidiu-se iniciar o trabalho dissertativo despertando para o estudo do mundo cibernético que de virtual só possui a denominação, portadora de algumas normas incriminadoras, regras de comportamento, mas que precisa melhorar o seu processo organizacional, definindo uma ordenação jurídica mais condizente aos tempos globalizados, donde o *jus perseguendi* esteja em consórcio com o *jus puniendi*.

O Estado não pode permitir existência de comportamentos de certos indivíduos que utilizam a informática para a prática de condutas danosas à sociedade, sem que não os puna. Na ausência de uma norma bloqueadora de tais atos, cabe ao Estado, em tempo hábil, tomar medidas necessárias para a sua implementação.

Como esse trabalho buscou-se revelar com maior clareza o desenvolvimento da prática delituosa na Rede Mundial de Computadores – Internet – que afetam direitos da personalidade, com ênfase à privacidade, através do entendimento da importância do seu processo histórico e a sua composição através de alguns elementos.

No decorrer do desenvolvimento deste trabalho ficou muito fácil de perceber o paralelismo do crescimento das tecnológicas computacionais com ênfase na Internet e a utilização desta pelo homem a fim de locupletar-se, realizar desmandos, atingir a honra e imagem e afetar o patrimônio.

O que foi muito desagradável é evidenciar nossa pobreza legislativa. No que tange o tema, mesmo comparando com outros Estados menores da América Latina e sem a magnitude da Nação Brasileira – com aspecto continental – somos suplantados.

Após esses destaques, observamos as normas que se contrapõe aos tipos penais que tenham como instrumento ou meio da consecução o computador e a Internet que buscam constranger os direitos da personalidade há tutela penal através das normas já tipificadas no Código Penal e legislação extravagante.

Buscamos compreender os problemas jurídicos informáticos de forma geral, e a conceituação dos delitos da informática os quais são aqueles em que o

agente se utiliza dos recursos informáticos como instrumento meio ou fim da consecução do delito.

Procuramos apresentar sugestões de cunho legislativo que de forma clara e imediata sanaria boa parte dos problemas que agora enfrentamos.

Procuramos compreender qual o processo que os agentes delituosos agem, quais as tecnologias e ferramentas por eles são abordadas, e enfatizar o porquê da necessidade de novos tipos penais que albergue os direitos da personalidade contrapondo-se aos delitos na Rede Mundial de Computadores.

E próximo à conclusão, destacamos os delitos informáticos, tipos de comportamentos definidos como aéticos, que embora afronta a sociedade como um todo, com prejuízos claros e mensuráveis e que o nosso ordenamento jurídico não tutela. Em seguida, uma descrição do Anteprojeto e Projetos de Lei em processo de tramitação nos setores competentes, com destaque e um breve comentário sobre o Projeto de Lei nº 84/99, que caso seja aprovada sem grandes alterações em seus artigos, ter-se-á instrumentos para combater de forma mais ampla e efetiva o *ciberterrorismo* e os delinquentes cibernéticos que tanto afetam a privacidade, a propriedade imaterial, colocando-nos, assim, em paridade com as nações desenvolvidas.

REFERÊNCIAS

AIETA Vânia Siciliano. **A violação da intimidade no ambiente de trabalho e o monitoramento eletrônico dos empregados**. São Paulo: RT, Revista de direito constitucional e internacional | vol. 55 | abr / 2006

ALLPORT, Gordon Willard. **Personalidade: Padrões e desenvolvimento**. Trd. Dante Moreira Leite, 4ª reimp., São Paulo, EPU, 1973.

ANDRADE. Rebeca Silva, ANDRADE. Roberta D'Ángeles Silva, **Breves Comentários sobre a Lei nº 12.737**. Instituto Universitário Paulista. Publicações. Disponível em: http://www.iunip.com.br/portal/publicacoes/breves_comentarios_lei_12-737.pdf. Acesso em: 12 dez 2012.

