FUNDAÇÃO EDSON QUEIROZ
UNIVERSIDADE DE FORTALEZA - UNIFOR
CENTRO DE CIÊNCIAS JURÍDICAS - CCJ
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO CONSTITUCIONAL

ASPECTOS CONSTITUCIONAIS E LEGAIS DO CRIME ELETRÔNICO

João Araújo Monteiro Neto

Fortaleza - CE
Março - 2008

JOÃO ARAÚJO MONTEIRO NETO

ASPECTOS CONSTITUCIONAIS E LEGAIS DO CRIME ELETRÔNICO

Dissertação apresentada ao Programa de Pós-Graduação em Direito como requisito parcial para a obtenção do título de Mestre em Direito Constitucional, sob a orientação de conteúdo do Professor Doutor Rosendo Freitas de Amorin e orientação metodológica Núbia Maria Garcia Bastos.

Fortaleza - Ceará
Março - 2008

M775a Monteiro Neto, João Araújo.
Aspectos constitucionais e legais do crime eletrônico / João Araújo Monteiro Neto. - 2008.
191 f.

Cópia de computador.
Dissertação (mestrado) – Universidade de Fortaleza, 2008.
"Orientação : Prof. Dr. Rosendo Freitas de Amorin."

1. Informática – Aspectos jurídicos. 2. Direito constitucional. 3. Sociedade da informação. I. Título.

CDU 34:681.3

JOÃO ARAÚJO MONTEIRO NETO

ASPECTOS CONSTITUCIONAIS E LEGAIS DO CRIME ELETRÔNICO

BANCA EXAMINADORA

Prof. Dr. Rosendo Freitas de Amorim
UNIFOR

Prof. Dr. José Júlio da Ponte Neto
UNIFOR

Prof. Dr. Juvêncio Vasconcelos Viana
UFC

Dissertação aprovada em:

Àquele de quem guardo as lições de uma vida, abreviada pela vontade de Deus, mas plena de sabedoria. Pai, onde estiveres saberás que o que forjou em mim é imortal.

Os desafios que eu por ventura possa superar, não serão capazes de abrandar a dor silenciosa de sua ausência, nunca.

Não há vitória que possa sobrepujar a ânsia de ouvir às histórias contadas à beira de uma fogueira acessa no relento. Ao sabor da brisa que corre do Parnaíba, a paz povoou o coração de todos aqueles que te acompanharam na luta pela conquista e um sonho. Teu exemplo será a pedra a guiar minha pequena jornada, agora e sempre.

AGRADECIMENTOS

A Deus, Regente Maior;

A todos os Professores da minha formação acadêmica,

Ao Professor Orientador Dr. Rosendo Freitas de Amorim pelo apoio e orientação e aos Professores. Drs. José Júlio da Ponte Neto e Juvêncio Vasconcelos Viana por aceitarem o convite de participarem da avaliação desse trabalho.

A minha mãe, pelo amor irresoluto e (in)paciente, pelo exemplo de mãe, professora e acima de tudo pelo amor que demonstrou nos momentos mais difíceis;

A Ariana. Não existem palavras que possam cativar o perdão, mas você sabe que tua ausência é minha morte.

A João Lucas e Ana Júlia pelo sentido conferido a minha vida.

E em especial aos amigos Francisco Otávio de Miranda Bezerra, Beatriz Rego Xavier e Juliene Tabosa, não pelos exemplos que são, nem pelo grande apoio fornecido, mas acima de tudo, pela amizade.

A todos aqueles que contribuíram para a construção desse trabalho, em especial aos alunos que me acompanharam e incentivaram-me no estudo da matéria bem como àqueles que através das revisões tornaram-se inestimáveis.

RESUMO

As facilidades e vantagens proporcionadas pelo uso de sistemas eletrônicos causaram uma crescente informatização das atividades cotidianas na era pós-industrial, fazendo dessa forma surgir a sociedade da informação. Esse novo contexto social modificou sensivelmente as esferas de relações econômicas e jurídicas. Como conseqüência desta vinculação da sociedade às tecnologias da informação, a criminalidade passou por processo semelhante, tornando-se apta a praticar ilícitos em meio eletrônico. Surgiram assim novos bens jurídicos aos quais à ordem constitucional precisava proteger. A segurança e a integridade dos sistemas eletrônicos caracterizam-se como exemplos concretos dos bens eletrônicos. Atos ilícitos danosos a esses bens começaram a ser perpetrados nascendo assim os crimes eletrônicos. Diante dessa nova realidade criminosa discute-se a evolução da sociedade da informação, o impacto da sociedade da informação na ordem constitucional e as suas conseqüências na esfera penal. O presente trabalho busca analisar os Crimes Eletrônicos e seu relacionamento com o ordenamento constitucional brasileiro, através de pesquisa bibliográfica busca analiticamente compreender os aspectos estruturais relacionados aos crimes eletrônicos, principalmente sobre a necessidade de construção de mecanismos legais eficientes na sua repressão.

Palavras-chave: Sociedade da informação. Constituição. Crime eletrônico.

ABSTRACT

The facilities and benefits offered by the use of electronic systems caused an increasing computerization of the daily activities in the post-industrial era thus making the emerging information society. This new social context changed appreciably the spheres of economic relations and legal. As a result of this linkage of the company to information technology, crime went through similar process, becoming able to practise in illegal electronic means. There were so new legal goods to which the constitutional order needed to protect. The safety and integrity of electronic systems characterize themselves as concrete examples of electronic goods. Acts illicit harmful to these goods began to be perpetrated the crimes electronicsl. Given this new reality criminal discusses the evolution of the information society, the impact of the information society in constitutional order and its consequences in the criminal sphere. This paper seeks review the Crimes Electronics and its relationship with the constitutional Brazil, through literature search analytically understand the structural issues related to electronic crimes, mainly on the need to build efficient legal mechanisms in their repression.

Keywords: Information Society. Constitution. Crime electronic.

SUMÁRIO

INTRODUÇÃO

O aperfeiçoamento de novas tecnologias permitiu a humanidade atingir patamares elevados de desenvolvimento. Práticas sociais, econômicas e culturais, foram drasticamente modificadas pela mediação tecnológica. O advento da terceira revolução industrial, focada na construção de mecanismos de produção ligados a informação, aliada ao fenômeno globalizante, transformou de forma paulatina os modelos de organização econômica e social mundial.

A reestruturação organizacional da sociedade surgida com o advento da revolução tecnoinformacional influenciou de forma direta os mecanismos de controle e manutenção da ordem social, dentre eles o Direito. O primeiro reflexo desse impacto deu-se na seara constitucional. A Constituição enquanto mecanismo regulador da ordem política e jurídica do Estado abarcou de forma primária a responsabilidade de dar contornos jurídicos à nova realidade social, econômica e cultural que surgia.

Dessa forma a Constituição, especificamente, a Carta Constitucional brasileira de 1988, seguindo a trilha do constitucionalismo moderno estabeleceu seus laços protetivos aos novos bens e valores jurídicos que surgiram com o advento da revolução informacional. A influência do novo contexto social na ordem jurídica constitucional se deu de forma marcante em dois grandes campos: o primeiro relaciona-se a necessidade de proteção dos novos direitos e valores surgidos, posto que se pautam como fundamentais para a manutenção do atual estágio de organização coletiva, dentre os quais se podem destacar o direito a informatização e ao acesso a informação, independentemente do meio utilizado, bem como o impacto dessa nova realidade sobre direitos e garantias já tutelados pela ordem constitucional, como por exemplo, a possibilidade de utilização de sistemas eletrônicos para realizar devassas a intimidade ou à privacidade do cidadão; em um segundo momento, esse novo contexto de organização social atinge a estrutura do Estado moderno, posto que em virtude de uma de suas características, a

desterritorialização, o Estado sofre uma diminuição na sua capacidade soberana de aplicar o seu ordenamento jurídico aos atos e fatos ocorridos no meio eletrônico.

Segundo o balizamento constitucional, coube ao Direito Penal estruturar mecanismos efetivos de prevenção e sanção às condutas lesivas a esses novos bens e valores surgidos com o advento da Sociedade da Informação e devidamente abarcados pela ordem político-jurídica materializada na Constituição.

A descoberta da vulnerabilidade dos sistemas eletrônicos permitiu à realização de condutas ilícitas prejudiciais a manutenção dos níveis mínimos de segurança e credibilidade necessários a continuidade do modo de produção informacional. Essas novas condutas praticadas contra, ou através de meios e bens eletrônicos, passaram a ser denominadas de *cybercrimes,* crimes virtuais, crimes informáticos ou crimes eletrônicos. Condutas as quais, em sua maior parte, encontram-se carentes de regulamentação. Essa lacuna legal só fortalece a sensação de que o espaço eletrônico assemelha-se a um verdadeiro "mundo sem lei", uma espécie de "velho oeste virtual" onde se proliferam as ações criminosas.

Assim, ganha ênfase a necessidade de proteger os sistemas estruturantes do novo modelo de organização social, seja na esfera econômica, seja no seu âmbito cultural. Ganha importância na seara jurídica a proteção dos sistemas eletrônicos, e dos bens a eles relacionados. A manutenção do modelo de produção pautado na informação depende da capacidade da ordem jurídica de conferir segurança e credibilidade aos negócios jurídicos firmados no meio eletrônico. Logo, torna-se indispensável para a proteção dos interesses em jogo a regulamentação penal da matéria.

No que tange a ordem jurídica brasileira, a regulamentação penal do uso das tecnologias da informação para a prática de delitos não se vincula somente à substituição de normas obsoletas ou à utilização de recursos hermenêuticos. Quanto à incriminação de condutas, ou seja, a tipificação, percebe-se, a existência de um vazio normativo materializado na carência de previsões legais aplicáveis a essas condutas, o que de plano inibe a tutela penal dessas situações, gerando assim uma situação de risco para a manutenção da sociedade.

A análise da situação apresentada propicia o surgimento de alguns questionamentos que foram analisados no presente trabalho: qual o impacto da sociedade da informação na ordem

jurídica constitucional? Como o Estado foi atingido por essa nova forma de organização social fundada na tecnologia informacional? Como o Direito Penal pode proteger o novo conjunto de bens surgidos pelo advento da sociedade da informação e que foram recepcionados pela ordem constitucional brasileira?

O novo contexto de organização social, além de suscitar o surgimento de bens carentes de proteção normativa, potencializou, através da mediação simbiótica entre tecnologia e informação, novas formas de violação a bens jurídicos já tutelados. Nesse esteio, têm-se como objetivos do presente trabalho analisar a evolução da sociedade da informação e a sua influência nas estruturas jurídicas. Especificamente, procura-se averiguar o tratamento constitucional dado à realidade fática e social advinda do estabelecimento da sociedade da informação, bem como se tenciona analisar os mecanismos legais utilizados na prevenção de práticas ilícitas lesivas ao conjunto de bens jurídicos oriundos no novo modelo de organização social, econômica e cultural.

Com relação aos aspectos metodológicos as questões suscitadas no início da pesquisa foram investigadas através de pesquisa bibliográfica, posto que se busca explicar o problema por meio de referências teóricas, procedendo a análise da literatura relacionada ao tema em livros, revistas, imprensa escrita e documentos, o que permite a coleta de dados e informações também em leis, projetos de lei e outros diplomas normativos.

No que tange à tipologia a pesquisa se caracteriza como pura, uma vez que a utilização dos resultados obtidos busca aumentar o conhecimento da área para construção de posicionamento sobre o tema; e no que remonta à abordagem, caracteriza-se como qualitativa, posto que se preocupa com a apreensão das ações humanas que ainda não tenham sido qualificadas.

Quanto aos objetivos visados a pesquisa é analítica, pois a partir da análise dos fenômenos, procura-se compreender determinações significativas sobre o problema, bem como suas características e causas, sendo ainda exploratória, já que tende a aprimorar idéias, definindo objetivos e suscitando maiores informações sobre o assunto estudado.

O primeiro capítulo procura contextualizar a Sociedade da Informação, através da análise dos elementos que serviram de base a sua estruturação, o seu desenvolvimento, o que

abarca o estudo da *Internet*, as suas características, bem como os seus impactos na reestruturação da ordem social, econômica e jurídica.

No segundo capítulo analisa-se o impacto da sociedade da informação no Direito Constitucional, especialmente no que tange a sua relação com os comandos protetivos constitucionais ao novo conjunto de bens jurídicos que surgiram com a informatização da sociedade e foram recepcionados pela ordem constitucional, bem como os impactos do modelo de organização tecnoinformacional na estrutura do Estado.

Destarte, o terceiro capítulo analisa as ferramentas utilizadas pelo Direito Penal para proteger os valores informacionais tutelados pela Constituição. Assim estuda-se inicialmente os aspectos gerais do Direito Penal, as relações da tecnologia da informação e dos sistemas eletrônicos com o Direito Penal, o conceito de crime eletrônico, sua classificação, os delitos eletrônicos já tipificados, bem como as perspectivas de regulação da matéria à nível nacional e internacional.

1 SOCIEDADE E TECNOLOGIA DA INFORMAÇÃO

Desde os primórdios de sua existência o homem, como ser cognoscente, trava uma batalha interminável contra sua insaciável necessidade de obter conhecimento. O aprimoramento dos meios de produção e distribuição, bem como dos suportes físicos necessários à disseminação de dados como partes basilares do ente informação, revolucionaram e ainda transformam de forma avassaladora a realidade da vida em sociedade.

A invenção da imprensa é um dos grandes marcos divisórios da evolução do homem coletivo. O processo de difusão de conhecimento tornou-se mais ágil e de certa forma muito mais acessível, tornando possível à chegada de informações a guetos sociais antes inatingíveis. No esteio da Revolução Industrial, novas criações do gênio humano refinaram o procedimento de produção, envio e armazenamento de informações, no entanto o homem para efetuar os registros de seus feitos ou para perpetuar conhecimento permanecia refém da escrita e do papel.

O grande paradigma da história humana moderna consubstancia-se na invenção e no aperfeiçoamento das novas tecnologias surgidas no período pós-industrial que impulsionaram o desenvolvimento de instrumentos que implodiram a realidade humana até então existente. O fator que desencadeou esta transformação foi o surgimento de uma nova tecnologia: a tecnologia da informação. O computador e os sistemas eletrônicos revolucionaram não só o modo de se viver, mas também o de agir do homem.

A informática, a telemática, a *Internet* e os sistemas eletrônicos, graças a fatores como economia e velocidade, superaram os demais meios de comunicação na esteira do fenômeno globalizante e vêm se expandindo a todos os prismas de utilização da vida moderna.

Atualmente os sistemas eletrônicos permitem o intercâmbio de dados e informações que concretizam desde relacionamentos interpessoais até pactos comerciais envolvendo movimentações financeiras vultosas.

As modificações decorrentes da utilização de sistemas eletrônicos modificaram drasticamente a contextualização das estruturas sociais, econômicas e jurídicas da sociedade moderna.

1.1 A sociedade da informação

O espírito humano sempre inovador e ávido por novas descobertas fez com que o espécime humano em um curto período de tempo abandonasse as antigas cavernas e a selvageria típica da raça animal para conquistar não só o mundo em que vive mas também o espaço sideral.

Contudo, um novo desafio surge. Buscando abrandar a chama da inovação, o homem busca agora colonizar uma nova era, um novo mundo fruto de sua criação intelectual, um espaço intangível, o mundo eletrônico.

O fogo, a roda, a escrita, a moeda, a pólvora, a energia elétrica, as máquinas de calcular, o computador, os sistemas eletrônicos. A evolução do conhecimento humano fez com que a cada nova descoberta a sociedade sofresse transformações nem sempre benéficas. A realidade social pós-industrial parecia estagnada quando o evoluir de um aparelho que simplesmente fazia cálculos modificou de forma profunda e irreversível a vida humana.

Os sistemas eletrônicos, antes simples coadjuvantes das atividades humanas, hoje assumem papel imprescindível na vida em sociedade moderna, pois está presente de forma direta ou indireta em todas as atividades humanas.

Dentre os impactos causados pela evolução da informática e dos sistemas eletrônicos ,o surgimento e o desenvolvimento da *Internet* alteraram sensivelmente as relações econômicas, e humanas, quebrando as barreiras geográficas e temporais.

A informação passou a ter valor estratégico. Surgiu segundo Casttels um novo modelo de produção capitalista:

> Assim, no modo agrário de desenvolvimento, a fonte do incremento de excedente resulta dos aumentos quantitativos da mão-de-obra e dos recursos naturais (em particular a terra) no processo produtivo, bem como na dotação natural desses recursos. No modo de desenvolvimento industrial, a principal fonte de produtividade reside na introdução de novas fontes de energia e na capacidade de descentralização do uso de energia ao longo dos processos produtivos e de circulação. No novo modo informacional de desenvolvimento, a fonte de produtividade acha-se na tecnologia de geração de conhecimentos, de processamento da informação e de comunicação de símbolos[1].

Entretanto, vale salientar que o que caracteriza essencialmente a revolução da Tecnologia da Informação, não é simplesmente o avanço na busca de conhecimentos e técnicas que possibilitassem o incremento da atividade industrial, como na primeira Revolução Industrial, marcada essencialmente pelo desenvolvimento técnico e científico da química, da mecânica e da eletricidade.

A Revolução da Tecnologia da Informação busca a aplicação do conhecimento na criação de novos mecanismos de processamento de dados e informações, sendo que o seu desenvolvimento é gerido por meio da sua difusão entre os usuários da própria informação, que dela se apropriam e a inovam constantemente, tal qual como diria Immanuel Kant, "o conhecimento é um processo de síntese, no qual o intelecto proporciona a forma e a experiência oferece o conteúdo"[2]. A Revolução Tecnológica funcionaria como um motor que se alimenta de informação e produz mais informação, sendo esta o pilar do sistema econômico vigente.

Assim, antes de adentrar especificamente nos desdobramentos jurídicos decorrentes da chamada revolução da tecnologia da informação, faz-se necessário primeiro a compreensão da evolução tecnológica que propiciou as bases materiais para a formação da sociedade da informação.

---

[1] CASTELLS**,** Manuel. **A sociedade em rede – A era da informação:** economia, sociedade e cultura. Tradução de Roneide Venâncio Majer. São Paulo: Paz e Terra, 1999. v.1. p.35.
[2] KANT, Immanuel. **Crítica da razão prática.** Tradução de Rodolfo Schaefer. São Paulo: Martin Claret, 2006. p.178.

1.1.1 Aspectos históricos da tecnologia e da sociedade da informação

A busca pelo conhecimento pode ser considerada como uma das principais, características do homem. Desde tempos imemoriais a humanidade permeia sua existência na Terra sustentando-se por meio de sua capacidade de apreender e se adaptar.

A informação: o poder da informação revolucionou a estrutura social humana moderna. Os patamares econômicos e sociais foram drasticamente modificados com o advento da chamada sociedade da informação e o desenvolvimento de novos valores sociais e econômicos pautados na prevalência da simbiose entre informação e tecnologia.