ARAÚJO, José Henrique Mouta. **Ações judiciais em defesa dos direitos fundamentais**: em busca de solução para casos concretos. In: DIAS, Jean Carlos; KLAUTAU FILHO, Paulo. (Coord.) Direitos fundamentais: teoria do direito e sustentabilidade. Rio de

ARDIZZONE, Salvatore, **A legislação penal italiana em matéria de computer crimes entre direito e política criminal**. Universidade Federal de São Carlos. Portal de e-governo, inclusão digital e sociedade do conhecimento. Disponível em: <http://www.egov.ufsc.br/portal/sites/default/files/anexos/10685-10685-1-PB.html>. Acesso em 12 dez 2012.

ARGENTINA. **CÓDIGO PENAL - Ley 26.388** - Modificación. Disponível em: http://www.oas.org/juridico/PDFs/arg_ley26388.pdf. Acesso em: 12 dez 2013.

ARRIGHI, Giovanni. **O Longo Século XX**: dinheiro, poder e as origens de nosso tempo. Rio de Janeiro: Contraponto, 1996.

ASSEMBLÉIA LEGISLATIVA DO ESTADO DE SÃO PAULO. **Informativo DDI 45**, Disponível em: http://www.al.sp.gov.br/StaticFile/documentacao/manual_proclgis_2.pdf. Acesso em: 12 mar. 2012.

BARROS. Marco Antônio de, GARBOSSA. Daniella D'Arco, Conte, Christiany Pegorari. **Crimes informáticos e a proposição legislativa**: considerações para uma reflexão preliminar. Revista dos Tribunais | vol. 865 | Nov / 2007.

BARROSO, Luís Roberto. **Fundamentos Teóricos e Filosóficos do Novo *Direito Constitucional Brasileiro (Pós-modernidade, Teoria Crítica e Pós-Positivismo)***. In *A Nova Interpretação Constitucional: Ponderação, Direitos Fundamentais e Relações Privadas*. Luís Roberto Barroso (organizador). 2ª Edição. Rio de Janeiro : Renovar, 2006.

BASTOS, Celso Ribeiro. **Comentários à Constituição do Brasil**. Editora Saraiva, 1989, volume 2.

BATISTA, Nilo. **Introdução Crítica ao Direito Penal Brasileiro**, 9ª ed. Rio de Janeiro: Editora Revan, 2004.

BELMONTE, Alexandre Agra. **Monitoramento da Correspondência Eletrônica nas Relações do Trabalho**. LTR, São Paulo, 2004.

BIELEFELDT, Heiner. **Filosofia dos direitos humanos**: fundamentos de um ethos de liberdade universal. Traduzido por Dankwart Bernsmüller. São Leopoldo: Unisinos, 2000.

BITENCOURT, Cezar Roberto. **Tratado de Direito Penal**, Parte Geral 1. 10ª ed. São Paulo. Saraiva. 2006.

BITTAR, Eduardo Carlos. Bianca. **Os Direitos da Personalidade**. 6. ed. / rev., atual. e ampl. por Eduardo C. B. Rio de Janeiro: Forense Universitária, 2003.

BOBBIO, Norberto. **A Era dos Direitos**. 11. ed. Rio de Janeiro: Campus, 1992.

BRASIL. **Decreto-Lei nº 1001 - Código Penal Militar**, Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del1001.htm. Acesso em 05 mai 2012.

_____. **Decreto-Lei no 2.848 Código Penal**. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em 05 mai 2012.

_____. **Lei nº 6.538, de 22 jul.1978. (Dispõe sobre os Serviços Postais.)**

Regula os direitos e obrigações concernentes ao serviço postal e ao serviço de telegrama em todo o território nacional. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L6538.htm. Acesso em 22 jun. 2011.

_____. **A Lei nº 11.900/2008 que altera dispositivos do Decreto-Lei no**

3.689, de 3 de outubro de 1941 - Código de Processo Penal, para prever a possibilidade de realização de interrogatório e outros atos processuais por sistema de videoconferência, e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2009/Lei/L11900.htm. Acesso em: 18 dez. 2011.

_____. **Constituição da República Federativa do Brasil de 1988.**

Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 10 jun 2012.

_____. **Lei nº 12.737, de 30 de novembro de 2012.** Dispõe sobre a

tipificação criminal de delitos informáticos; altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12737.htm#art2.

Acesso em: 12 dez 2012.

CANOTILHO, J.J. Gomes. **Direito Constitucional e Teoria da Constituição.**

Portugal: Almedina, 2003.

CAPEZ, Fernando. **Curso de Direito Penal:** Parte geral. Vol. 1. 7.ed. rev. e atual.

São Paulo: Saraiva, 2004

CARUSO, Carlos A. A., STEFFEN, Flavio Deny, **Segurança em Informática**, 3a

Edição Revista e Ampliada,. 3a ed. rev. ampl. - São Paulo, 2006.

CARVALHO, Ana Paula Gambogi. **O consumidor e o direito à autodeterminação**

informacional: considerações sobre os bancos de dados eletrônicos. Revista de Direito do Consumidor | vol. 46 | Abr / 2003.

CARVALHO, Kildare Gonçalves. **Direito constitucional** 10ª ed.. Belo Horizonte: Del

Rey, 2004. p 390.

CASABONA. Carlos María Romeo. **Dos delitos informáticos ao crime cibernético**: uma aproximação conceitual e político-criminal. Ed: RT. Ciências penais | vol. 4 | jan / 2006.

CASTRO, Carla Rodrigues Araújo de. **Crimes de Informática e seus Aspectos Processuais**. 2 ed. rev., ampl. E atualizada. Rio de Janeiro.

COMPARATO, Fábio Konder. **A Afirmação Histórica Dos Direitos Humanos**. São Paulo: Saraiva, 2008. 6a ed.

CORRÊA, **Gustavo Testa**. **Aspectos Jurídicos da Internet**. São Paulo: Saraiva, 2000.

COUTINHO, Jacinto Nelson de Miranda, **O Papel do Pensamento Economicista no Direito Criminal de Hoje**. Revista Brasileira de Ciências Criminais nº. 32, 2000.

CRESPO, Marcelo Xavier de Freitas, **Crimes Digitais**. São Paulo: Saraiva, 2011.

D'AVILA, Fabio Roberto e DARCIE, Stephan Doering. **Algumas Reflexões sobre os Crimes de Perigo Concreto**. In Boletim IBCCRIM. São Paulo : IBCCRIM, ano 18, n. 218, jan., 2011.

DIMOULIS, Dimitri; MARTINS, Leonardo. **Teoria geral dos Direitos Fundamentais**. São Paulo: Revista dos Tribunais, 2006.

ESPAÑA. **Ley Orgánica 10/1995, de 23 de noviembre de 1995, del Código Penal**. Disponível em: <http://www.juecesdemocracia.es/legislacionvigente/penal/general/codigopenal.pdf>. Acesso em 12 dez 2012.

_____. **Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal**. Disponível em: <http://civil.udg.es/normacivil/estatal/persona/pf/Lo5-92.htm>. Acesso em: 12 dez 2012.

FERRARO. Valkíria Aparecida Lopes; DE PAULA, Rogério Martins; PAIVA. Renata Silveira de. Semina: **A Sociedade da Informação na Economia Globalizada: Alguns Aspectos do Direito Cibernético**. Ciências Sociais e Humanas, Londrina, v. 25, set. 2004.

FERREIRA FILHO, Manoel Gonçalves. **Curso de Direito Constitucional**, 25 Ed., São Paulo: Saraiva, 1999.

_____. **Direitos Humanos Fundamentais**. 4ª Ed. revista São Paulo: Saraiva, 2000. p22.

FERREIRA, Lóren Formiga de Pinto. FERREIRA JÚNIOR, José Carlos Macedo de Pinto, **Os "Crimes de Informática" e seu enquadramento no Direito Penal Pátrio**. Revista dos Tribunais | vol. 893 | Mar / 2010 | DTR\2010\137.