Os elementos precursores dessa nova ordem social e econômica não são tão recentes como uma análise superficial pode apontar, remonta a construções teóricas e a instrumentalizações práticas afeitas há séculos pretéritos. Assim, visando uma compreensão mais acurada do tema, torna-se imprescindível reconstituir historicamente o papel das novas tecnologias para o desenvolvimento da Sociedade da Informação.

A idéia da informação como base de construção de uma nova forma de estruturação e organização social, em uma análise superficial, é recente, remonta sem sombra de dúvidas, no máximo, ao século passado, tendo sido enfatizado somente nos últimos 50 anos. Entretanto, um exame mais acurado vai perceber que as sementes dessa nova estrutura foram lançadas há muitos séculos atrás.

A idéia de civilização está intimamente ligada à informação. O homem, ou seja, o *homo sapiens* tem sua essência, e inclusive, sua classificação evolutiva atrelada à informação. As bases dessa nova organização social têm como marco o século XVI. Nesse período, a noção de científico atrela-se à idéia de mensurável e do enumerável. O conhecimento científico vincula-se de forma irreversível a noções matemáticas, o número passa a encarnar algo místico, sinônimo da verdade, chegando inclusive, o cálculo, ser considerado pelo engenheiro francês Sébastien Lê Prestre de Vaunban[3], o único instrumento efetivo para o combate ao caos.

[3]Engenheiro militar de fortificações, Sébastien Lê Prestre, desenvolveu estratégias militares de ataque e de defesa que se fundavam na coleta e processamento das informações sobre o sítio de ataque, e na construção de redes de trincheiras que facilitassem o ataque aos pontos mais vulneráveis da fortificação.

> A idéia de uma sociedade regida pela informação está, por assim dizer, inscrita no código genético do projeto de sociedade inspirado pela mística do número. Ela data, portanto, de muito antes da entrada da noção de informação na língua e na cultura da modernidade. Esse projeto, que ganha forma nos séculos XVII e XVIII, entroniza a matemática como modelo do raciocínio e da razão útil. O pensamento do enumerável e do mensurável torna-se o protótipo de todo discurso verdadeiro ao mesmo temo que instaura o horizonte na busca da perfectibilidade das sociedades humanas. Momento forte da materialização da língua dos cálculos, a Revolução Francesa faz dele o modelo de igualdade cidadã e dos valores do universalismo[4].

O ideário de igualdade e de universalização construídos pela estruturação de uma linguagem científica baseada no número, ou seja, em bases matemáticas, concretizou-se com a unificação do sistema decimal de pesos e medidas, que simbolizou o fim de um das tradições do sistema feudal, o engodo anárquico de medidas utilizado pelos senhores feudais para dominar o comércio:

> O metro aparece como a realização do ideal secular de transcendência na troca. Encontrada na Natureza, nessa Natureza dos filósofos das luzes, comum a todos, a nova unidade é glorificada como fruto da razão emancipadora: portadora dos valores universais, ela aproxima as pessoas[5].

A influência do número, da matemática e do cálculo no desenvolvimento da sociedade da informação é tão marcante que o surgimento das máquinas ancestrais dos computadores modernos, as chamadas máquinas de fazer cálculos liga-se diretamente ao período de desenvolvimento do capitalismo moderno e da expansão européia rumo ao "novo mundo". É nesse período que Gottfried Wilhelm Leibniz, filósofo e matemático alemão considerado o pai da cibernética, partindo de pesquisas e postulações sobre a essência da lógica, inicia o processo de construções científicas que permitem a elaboração da tese de que o pensamento pode ser manifestado no interior de uma máquina.

Essas postulações são reforçadas pelas necessidades práticas do regime econômico que surgia. O capitalismo e seus meios operacionais necessitavam de instrumentos rápidos e eficazes de cálculo. O expansionismo do capitalismo rumo às Índias e às Américas faz surgir três grandes nichos onde a velocidade de apuração e de tratamento de informações (números), faz nascer a necessidade de instrumentos de cálculo: os setores de informação, construção naval e de navegação.

---

[4] MATTELART**,** Armand. **História da sociedade da informação**. Tradução de Nicolas Nyimi Campanário. São Paulo: Loyola, 2002. p.11.
[5] KULA apud Ibid., 2002. p.28.

O grande volume de informações oriundas das operações além mar precisavam ser coletadas, armazenadas, tratadas e difundidas de forma célere na forma de dados que alimentassem os principais atores do novo sistema econômico, os negociantes, os comerciantes, os financiadores e os especuladores.

Em outro patamar, a expansão ultramarina forçou o desenvolvimento da indústria naval, exigindo a construção otimizada de navios maiores, mais resistentes, de maior navegabilidade e mais eficientes, o que induziu a elaboração de técnicas de engenharia mais refinadas obtidas através de complexas estruturas matemáticas.

Por último, a necessidade de navegar afastando-se da costa fez com que se desenvolvessem novas formas de navegação mais precisas que culminaram dentre outras coisas com o aperfeiçoamento de um mecanismo que é considerado como o ancestral dos instrumentos programados, o relógio.

Apesar da busca constante pelo aprimoramento das máquinas de fazer contas foi somente a partir da segunda metade do século XIX, que Charles Babbage[6] conseguiu desenvolver um artefato capaz de calcular automaticamente.

Inspirado no método utilizado pelo engenheiro francês Marie Ricche de Prony[7] para construção de complexas tabelas trigonométricas e logarítmicas, ele adaptou a esse método os princípios da teoria da divisão de trabalho formulada por Adam Smith.

Babbage, na busca de construir uma máquina de realizar cálculos, combinou dois grandes modelos. O primeiro, o conceito de divisão de trabalho formulado por Adam Smith que até então era aplicado somente às atividades físicas, ou melhor, às atividades fabris, utilizando-o no desenvolvimento de atividades mentais, como as operações matemáticas estruturados por Prony. O segundo, foi a máquina de tecelagem semi-automática desenvolvida

[6] Charles Babbage, matemático inglês, professor de Cambridge, recebeu uma bolsa do governo britânico para desenvolver uma calculadora com capacidade até a vigésima casa decimal. Acabou criando uma máquina que é considerada como o primeiro computador de uso geral.

[7] Ele havia distribuído às tarefas em três oficinas de funções bem distintas. O primeiro grupo, composto de cinco a seis geômetras, era encarregado da pesquisa das fórmulas mais simples o segundo, de sete a oito matemáticos, traduzia essas fórmulas em números. O último, de sessenta a oitenta calculadores, dezenove dos quais só sabiam as duas primeiras regras aritméticas, realizava as operações indicadas e confeccionava as tabelas. Foi assim que Prony conseguiu encher dezessete grandes volumes. Ibid., 2002. p. 40.

por Jacquard[8], especialmente no que tange ao modelo de inserção de dados para a estruturação da trama a ser tecida. Assim, Babbage:

> concebe sucessivamente uma máquina analítica (analytical engine) e uma máquina diferencial (difference engine). Esses moinhos de números que combinam o arsenal das técnicas disponíveis (máquina a vapor, moinho, automatismo progamáveis, mecânica) tecem modelos algébricos como a máquina de tecer de Jacquard tece flores e folhas. É assim que eles são definidos por Ada Augusta, condessa de Lovelace (1812-1852), filha de Lorde Byron, a quem se deve um dos raros trabalhos sobre essas máquinas publicados ainda durante a vida do inventor.[9]

Surge dessa forma o artefato que é considerado um dos primeiros ancestrais do computador, ou seja, a primeira máquina desenvolvida para tratar informações, especificamente números. O moinho de números de Babbage é considerado o primeiro de uma linhagem que revolucionou a vida em sociedade, e hoje é o instrumento base para a estruturação de um novo modelo de organização econômica e social.

No contexto evolutivo das máquinas de tratamento de informações, ganha destaque a utilização, em 1890, de uma máquina que utiliza cartões perfurados para o tratamento automático dos dados obtidos no recenseamento geral dos Estados Unidos. Fato peculiar é que a partir de 1896 essa mesma máquina passa a ser produzida em escala industrial sendo desde então comercializada pela *Holletrith Tabulanting Corporation*, empresa que serviu de alicerce para o surgimento da *International Bussines Machine – IBM*.

Nesse mesmo período, surge também uma iniciativa interessante que marcou o desenvolvimento da atividade científica e que influenciou o desenvolvimento da sociedade da informação: foi a visionária fundação em 1895 do Instituto Internacional de Bibliografia pelos advogados Paul Otlet e Henri La Fontaine. O principal objetivo do Instituto era organizar de forma sistemática toda documentação, especificamente publicações de natureza científica produzidas pela humanidade. Próximo a primeira guerra mundial o acervo do Instituto já abarcava um repertório bibliográfico universal, um conjunto icnográfico universal, um guia de bibliotecas, um conjunto de arquivos documentais de caráter internacional, bem como tinha instituído uma biblioteca internacional e um museu internacional dos métodos de tratamento

[8] Joseph Marie Jacquard, mecânico francês, (1752-1834) inventou um tear mecânico controlado por grandes cartões perfurados. A invenção de Jacquard caracterizou-se como uma das primeiras formas de programação de máquinas e serviu de base para o desenvolvimento dos primeiros computadores. Os buracos ou suas ausências nos cartões perfurados indicavam a posição do fio na urdidura no momento da passagem do fio pela trama, o que causava dessa forma o direcionando assim o desenho a ser tecido.
[9] Ibid., 2002. p.40.

de documentação de informações. Além desse aspecto, a implantação do Instituto Internacional de Bibliografia fomentou o surgimento, em 1910, do escritório central da união das associações internacionais, que tinha como meta principal o estabelecimento de uma rede de instituições científicas cujo objetivo era organizar formas e métodos de trocas de informações, bem como assegurar mecanismos de cooperação e coordenação de esforços em busca da estruturação de um sistema geral formado pela soma de todos os sistemas menores.

> O objetivo atribuído ao escritório mostra, de outro modo, a intuição política que presidiu a criação do Instituto: Fazer do mundo inteiro uma única cidade e de todos os povos uma única família. Essa utopia da cidade mundial ou mundaneum é defendida por Paul Otlet, que luta para concretizá-la em Bruxelas ou em Genebra, associando-se a arquitetos como Le Corbusier. Mais ambicioso ainda, ele formula um projeto de sociedade intelectual das nações [Otlet, 1919]. Otlet forja o termo mundialismo para melhor marcar a simbiose com um pensamento da rede universal, ao mesmo tempo técnico e social. Um pensamento que se forjou no ritmo do enlaçamento do globo tanto pelas múltiplas redes cidadãs que surgem na segunda metade do século XIX a favor do reconhecimento das liberdades de imprensa, de expressão e de associação, dando um impulso inesperado às trocas entre as sociedades civis[10].

Assim, a sociedade da informação desenvolvia seus primeiros elementos estruturais. Vale ressaltar que até esse momento, apesar dos avanços apontados, o computador, ou melhor, as complexas máquinas de efetuar cálculos eram mecanismos rudimentares de alcance muito limitado, bem como enfrentavam um problema sério, a falta de instrumentos que automatizassem os processos internos realizados para efetuar as operações matemáticas.

Procurando aperfeiçoar a eficácia desses "moinhos de números", Alan Turing[11], em 1936, desenvolve um princípio técnico inovador: a programação, ou seja, a construção de estruturas lógicas que permitem a decodificação e interpretação do problema a ser tratado. Esboça-se a idéia do programa como o mecanismo necessário a compreensão e tratamento das informações que devem ser utilizadas pela máquina. Surge a partir daí as primeiras menções a possibilidade de se criar o chamado cérebro eletrônico.

A partir desse período três grandes fatores vão influenciar o desenvolvimento avassalador das ferramentas ligadas a tecnologia da informação, especificamente para o aprimoramento das grandes calculadoras, ou seja, dos ancestrais mais próximos dos sistemas

[10] Ibid., 2002. p.47-49.
[11] Alan Mathison Turing foi um matemático britânico que consagrou-se com a projeção de uma máquina que, de acordo com um sistema formal, pudesse fazer operações computacionais, ou seja tratar informações.

eletrônicos atuais: a decodificação de correspondências estratégicas, o desenvolvimento de tabelas de tiros de artilharia antiaérea e o desenvolvimento da bomba atômica.

Apesar de possuírem influências distintas no desenvolvimento das grandes calculadoras, esses três fatores possuem uma circunstância essencial: a utilização para fins militares da ciência, especificamente o desenvolvimento de novos instrumentos tecnológicos para serem utilizados como trunfos bélicos.

"A problemática da ciência das linguagens secretas será um dado recorrente da história que conduz às máquinas inteligentes do século XX[12]." Esse problema agravou-se durante a segunda guerra mundial quando as máquinas codificadoras eletromagnéticas Enigma, desenvolvidas pelos técnicos germânicos no período entre guerras, geravam mensagens criptografadas impossíveis de serem decodificadas pelos técnicos do serviço de inteligência dos aliados. Forçou-se dessa forma, o desenvolvimento de máquinas que efetuando enormes quantidades de cálculos pudessem decifrar a combinação alfanumérica que serviria de chave para as mensagens criptografadas interceptadas.

Em segundo plano, a necessidade de conferir maior precisão ao sistema de defesa antiaéreo exigiu a criação de tabelas de tiros mais precisas à grandes distâncias, o que exigia a realização de inúmeras operações matemáticas logarítmicas em um curto espaço de tempo. Assim, mais uma vez, fez-se necessário o desenvolvimento de equipamentos especificamente desenvolvidos para a realização precisa de grandes equações matemáticas balísticas.

Em um terceiro momento, o Projeto Manhattan, que culminou com o desenvolvimento da bomba atômica, também exigiu a construção de mecanismos eletrônicos de cálculo, haja vista a necessidade de comprovação prática das inúmeras equações logarítmicas que serviam de base às construções científicas relacionadas aos efeitos das teses nucleares.

Como fruto desse trabalho de pesquisa e desenvolvimento subsidiado pelo exército norte-americano surge o primeiro computador eletrônico: O *Eletronic Numerical Integrator and Calculator* (ENIAC) – (Computador e Integrador Numérico Eletrônico). Desenvolvido pelo Instituto de Tecnologia de Massachusetss (MIT.) o ENIAC se caracterizou como a

[12]Ibid., 2002. p.16.

primeira versão de computador para o uso geral, e além de pesar "30 toneladas, foi construído sobre estruturas metálicas com 2,75 m de altura, tinha 70 mil resistores e 18 mil válvulas a vácuo e ocupava a área de um ginásio esportivo. Quando ele foi acionado, seu consumo de energia foi tão alto que as luzes de Filadélfia piscaram[13]".

Logo em seguida, os físicos Bardeen, Brattain e Shockley, da empresa *Bell Laboratories* desenvolveram um componente que revolucionou a indústria eletrônica acelerando a utilização de instrumentos eletrônicos nos mais diversos campos. O transistor:

> possibilitou o processamento de impulsos elétricos em velocidade rápida e em modo binário de interrupção e amplificação, permitindo a codificação da lógica e da comunicação com e entre as máquinas: esses dispositivos têm o nome de semicondutores, mas as pessoas costumam chamá-los de chips (na verdade, agora constituídos de milhões de transistores)[14].

O desenvolvimento do transistor deu impulso ao surgimento da microeletrônica, que hoje pode ser considerada como um dos campos tecnológicos que mais contribuiu para a estruturação dos sistemas eletrônicos e, conseqüentemente, da sociedade da informação. A continuidade das pesquisas permitiu a utilização de novos materiais para a construção de transistores, onde houve destaque do silício, fato que permitiu reduzir custos e fomentar a produção em larga escala. O avanço no campo da microeletrônica permitiu o redimensionamento dos computadores, o que acarretou o lançamento em 1951 pela Remington Rand do UNIVAC-1, uma versão comercial primitiva de computador.

Vale destacar que em 1949, foi construída por Maurice V. Wilkes, da Universidade de Cambridge, na Inglaterra, uma das primeiras máquinas capaz de armazenar programas: o *Delay Storage Automatic Calculator* (EDSAC)[15].

Nesse período surge o embrião da discussão científica sobre as potencialidades da informática e dos sistemas eletrônicos, seu controle, suas comunicações e sua possível estruturação em sistemas. A idéia de uma máquina de calcular é ampliada. O computador, ganha um viés mais universal, amplo, completo. Percebe-se a possibilidade da máquina não só calcular, mas também pensar, sendo a mesma "teoricamente capaz de resolver qualquer

[13] CASTELLS, Manuel, op. cit., 1999. p.60.
[14] CASTELLS, Manuel, op. cit., 1999. p.58.
[15] VERZELLO, Robert; REUTTER III, John. **Processamento de dados**: sistemas e conceitos. Tradução de Regina Szwarcfiter. São Paulo: McGraw-Hill, 1984. p.524.

problema formulado de modo razoavelmente preciso, isto é, que pode ser sistematizado, matematizado, modelizado, reduzido a um algoritmo."[16]

Essa mudança de concepção deve-se em boa parte a John von Neumann, matemático de origem húngara, que contribui de forma significativa para a construção do modelo teórico do primeiro computador. Foi graças às von Neumann que o ciclo das grandes máquinas de calcular se encerrou. Influenciado pelas idéias de Turing seu objetivo principal era desenvolver um cérebro artificial. Para isso reformulou drasticamente a organização dos processos utilizados nas grandes máquinas de calcular. Adotando critérios lógicos e matemáticos, von Neumann criou uma estrutura de tratamento de informações que ficou conhecida como a "arquitetura von Neumann" e ainda serve de base para a organização dos métodos computacionais modernos.

> Por arquitetura, é preciso que se entenda o modo pelo qual os diferentes elementos de um computador são organizados entre si. Os construtores procuraram, sem dúvida, melhorar esses diferentes elementos e propor modos de organização interna mais racionais, mas o impulso dado por von Neumann continuará determinante. Os quatro elementos fundamentais, desde sua origem, são a memória, que armazena as informações e os programas, a unidade lógica, que processa a informação, a unidade de controle, que organiza o funcionamento interno da máquina e, para terminar, os diferentes órgão de entrada e de saída (teclados, telas, impressoras etc.).[17]

Esse modelo de organização das estruturas de tratamento das informações foi capaz de deflagrar uma verdadeira revolução no processo de desenvolvimento dos computadores. Associada a essa mudança de concepção estrutural um outro fator fortaleceu os investimentos no desenvolvimento dessa nova tecnologia. Com o fim da segunda grande guerra mundial e a conseqüente polarização capitaneada pelos Estados Unidos da América de um lado e pela União das Repúblicas Socialista Soviéticas do outro, a chamada guerra fria, o interesse militar voltou a ser a linha mestre nas pesquisas científicas, principalmente as ligadas ao desenvolvimento de tecnologias da informação.

Um dos grandes pólos de desenvolvimento dessa pesquisas foi a indústria aeroespacial. A doutrina militar sustentava que o país que dominasse o teatro operacional aéreo teria supremacia sobre as outras praças bélicas. Dessa forma, foi justamente no campo do desenvolvimento de artefatos bélicos aéreos que se começou a utilizar o embrionário conceito

---

[16]EDWARDS apud MATTELART, Armand, op. cit., 2002. p.58.
[17]BRETON**,** Philippe. **História da informática**. Tradução de Elcio Fernandes. São Paulo: Universidade Estadual Paulista, 1991. p.187.

de inteligência artificial. Exemplo marcante dessa política foi à implantação por parte da força aérea norte-americana, em 1955, do Semi-Automatic Ground Environment System – SAGE, um sistema de defesa aérea que de forma inédita possuía a capacidade de detectar, avaliar e responder em tempo real agressões aéreas, através da utilização de computadores interligados.

Entretanto, o ponto de contribuição marcante desse período, além do aprimoramento dos computadores, como máquinas aptas a exercerem várias funções, foi o lançamento em 1957, pelos soviéticos, do primeiro satélite artificial, o Sputnick. A luta pela conquista espacial forçou os Estados Unidos, por intermédio do Pentágono, a criar uma agência que estruturasse, fiscalizasse e coordenasse os contratos de pesquisas federais. Surgiu assim a Defense Advanced Research Projects Agency – DARPA, instituição que no exercício de suas atribuições influenciou de forma única, como adiante se verá, o surgimento de um dos maiores ícones da sociedade da informação, a *INTERNET*.

No mesmo ano, 1957, outros dois engenheiros: Jack Kilby, da *Texas Instruments*, e Bob Noyce (fundador da INTEL) impulsionaram o campo da microeletrônica com a invenção do Circuito Integrado, cuja explosão tecnológica intensificou-se durante a década de 1960, quando o design dos chips foi aprimorado, permitindo o desenvolvimento de circuitos integrados cada vez mais rápidos, eficientes, menores e baratos.

Ainda sob influência do efeito "Sputinck", o pentágono e a *National Aeronautics and Space Administration* – NASA –, fundada em 1958, passaram a subsidiar pesquisas científicas ligadas a área de tecnologia militar. Esse tipo de subsídio foi um dos principais motores do desenvolvimento da indústria eletrônica norte americana e permitiu que em 1964, a empresa *International Business Machines* – IBM – criada pelo engenheiro americano Hermam Hollerrith, aproveitasse a tecnologia desenvolvida e dominasse a incipiente indústria de computadores com o desenvolvimento seu modelo *Mainframe 360/37.* Dando seqüência ao processo de aprimoramento e desenvolvimento de novas tecnologias, em 1969, *a Bell Laboratories,* empresa vinculada à AT&T produziu, industrialmente, o primeiro computador eletrônico, o ESS-1, que utilizava o sistema operacional UNIX.

O continuo desenvolvimento dos computadores e dos sistemas eletrônicos se consolidou durante a década de 1970, período em que a Guerra Fria começou a dar sinais de declínio e que é considerado por Castells como o ponto de mutação que levou ao desenvolvimento da

Sociedade Informacional. A raiz da Revolução da Tecnologia da Informação selou-se nos Estados Unidos, uma vez que, a fonte tecnológica mais notória do mundo surgiu no Vale do Silício, localizado no condado de Santa Clara, 48 km ao sul de São Francisco, entre Stanford e San Jose. Tal região foi o centro das inovações eletrônicas no setor de tecnologias de informação.

> O Vale do Silício foi transformado em meio de inovação pela convergência de vários fatores, atuando no mesmo local: novos conhecimentos tecnológicos; um grande grupo de engenheiros e cientistas talentosos das principais universidades da área; fundos generosos vindos de um mercado garantido e do Departamento de Defesa; e, nos primeiros estágios, liderança institucional da Universidade de Stanford.[18]

Foi justamente do Vale do Silício que, em 1971, a difusão da microeletrônica dilatou-se intensamente. Nesse ano, o engenheiro da INTEL, Ted Hoff, conseguiu estruturar em um único chip todos os componentes necessários ao processamento de dados e informações, criando assim, o microprocessador, ou seja, um computador em um único chip. Este componente foi o responsável pela pulverização da informática em todos os nichos imagináveis, desde as atividades mais cotidianas as mais complexas. A microeletrônica potencializou de forma vertiginosa a capacidade da computação em agilidade, eficácia, flexibilidade, economia, mais ainda, permitiu a substituição do computador analógico pelo computador digital.

Em 1975, Ed Roberts, procurando desenvolver ferramentas eletrônicas para uma empresa japonesa de máquinas de calcular, construiu o *Altair*, um computador de pequena escala, quase artesanal, que era equipado com um microprocessador. Em seguida, 1976, Steve Wozniac e Steve Jobs, através da *Apple Computers*, tomando como modelo o *Altair*, idealizaram e desenvolveram o primeiro microcomputador de sucesso comercial, e um marco da difusão da informática na sociedade, o *Aplle I*.

O avanço tecnológico, especificamente, na seara computacional, fez surgir algumas demandas específicas. As antigas máquinas de calcular eletrônicas foram substituídas por equipamentos capazes de processar uma gama variada de informações, entretanto, para que pudesse realizar essas tarefas, os computadores necessitavam de instruções que ordenassem e organizassem as operações a serem processadas. Surgiu a necessidade de uma ferramenta que

[18] CASTELLS, Manuel, op. cit., 1999. p.71.

permitisse ao usuário controlar e organizar de acordo com seus objetivos as atividades de processamento que os computadores realizavam. Nasceu a idéia do *software*.

O surgimento do *software* está ligado à adaptação realizada por Bill Gates e Paul Allen do *Beginner´s All-purpose Symbolic Instructions Code* – BASIC (Código de Instrução Simbólica de Propósito Geral para Iniciantes), que foi desenvolvido para operacionalizar o *Altair 8800*. Além de servir para organizar as atividades básicas de funcionamento e processamento de um computador, os *software*s passaram a potencializar a utilização dos microcomputadores, permitindo que os mesmo passassem a desenvolver inúmeras outras funções. Ressalte-se que percebendo a potencialidade do instrumento desenvolvido, Gates e Allen fundaram a *Microsoft Corporation*, hoje multinacional que domina o mercado de *softwares*.

A difusão da microeletrônica e a potencialização dos sistemas eletrônicos através da utilização de *softwares* configuram-se como marcos propulsores do desenvolvimento técnico que fomentaram o avanço da tecnologia da informação na estrutura social. Esse avanço ganhou contornos estáveis e moldes quase que definitivos, quando, com o surgimento de novas tecnologias opteletrônicas (fibras ópticas e *lasers*) se possibilitou o aumento da capacidade dos computadores funcionarem interligados, formando redes eletrônicas cada vez mais ágeis e capazes de transportar maiores quantidades de informação.

Aproveitando o intenso desenvolvimento tecnológico dos anos 70, a década de 80 foi palco da irradiação das tecnologias da informação para as mais diversas aplicações. Iniciou-se nesse momento, o período de popularização das novas tecnologias. Nessa época a Guerra Fria, já em franco declínio, ocasionou ainda investimentos vultosos por parte dos Estados Unidos no desenvolvimento de novas tecnologias bélicas que se vinculavam diretamente ao desenvolvimento de novas ferramentas, componentes e estruturas eletrônicas ligadas ao tratamento e distribuição de informações. Exemplo cabal dessa postura foi a imposição de inúmeras sanções econômicas à União Soviética, bem como o retorno ao desenvolvimento de uma política armamentista tecnológica materializada no visionário projeto Guerra nas Estrelas.

Afora as perspectivas militares, em 1981, a *IBM*, procurando contra-atacar o sucesso da *Apple*, lançou o que viria a ser um dos maiores marcos da história da computação: o *Personal*

Computer (PC) – (Computador Pessoal), que nas palavras de Carvalho "nascia bastante limitado, com 64 Kbytes de memória e um único acionador de disquetes, porém era uma revolução em comparação com os equipamentos disponíveis até então[19]". Na mesma onda evolutiva, aproveitando-se do sucesso da *IBM*, a *Microsoft* aceitou o desafio de desenvolver o sistema operacional a ser utilizado no PC. Assim, contratou Tim Paterson, o engenheiro-chefe de uma empresa de Seattle e seguindo as orientações estabelecidas pela *IBM* desenvolveu um sistema operacional relativamente fácil de ser operado, nascia o Sistema Operacional de Disco da *Microsoft*, o MS-DOS.

Na primavera de 1983, a *IBM* lançou o PC/XT, seu primeiro microcomputador com disco rígido, cuja capacidade de armazenagem era de dez megabytes de informação. No mesmo ano, a *Microsoft* levou a computação gráfica para o IBM/PC através de um produto chamado *Windows*. O objetivo era criar um *software* capaz de ampliar o MS-DOS e através do uso do *mouse*, tornar a utilização do computador mais prática e ágil, ou seja, conferir o máximo de acessibilidade aos recursos disponibilizados pela máquina. A concepção inovadora do *Windows* permitiu que de forma revolucionária o usuário do computador pudesse acessar e utilizar diversos recursos do computador ao mesmo tempo, através da utilização de janelas independentes.

A busca pelo desenvolvimento de instrumentos que facilitassem o acesso às vantagens das novas tecnologias não cessou, e em 1984, apoiando-se nas pesquisas desenvolvidas pelo Centro Palo Alto da *Xerox Corporation*, a *Apple* lançou a tecnologia de interação entre usuário e computador baseada em ícones e potencializou a interface da máquina através do *Machintosh*.

A partir de então a popularização da informática e dos sistemas eletrônicos foi inevitável. A crescente evolução da informática rumou para três pontos importantes: O primeiro ponto foi a necessidade de aumentar as performances técnicas dos computadores através de mecanismos que reduzissem custos, tornando os computadores mais acessíveis. Nesse momento específico da evolução dos computadores ganha importância a Nanotecnologia, que permitiu a miniaturização de componentes importantes como, por exemplo, os processadores, que hoje podem possuir dois núcleos de processamento em um

[19] CARVALHO, Ademir. **Centro de informações:** a descentralização da informática. São Paulo: Érica, 1991. p.3.

único processador, o que traz ganho de eficiência, redução de espaço físico e do consumo de energia. Pode-se agregar ainda a evolução das memórias internas, as chamadas memórias *RAM* e *ROM*, bem como o aumento da capacidade de armazenamento de informações no chamado *Hard Disk* – HD, ou discos rígidos, que hoje beiram a casa dos gigabytes.

O segundo ponto foi justamente a necessidade de tornar o computador um equipamento de fácil manuseio, ou seja, o usuário deveria poder ser uma pessoa que carecesse de conhecimentos técnicos especializados para tal fim. Exemplos de luta pela "desmistificação" do uso do computador e dos sistemas eletrônicos vão desde a criação de *softwares* mais simples e dotados de ferramentas de ajuda, até o desenvolvimento de equipamentos como o mouse que propiciaram maior mobilidade e facilidade de manuseio dos comandos necessários à operação dos sistemas eletrônicos.

O terceiro foi a necessidade de potencializar o alcance da informática e dos sistemas eletrônicos através da utilização das estruturas de telecomunicação, o que possibilitaria a formação de redes de computadores ou redes eletrônicas e permitiu o surgimento da *Internet*, aspecto que será abordado no subtópico seguinte.

A conjugação desses três pontos, bem como a adoção de um novo modelo de desenvolvimento capitalista focado na informação permitiu o surgimento de um novo paradigma social.

1.1.2 A internet e a sociedade em rede

Apesar de parecer ter surgido da simples conexão espontânea de computadores, a *Internet* não se desenvolveu do nada. Trata-se do fruto de um planejamento estratégico que remonta a década de 60. Ameaçado pelo véu da Guerra Fria, e temeroso de ataques militares oriundos do bloco soviético, o governo norte-americano, através do Departamento de Defesa, fomentou o projeto ARPANET, que foi criado e desenvolvido pela *Advanced Research Projects Agency* – Rede de Agência de Projetos de Pesquisa Avançada – (ARPA).

Consistia o Projeto ARPANET em uma rede de comunicação entre computadores visando à troca de informações para que, no caso de destruição de uma máquina, estas não fossem perdidas. De forma singela caracterizava-se como uma série de pequenas redes de computadores locais interligados com redes regionais que se comunicavam entre si, criando desta feita uma rede nacional que impedia, no caso de ataques soviéticos, que a rede de comando dos Estados Unidos fossem interrompida. Ademais, se evitava a concentração de informações vitais em uma única máquina, o que tornava o sistema de defesa ianque bastante vulnerável.

> Nas origens da *Internet* está o trabalho de uma das instituições e pesquisa mais inovadoras do mundo: a Agência de Projetos de Pesquisa Avançada do Departamento de Defesa dos Estados Unidos (DARPA). Quando, no final dos anos 50, o lançamento do primeiro Sputnik alarmou o *establishment* militar norte-americano de alta tecnologia, a DARPA assumiu varias iniciativas ousadas, algumas das quais mudaram a história da tecnologia e estabeleceram a era da informação em grande escala. Uma dessas estratégias, que desenvolvia uma idéia concebida por Paul Baran da Rand Corporation, era projetar um sistema de comunicação invulnerável a ataque nuclear. Com base na tecnologia de comunicação por comutação de pacotes, o sistema tornou a rede independente de centros de comando e controle, de modo que as unidades de mensagens encontrariam suas rotas ao longo da rede, sendo remontadas com sentido coerente em qualquer ponto dela.[20]

Dessa forma, a ARPANET, em 1969, permitiu a comunicação efetiva e descentralizada entre os vários centros militares considerados estratégicos na estrutura militar norte-americana. Mais ainda, os vários centros de pesquisa vinculados à DARPA ou que cooperavam como Departamento de Defesa dos Estados Unidos passaram a ter acesso à rede de informações e passaram a utilizá-la para todos os tipos de comunicações. Em determinado momento, ficou impossível distinguir o conteúdo das comunicações, que inicialmente deveriam ser restritas às pesquisas militares, das conversações científicas e até mesmo dos assuntos voltados a interesses pessoais.

Assim, com o acesso quase que irrestrito dos cientistas à rede, a DARPA optou por cindi-la. Surgiram assim a ARPANET, ligada aos objetivos científicos e as universidades, e a MILNET, focada na comunicação e nos aplicativos militares. No mesmo período, por volta dos anos 80, a Fundação Nacional de Pesquisa norte americana aproveitando a estrutura existente decidiu financiar a criação de outras duas redes de comunicação entre computadores. Uma voltada para a comunidade científica, a CSNET, e outra desenvolvida através de uma parceria com a *IBM* que se voltava para comunidades estudiosas de matérias não científicas, a

[20] CASTELLS, Manuel, op. cit.,1999. p.375.

BITNET. Deve-se ressaltar que todas essas redes de computadores usavam como sistema de comunicação a ARPANET. A junção de todas essas redes deu origem a chamada ARPA-*INTERNET* que posteriormente passou a ser chamada de Internet, mas que continuava vinculada ao Departamento de Defesa norte americano, órgão responsável pelo seu financiamento, e à Fundação Nacional da Ciência, a quem cabia a sua operação.

Deve-se frisar, entretanto, que no início, o acesso à rede ARPANET, era reservado somente as redes de computadores das universidades científicas consideradas de elite, o que deixava uma grande parte de pesquisadores sem acesso às facilidades decorrente de seu uso. Aproveitando a invenção do *modem*[21], um pequeno equipamento que passou a permitir "que computadores transferissem arquivos diretamente sem passar por um sistema principal" utilizando-se de uma linha telefônica, outras universidades começaram a estrutura pequenas redes, que sem usar o suporte da ARPANET passaram a se comunicar e criaram a Usenet. Esta rede serviu de exemplo para a criação de inúmeras redes computacionais de pequeno porte que se intercomunicavam. Posteriormente, a junção de todas essas pequenas redes deu origem a *Internet*.

Em meados de 1990, o projeto ARPANET foi desativado. Contudo a semente da Internet já tinha sido plantada. Percebendo o enorme potencial oferecido por esse meio de comunicação, as Universidades norte americanas aproveitaram a estrutura existente e interligaram-se, formando assim uma rede nacional de troca de informações científicas, uma vez que, os custos de uso da *Internet* para o envio de informações escritas eram muito menos onerosos do que os dos meios então existentes. Em face das facilidades e dos baixos custos, a rede que interligava as universidades americanas se expandiu para fora dos limites dos Estados Unidos e acabou tomando um caráter mundial, passando a servir de elo de comunicação entre meios acadêmicos de todo o mundo.

O primeiro passo para a expansão da rede foi o surgimento do *Internetting Project* em 1973. Esse projeto visava à criação de um sistema que interligasse todas as redes locais até então existentes. Era necessária a criação de uma ferramenta que possibilitasse a interconexão das diversas redes, tal fato não era tão simples, uma vez que os sistemas de computadores

[21] O *modem* foi inventado por dois estudantes de Chigago, Ward Christnsen e Randy Suess, em 1978, quando tentavam encontrar um sistema para transferir programas de um microcomputador ao outro via telefone, a fim de evitar uma longa viajem entre suas localizações durante o inverno de Chicago. CASTELLS, Manuel, op. cit., 1999. p.377.

existentes eram formados por máquinas diferentes bem como utilizavam *softwares* distintos, dificultando assim a troca de informações. Esse obstáculo foi transposto em 1974 com o desenvolvimento do Protocolo de comunicação TCP/IP. O *Transmission Control Protocol/Internet Protocol*, criado por Robert Kanh, foi utilizado como sistema base de interligação entre computadores de diferentes modelos[22]. O TCP/IP funciona como um elo entre as máquinas, ou seja, um dialeto comum, uma espécie de acordo que permite a comunicação e o processamento das informações trocadas.

> A capacidade de comunicação não era suficiente para estabelecer uma rede mundial. Os computadores precisavam ser capazes de conversar entre si. O obstáculo foi superado com a criação do UNIX, sistema operacional que permitia o acesso de computador a computador. Esse sistema foi inventado pela Bell Laboratories em 1969, mas sua utilização ampliou-se apenas após 1983, quando pesquisadores de Berkley (novamente com fundos da ARPA) adaptaram ao UNIX o protocolo TCP/IP com isso, os computadores puderam não apenas comunicar, mas também codificar e decodificar pacotes de dados que viajavam em alta velocidade na Internet. Como a nova versão do UNIX foi financiada com recursos públicos, o *software* foi disponibilizado apenas pelo custo de distribuição. O sistema de redes surgiu em grande escala como redes locais e redes regionais conectadas entre si e começou a se expandir para qualquer lugar onde houvesse linhas telefônicas e computadores munidos dos equipamentos baratos chamados modens.[23]

O segundo elemento que levou a expansão da *Internet* foi o desenvolvimento da *"World Wide Web (WWW ou W3).* Criada em 1989 no Laboratório Europeu de Física e Altas energias, caracteriza-se por ser composta de hipertextos, que são documentos (textos, imagens ou sons) que se manifestam de maneira particular, podendo se inter-relacionar com outros documentos. Isto tornou simples a utilização e o acesso a serviços e informações, uma vez que o usuário não precisa conhecer os vários protocolos de acesso, mas tão simplesmente clicar seu *mouse.*

Contudo, até então a *Internet* resumia-se a uma grande rede de intercomunicação de meios acadêmicos, não despertando interesse por parte de investidores. A maioria dos autores especializados pré-estabelece como um dos fatores determinantes para que a *Internet* chegasse aos patamares atuais, foi o desenvolvimento dos *Browsers* – Folheadores. Um *Browser*, batizado no Brasil de Navegador, é um programa que permite a reprodução de imagens, textos

---

[22] "Unida através de uma linguagem comum ou protocolo, a Internet permite aos usuários individuais que interajam, a seu modo, com qualquer outra rede ou usuário individual que seja também parte do sistema. Ou seja, a Internet é uma rede de computadores que fala a mesma língua, o protocolo IP. [...] As mensagens e comandos são transformados, em seu ponto de origem em pacotes de informações, cada qual com seu próprio endereço e instruções de destino, e assim transmitidos através de redes interligadas, para serem remontados no destinatário. Computadores especializados mandam cada pacote de maneira progressiva, selecionando o caminho menos congestionado". KAMINSKI**,** Omar. Aspectos jurídicos que envolvem a rede das redes. In: _____ (Org.). **Internet legal –** O Direito na tecnologia da informação: Doutrina e jurisprudência. Curitiba: Júrua, 2007. p.37.

ou sons armazenados em outros computadores a muitas centenas de quilômetros de distância. A principal revolução inserida por este *software* foi que com a sua utilização pode-se passar de uma página para a outra sem a necessidade de conhecimentos técnicos acurados. Esses programas foram os principais facilitadores da utilização da Rede pelos usuários domésticos, sendo que o primeiro foi criado em 1993 no Centro Nacional de Aplicações para Supercomputadores da Universidade de Illianois, localizada nos Estados Unidos.