FIÚZA, Cezar. **Direito Civil: Curso Completo**. Belo Horizonte: Del Rey, 2004.

FRAGOSO, Heleno Cláudio. **Lições de Direito Penal: a nova parte geral**, 7ª ed. Rio de Janeiro: Forense. 1985.

FRANÇA, Limongi Rubens. **Instituições de Direito Civil**. 3.ª. Ed. atual. São Paulo: Saraiva, 1994.

_____. **Manual de direito civil**. 3. ed. rev. São Paulo: Revista dos Tribunais, 1975. v. 1.

GLANZ, Semy, **Internet e responsabilidade civil**. Revista de Direito Bancário e do Mercado de Capitais | vol. 23 | Jan 2004.

Globo *online*, BOM DIA BRASIL. **Senado aprova Lei Carolina Dieckmann sobre Crimes de Internet**. Disponível em: Acesso em: 10 dez. 2012.

GOFFREDO da Silva Telles Jr, **Direito subjetivo, enciclopédia Saraiva do Direito**, São Paulo: Saraiva, 1977.

GOMES, Orlando. **Introdução ao Direito Civil**. 18. ed. Rio de Janeiro: Forense, 2001.

GUILDORD, J., "On Personality", in Mischel, W., **Introduction to Personality**, New York, Holt Rinehart and Wilson, 1973.

HABERLE, Peter. **A Dignidade Humana como fundamento da comunidade estatal**. In: SARLET, Ingo Wolfgang (Org.). **Dimensões da Dignidade: ensaios de**

filosofia do direito e direito constitucional. 2a ed. Porto Alegre. Livraria do Advogado. 2.009.

HUNGRIA, Nelson. **Comentários ao Código Penal**, 1967, v. VII, Rio de Janeiro, Forense.

IBGE. **Pesquisa Nacional por Amostra de Domicílios-PNAD 2009**,. Disponível em: http://www.ibge.gov.br/home/presidencia/noticias/noticia_visualiza.php?id_noticia=1708. Acesso em: 07 Nov. 2012.

INGLATERRA. **Computer Misuse Act 1990**: 1990 CHAPTER 18 An Act to make provision for securing computer material against unauthorised access or modification; and for connected purposes. Disponível em: <http://www.legislation.gov.uk/ukpga>, Acesso em 10 dez 2012.

ISHIDA, Válter Kenji. **As modificações promovidas pela Lei Carolina Dieckmann no Código Penal**. Jornal Carta Forense. Artigos Penal, Disponível em: <http://www.carteforense.com.br/conteudo/artigos/as-modificacoes-promovidas-pela-lei-carolina-dieckmann-no-codigo-penal/9986>, Acesso em: 13 dez 2012.

JESUS, Damásio Evangelista de, **Direito Penal – Parte Geral**, 34ª ed., São Paulo, Saraiva, 2013.

_____. **Código Penal Anotado**, 13ª Ed. São Paulo. Saraiva, p.608.

_____. **Comentários em Palestra Proferida no I Congresso Internacional do Direito na era da Tecnologia Informação**, realizado pelo Instituto Brasileiro de Política e Direito da Informática — IBDI, em novembro de 2000, no auditório do TRF da 5ª Região, em Recife-PE., Op. Cit *apud* ARAS, Vladimir. **Crimes de informática. Uma nova Criminalidade**. Brasília. UFSC. Portal de e-governo, inclusão digital e sociedade do conhecimento. Disponível em: <http://www.egov.ufsc.br/portal/conteudo/crimes-de-informatica-uma-nova-criminalidade>. Acesso em: 12 dez. 2011.

_____. **Direito Penal**, Parte geral. vol.1.ed. 29. rev. e atual. São Paulo: Saraiva, 2008. p. 194.

_____. **Direito penal**, 27ª ed., São Paulo, Saraiva, 2003, p.260.

_____. **Direito Penal**, ed. 23a. Vol. 1, parte geral. São Paulo, Saraiva:1999. p. 41.

JORNAL JURID. Órgão **Especial rejeita denúncia contra juíza**. Disponível em: <http://jornal.jurid.com.br/materias/noticias/orgao-especial-rejeita-denuncia-contra-juiza> Acesso em 10 Jun. 2010.