A junção desses três fatores, associados à própria natureza da *Internet* fomentou o processo de desenvolvimento explosivo que impactou de forma definitiva a sociedade. As maiores economias mundiais vêem a *Internet*, o Ciberespaço, como um campo extremamente fértil para o desenvolvimento econômico, uma vez que se trata de um sistema ágil e em grande expansão. O poder de crescimento da rede e sua capacidade de auto expansão ficam evidentes quando se traça um paralelo entre a *Internet* e a energia elétrica:

> Veio surgindo então um sistema ágil e interativo de acesso a informações como jamais visto anteriormente, que trouxe um novo modo de distribuição de riquezas e de produção completamente diferenciado dos métodos até então conhecidos. Exatamente quando essa revolução começou é de difícil precisão, porque sempre ficará a dúvida se foi com a expansão dos microcomputadores ou se com o surgimento do primeiro programa que facilitava a navegação pelas páginas da WEB. O que podemos conferir é que 5 anos depois do lançamento do primeiro provedor de acesso à *Internet* nos Estados Unidos, 40% das casas americanas estavam conectadas à rede. Se olharmos para trás, vamos ver que fora m necessários 35 anos, à partir do surgimento da primeira usina geradora de energia para que 40% das residências norte americanas desfrutassem da luz elétrica.[24]

O impacto da *Internet* na estrutura da sociedade ainda não pode ser avaliado de forma segura. A sua utilização comercial ainda não completou 20 anos. Contudo algumas conseqüências são facilmente percebidas. Gilberto Dupas afirma que "as tecnologias da informação encolhem o espaço. As diversas 'teles' anulam distâncias, desmaterializando os encontros" [25].

> O planeta encolhe. Foram precisos três anos para que Magellan desse a volta ao mundo por mar (1519-1522). Eram necessários ainda 80 dias para que um intrépido viajante do século XIX, utilizando estradas, trem e navegação a vapor, desse a volta ao mundo. No final do século XX, o avião à jato circunda-o em 24 horas. E, principalmente, tudo está instantaneamente presente, de um ponto do planeta ao outro, pela televisão, telefone, fax, *Internet*...[26]

---

[23] CASTELLS, Manuel, op. cit., 1999. p.376.
[24] BRASIL, Angela Bittencourt. **Informática jurídica:** O ciber direito. Rio de Janeiro: Juris Doctor, 2000. p.21.
[25] DUPAS, Gilberto. **Ética e poder na sociedade da informação –** De como a autonomia das novas tecnologias obriga a rever o mito do progresso. São Paulo: UNESP, 2000. p.56.
[26] MORIN, Edgard. **Os sete saberes necessários à educação do futuro.** Tradução de Catarina Eleonora F. da Silva. 11. ed. São Paulo: Cortez, 2006. p.67.

Fortalecendo essa constatação Eduardo Matias faz um paralelo bastante interessante:

> A tecnologia da informação teria diminuído a relevância não apenas do problema dos custos, mas também da questão do tempo e da distância. Por volta de 1830, uma carta postada na Inglaterra levava entre cinco e oito meses para chegar à Índia, e uma troca de correspondências poderia levar até dois anos, caso fosse afetada pela estação das monções. Hoje, a mesma comunicação dá instantaneamente, por correio eletrônico. A natureza das comunicações modernas permitiria assim aniquilar a distância e os limites territoriais como barreiras à atividade econômica. O ciberespaço poderia ser comparado a um oceano, que margeia os países, cidades e lares do mundo, permitindo uma navegação virtual e instantânea entre eles.[27]

Essa talvez seja a mais visível e palpável das transformações causada pela *Internet*: o rompimento dos obstáculos de tempo e de espaço. As distâncias, as noções de espaço, de território, são pulverizadas pela estrutura capilar da rede. As informações circulam sem obedecerem às fronteiras ou obstáculos físicos, como a distância entre os sistemas eletrônicos que se comunicam.

A rede de computadores virtualmente interligados gera uma espécie de Ágora virtualizada, claro que dissociada dos fins exclusivamente políticos, e permite o surgimento de um espaço propicio à difusão de idéias e a troca de opiniões. Manuel Castells sustenta que: "As novas tecnologias da informação estão integrando o mundo em redes globais de instrumentalidade. A comunicação mediada por computadores gera uma gama enorme de comunidades virtuais" [28]. Atestando o grau de inserção atual da *Internet*, Benedito Hespanha [29] expõe que:

> [...] a *Internet* se tornou foro comum e universal de troca de idéias, de pesquisas, de estudos, e de conhecimentos mais céleres e variados; além disso, os sistemas de rede de computadores possuem estrutura técnica adequada que assegura entre os povos o fomento de relações públicas, políticas e privadas mais estreitas e, afinal, incentiva a melhoria da qualidade da vida social e dos serviços prestados às sociedades nos setores econômico, fiscal comercial, cultural e universitário, especialmente no uso de uma nova metodologia para a produção científica de conhecimentos mais sólidos.

Essa interconexão social causada pela *Internet* funde-se a capacidade da rede de fomentar de maneira prática a produção, a difusão e o acesso à informação. A conjugação dessas duas características permitiu de forma única o desenvolvimento e o fortalecimento do que Castells denominou de modo de produção informacional. O acesso à informação passou a

---

[27] MATIAS, Eduardo Felipe P. **A humanidade e suas fronteiras** – do Estado soberano à sociedade global. São Paulo: Paz e Terra, 2005. p.118.
[28] CASTELLS, Manuel, op. cit., 1999. 1v. p.38.
[29] HESPANHA, Benedito. O poder normativo da internet e a regulamentação dos crimes virtuais: uma análise crítica à legislação penal brasileira. **Justiça do Direito,** Rio Grande do Sul, v. 1, n. 16, p.29-64, 2002. p.49.

ser considerado como acesso ao poder. A detenção dos mecanismos de produção, difusão e de acesso à informação são consideradas ferramentas econômica e politicamente valiosas. A mudança estrutural causada na organização social ocasionada pela terceira revolução tecnológica, cujo principal símbolo é a *Internet*, configura-se como um paradigma que reestruturou o contexto social mundial, a sociedade hoje é uma rede:

> Rede, como espaço, é a palavra chave. Aparece na maioria das disciplinas, alimenta metáforas, perde em precisão o que ganha em extensão. O homem contemporâneo está preso cada vez mais no universo das redes; suas práticas, seu modo de vida são modificados a partir disso, o exterior é introduzido e acolhido pela máquina de comunicar.[30]

Essa nova sociedade interligada por redes eletrônicas conjuga estruturas e valores pautados na informação. Esse novo contexto informacional figura como um ponto de ruptura capaz de estabelecer as condições que moldam as relações sociais e econômicas atuais, ou seja, configura-se como um paradigma estrutural da sociedade moderna: o paradigma informacional.

1.1.3 O paradigma informacional

O contexto social atual modificou-se drasticamente. Os valores estruturantes da organização econômica e social ganharam novos contornos. O desenvolvimento tecnológico incorporou-se de forma indissociável das estruturas sociais, mais ainda, da vida. Muitas modificações ocorreram, e ainda estão em curso:

> [...] nós mesmos mudamos de tal forma que não nos reconhecemos, pois não conseguimos mais viver sem muletas tecnológicas. Estou falando do celular, do e-mail, do editor de textos, do micro [...] sem falar de todas as novidades, controles e facilidades que a tecnologia introduziu no dia-a-dia da vida das pessoas em geral.[31]

Essa inserção da tecnologia no cotidiano social não se deu de forma abrupta, mas sim de forma paulatina, fruto de um movimento evolutivo que historicamente demonstra que os parâmetros sociais para a aferição do grau de riqueza e de poder das estruturas sociais, pautaram-se em vários elementos como a terra, os metais, os escravos, os exércitos e as indústrias. Hoje, o vetor tecnológico, especificamente, o campo ligado à informação desponta como o novo elemento a fundamentar a construção de vínculos produtivos e sociais.

---

[30] DUPAS, Gilberto, op. cit., 2000. p.77.
[31] ROVER, Aires José (Org.). **Direito e informática**. Barueri: Manoele, 2004. p.XII.

> A sociedade está sob o 'choque informático': as suas estruturas econômicas, sociais e culturais serão profundamente abaladas. Haverá uma reestruturação industrial, um reordenamento social, uma mutação cultural. Mais ainda: serão afetados os hábitos, os conhecimentos, as competências, o universo cultural e mesmo a razão de ser dos indivíduos.[32]

A análise desse processo de transformação social tem seu marco inicial na Revolução Industrial. Esse processo de "tecnificação do mundo e de cientificação das atividades sociais"[33] se deu através de três etapas: em um primeiro momento os avanços tecnológicos permitiram o desenvolvimento de máquinas e artefatos que potencializassem a capacidade do homem de explorar os recursos encontrados na natureza. O segundo momento é nitidamente marcado pela conjugação de dois fatores: desenvolvimento de novos ramos do conhecimento científico, como a química e a física, que propiciaram a descoberta e o desenvolvimento de tecnologias e instrumentos revolucionários como, por exemplo, a eletricidade; e a estruturação do sistema fabril, que otimizando as práticas de produção rompeu as barreiras da produtividade manual. A derradeira etapa caracteriza-se pelo desenvolvimento de mecanismos que permitem a automação da estrutura fabril e pelo surgimento de tecnologias que sejam capazes de formular mecanismos e instrumentos programáveis.

Reforçando essa análise, Poliana Delpupo expõe o pensamento de Alvin Tofler sobre o processo evolutivo social:

> O autor [...] chama de onda o conjunto de diversos fatores, principalmente de ordem econômica, que produzem transformações substanciais numa sociedade.
> A Primeira Onda fornece recursos agrícolas e minerais e a Segunda Onda denominada industrial, fornece mão-de-obra para suprir as necessidades do consumo de massa, e o setor da Terceira Onda cria e explora conhecimentos. O trabalho braçal vai sendo substituído pelo trabalho intelectual. Os conhecimentos não são só produzidos como também comercializados. Os países da Terceira Onda vendem ao mundo os produtos mais sofisticados da atualidade: informação, cultura, inovações, diversão, tecnologia de ponta, educação, *software*, administração, assistência médica e financeira e muitos outros serviços.[34]

O aumento da importância dos sistemas eletrônicos no contexto estrutural da sociedade moderna demonstra a ocorrência de uma nova revolução mundial. Entretanto, diferindo das anteriores, não se trata de uma revolução tecnológica fundada nos mesmos padrões nos quais

---

[32] BENAKOUCHE, Rabah. O choque informático. In: _____ (Org.). **A informática e o Brasil**. São Paulo: Polis, 1985. p.07.
[33] FERNANDES**,** Ângela Silva et al. Tecnologia e comunicação. In: Antônio Miranda; Elmira Simeão (Org.). **Informação e Tecnologia:** Conceitos e recortes. Brasília: Universidade de Brasília, Departamento de Ciência da Informação e Documentação, 2005. p.24.
[34] DELPUPO, Poliana Moreira. O consumo na Internet e a responsabilidade civil do provedor. In: ROVER**,** Aires José (Org.). **Direito e informática**. Barueri: Manoele, 2004. p.324.

se fundaram a primeira e a segunda revolução tecnológica industrial. Trata-se na verdade de "uma revolução muito mais profunda, qualificada de escritural, e comparável a aparição do alfabeto ou ainda à invenção da imprensa".[35]

Assim, nesse novo estágio de desenvolvimento social, a energia, enquanto fator elementar das duas etapas anteriores de desenvolvimento tecnológico (vapor e eletricidade), é substituída por um novo vetor, os sistemas de informação. A informação passa a ser o novo eixo do mundo, englobando aspectos econômicos e sociais, caracterizando-se como parâmetro, unidade, elemento balizador da sociedade.

Analisando o assunto Castells afirma que os contornos da atual revolução tecnológica não se fundam na centralização de conhecimentos e informações, mas na "aplicação desses conhecimentos e dessa informação para a geração de conhecimento e de dispositivos de processamento/comunicação da informação, em um ciclo de realimentação cumulativo entre inovação e o uso[36]".

O impacto da informação na contextualização de um novo modelo social foi antevisto por Norbert Wierner na década de 50:

> A tese dêste livro é a de que a sociedade só pode ser compreendida através de um estudo das mensagens e das facilidades de comunicação de que disponha; e de que, no futuro o desenvolvimento dessas mensagens e facilidades de comunicação, as mensagens entre o homem e as máquinas, entre as máquinas e o homem, e entre a máquina e a máquina, estão destinadas a desempenhar papel cada vez mais importante.[37]

O visionário matemático norte americano verificando o estado de efevercência científica criado pelo estado beligerante decorrente da divisão mundial bipartida, que nas relações sociais e na estruturação da sociedade moderna, percebeu que a informação teria papel cada vez mais significativo. Vale salientar que o mais interessante é que as previsões de Wierner se ligam ao desenvolvimento de máquinas capazes de coletar, utilizar, estocar, transmitir e tratar informações.

---

[35] MATIAS, Eduardo Felipe P., op. cit., 2005. p.117.
[36] CASTELLS, Manuel, op. cit., 1999. 1v. p.51.
[37] WIERNER, Norbert. **Cibernética e sociedade** – O uso humano de seres humanos. São Paulo: Cultrix, 1950. p.16.

O estudo do impacto da adoção desse novo modelo econômico-social pautado na informação deu margem ao surgimento das chamadas “teorias da sociedade da informação”. Estas teorias fundam-se na idéia de que as mudanças ocorridas nas sociedades contemporâneas tiveram como causa a valorização do papel da informação e da comunicação nas relações sociais e econômicas.

Dentre as correntes de pensamento que analisam o papel da informação no contexto social atual ganham destaque duas posições. A primeira congrega autores que sustentam que a situação atual configura um momento de ruptura estrutural de paradigma nos mais variados campos sociais. Trata-se de uma mudança radical de parâmetro, de uma nova etapa do processo evolutivo social que fomentou o surgimento de um novo tipo de sociedade, a “sociedade da informação”.

O segundo grupo de analistas assevera que as mudanças que ocorreram não se concretizaram em rupturas como os modos de organização social e econômico existentes. No máximo seriam evoluções de um contexto já previamente definido.

O atual nível de influência da informação nos mecanismos de organização econômica, social e cultural demonstra de forma clara que hoje o parâmetro de organização das relações sociais funda-se no âmbito informacional. A ruptura causada pela adoção desse novo modelo configura-se necessariamente um ponto de esfacelamento dos moldes sociais de organização passados. Hoje, a sociedade é nitidamente informacional, baseada na importância estratégica, econômica e política da informação. Produzir, tratar e armazenar dados e informações, ou seja, controlar o fluxo informacional significa possuir o mecanismo atual de dominação. Informação é poder.

Esse novo paradigma estrutural da sociedade, segundo Castells, possui cinco características. O primeiro elemento do paradigma da sociedade da informação repousa no papel da informação enquanto elemento fundador dessa nova ordem social. A informação caracteriza-se como sua matéria prima, seu elemento base, sua essência. Ressalte-se que o nexo entre o desenvolvimento tecnológico e a informação reside na idéia do desenvolvimento contínuo de mecanismos e ferramentas que potencializem o ciclo de produção e circulação de informações. A tecnologia torna-se um vetor do desenvolvimento informacional, apóia à construção de estruturas sociais e econômicas cada vez mais vinculadas a informação.

A segunda característica vincula-se ao alto grau de penetrabilidade da informação e de suas ferramentas tecnológicas nas atividades humanas. Dessa forma, as tecnologias associadas ao tratamento e informação, bem como relacionadas à comunicação de informações, quando não determinam as atividades humanas e os processos sociais individuais e coletivos exercem forte influência na sua contextualização.

O terceiro ponto estabelecido repousa na construção de uma sociedade regida e organizada pela lógica das redes. "As redes formam um novo tecido tecno-social, decorrente dessa multiplicidade de canais e das múltiplas possibilidades de interação social.[38]". A idéia de rede fomenta o fortalecimento da idéia de conexão, conectividade, globalidade, globalização, o surgimento do que se denomina de "aldeia global".

Vale salientar que a estrutura reticular, ou seja, de vários pontos que se interligam, se comunicam, através de inúmeras rotas ligadas por nós, pode ao mesmo tempo unificar e excluir, possibilitar a organização produtiva, ou o caos estéril.

> Redes constituem a nova morfologia social de nossas sociedades, e a difusão da lógica de redes modifica de forma substancial a operação e os resultados dos processos produtivos e de experiência, poder e cultura. [...] A presença na rede ou a ausência dela e a dinâmica de cada rede em relação às outras são fontes cruciais de dominação e transformação de nossa sociedade: uma sociedade que, portanto, podemos apropriadamente chamar de sociedade em rede, caracterizada pela primazia da morfologia social sobre a ação social.[39]

A flexibilidade das organizações e das instituições caracteriza-se como o quarto elemento que fundamenta o paradigma informacional. A maleabilidade da sociedade da informação permite que os processos e as estruturas sociais, em procedimentos reversíveis, possam ser alterados significativamente pela reorganização de seus componentes elementares.

Enfim, o último elemento característico fixa-se na convergência de elementos tecnológicos específicos para um sistema de produção e difusão de informação altamente integrado e difundido no contexto social.

---

[38] FERNADES, Ângela Silva et al., op. cit., 2005. p.25.
[39] SCHAFF, Adam. **A sociedade informática.** Tradução de Carlos Eduardo Jordão Machado e Luís Arturo Obojes. 4. ed. São Paulo: UNESP, 1995. p.100.

Esse novo formato de organização social pautado na importância multifocal da informação começou a se fortalecer no final da década de 60. A bipolarização mundial estava atingindo níveis críticos de tensão quando os líderes dos dois grandes pólos mundiais, Estados Unidos da América e União das Repúblicas Socialistas Soviéticas (URSS), iniciaram um processo de reaproximação movido pela celebração de inúmeros acordos bilaterais que buscavam dentre outros fins a minimização de conflitos bélicos nucleares.