JUSBASIL, Jurisprudência. **TST - Agravo de instrumento em recurso de revista: airr 1542402420055020055** Disponível em: <http://www.jusbrasil.com.br/jurisprudencia/3157228/agravo-de-instrumento-em-recurso-de-revista-airr-1542-1542-2005-055-02->

_____. **TST - Recurso de Revista: RR 613002320005100013 61300-23.2000.5.10.0013**. Disponível em: <http://www.jusbrasil.com.br/jurisprudencia/3487039/recurso-de-revista-rr-613002320005100013-61300-2320005100013-tst>, Acesso em: 13 nov 2011.

KANT, Immanuel. **Fundamentação da Metafísica dos Costumes**. Edições 70, Lda. 2007, Lisboa- Portugal.

LAFER, Celso. **A reconstrução dos Direitos Humanos**. São Paulo, Companhia das Letras, 1998.

LEAL, João José. **Direito Penal Geral**. São Paulo: Atlas, 1998.

LEONARDI, Marcel. **Tutela e Privacidade na Internet**. São Paulo: Saraiva, 2012.

LEONEL, Ana Lúcia. **O Princípio da Dignidade da Pessoa Humana e a Função Social do Contrato no Direito Privado Brasileiro**. Osasco/SP:UNIFIEO/Centro Universitário FIEO, 2007. Dissertação(Mestrado).

MACEDO JÚNIOR, Ronaldo Porto. **Revista de Direito do Consumidor**. vol. 32, Editora Revista dos Tribunais, Out. 1999.

MAGNOLI, Demétrio. **Globalização: Estado Nacional e Espaço Mundial**. São Paulo: Moderna, 2003.

MARTINS, Guilherme Magalhães. **Formação dos Contratos Eletrônicos de Consumo via Internet**. 1. ed. Rio de Janeiro: Forense, 2003.

MARZOCHI, Marcelo de Luca. **Aspectos Jurídicos da Internet no Brasil**, São Paulo, LTR, 2000.

MATEUCCI, Carlos Roberto Fornes. **Privacidade e Internet, Revista de Direito Privado** | vol. 19 | p. 46 | Jul / 2004, Doutrinas Essenciais de Responsabilidade Civil | vol. 8 | Out / 2011DTR\2004\427

MEDEIRO, Assis. Livro Hackers - **Entre a Ética e a Criminalização**, Visual Books, São Paulo, jul, 2002.

MELLO, Celso D. de Albuquerque. **Curso de Direito Internacional Público**. 10. ed. Rio de Janeiro: Editora Renovar, 1994.

MESQUITA, Renata, Biblioteca da França se volta contra o Google, Revista Abril. Info-Online Disponível em: <http://info.abril.com.br/aberto/infonews/022005/22022005-10.sh>. Acesso em: 22 abril 2012.

MIRABETE, Júlio Fabbrini. **Manual de Direito Penal**, Ed: Atlas, 1990.

_____. **Manual de direito penal**. São Paulo: Atlas, 1991.

MIRANDA, Roberto Campos da Rocha. "**O uso da informação na formulação de ações estratégicas pelas empresas**". Ciência da Informação, Brasília, v.28, n.3, p.284-290, set./dez.

MONTEIRO, João Araújo Neto, **Crimes Informáticos uma abordagem dinâmica ao Direito Penal Informático**, Revista Pensar, Fortaleza, v. 8, n. 8, p. 39-54, fev. 2003.

MORAES, Amaro. NETO, Silva. **E-mails indesejados à luz do direito: spam**. São Paulo: Quartier Latin, 2002.

MORAIS, Alexandre. **Direito Constitucional**. Ed. Atlas, São Paulo, 2005.

NUCCI, Guilherme de Souza. **Código Penal Comentado**, 9ª ed. São Paulo. Revista dos Tribunais, 2009.

OLIVEIRA, Euler Sinoir de. **A Inconstitucionalidade da Violação de E-mail do Empregado pelo Empregador**. Revista Justiça do Trabalho, Porto Alegre, ano 22, nº 261, setembro 2005.

ONU. **Declaração Universal dos Direitos Humanos**, Disponível em: http://portal.mj.gov.br/sedh/ct/legis_intern/ddh_bib_inter_universal.htm. Acesso em 12 dez. 2012.

PARAGUAY. Ley nº 1.160/97, **Código Penal. Asunción. 1997**. Disponível em: http://www.leyes.com.py/todas_disposiciones/1997/leyes/ley_1160_97.htm. Acesso em 10 jan. 2009.

PEREIRA FILHO, Valdir Carlos. **Responsabilidade Civil dos Bancos em operações financeiras realizadas pela internet**, Revista de Direito Bancário e do Mercado de Capitais | vol. 42 | p. 163 | Out / 2008 | DTR\2011\1538.

PEREIRA, Ana Amélia Menna Barreto de Castro, **Correio Eletrônico corporativo – aspectos jurídicos**, in revista de Direito do Trabalho, n.110, abril/junho de 2003.

PEREIRA, Caio Mário da Silva. **Instituições de Direito Civil**: volume 2: teoria geral das obrigações. 19. ed. Rio de Janeiro: Forense, 1999.

_____. **Instituições de Direito Civil**. Rio de Janeiro, Forense 1994. 13ª ed.

PINHEIRO, Patrícia Peck. **Direito Digital**. 4. ed. rev., atual. e ampl. São Paulo: Saraiva, 2010.

PORTUGAL. **Lei n.º 109/91, 13 de agosto de 1991. Lei da Criminalidade Informática**. Disponível em: https://ciist.ist.utl.pt/docs_da/Lei_109-91_Lei_da_Criminalidade_Informatica.pdf. Acesso 15 jan. 2011.

QUEIROZ. Regis Magalhães Soares, LUCCA, Newton De e SIMÃO FILHO. Adalberto (coordenadores) e outros de. **Direito & Internet – Aspectos Jurídicos Relevantes**. 1ª ed. , Bauru-SP, Edipro, 2001, 1ª reimpressão.

Revista **Veja on-line**. Edição 1716. 5 set. 2001. Disponível em: http://veja.abril.com.br/050901/p_076.html. Acesso em 15 maio. 2012.

RIBEIRO, Luciana Antonini. **A Privacidade e os Arquivos de Consumo na Internet** - uma primeira reflexão. Revista de Direito do Consumidor | vol. 41 | Jan / 2002.

ROCHA, Manuel Lopes. **Direito da Informática Legislação e Deontologia** – Lisboa: ed. Cosmos,1994.

RODRIGUES, Silvio. Direito Civil – **Parte Geral**. v 1. 32 ed. Saraiva. São Paulo: 2002.

ROSA, Fabrizio. **Crimes de Informática**. 2. ed. Campinas: CookSeller, 2005.

ROSSINI, Augusto Eduardo de Souza. **Brevíssimas considerações sobre delitos informáticos**. Caderno Jurídico, São Paulo, n. 4, ano 2, jul. 2002.

SANTOS, Milton. **Por uma outra Globalização: do pensamento único à consciência universal**. 6ª ed. - Rio de Janeiro: Record, 2001.

_____. Técnica, espaço e tempo, p. 17. São Paulo: Hucitec, 2000, p. 15-17.

SARLET, Ingo Wolfgang. **Dignidade da Pessoa Humana e Direitos Fundamentais**. Porto Alegre: Livraria do Advogado, 2001, p. 60.

_____; FIGUEIREDO, Mariana Filchtiiner. **Reserva Do Possível, mínimo existencial e Direito à Saúde**: algumas aproximações. In: SARLET, Ingo Wolfgang; TIMM, Luciano Benneti. (Coord.) Direitos fundamentais, orçamento e *reserva do possível*. 2. ed. Porto Alegre: Livraria do advogado, 2010.