Foi nesse contexto, "sob a sombra da tese dos fins, começando com o fim da ideologia, que foi incubada, ao longo da Guerra Fria, a idéia da sociedade da informação como alternativa aos dois sistemas antagônicos.[40]" Essa idéia começa a se fortalecer nos meios acadêmicos, econômicos e políticos no fim da década de 60, passando a ganhar força com o impulso fornecido pelo desenvolvimento tecnológico advindo do surgimento das primeiras máquinas "inteligentes" construídas no período da 2ª Guerra Mundial.

A derrocada do modelo socialista com o desaparecimento da União das Repúblicas Socialistas Soviéticas teve início com a abertura política e a reestruturação econômica realizadas por Mikhail Gorbachev. A dissolução da URSS e o surgimento da Comunidade de Estados Independentes em 1991 figura como o primeiro grande golpe na estrutura bipolar. Este acontecimento reforça a hegemonia dos Estados Unidos da América. A queda do muro de Berlim marcou o fim da Guerra Fria finalizando a dicotomia econômica e social existente.

O fim da bipolarização faz despontar um novo modelo de organização geopolítica. O mundo passa a ser organizado pelo modelo hegemônico norte-americano. Os Estados Unidos da América e sua economia capitalista passam a dominar o cenário mundial. O sistema capitalista passa a gerenciar o sistema de organização internacional impondo a nível global suas premissas básicas: trabalho assalariado, propriedade privada dos meios de produção e organização da atividade produtiva controlada pelo sistema de preços e focada na obtenção de lucro.

A consolidação do capitalismo como modelo econômico hegemônico ocasionou uma série de mudanças nas relações econômicas, sociais e políticas. Vale ressaltar que o

[40] MATTELART, Armand, op. cit., 2002. p.25.

desenvolvimento de novas tecnologias nas três décadas anteriores, principalmente na década de 70, potencializou essas mudanças.

> Desde os anos 60, o capitalismo ingressara numa nova fase de desenvolvimento, baseada numa dinâmica produtiva com sofisticada tecnologia. As suas bases principais eram a **microeletrônica** – que envolvia a computação, comunicações e robótica –, a **biotecnologia** e a **química fina**. Chamada por alguns de **Terceira Revolução Industrial**, a nova etapa produtiva passou a exigir ainda mais investimentos nas pesquisas e na implementação tecnológica, cuja viabilização passou a depender, principalmente, de **grandes conglomerados empresariais**, possuidores de enormes volumes de capitais. (grifos do autor)[41]

O avanço do desenvolvimento tecnológico, notadamente nos campos da microeletrônica e das telecomunicações, permitiu a construção das bases de uma nova sociedade focada no valor econômico e social da informação e tutelada por uma nova ordem política mundial organizada pelo paradigma informacional. Analisando a evolução da sociedade da informação, Matterlart afirma que o "paradigma tecnoinformacional tornou-se o pivô de um projeto geopolítico que tem como função garantir o rearranjo geoeconômico do planeta em torno dos valores da democracia de mercado e em um mundo unipolar"[42].

As mudanças decorrentes desse novo paradigma extrapolam o aspecto econômico e influência de forma profunda toda a sociedade, uma vez que alcançou todos os seus elementos estruturais:

> Não está longe o dia em que você poderá realizar negócios, estudar, explorar o mundo e suas culturas, assistir a um grande espetáculo, fazer amigos, freqüentar mercados da vizinhança e mostrar fotos a parentes distantes sem sair de sua escrivaninha ou de sua poltrona. Ao deixar o escritório ou sala de aula você não estará abandonando sua conexão com a rede. Ela será mais que um objeto que se carrega ou um aparelho que se compra. Será seu passaporte para uma nova forma de vida, intermediada.[43]

As palavras visionárias de Bill Gates em 1995 concretizam-se a cada instante. As atividades econômicas e sociais cotidianas materializam os efeitos do paradigma informacional de forma concreta. A adoção em larga escala das modernas inovações tecnológicas demonstra a influência da tecnologia e da informação na organização social atual, posto que até os relacionamentos interpessoais passam a ser marcadamente mediados pela via tecnológica, o meio eletrônico, o que de certa forma significa uma desmaterialização

---

[41] VICENTINO, Cláudio. **História geral**. 8. ed. São Paulo: Scipione, 1997. p.462.
[42] MATTELART, Armand, op. cit., 2002. p.139.
[43] GATES, Bill. **A estrada do futuro.** Tradução de Beth Vieira et al. São Paulo: Companhia das Letras, 1995. p.15.

do mundo social, a chamada virtualização das atividades e das realidades que Pierre Lévy estudou profundamente. "Os instrumentos informáticos penetraram de tal modo na sociedade que têm modificado não só nossa linguagem, mas também nosso estilo de vida, incidindo profundamente nos meios de comunicação e nas relações interindividuais" [44].

Nesse contexto verifica-se que o impacto do desenvolvimento de novas tecnologias e o desenvolvimento do potencial econômico da informação alteraram profundamente o modo de ser e de viver do ser humano. "O indivíduo é uma formação histórica ou, dito de outro modo, é um produto das relações sociais"[45], ou seja fruto, das influências da eleição de um novo binômio estrutural da sociedade: tecnologia e informação. Vale salientar que a influência do desenvolvimento tecnológico não atua somente sobre os indivíduos, a modificação dos parâmetros individuais e coletivos reflete a forma através da qual uma sociedade se relaciona com o desenvolvimento tecnológico informacional. Apesar de não ser fator determinante na evolução histórica, ou até na configuração de mecanismos de mudanças sociais, o desenvolvimento científico e tecnológico reflete um importante parâmetro da capacidade de transformação de determinada sociedade.

Analisando o contexto social surgido com o advento do paradigma da tecnologia da informação, Castells constrói uma teoria que procura compreender as transformações ocorridas nas formas de organização sociais modernas. No seu ponto de vista, surge uma nova forma de estruturação da sociedade, uma nova forma de organização social e econômica, a sociedade em rede, que reputa a construção de funções e processos sociais e produtivos pautados no valor da informação e na forma de redes.

> Redes constituem a nova morfologia social de nossas sociedades, e a difusão da lógica de redes modifica de forma substancial a operação e os resultados dos processos produtivos e de experiência, poder e cultura. [...] A presença na rede ou a ausência dela e a dinâmica de cada rede em relação às outras são fontes cruciais de dominação e transformação de nossa sociedade: uma sociedade que, portanto, podemos apropriadamente chamar de sociedade em rede, caracterizada pela primazia da morfologia social sobre a ação social.[46]

Apesar de ter seu contexto inicial restrito à sociedade norte americana nos anos 60, essa nova forma de organização sócio-econômica começou a ser difundida de forma paulatina até

---

[44] PAESANI, Liliane. **Direito de informática**. 3. ed. São Paulo: Atlas, 2006. p.17.
[45] SCHAFF, Adam, op. cit., 1995. p.100.
[46] CASTELLS, Manuel, op. cit., 1999. p.497.

se tornar o modelo hegemônico na geopolítica mundial. Um dos primeiros países a focar de forma concreta o estabelecimento de uma sociedade fundada economicamente e socialmente na tecnologia da informação foi o Japão. No início dos anos 70 a *Japan Computer Usage Development Intitute* (Jacudi) estabelece um plano de ações concretas que visava como meta para o ano 2000 à transformação da sociedade japonesa em uma sociedade da informação. Mattelart afirma que no contexto de transformação social japonês se destaca a existência de um cronograma dividido em quatro fases que permitiriam ao Japão se constituir como a primeira sociedade informacional da história.

> Essas fases se interpenetram: o primeiro período (1945-1970) é marcado pela predominância da megaciência e pelo sujeito país; o segundo (1955-1980), pela organização e pela empresa; o terceiro (1970-1990), pelos serviços sociais e pela sociedade; o último (1980-2000), pelos particulares e pelo ser humano.[47]

Apesar de ter estabelecido as bases estruturais da sociedade da informação na década de 60, especialmente no que tange ao desenvolvimento de tecnologias voltadas para o tratamento de informações, o governo norte americano tardou a desenvolver e implantar políticas sólidas que iniciassem o processo de transformação social informacional. A própria terminologia sociedade da informação só passa a ser utilizada no mesmo período em que o Japão oficialmente estabelece como meta o alcance da sociedade informacional. Nesse contexto a *Defense Adavnced Research Projects Agency* – DARPA volta a ter papel primordial no desenvolvimento dos mecanismos tecnológicos que darão suporte ao processo de busca pela sociedade da informação. Assim, os sistemas e ferramentas de produção e controle do fluxo informacional, desenvolvidos nesse período, serão efetivamente colocados em prática somente na Guerra do Golfo[48].

Por volta de 1975, a Organização de Cooperação e de Desenvolvimento Econômico (OCDE), que até então congregava 24 dos países mais ricos do mundo, inicia um processo de discussão sobre a sociedade da informação, fomentando a pesquisa sobre o tema e conseqüente elaboração de estudos sobre o tema, passando assim, a difundir em nível internacional, a sociedade da informação. Algum tempo depois os ministros que formavam o conselho da Comunidade Européia passam a adotar a noção de sociedade informacional e a utilizam como um conceito base de um programa de desenvolvimento tecnológico e social, o *Forecasting and Assessment in the Field of Science and Techonology – FAST.*

---

[47] MATTELART, Armand, op. cit., 2002. p.109.
[48] MATTELART, Armand, op. cit., 2002. p.121.

Como resultado desse momento de reflexão científica sobre a sociedade da informação o relatório *The New World of Information Order*, publicado em 1977 pelo governo norte-americano, destacou uma questão fundamental para o desenvolvimento da sociedade da informação, e que ainda hoje consiste em um ponto fundamental a nortear a discussão sobre a sociedade informacional. O dilema repousa em três fatores importantes no contexto de organização da sociedade mediada pela informação. Como regular o aumento do fluxo informacional e manter as pessoas, a sociedade e o Estado seguros? Ou seja, como potencializar a produção e o livre fluxo de informações sem expor a perigo a intimidade e a privacidade das pessoas, o direito de propriedade dos dados e informações, e a segurança nacional.

Além dos aspectos tecnológicos estruturais que fomentaram o desenvolvimento das ferramentas de produção e manejo da informação enquanto fator econômico, as três questões acima explicitadas nortearam a discussão que estabeleceu as bases políticas para a implantação de políticas públicas que objetivassem o alcance da sociedade da informação.

Percebendo a formação de um novo contexto de organização social e econômico a Comunidade Européia, após a realização de estudos aprofundados e de um processo de ampla discussão política, publicou em 1987 o chamado "Livro Verde" sobre as comunicações. O estabelecimento desse conjunto de orientações e indicações políticas consistiu no primeiro passo concreto rumo a instituição da sociedade da informação pela Comunidade Européia. Seu objetivo básico era a formação de uma política pública unificada no que tangia às telecomunicações, elemento estrutural indispensável para a construção de um fluxo informacional. Como proposta básica, o Livro Verde da Comunidade Européia estabelecia a necessidade de extinção dos monopólios estatais sobre os meios de telecomunicações fomentando assim o surgimento de um mercado único de redes de informações. Esse novo cenário deveria ser balizado pela busca da liberalização, da plena concorrência e da busca pela prestação universal.

A partir de então, o processo de implantação da sociedade da informação passa a ser pauta da discussão dos encontros que envolvem as grandes potencias mundiais. Dessa forma o conceito de sociedade da informação passa ser difundido como um novo modelo de organização social e econômico capaz de tornar o mundo mais solidário, democrático e aberto, ou seja, propagou-se a idéia de um futuro tecnoinformacional afastado dos debates

cidadãos, mascarando-se assim sua origem: um reorganização conjuntural do capitalismo influenciada por uma nova construção geopolítica[49].

> No final de fevereiro de 1995, os paises mais ricos, no G7, ratificam em Bruxelas o conceito de global *society of information*, ao mesmo tempo que reiteram solenemente sua vontade de chegar o mais rápido possível à liberalização dos mercados das telecomunicações. Essa reunião de cúpula é a primeira consagrada a esse tema. Nela, Al Gore pronuncia um discurso sobre a Promessa de uma nova ordem mundial da informação. Para construir as infra-estruturas informacionais, recorre-se à iniciativa do setor privado e às virtudes do mercado.[...] Em julho de 1997, o presidente Clinton expõe a doutrina de Washington sobre o comércio eletrônico: os governos devem respeitar a natureza original desse meio e aceitar que a concorrência global e as escolhas do consumidor definem as regras do jogo do mercado digitalizado.[50]

O discurso de incentivo à adoção do processo de organização social informacional procura enfatizar a possibilidade de implantação, nesse tipo de sociedade, dos preceitos democráticos e solidários de forma mais profunda e eficiente. Trata-se de um argumento de forte poder de convencimento, mas que na verdade apenas encobre os verdadeiros objetivos dessa nova estrutura de organização social e econômica: a exploração econômica de novas fontes de riquezas fundadas na informação, como bem demonstra a postura norte-americana, acima citada, de incentivo e intervenção na estrutura organizacional da *Internet*, ferramenta exponencial da sociedade da informação.

O avanço tecnológico, especialmente o dos meios de comunicação sempre reforçaram a possibilidade de se implantar uma sociedade mais justa, igualitária e solidária, melhor explicitando, mais democrática. Ocorre que essas ferramentas, historicamente, se comportaram como mecanismos de ampliação dos meios de dominação social e catalisadores do processo de diferenciação econômica das sociedades. Sobre o assunto Mattelart faz o seguinte paralelo:

> Foi dito algo em relação ao telégrafo que me parece infinitamente correto, e que faz sentir toda a sua importância; é que o fundo dessa invenção pode bastar para tornar possível o estabelecimento da democracia em uma grande população. 'Muitos homens respeitáveis, entre os quais se deve contar Jean Jacques Rosseau, pensaram que o estabelecimento da democracia era impossível nas grandes populações. Como tal povo pode deliberar? Nos antigos, todos os cidadãos se reuniam em uma praça; eles comunicavam sua vontade... a invenção do telégrafo é um novo dado que Rousseau não pôde fazer entrar em seus cálculos. Ele pode servir apara falar a grandes distância tão correntemente e distintamente quanto em uma sala. Não há impossibilidade alguma de todos os cidadãos da França darem a conhecer suas vontades, num tempo curto, para que essa comunicação seja considerada

[49] MATTELART, Armand, op. cit., 2002. p.07.
[50] MATTELART, Armand, op. cit., 2002. p.132.

> instantânea'. Esse texto data de março de 1975 e foi escrito por um homem de ciência: Alexandre Vandermonde (1735-1796), titular da primeira cátedra de economia política fundada na França. Em agosto de 1794, o Ministério da Guerra havia inaugurado a primeira linha de telégrafo ótico (Paris-Lille);
>
> Esse discurso profético sobre as virtudes democráticas da comunicação de longa distância será rapidamente desmentido pela manutenção do embargo decretado sobre o código ou língua dos signos criptografada e pela rejeição à autorização do uso cidadão em nome da segurança interna e da defesa nacional. E isso praticamente até a chegada do telégrafo elétrico. Ninguém a não ser o emissor do original e o destinatário final conhecem as chaves do código formulado pelo inventor dessa técnica, Claude Chappe. A arquitetura da rede corresponderá a um modelo estrelado ou piramidal, resplandecendo a partir do cume parisiense já em vigor para a rede de estradas, ele se perenizará por meio da estrada de ferro e do conjunto de redes de telecomunicações posteriores.
>
> A cada geração técnica será reavivado o discurso salvador de concórdia universal, de democracia descentralizada, de justiça social e de prosperidade geral. A cada vez, também, se verificará a amnésia em relação à tecnologia anterior. Do telégrafo ótico ao cabo submarino, do telefone à *Internet*, passando pela radiotelevisão, todos esses meios destinados a transcender a trama espacial-temporal do tecido social renovarão o mito das descobertas com a agora da Ática. Nem a diferença, frequentemente radical, das condições históricas de sua implantação institucional, nem os desmentidos flagrantes às promessas abalarão esse imaginário técnico de natureza milenarista. [51]

Dessa forma, a construção teórica de uma nova organização social mais justa e democrática, serve como pano de fundo para a consolidação de um novo modelo de exploração econômica onde a "expressão informação é poder" foi potencializada ao extremo.

Nesse modelo social, o saber passa a ser origem do poder, passa a ser encarado como um mecanismo de dominação econômica e política, não importando sua natureza, se livre (criada pela televisão, pelo rádio, pelo marketing), se comercial (passível de apreciação econômica e base do comércio eletrônico), ou estratégica.

O grande emblema dessa nova forma de organização indica a amplitude das novas formas de geração de riqueza econômica, bem como demonstram o enorme poder que emana das empresas informacionais. Em 2000, a união entre duas empresas gigantes demonstrou que a simbiose entre a nova economia (informação – bem intangível) e a economia real (produtos e serviços reais) demonstrou de forma concreta o poder do paradigma informacional. A *América On Line –AOL*, primeiro fornecedor mundial de acesso à *Internet*, comprou um dos maiores grupos de produção de conteúdo multimídia, a *Time–Warner*. Dessa forma a simbiose entre acesso à informação e conteúdo da informação estava completa, um único

[51] MATTELART, Armand, op. cit., 2002. p.31.

grupo empresarial tinha sob o seu controle as ferramentas que permitiam a criação de informações e mais ainda, o controle sobre os suportes hábeis a difundi-la. "A ambição da AOL pode ser lida nas paredes de sua matriz: AOL *everywhere, for everyone*"[52] (AOL em todo o lugar, para todo mundo), ou seja, criação e distribuição de informação de todas as formas possíveis e imagináveis.

Assim, a sociedade da informação, enquanto marco da reorganização estrutural de um novo modelo econômico e geopolítico, torna-se objetivo hegemônico das grandes potências mundiais, e conseqüentemente, dos países que gravitam ao seu redor no modelo de uma sociedade globalizada. Conceito esse, globalização, que se relaciona muito intimamente com a idéia de sociedade da informação. O surgimento de uma sociedade mundializada, ligada através de redes que permitem o fluxo informacional instantâneo corrobora com a necessidade de criação de um mercado global. A expressão "sociedade da informação" tem origem na tradução do termo *Global Information Society,* ou *Holistic Information Society,* que significa justamente o surgimento de uma sociedade baseada no valor econômico e social da informação enquanto meio de unificação ou sistematização das diversas esferas sociais, tendo como objetivo principal a facilitação do acesso as novas tecnologias, na busca de fomentar o desenvolvimento dos níveis mínimos de infra-estrutura informacional que potencialize o surgimento de novos mercados e o desenvolvimento da economia. "A sociedade caminha para a *globalização* como conseqüência da revolução tecnológica e da explosão da comunicação que universaliza hábitos, culturas e formas de produção e consumo."[53]

O cenário econômico mundial sofreu transformações drásticas influenciadas pela crise de superprodução vivenciada pelo capitalismo liberal norte americano em 1929. A doutrina da não intervenção estatal deu lugar a políticas focadas na intervenção do Estado no cenário econômico, como por exemplo, o plano *New Deal* implantado por Roosevelt nos Estados Unidos da América. O Estado passa a intervir diretamente na economia, figura como um gestor que através da utilização dos recursos do planejamento busca conferir a máxima eficiência econômica e social do sistema.

Contudo, a partir da década de 50, o expansionismo das grandes corporações e o surgimento dos conglomerados empresariais multinacionais, bem como a busca pela

[52] MATTELART, Armand, op. cit., 2002. p.127.
[53] PAESANI, Liliana Minardi, op. cit., 2006. p.18.

equalização das políticas fiscais internacionais que acarretariam na negociação das barreiras alfandegárias começaram a minar o neocapitalismo liberal fundado na teoria Keynes. A crise do petróleo de 1973 demonstrou a incapacidade do neocapitalismo de lidar com fatores conturbados do sistema capitalista como, por exemplo, a superprodução sem consumo. Assim, as idéias intervencionistas perderam força e deram lugar à defesa de idéias liberais, focadas na completa liberdade de mercado. A essa reorganização das idéias liberais deu-se o nome de Neoliberalismo, corrente econômica fundada principalmente no repúdio a qualquer forma de limitação aos mecanismos do mercado por parte do Estado, e que foca a privatização da economia, o anti-nacionalismo, o ajuste de gastos públicos, a flexibilização das regras trabalhistas, a diminuição da carga fiscal e a privatização dos serviços públicos.[54]

A dinâmica de reorganização do sistema capitalista, associada ao desenvolvimento tecnológico, permitiu a edificação das bases mínimas de uma sociedade globalizada e organizada sobre a égide da informação.

> O capitalismo global caracteriza-se por ter na inovação tecnológica um instrumento de acumulação em nível e qualidade infinitamente superiores aos experimentados em suas fases anteriores; e por utilizar-se intensamente da fragmentação das cadeias produtivas propiciadas pelos avanços das tecnologias da informação.[55]

A grande modificação ocorrida na estrutura produtiva do capitalismo tecnoinformacional reside na construção de uma cadeia econômica e social formada por uma pluralidade de atividades produtivas que dependem necessariamente de uma organização gerencial das redes informacionais pautada na utilização de instrumentos tecnológicos. "A tecnologia acabou se transformando basicamente em expressão da competição global, objetivando ampliar a participação nos mercados globais e a acumulação para, por sua vez, permitir novos investimentos em tecnologia e realimentar o ciclo de acumulação."[56]

A difusão das tecnologias da informação, potencializadas pelo barateamento dos meios que possibilitam o seu acesso tem alterado sensivelmente o contexto social, não só a nível individual, mas principalmente aos grupamentos coletivos. A intensificação do meio eletrônico fez surgir novos valores, novos bens, novas relações interpessoais, novas formas de organização social, de inclusão e exclusão.

---

[54] WARNIER, Jean Pierre. **A mundialização da cultura**. Tradução de Viviane Ribeiro. São Paulo: EDUSC, 2003. p.63.
[55] DUPAS, Gilberto, op. cit., 2000. p.108.
[56] DUPAS, Gilberto, op. cit., 2000. p.23.

Ressalte-se que o discurso que fundamenta essa nova forma de organização social defende a construção de uma ordem social mais democrática, mais justa e humana. Contudo, na prática o binômio sociedade da informação e tecnologia tem aumentado o fosso entre os países ricos e os países pobres, e entre os ricos e pobres de um mesmo país. Mais ainda, criou uma nova e vetusa forma de exclusão social: a digital, eletrônica ou informacional.

A marginalização informacional, ou dívida digital. A fratura digital acentua-se a cada avanço tecnológico e cria barreiras mais difíceis de transpor que as erigidas por outras formas de exclusão social.

> De modo mais simples, pode-se acrescentar o fato de que no momento em que cintilam as promessas de infovias, uma multidão de países ou regiões do planeta não tem sequer uma rede rodoviária digna desse nome e de que mais de 600 mil cidades não tem eletricidade! Com 19% da população mundial, os países da OCDE tinham 91% dos usuários da *Internet*. Mais da metade deles estavam nos Estados Unidos, que representam apenas 5% da população do planeta. Sem falar do fato de que, assim como no século XIX Londres foi o local de passagem obrigatório das redes transcontinentais do sistema de cabos submarinos mundial, hoje os Estados Unidos se tornaram o núcleo pelo qual devem necessariamente transitar os internautas dos países menos favorecidos para se conectar entre si. Os mais pobres pagam pelos mais ricos. Quando um habitante dos Estados Unidos envia um e-mail a um africano, é o africano quem paga. [...] A situação da Índia é representativa da complexidade do sistema tecnoglobal de duas velocidades. Esse país é o segundo exportador de programas de computador depois dos Estados Unidos e o primeiro especialista em informática. Mas com mais de um bilhão de habitantes, a metade dos quais analfabetos, a Índia conta com em 2001 com 26 milhões de linhas telefônicas e a taxa de penetração da *Internet* não ultrapassa 0,2%.[57]

Percebe-se que a idéia de uma sociedade informacional, interligada em redes de produção e consumo, possui um grande potencial de democratização, posto que através da redução dos custos de acesso à informação, ao saber, permite a formação de seres humanos mais capazes de intervir de forma consciente na realidade social.

Entretanto, o enfoque dado à sociedade da informação, enquanto vetor do fenômeno globalizante, repousa na idéia de expansão da apropriação de um novo tipo de capital econômico através da criação de um mercado global, limitando-se direitos fundamentais, aumentando os níveis de exclusão e reduzindo a força dos Estados nacionais.

[57] MATTELART, Armand, op. cit., 2002. p.160.

1.1.4 Sociedade informacional e direito

A modificação contextual da forma de organização social ocasionada pelo modelo de desenvolvimento tecnoinformacional, ao alterar de forma significativa as estruturas sociais e econômicas, ocasionou conseqüentemente, o surgimento de novas situações que afetaram sensivelmente as relações sociais e econômicas, principalmente na seara jurídica.

> É preciso considerar também que este novo cenário traz implicações jurídicas. Em vários casos, as leis existentes são também aplicáveis aos novos pressupostos do contexto virtual. Em outros, uma nova regulamentação é necessária para se ter mais segurança no emprego das ferramentas eletrônicas e maior certeza quanto a validade e eficácia das transações celebradas por meio eletrônico.[58]

Assim, nesse novo espaço social que surgiu, e diante do leque inimaginável de possibilidades de relações comerciais, trabalhistas, pessoais, produtivas entre outros, percebeu-se a necessidade de conferir segurança jurídica a essas novas situações, posto que o vazio normativo existente tornou extremamente inseguro a continuidade da celebração de negócios jurídicos nesse novo contexto social.

Novos bens e novos valores carentes de tutela jurídica emergiram. A valorização econômica da informação ocasionou mudanças significativas nas cadeias produtivas e na estrutura do próprio capitalismo, o que pressionou de forma significativa a movimentação da máquina jurídica estatal no sentido de normatizar esse novo conjunto de relações.

> Nos dias de hoje há um constante aumento da complexidade de todas as relações sociais; o volume de informações cresce violentamente, é difícil acompanhar a rapidez com que elas são criadas, alteradas, atualizadas, revistas. A informação passa a ser mercadoria de primeira grandeza no mercado globalizado, altamente valorizada e rentável. Por isso o interesse constante e permanente pela informação. Todos desejam obtê-la. Há os que tentam ser os donos, para usufruir das vantagens.[59]

Como resguardar a integridade dos sistemas eletrônicos contra violações que afetem a sua segurança, o seu funcionamento, a sua veracidade? Como regular a apreciação econômica da informação, do dado? Como regular o fluxo informacional sobrepesando os valores

---

[58] BASSO, Maristela; ALMEIDA, Guilherme A. É preciso difundir mentalidade digital nas empresas. In: KAMISNSKI, Omar (Org.), op. cit., 2007. p.123.

[59] VEIGA**,** Luiz Adolfo Olsen da; ROVER**,** Aires José. Dados e informações na internet: é legítimo o uso de robôs para a formação de base de dados de clientes? In: ROVER, Aires José (Org.), op. cit., 2004. p.31.

econômicos e o direito constitucional fundamental à intimidade? Como conferir autenticidade às transações firmadas por meio eletrônico?

A carência de legislação regulando a matéria cria um vazio normativo que gera insegurança e instabilidade no meio informacional. Mais ainda, abala de forma impactante os pilares da sociedade da informação, o que coloca em risco a manutenção da própria estrutura social atual. Analisando e ilustrando o contexto apresentado, Érica Ferreira expõe que:

> Este vácuo que ainda persiste decorre não apenas da novidade desta tecnologia, bem como da rapidez com que ela evolui, possui vida própria realizando uma metamorfose quase que constante, todo dia aparecem novidades tecnológicas, e a principal pergunta que paira no ar é: como o Direito vem se adequando e respondendo às novas exigências da vida contemporânea, sobretudo quanto à regulamentação dos atos gerados coma Internet? Quem controla o que se passa na rede? Como se evitam danos durante a navegação? Como se cometem crimes virtuais e como identificar o seu autor? Quem irá puni-lo e com base em que arcabouço normativo?[60]

Assim, deve-se ressaltar que nessa nova sociedade, novos interesses, novas demandas surgem, e desta maneira nascem, como frutos da atividade humana, novas aspirações jurídicas, novos direitos. Norbert Bobbio já previa que:

> o desenvolvimento da técnica, a transformação das condições econômicas e sociais, a ampliação dos conhecimentos e a intensificação dos meios de comunicação poderiam produzir mudanças na organização da vida humana e das relações sociais, criando condições favoráveis para o nascimento de novos carecimentos. [61]

Mais ainda, o filósofo italiano sustentou que "assim como as demandas de proteção social nasceram com a revolução industrial, é provável que o rápido desenvolvimento técnico e econômico traga consigo novas demandas que hoje não somos capazes de prever."[62] Dessa forma não pode o Direito se furtar a, mesmo que tardiamente, responder aos anseios sociais de normatização da realidade social informacional. Assim, deve o Direito procurar definir novas formas de proteção, mesmo que provisórias, sob pena de se podar, ainda no nascedouro, aos direitos fundamentais de quarta geração nominados genericamente de direitos de acesso à informação.

---

[60] FERREIRA, Érica Lorenço de Lima. **Internet –** Macrocriminalidade e jurisdição internacional. Curitiba: Júrua, 2007. p.20.
[61] BOBBIO, Norberto. **A era dos direitos**. Trad. Carlos Nelson Coutinho. 10. ed. Rio de Janeiro: Campus, 1992. p.34.
[62] Ibid., 1992. p.49.

O direito posto de forma concreta, por ser estanque, não pode acompanhar em nível de igualdade as transformações sociais decorrentes do avanço tecnológico. Mas nem por esse motivo pode o Direito ficar inerte. Inúmeras são as situações em que o Direito foi impactado por novos fenômenos jurídicos e que após a assimilação desses novos contextos consegue responder aos anseios sociais de regulamentação. Analisando a matéria Eurípede Brito da Cunha Júnior expõe que:

> Carnelluti constatou, com clareza, que perplexos viram-se os juristas daquela época diante do problema da definição e tratamento dos fenômenos jurídicos relativos à eletricidade. Aqueles considerados por ele como juristas dúcteis, práticos, contornaram os problemas por meio de deduções lógicas. Para ele, a necessidade de sistematização teórica tornou-se imperativo, vez que as relações jurídicas sobre a eletricidade se tornaram o primeiro, ou antes, o mais antigo exemplo de uma série cada vez mais numerosa, referindo-se à título e exemplo, à radiodifusão e a televisão, está última então prestes a entrar em operação.[63]

Os avanços alcançados pelo desenvolvimento dessa relação simbiótica entre sociedade da informação, tecnologia e globalização, são inegáveis. Entretanto essa nova conjuntura organizacional das atividades e relações sociais e econômicas também causou impactos negativos não só na sociedade, mas também na organização do Estado a nível interno (ordem jurídica), mas também a nível internacional (soberania). No próximo capítulo analisar-se-á os impactos da sociedade da informação na ordem constitucional.

[63] CUNHA JÚNIOR**,** Eurípede Brito. Os Contratos eletrônicos e o novo Código Civil. **Revista do Centro de Estudos Judiciários - CEJ**, Brasília, n. 19, p.62-77, out./dez. 2002. p.63.

2 ASPECTOS CONSTITUCIONAIS DA SOCIEDADE DA INFORMAÇÃO

As mudanças advindas com o avanço tecnoinformacional impactaram de forma profunda as estruturas organizacionais da sociedade moderna. Os moldes sociais foram alterados. A sociedade atingida pelo paradigma informacional se reestruturou através de novas relações econômicas, culturais e jurídicas.

Os efeitos, no campo jurídico, dessa nova forma de sociedade ainda são extremamente recentes, mas apresentam um grau de densidade compatível com a profundidade das transformações ocorridas na sociedade.

Como instrumento regulador da ordem político-jurídica coube ao Direito Constitucional sentir os primeiros impactos dessa nova realidade social e jurídica. Logo as Cartas Constitucionais, absorvendo, as nuanças advindas da sociedade informacional, passou a tutelar e a sofrer forte influência dos valores e bens jurídicos advindos desse novo modelo de organização social. O presente capítulo busca analisar as influências da sociedade da informação na ordem constitucional.

2.1 O impacto da tecnologia da informação na ordem jurídica constitucional

O contexto social hodierno esta sendo moldado por tendências direcionadas pela combinação de dois fenômenos mundiais: a globalização e o desenvolvimento tecnológico informacional. Esses dois vetores causaram mudanças radicais nos meios e métodos de organização social econômica e cultural. Essa nova sociedade, fruto de uma reorganização pautada pela reestruturação dos mecanismos de organização do sistema econômico dominante, o capitalismo, caracteriza-se pela globalização das atividades estratégicas

econômicas e pela flexibilização da cadeia produtiva através do redimensionamento do trabalho e da sua organização pautada em redes comunicativas que são mediadas por instrumentos tecnológicos.

Entretanto, apesar da mediação tecnológica o homem continua sendo caracterizado como um ser de hábitos e cultura essencialmente de natureza associativa, "o indivíduo é um indivíduo social não só em sentido genético, mas também no sentido de sua existência conjunta no interior da estrutura social"[64]. Analisando o assunto Aristóteles já havia previsto que o homem, por sua própria natureza, poderia ser considerado um animal que tinha por característica possuir hábitos associativos, coletivos, sendo assim, "um animal político."[65]

O conceito de sociedade apresenta diversos aspectos, podendo ser focado por inúmeras ciências distintas como a sociologia ou a ciência política. O termo apresenta diversas acepções, chegando inclusive a ser aplicado de forma genérica com o objetivo de caracterizar "todo complexo de relações do homem com seus semelhantes"[66].

A compreensão deste termo, que constitui a essência da vida humana e conseqüentemente a base para a estruturação dos mecanismos sociais como o Direito, é extremamente importante para o estudo do impacto da sociedade informacional no campo jurídico.

Nesse sentido, vale destacar a conceituação que Agerson Tabosa Pinto tece ao analisar o assunto. O referido autor entende que a "Sociedade é o conjunto de grupos particulares, que vivem em comunidade de território, língua, costumes e objetivos."[67] A delimitação realizada pelo autor permite compreender o que é a sociedade. Mais ainda, expõe com simplicidade quais os elementos necessários a caracterizar uma sociedade. A vida coletiva, em uma mesma base local, ou seja, sob um mesmo território, com uma finalidade específica, logo buscando objetivos mínimos comuns e regrada por um arcabouço cultural mínimo idêntico (língua e costumes), enseja a caracterização da vida em sociedade.

---

[64] SCHAFF, Adam, op. cit., 1995. p.102.
[65] ARISTÓTELES. **A política.** Tradução Nestor Silveira Chaves. Rio de Janeiro: Ediouro, [s.d.].
[66] TALCOTT apud BONAVIDES, Paulo. **Ciência política.** 11. ed. São Paulo: Malheiros, 2005. p.57.
[67] PINTO, Agerson Tabosa. **Teoria geral do Estado.** Fortaleza: Imprensa Universitária - UFC, 2002. p.11.

Além da sociabilidade, diretamente ligada a sua essência, o homem, quando concretamente inserido em um ambiente social, ou seja, vivendo em sociedade, desperta inúmeras outras necessidades que servem de parâmetros inclusive para sua caracterização. Essas necessidades básicas, que podem ser consideradas inatas aos homens só se potencializam quando da vida coletiva e só em sociedade podem ser plenamente desenvolvidas e saciadas.

Uma dessas necessidades essenciais do homem vincula-se ao conhecer. O homem desde os tempos mais remotos lida com o seu desejo nato de aprender, de compreender, de pensar, não só a realidade que o cerca, mas também a si mesmo, e a todos que o rodeiam. Essa busca pelo conhecimento, pela construção do saber, não é uma tarefa solitária nem tampouco egoística. A construção do conhecimento sempre se caracterizou pela natureza social do homem, o desenvolvimento de idéias e teorias sempre estiveram associadas a sua divisão, ou seja, ao compartilhamento, a difusão, a comunicação.

Logo a comunicação, o comunicar, a troca de informações, está ligada de forma efetiva a idéia de sociedade, seja porque é algo impossível de dissociar do homem e da vida coletiva, seja porque a ausência de comunicação impede de forma objetiva a concretização da sociedade.

Atualmente, em virtude das mudanças ocorridas nas estruturas sociais, econômicas e políticas e da difusão informacional decorrente da união entre a globalização e o desenvolvimento tecnológico, a comunicação, e principalmente, os sistemas de comunicação e informação tiveram sua função social potencializada. Hoje, mais do que nunca, a idéia de comunicação é vinculada profundamente à sociedade, chegando-se inclusive a poder afirmar que "não há história sem mudança, nem sociedade sem informação." [68] Corroborando com essa linha de pensamento Aluízio Ferreira apregoa que:

> A historicidade dos fatos sociais compreende a ação humana individual e coletiva situada espacial e temporalmente, o que subentende que a fatores de índole individual e societária associam-se especificidades da época e lugar em que se desenrola a atividade humana.[69]

[68] BENEYTO, Juan. **Informação e sociedade:** os mecanismos sociais da atividade informática. Petrópolis: Vozes, 1997. p.11.
[69] FERREIRA, Aluízio. **Direito à informação, direito à comunicação:** direitos fundamentais na constituição brasileira. São Paulo: Celso Bastos editor, 1997. p.168.

Deve-se ressaltar que a ligação entre comunicação e sociedade reflete diretamente a relação indissociável entre linguagem e comunicação, e conseqüentemente entre a informação e o homem, posto que a linguagem constitui um dos elementos essenciais para o estabelecimento de relações entre os homens, permitindo assim a sua socialização. O avançar da sociedade em busca da informação, mormente no contexto social atual, configura-se como a satisfação de uma necessidade psicológica dos indivíduos, principalmente hoje quando o arcabouço social funda-se sobremaneira na estruturação econômica e social pautada na informação. Saliente-se que nesse sentido, o desenvolvimento de raízes sociais focadas na idéia de relações comunicativas baseadas na informação demonstram existência de um sintoma de amadurecimento do desenvolvimento das estruturas sociais.