SAWAYA, Márcia Regina. **Dicionário de Informática e Internet**. São Paulo, Nobel, 3ª reimpressão 2010.

SILVA, De Plácido e. **Vocábulo Jurídicos**. Rio de Janeiro: Forense, 1999.

SILVA, José Afonso da. **Curso de Direito Constitucional Positivo**. Ed. Malheiros, 2002.

SIMON NORA e ALAIN MINC, **L'Informatisation de la société**, ed. La Documentation Française, "Rapport Nora-Minc": Paris, 1978.

Tanenbaum, Andrew S. *Redes de Computadores* Tradução: Vandenberg D. de Souza. Rio de Janeiro: Campus, 2002.

TARGINO, Maria das Graças. **Novas Tecnologias de Comunicação**: mitos, ritos ou ditos? *Ciência da Informação*, Brasília, v.24, n.2, maio/ago. 1995..

TAYLOR, Charles. **Responsability for self**», in AMÉLIE O. RORTY (org.), *The Identities of Persons*, Berkeley/Los Angeles/Londres, 1984.

TIEDMANN Klaus. **Poder Econômico e Delito**. Traduzido por Amélia Mantilla Villegas, Barcelona, 1985, apud LUIZ GUILHERME MOREIRA PORTO - "Fraude Informática", ob. coletiva *Comércio Eletrônico*, coordenadores Ronaldo Lemos da Silva Júnior e Ivo Waisberg, co-edição IASP e Ed. RT. S. Paulo FERREIRA, Ivete Senise. *A Criminalidade Informática*, in *Direito e Internet - Aspectos Jurídicos Relevantes*, Bauru (SP), Edipro, 2000.

UNITED STATES, **Low 18 U.S.C. 1030**, October 24, 2001. Disponível em: <http://www.law.cornell.edu/uscode/text/18/1030>. Acesso em: 10 jan. 2012.

_____. **Computer Law - State of Wisconsin Statute**. Disponível em: <http://courses.cs.vt.edu/cs3604/lib/Crime/wisconsin.law.html>. Acesso em: 20 jun 2011.

_____. **Low Code@21-3755**. Disponível em: [http://kansasstatutes.lesterama.org/Chapter_21/Article_37/21-UNITED STATES, Low Code@21-3755](http://kansasstatutes.lesterama.org/Chapter_21/Article_37/21-UNITED_STATES_Low_Code@21-3755), Disponível em: <http://legislature.idaho.gov/idstat/Title18/T18CH22SECT18-2201.htm>. Acesso em: 10 jan. 2010.

VENTURA, Luis Henrique. **Comércio e Contratos Eletrônicos**: aspectos jurídicos. São Paulo: EDIPRO, 2001.

Vianna ,Túlio Lima. **Dos Crimes por Computador**. *Revista dos Tribunais* | vol. 801 | Jul / 2002DTR\2002\382.

VIEIRA, Eduardo. **Os Bastidores da Internet no Brasil**. Barueri, Manole, 2003.

VOLPI NETO, Angelo. **Comércio Eletrônico - Direito e Segurança**. Curitiba. Juruá, 2002.

WEICHERT, Marlon Alberto. **Dicionário de direitos humanos**. Disponível em: <http://www.esmpu.gov.br/dicionario/tiki-index.php?page=Informa%C3%A7%C3%A3o>, Acesso em: 19 dez. 2012.

WILLING, David S. **A internet e a Constituição dos Estados Unidos**. São Paulo: Consulex, ano 1, n.4, abr. 1997.

WURMAN, Ricardo S. **Ansiedade de informação**: como transformar informação em compreensão. 5.ed. São Paulo: Cultura Editores, 1995..

ZAFFARONI, Eugênio Raul; BATISTA, Nilo. **Direito Penal Brasileiro I**. Rio de Janeiro: Editora Revan, 2006.

ZANELATO, Marco Antônio, **Condutas Ilícitas Na Sociedade Digital**. Revista de Direito do Consumidor | vol. 44 | p. 206 | Out / 2002DTR\2002\757