A informação, como elemento estrutural do conhecimento, além de permitir a apreensão dos fatos e da realidade que cerca os indivíduos, também permite a construção de relações e vínculos sociais, econômicos e culturais que sem a sua existência não seriam possíveis. Isso fica mais patente quando se observa a constituição da sociedade informacional, onde os meios de comunicação foram massificados e potencializados pelas ferramentas tecnológicas desenvolvidas nos últimos trinta anos, fragmentando assim barreiras econômicas, políticas, religiosas e culturais.

> [...] esses meios de comunicação de massa fazem parte da paisagem social moderna. Eles penetram em todas as esferas da vida social, no meio urbano ou rural, na vida profissional, nas atividades religiosas, no lazer, na educação, na participação política. Tais meios de comunicação não só transmitem informações, não só apregoam mensagens. Eles também difundem maneiras de se comportar, propõem estilos de vida, modos de organizar a vida cotidiana, de arrumar a casa, de se vestir, maneiras de falar e de escrever, de sonhar, de sofrer, de pensar, de lutar, de amar.[70]

Percebe-se dessa forma que a mensagem informativa é capaz de aproximar, divertir, distrair, ensinar os indivíduos e a coletividade. Mais ainda, pode ser um eficiente mecanismo de direcionamento de comportamentos, de vontades e de pensamentos. O novo contexto comunicativo da sociedade da informação pauta-se diretamente na mecânica dos meios e comunicação em massa onde a informação não é direcionada a um único destinatário, seja ele um indivíduo ou um grupo de pessoas, mas sim a toda a coletividade de forma indiscriminada.

---

[70] SANTOS, José Luiz dos. **O que é cultura.** 14. ed. São Paulo: Brasiliense, 1994. p.89.

Desta forma, uma dos principais efeitos dos meios informacionais é justamente permitir que o homem, ao ser colocado em contato com a sua realidade, possa conhecer o mundo que o cerca por meio da compreensão das relações assimiladas, e assim, ter consciência da necessidade de valorar e ajustar seus comportamentos e suas relações no meio social, para uma melhor adequação ao contexto societário em que vive.

Ante o exposto, se percebe que o contexto social moderno desvincula-se completamente dos modelos de comunicação de períodos históricos anteriores. Os liames de informação mediados pelos vínculos de vizinhança ou aproximação existentes entre indivíduos associados estão sendo reestruturados. Na verdade, no âmbito da sociedade da informação, essas espécies de liames estão sendo permutados por vínculos decorrentes do uso de ferramentas e instrumentos tecnológicos utilizados na mediação da informação. Isso pode facilmente ser evidenciado pelo fato de determinados comportamentos sociais tornarem-se raros no atual contexto social. As visitas a amigos, ou profissionais, são escassas, até mesmo os contatos telefônicos perderam sua funcionalidade diante das inúmeras ferramentas propiciadas pelo momento tecnológico atual (*e-mail*, mensagens de texto etc.). O que caracteriza o atual patamar de desenvolvimento da sociedade é justamente o binômio flexibilidade – velocidade de produção e difusão do fluxo informacional.

> Uma conseqüência do papel da informação é o reconhecimento da importância que tem para se agir, por meio dela, sobre os homens. Para considerar-se plenamente cidadão, o homem contemporâneo precisa dispor de fontes informacionais que lhe permitam conhecer o que se passa e, em seguida, formar juízos sobre os acontecimentos.[71]

Entretanto, outro ponto que merece ser destacado é a transformação ocorrida na esfera conceitual no que tange ao significado do que seja informação. No cenário social moderno, a informação deixou de se relacionar tão somente ao conteúdo da mensagem, passando a significar à própria forma do fluxo informacional. Essa modificação permitiu que a informação transformasse a cadeia produtiva, e se tornasse em um dos bens considerados como matéria-prima da atual ordem econômica. Hoje, a partir dessa nova concepção, a informação, além de ser considerada um bem na concepção econômica, pode ser caracterizada como um bem jurídico, intangível, inesgotável, reprodutível, comunicável e plural, que dependendo do contexto de fruição pode ser vinculado a uma valoração econômica.

---

[71] BENEYTO, Juan, op. cit., 1997. p.15.

Desse modo, a informação independentemente da maneira plural em que possa ser apresentada (classificação segundo o suporte midiático utilizado: oral, escrita, visual, audiovisual; classificação segundo a finalidade: jornalística, publicitária, institucional, etc.; classificação de acordo com o conteúdo: político, econômico, religioso, cultural, entretenimento etc.), corresponde a um direito fundamental de qualquer cidadão e deve necessariamente ser tutelado pela ordem jurídica constitucional. De forma mediata o direito à informação vincula-se à própria informação. Em um segundo plano significa a faculdade que deve ser garantida pelo Estado a qualquer cidadão de colher, fornecer e receber informações. "Estar em pleno gozo do direito à informação significa estar informado, independentemente do modo de obtenção (direta ou indiretamente) da informação"[72]. Vale salientar que o direito à informação deve ser compreendido por meio de uma relação que deve ser equacionada entre o direito de ser informado e o direito de informar, de modo que se resguarde um equilíbrio fundamental para a manutenção da liberdade de informação em uma sociedade multicultural e difusa.

A importância do Direito à Informação como um direito fundamental do homem é demonstrada pela sua relação essencial com a democracia moderna. É com a liberdade de informação, garantida constitucionalmente, que se potencializa a implantação dos demais direitos. Mais ainda, é com a busca pela difusão dos direitos que a informação ganha maior relevância tanto nos meios de comunicação tradicionais, como nos meios eletrônicos. Dessa forma, a relevância da informação para a sociedade e para os indivíduos exige por parte do Estado uma tutela jurídica protetiva a sua altura. Logo, o Direito à Informação passou a ser normatizado em nível constitucional.

A ordem jurídica constitucional brasileira reserva espaço especial à proteção da informação. A Constituição Federal de 1988 consolidou em seu texto pétreo um Título reservado exclusivamente aos direitos e garantias fundamentais. Nesse contexto, a estrutura constitucional dividiu o referido Título em cinco capítulos que versam sobre os direitos individuais e coletivos, os direitos sociais, os direitos de nacionalidade e os direitos políticos. No que tange aos direitos individuais e coletivos, estes correspondem ao conjunto de direitos ligados à idéia de pessoa humana e de seus atributos de personalidade, como a vida, a honra e a liberdade. A esses direitos se atribui à natureza de fundamentais:

[72] FERREIRA, Aluízio, op. cit., 1997. p.168.

> [...] se tem preferido ultimamente a expressão 'direitos fundamentais', por traduzir melhor que as demais [nomenclaturas] a idéia de interesses humanos básicos e gerais tutelados pelo Estado a partir da sua positivação constitucional, bem como por não sugerir vinculação a perspectivas puramente jusnaturalistas ou a reduzir-se a meros comandos de direito positivo abstraídos do caráter transcendental da natureza do homem e da sua historicidade. [...] os direitos fundamentais podem ser definidos como direitos instituídos historicamente como respostas a pretensões correspondentes a necessidades humanas fundamentais identificadas e reconhecidas, também historicamente, em favor dos membros da coletividade em geral ou em proveito de membros da coletividade em geral ou em proveio de integrantes indistintos de grupos ou camadas dessa mesma coletividade (seres categorizados).[73]

Quando se analisa a estruturação jurídica do Direito Fundamental, primeiro grande problema que se desenha no estudo dos direitos fundamentais é a grande imprecisão conceitual. Expressões como: "direitos humanos", "direitos do homem", "direitos subjetivos", "direitos civis", "liberdades públicas" e várias outras aparecem na doutrina e muitas vezes, erradamente, apontadas como sinônimos.

A confusão mais recorrente se opera entre as expressões direitos humanos e direitos fundamentais. Entretanto, podem ser diferenciados na medida em que os primeiros representam princípios supranacionais, pré-positivos, que resumem a concepção de uma convivência digna, livre e igual de todos os seres humanos, válidos para todos os povos e em todas as épocas históricas. A conceituação de direitos fundamentais, por sua vez, demonstra maior dificuldade.

Segundo cita Paulo Bonavides[74], Konrad Hesse entende os direitos fundamentais como aqueles que visam à criação e manutenção dos pressupostos elementares de uma vida na liberdade e na dignidade humana. Nasce desta definição a finalidade precípua dessa gama de direitos, além de ser notável o seu largo âmbito de abrangência, o que por certo desfavorece uma precisa identificação.

Para atender a esta necessidade de identificação, há um conceito mais simples e restrito, também de Hesse, que considera direitos fundamentais aqueles que o direito vigente desta forma qualifica. Emerge, neste particular, a importância da positivação destes direitos, como uma forma de melhor identificá-los e distingui-los dos demais.

---

[73] FERREIRA, Aluízio, op. cit., 1997. p.63-64.
[74] BONAVIDES, Paulo. **Curso de direito constituciona**l. 6. ed. Rio de Janeiro: Forense, 1996. p.514.

Já Carl Schmitt, também citado por Bonavides[75], a par da adoção da definição restrita, na esteira do que preconizou Hesse, entende, ademais, que os direitos fundamentais são aqueles que recebem da Constituição um grau mais elevado de garantia ou de segurança. No Direito brasileiro, por exemplo, tem-se a proteção concedida pela Constituição, que impede qualquer deliberação de emenda tendente a abolir os direitos e garantias fundamentais (Art. 60, § 4º, IV). Acrescenta ainda o referido autor, que os direitos fundamentais variam conforme a ideologia, a espécie de valores e princípios que a Constituição de cada Estado consagra, de forma que o conceito de direitos fundamentais modifica-se ao sabor das opções de cada Estado.

Fixada a dificuldade de precisar conceitos nesta matéria, partir-se-á com uma definição que agrega elementos que bem se amoldam aos objetivos deste estudo. Para Ana Maria D´Ávila Lopes "os direitos fundamentais podem ser definidos como os princípios jurídica e positivamente vigentes em uma ordem constitucional que traduzem a concepção de dignidade humana de uma sociedade e legitimam o sistema jurídico estatal"[76]

Pode-se notar certo consenso nos doutrinadores em apontar características dos direitos fundamentais. Foge ao foco deste estudo analisá-las pormenorizadamente, razão pela qual as enumerar-se-á, com uma rápida justificação e demonstração de existência, sempre com o intuito de melhor individualizar os direitos fundamentais, de molde a evitar confusão com outros.

É comum a atribuição do caráter universal aos direitos fundamentais, na medida em que estes seriam usufruíveis por todo e qualquer ser humano como decorrência desta condição. Este entendimento carrega o mérito de garantir proteção abrangente aos seres humanos, principalmente frente ao Estado. Entretanto, não se pode olvidar que existem direitos fundamentais que, mercê de sua especificidade – por serem direcionados a determinado grupo de indivíduos - fogem a esta definição.

Há ainda o caráter absoluto dos direitos fundamentais, bastante defendido e que tem sua gênese na constatação de que estes se situam no topo da hierarquia jurídica, não tolerando

---

[75] Ibid., 1996. p.515.
[76] LOPES, Ana Maria D´Ávila. **Direitos fundamentais como limites ao poder de legislar**. Porto Alegre: Sérgio Antonio Fabris Júnior editor, 2001. p.35.

qualquer restrição. De fato os direitos fundamentais têm prevalência sobre os demais por serem elementos basilares do Estado Democrático de Direito. Entretanto, podem encontrar limitações no embate com outros valores constitucionais ou mesmo entre si. Destarte, deve-se entender este absolutismo de molde a afastar a idéia de direitos intocáveis e incontrastáveis.

É importante destacar a historicidade dos direitos fundamentais, visto que possuem valia distinta de acordo com a época ou o lugar que são previstos. Essa característica denuncia que os direitos fundamentais não nascem todos de uma vez, conforme leciona Norberto Bobbio:

> Nascem quando devem ou podem nascer. Nascem quando o aumento do poder do homem sobre o homem cria novas ameaças à liberdade do indivíduo ou permite novos remédios para suas indigências: ameaças que são enfrentadas através de demandas de limitação de poder; remédios que são providenciados através da exigência de que o mesmo poder intervenha de modo protetor. [77]

Diz-se também que os direitos fundamentais carregam os atributos da inalienabilidade e indisponibilidade. Com efeito, o titular dos mesmos não pode deles dispor. Destarte, a preterição de um direito fundamental será sempre reprovável, ainda que o titular deste firme seu consentimento com a violação. A proteção, portanto, independe da vontade do titular, visto que pauta-se na ligação indissolúvel destes direitos com o princípio da dignidade da pessoa humana, fonte de todos os direitos fundamentais.

Entretanto, mais uma vez, não há que se considerar estas características imutáveis, visto que cedem diante da colisão de direitos fundamentais, razão pela qual se mostra ainda mais importante o seu estudo. Efetivamente, diante de situações concretas, é normal que um direito fundamental precise ser posto à disposição a fim de que outro, o qual se mostre mais relevante, possa ter aplicação.

A característica da constitucionalização é exatamente a que possibilita uma distinção entre os "direitos fundamentais" e os "direitos humanos". Estes últimos representariam direitos não positivados por nenhuma ordem positiva, mas (fiéis à sua índole jusnaturalista) seriam aspirações de respeito ao ser humano. Já os diretos fundamentais são aqueles previstos por determinada ordem jurídica estatal, sendo, por esta razão, garantidos e limitados no espaço e no tempo. Por constarem da lei fundamental de um Estado, estes direitos têm

---

[77] BOBBIO, Norberto, op. cit., 1992. p.06.

modificação dificultada, ou mesmo impossibilitada, impondo observância a todos os particulares e órgãos estatais.

Aqui se vislumbra mais uma característica dos direitos fundamentais, a saber, a vinculação aos poderes públicos. Com efeito, os poderes (funções) estatais devem pautar sua atuação pela observância destes direitos; são poderes autolimitados. Não há sequer possibilidade de que esta autolimitação seja modificada por arbítrio de qualquer destes. Isto porque o poder que estabeleceu tais direitos como basilares da ordem jurídica (poder constituinte originário) é superior aos poderes constituídos. Na ordem constitucional brasileira tem-se a previsão expressa do Art. 60, §4º, IV da CF.

Avulta desta característica o caráter de oposição ao Estado, típico dos direitos de primeira geração (dimensão), que surgiram a partir do surgimento da concepção individualista da sociedade, em oposição à atuação dos Estados absolutistas. Paulo Bonavides esclarece:

> Os direitos da primeira geração ou direitos de liberdade têm por titular o indivíduo, são oponíveis ao Estado, traduzem-se como faculdades ou atributos da pessoa e ostentam uma subjetividade que é seu traço mais característico; enfim, são direitos de resistência ou de oposição perante o Estado.[78]

Os direitos fundamentais têm aplicabilidade imediata. Exemplo claro é o § 1º do Art. 5º da Constituição brasileira: "As normas definidoras dos direitos e garantias fundamentais têm aplicabilidade imediata". Desta forma o poder constituinte originário retira da dependência do legislador infraconstitucional a efetividade dos direitos fundamentais, de molde a evitar que as normas que os garantem quedem como letra morta, por conseqüência imediata da inércia do legislador. Explicita-se o caráter preceptivo (e não programático) das normas que veiculam direitos fundamentais.

Ressalte-se, ademais, a função dignificadora destes direitos. Com efeito, seu principal objetivo é resguardar a dignidade da pessoa humana, na medida em que representam, verdadeiramente, concretizações e densificações deste princípio fundamental, mormente na ordem constitucional brasileira.

---

[78] BONAVIDES, Paulo, op. cit., 1996. p.517.

Por fim, que os direitos fundamentais representam mesmo elementos legitimadores da ordem estatal, visto que esta surge e mantém-se desde que garanta a previsão e observância destes valores fundamentais.

Uma natural classificação dos direitos fundamentais em diferentes grupos surge em razão das variadas funções que eles desempenham na ordem jurídica. Jellinek, no final do século XIX, sistematizou uma classificação tendo por base esta disparidade de funções, que ainda carrega firme a marca da atualidade.

Jellinek desenvolveu uma teoria dos quatro *status* em que o indivíduo pode se encontrar frente ao Estado. Por este meio foi possível conhecer melhor o conteúdo e estrutura dos direitos fundamentais. A primeira relação é a de subordinação ao Estado, sendo o indivíduo detentor de deveres. Esta corresponde ao chamado *status* passivo.

A segunda se estabelece em razão do reconhecimento do valor da pessoa humana, o que leva à redução do poder estatal frente a esta. Há uma limitação do poder estatal na sua atuação perante os indivíduos. Este é o *status* negativo.

O terceiro *status* surge da constatação que, em determinadas situações, o Estado precisa intervir para garantir um direito fundamental, através de uma atuação positiva. Por esta razão, este é denominado *status* positivo.

A quarta relação envolve uma atuação do indivíduo, que desfruta de uma competência para influir sobre a vontade estatal. Esta só se torna possível através da atuação dos cidadãos. O direito de voto é um clássico exemplo. Trata-se neste caso do status ativo.

A moderna classificação dos direitos fundamentais foi inspirada na teoria de Jellinek. Conforme nos ensina Ingo W.Sarlet[79] a citada construção, na medida em que foi sofrendo reparos e críticas, manteve-se viva mediante um contínuo processo de redescoberta pela teoria constitucional. Hoje se fala em três grandes grupos de direitos fundamentais: a) de defesa; b) a prestação e c) de participação, que correspondem, respectivamente, aos status negativo, positivo e ativo.

[79] SARLET, Ingo Wolfgang. **Eficácia dos diretos fundamentais**. Porto Alegre: Livraria do Advogado, 2004. p.169.

Importante também proceder a uma análise das principais características de cada grupo ou classe de direitos fundamentais, a iniciar pelos de defesa. Sobre estes, resume Paulo Gustavo Gonet Branco:

> Os direitos de defesa caracterizam-se por impor ao Estado um dever de abstenção, um dever de não interferência, de não intromissão no espaço de autodeterminação do indivíduo. Esses direitos objetivam a limitação da ação do Estado. Destinam-se a evitar ingerência do Estado sobre os bens protegidos (liberdade, propriedade...) e fundamentam pretensão de reparo pelas agressões eventualmente consumadas.[80]

Esses direitos, claramente inspirados no *status* negativo de Jellinek, referem-se principalmente às liberdades individuais e, na Constituição brasileira são encontrados em larga escala no Art. 5º. Na maioria das vezes, portanto, são veiculados por normas de elevada densidade normativa, o que possibilita aplicabilidade imediata, a prescindir da atuação legislativa.

Os direitos fundamentais a prestação são geralmente identificados com os direitos sociais. Existem para assegurar uma atuação positiva do Estado a fim de suprir necessidades básicas dos indivíduos. São direitos de promoção. Possuem baixa densidade normativa por se subordinarem à atuação do legislador para sua efetivação e dependerem muito da orientação política e das prioridades do país em determinado momento histórico, da disponibilidade econômica, e principalmente, da vontade política do grupo que está a frente do governo Estado. Constituem a chamada reserva do possível. Remetem ao *status* positivo da teoria de Jellinek. Podem ser divididos em dois grupos: direitos fundamentais a prestações jurídicas e direitos fundamentais a prestação material.

Os primeiros são direitos dos indivíduos perante o Estado a fim de que este elabore determinada previsão normativa ou realize certos atos jurídicos. Neste rol estão as garantias institucionais. A Constituição Federal, inclusive, prevê instrumentos aptos a garantir a efetividade desta espécie de direitos, a saber, a ação direta de inconstitucionalidade por omissão e o mandado de injunção.

Os direitos fundamentais a prestação material têm por objeto uma utilidade concreta, representada por um bem ou serviço. Por serem os direitos sociais por excelência, são

---

[80] BRANCO, Paulo Gustavo Gonet. **Hermenêutica constitucional e direitos fundamentais**. Brasília: Brasília Jurídica, 2002. p.120.

denominados direitos a prestação em sentido estrito. São direitos do cidadão perante o Estado no sentido de que este lhe forneça determinadas prestações materiais.

Os direitos fundamentais de participação visam sempre à garantia da participação da vontade do cidadão nas decisões que concernem aos rumos a serem tomados pelo Estado. Podem ser agrupados sob a epígrafe de direitos políticos, correspondendo, assim, ao último *status* da Teoria de Jellinek (ativo).

Assim, encaradas como necessidades fundamentais do homem, a informação e a comunicação, enquadram-se como imperativos jurídicos fundamentais para a organização da sociedade e do Estado, o que inferiu a necessidade de proteção constitucional da matéria. Figura importante também ressaltar que o direito à informação é essencialmente um direito individual e social, haja vista que o ato de se comunicar é naturalmente uma atividade que atende e pauta-se em carências e necessidades pessoais e coletivas.

A ordem constitucional brasileira, atualmente balizada pela Constituição Federal de 1988, faz parte de um conjunto de legislações constitucionais modernas que procuram através de inúmeros instrumentos constitucionais reconhecer e garantir o direito à liberdade e pensamento, especialmente no que tange às esferas relacionadas com a informação e a comunicação como direitos fundamentais. Ressalte-se que a tutela constitucional dos direitos relacionados à informação pauta-se em uma equação de freios e contrapesos, através de disposições que buscam ao mesmo tempo reforçar e limitar o referido direito.

Materialmente, o direito à informação encontra-se inserido no direito a liberdade previsto no caput do artigo 5º, que compreende, dentre outras formas de liberdade, a de pensamento. Dentre as previsões constitucionais relacionadas à liberdade de pensamento e de informação pode-se destacar:

> Art. 5 – 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:
>
> IV – é livre a manifestação de pensamento, sendo vedado o anonimato;
>
> V – é assegurado o direito de resposta, proporcional ao agravo, além de indenização por dano material, moral ou à imagem;

> IX – é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença;
>
> XIV – é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício ao exercício profissional;
> XXXIII – todos têm direito a receber dos órgão públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade de do Estado;
>
> LXXII – conceder-se-á habeas data:
>
> a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constante de registros ou banco de dados de entidades governamentais ou de caráter público;
>
> b) para retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo;

Os direitos e as garantias fundamentais estabelecidas nos incisos do art. 5º procuram conferir garantias ao exercício das liberdades básicas do cidadão, dentre as quais se destacam a liberdade de pensamento e de informação. A chamada liberdade informática, decorrente diretamente do modo de vida informacional no qual a sociedade brasileira vem sendo inserida, configura-se como o direito que o cidadão possui de livremente utilizar instrumentos da tecnologia da informação para informar e para informar-se. Esse direito é reconhecido por Paesani[81] como uma decorrência da liberdade de informação que se fundamenta em norma constitucional materializada no art. 220, *in verbis*: "A manifestação do pensamento, a criação, a expressão e a informação, sob qualquer forma, processo ou veículo não sofrerão qualquer restrição, observado o disposto nesta Constituição."

Apesar de ser considerado como uma conseqüência do estado de exceção vivenciado pelo Brasil em momento histórico anterior a ordem constitucional vigente, onde todos os meios de informação do cidadão foram tolhidos pela política de censura e desinformação do Estado, o preceito constitucional insculpido no artigo 220 da Constituição representa uma das maiores garantias democráticas existentes na carta constitucional. O movimento de redemocratização da sociedade permitiu o reflorescimento do direito de informação sob a égide de um novo prisma, o da tecnologia da informação. Uma das chaves do processo democrático é a disponibilidade de acesso a todos os cidadãos à circulação de informações. E aí reside a magnitude do dispositivo constitucional previsto no artigo 220: a ausência de

[81] PAESANI, Liliana Minardi, op. cit., 2006. p.21.

restrição aos meios de difusão de informação o que permite a expansão da proteção em análise aos meios tecnológicos.

Logo, a partir da utilização de meios de produção e difusão de informação cada vez mais sofisticados e avançados tecnologicamente, o que na maioria das vezes pressupõe um custo elevado, surge a possibilidade de se criarem novos mecanismos de segregação social, especialmente no que tange ao exercício da cidadania. Assim, "Para que a cidadania seja plena, precisamos investir na autonomia do cidadão e na democratização da informação, o que implica potencializar processos horizontais de organização, produção e aprendizagem coletiva que se constroem com o acesso às informações."[82] Contudo, ao analisar assunto Ingo Wolfgang Sarlet conclui que:

> se a expansão e complexificação dos processos comunicativos na sociedade de massas, ainda mais considerando os avanços tecnológicos que potencializam as possibilidades das liberdades comunicativas e informativas mediante o recurso à informática e comunicação de dado, serve, por um lado, como poderoso recurso à ampliação da s liberdades fundamentais de um modo geral (basta aqui lembrar do papel dos meios de comunicação na prevenção e repressão a violação de direitos), também é verdade que não tem sido poucos os abusos praticados mediante a utilização da tecnologia da comunicação, como dão conta os lamentáveis exemplos da pornografia infantil, da discriminação de minorias dentre tantos outros.[83]

Hoje, o volume e a variedade de informações que podem ser amealhadas por meio dos recursos tecnológicos existentes permitem reunir sobre um único cidadão dados que vão desde o seu perfil de saúde até seu equilíbrio econômico. A utilização dos recursos de tratamento de informações pra fins de coleta de dados dos cidadãos pode atingir diretamente a dignidade da pessoa humana de duas formas bastante lesivas: a primeira reputa na ofensa direta aos direitos de intimidade, privacidade e sigilo tutelados constitucionalmente nos incisos X e XII do artigo 5º da Constituição Federal de 1988. Ademais, diante da profusão de dados e informações relacionadas ao indivíduo, este corre o risco de ser reduzido a mais um simples número, não passando de mais uma mercadoria globalizada. Para ilustrar melhor a amplitude do problema transcreve-se abaixo exemplo citado por Têmis Limberger:

> Loja filma todas as reações de seus consumidores. Diante da constatação de que as pessoas omitem ou alteram informações quando são questionadas em pesquisas de consumo, determinada loja de departamentos resolveu usar centenas de câmeras de

[82] PRETTO, Nelson; BONILLA, Maria Helena. **Sociedade da informação:** democratizar o quê? Salvador. Disponível em: <http://www.faced.ufba.br/not/83.htm>. Acesso em: 11 out. 2007.
[83] SARLET, Ingo Wolfgang (Org.). **Direitos fundamentais, informática e comunicação e algumas aproximações**. Porto Alegre: Livraria do Advogado, 2007. p.07.

> circuito interno de tv, microfones ultra-sensíveis e uma central de última geração na qual se concentraram monitores. Os consumidores são filmados em todas as suas reações: quanto tempo ficam paradas diante de um produto, qual o cartaz de ofertas que foi mais observado, quais são as reações diante dos preços. O consumidor é observado como um peixe num aquário. Como advertência aos que entram na loja, foi colocado um cartaz com os seguintes dizeres: 'Este lugar está sendo filmado para teste; se isso o incomoda, volte quando este aviso não estiver aqui.'[84]

A quantificação e armazenamento das várias fontes de informações existente permitem, atualmente, a construção de inúmeros tipos diferentes de mecanismos de sistematização e análise dos dados e das informações obtidas. O simples cruzamento de fontes de dados completamente distintas podem gerar a construção de informações que violem frontalmente as previsões constitucionais protetivas à intimidade e à privacidade. Tome-se, por exemplo, o potencial existente no conhecimento advindo do cruzamento dos dados coletados por uma empresa administradora de cartão de crédito, com os dados provenientes da utilização de um cartão de movimentação bancária, com as informações colhidas através da invasão do banco de dados de uma empresa prestadora de serviços de saúde, com os dados de uma biblioteca como os livros locados, e mais a infinidade de informações disponíveis na *Internet*. Esse conjunto informacional isolado já possui por si só um risco de dano elevado, e versam sob aspectos íntimos de qualquer indivíduo, não devendo de forma alguma cair em domínio público. Imagine-se o potencial advindo da soma de todos esses dados? A lesividade da chamada "engenharia social", nome da conduta acima narrada expõe de forma clara o viés negativo da utilização das ferramentas tecnológicas, e a necessidade premente de intervenção do Estado nessa esfera.

Assim, Augusto Eduardo de Souza Rossini[85] aborda várias condutas que violam a privacidade na Rede Mundial de Computadores exemplificando pelos *spamming* (forma de envio de mensagens publicitárias por correio eletrônico), *cookies* ou "biscoitinhos da *web*" (pequenos arquivos de textos que são gravados no computador do usuário pelo *browser* (navegador) quando ele visita determinados sites de comércio eletrônico), *spywares* (programas espiões que enviam informações do computador do usuário da rede para desconhecidos), *hoaxes* (*e-mails* que possuem conteúdos alarmantes e falsos, geralmente apontados como remetentes empresas importantes ou órgãos governamentais, ou "boatos espalhados por mensagens de correio eletrônico, que servem para assustar o usuário de

[84] LIMBERGER, Têmis. Direito e informática: os desafios de proteger os direitos do cidadão. In: SARLET, Ingo Wolfgang (Org.), op. cit., 2007. p.216.
[85] ROSSINI, Augusto Eduardo de Souza. Brevíssimas considerações sobre delitos informáticos. **Caderno Jurídico,** São Paulo, n. 4, ano 2, jul. 2002.

computador"[86]), *sniffers* (programas espiões assemelhados aos *spywares*, que introduzidos no disco rígido, visam a rastrear e reconhecer *e-mails* que circulam na rede) e *Trojan Horses* ou "cavalos de tróia" (vírus que, uma vez instalados nos computadores, abrem suas portas, tornando possível a subtração de informações).

Cresce assim a necessidade do Estado intervir na fruição dos meios tecnológicos de produção e difusão de conhecimento e informação. Essa intervenção, normatizada pelas balizas constitucionais, deve entretanto, ser focada não na completa dominação dos meios comunicativos através da imposição de conteúdos, mas sim através da fiscalização e inibição de práticas nocivas, seja por meio da regulamentação administrativa dos meios e ferramentas ainda não regulados, seja exercendo sua função de zelar pelos bens jurídicos advindos com essas transformações sociais através do direito civil e penal.

Contudo, diante das características apresentadas pelo atual contexto organizativo social, e das peculiaridades das relações travadas por intermédio dos meios eletrônicos, o Estado ainda possui plena capacidade de impor de maneira soberana regras e limites à nova ordem que se apresenta?

2.2 O impacto da tecnologia da informação na estrutura do Estado nacional

O homem enquanto ente social buscou ao longo de sua evolução construir mecanismos de organização capazes de agregar aos grupamentos sociais maior capacidade de resistência aos obstáculos naturais que assolavam a marcha do gênero humano. A sua capacidade de organização e abstração fizeram com que a humanidade superasse todas as intempéries surgidas no transcorrer de sua existência.

O grau de organização e especialização da sociedade humana atingiu níveis extremamente profundos e densos, possibilitando assim, que o homem apesar de sua frágil constituição corporal, pudesse se sobressair na luta pela sobrevivência individual e coletiva.

[86] CONCERINO, Arthur José. Internet e segurança são compatíveis? In: LUCCA, Newton de; SIMÃO FILHO, Adalberto (Coord.). **Direito e Internet:** aspectos jurídicos relevantes. Bauru: Edipro, 2000. p.135.

Elemento primordial na constituição dessa organização social e figura indispensável para o desenvolvimento da sociedade humana foi o surgimento do Estado.

Apesar de atualmente o termo Estado ser facilmente compreendido, mesmo que de forma leiga, sua conceituação nos meios acadêmicos ainda não se deu de forma pacífica. O termo Estado, originado do latim *status*, surgiu inicialmente na obra "O Príncipe" de Maquiavel e data de 1513, associando-se diretamente a situação de convivência permanente de determinada sociedade política, passou a denominar as chamadas cidades independentes italianas.

Contudo vale salientar que o surgimento do termo especifico não necessariamente significa que o Estado tenhas nascido nesse período, posto que é justamente sobre a época que este surgiu que repousa um dos maiores pontos de discórdia entre os doutrinadores.

Ressalte-se que o aprofundamento das discussões acerca do Estado, como aconteceu com as ciências humanas, ocorreu notadamente no século XX. As discussões relacionadas às teorias do Estado e da sociedade, as conjecturas acerca da história humana, bem como sob as questões de método nortearam os debates e figuraram como elementos basilares da pesquisa filosófica dessa época. Assim, os debates relacionados à figura do Estado ganharam ênfase influenciando inúmeras teorias relacionadas à sociologia, à antropologia, à economia e à filosofia do direito. Antes de conceituar o Estado, configura-se extremamente importante tecer algumas linhas sobre os principais questionamentos discutidos pela doutrina em relação a este. O primeiro refere-se a necessidade de estabelecer em que momento da evolução da sociedade humana surgiu o Estado. Já o segundo ponto repousa na necessidade de se estabelecer como foi constituído o Estado, como por exemplo, se foi um fenômeno natural ou uma criação humana. E o terceiro ponto figura na necessidade de caracterizar e analisar seus elementos essenciais.

Afirmar precisamente em que época surgiu o Estado configura-se uma tarefa impossível, e muitos pensadores procuraram estabelecer marcos, muitas vezes não fundamentados, de quando o Estado surgiu. Das inúmeras teorias existentes podem se destacar três grupos principais.

A primeira corrente sustenta que o Estado, bem como a sociedade, sempre existiram de forma indissociável. Posto que desde que o homem passou a se organizar em sociedade, ou seja, integrado em uma organização social, existiu um elemento dotado de poder e autoridade que dirigia os rumos e o comportamento da organização social. Assim, o Estado seria considerado um elemento inseparável da sociedade humana, e onde esta existisse o Estado estaria presente, funcionando sempre como o princípio organizador e unificador de toda e qualquer organização social da humanidade.[87]

Verifica-se antes de qualquer coisa que a concepção formulada por essa corrente induz a um alcance muito grande do conceito de Estado, conferindo-lhe um espectro de incidência muito amplo, o que desnatura-lhe e impossibilita a sua utilização.

A Segunda concepção admite que as organizações sociais humanas existiram durante algum período sem a figura do Estado, sendo este até então uma estrutura dispensável para a manutenção da organização social humana. Contudo, em determinado momento histórico, e em virtude de alguma necessidade especial de cada organização social, este foi constituído com a finalidade de otimizar o processo organizativo dos grupos sociais atendendo as suas necessidades e conveniências. Vale ressaltar que esse posicionamento sugere que o Estado seja decorrência da evolução dos grupamentos sociais existentes e que isso aconteceu em momentos históricos distintos, não existindo assim concomitância na formação do Estado nos mais diferentes lugares.[88]

A terceira corrente fundamenta o surgimento do Estado no momento em que a organização social atinge determinado nível de organização possuindo certas características bem delimitadas. Assim, o Estado não se compõem de um conceito estanque, estático, mas sim um conceito histórico e concreto, relacionado, por exemplo, com o desenvolvimento da idéia e da prática de soberania, o que efetivamente aconteceu somente no século XVII.

Outro aspecto importante repousa na definição das causas que levaram ao surgimento do Estado, posto que, dentre as três principais correntes que apontam o nascimento do Estado, destacam-se as que demonstram que o Estado não surgiu atrelado à sociedade, e sim surgiu do seu evoluir. Assim, deve-se procurar estabelecer quais as causas que desencadearam o

[87] DALLARI, Dalmo de Abreu. **Elemento de teoria geral do Estado**. 19. ed. São Paulo: Saraiva, 1995.
[88] Ibid., 1995.

processo de formação do Estado. Nesse sentido destacam-se duas grandes correntes: a teoria da formação natural ou espontânea do Estado e a teoria contratual do surgimento do Estado.

A teoria da formação natural do Estado sustenta que o surgimento do Estado decorreu da evolução natural dos grupamentos sociais, sendo, portanto, uma simples conseqüência do desenvolver das organizações sociais humanas, ou seja, um passo natural no desenvolver da humanidade e funda-se em quatros possíveis origens: a familiar defende que o Estado surgiu de uma evolução natural da organização familiar; a baseada nos atos de força ou de conquista, que sustenta ter o Estado surgido das relações de dominação entre os grupos sociais; mais fortes em detrimento dos mais fracos; as fundadas em causas econômicas defendem que o Estado surgiu para regular as relações econômicas existentes entres os grupos sociais, e por último, a baseada no desenvolvimento interno da sociedade que edificaram a idéia de que o Estado seria um germe, uma potencialidade, em todas as sociedades humanas, as quais, todavia, prescindem dele quando se mantêm simples e pouco desenvolvidas. Mas aquelas sociedades que atingem maior grau de desenvolvimento e alcançam uma forma complexa têm absoluta necessidade do Estado, e então ele se constitui. Assim, seria o próprio desenvolvimento espontâneo da sociedade que dá origem ao Estado, não havendo influência de fatores externos aos grupamentos sociais.[89]

A segunda grande corrente, denominada contratualista, fundamenta o surgimento do Estado na existência de um ato de vontade, ficto, dos homens formadores da organização social que o fundou. As teorias que sustentam a formação contratual do Estado, apesar de divergirem nas causas, apresentam ponto em comum: a crença em que foi a vontade de alguns ou de todos os homens que criaram o Estado, ou seja, que este originou-se de uma convenção fictícia firmada entre os homens membros da sociedade.

A teoria contratualista, que concebe o poder estatal como produto da vontade humana, considera ser mais vantajosa para o homem a associação, não só para defendê-lo de um mundo hostil, como também, para satisfazerem melhor as necessidades, de forma que Hobbes viu no temor dos homens a razão para o surgimento das sociedades e do Estado, reconheceu, ainda, que, estes proporcionam ao homem segurança, tendo em vista que no estado natural o homem tinha que estabelecer seus direitos através da força.

---

[89] Ibid., 1995.

Dessa forma, o Estado surgindo de uma convenção teórica firmada entre os homens, procura estabelecer condições para a efetiva proteção de garantias essenciais como a vida, a liberdade e a propriedade, que só estariam efetivamente respaldadas dos demais, com o surgimento de um ente responsável pela regulamentação da organização social, ou seja, o Estado. Verifica-se dessa forma que não existe um consenso firmado pela doutrina acerca da origem, bem como sob o momento em que surgiu o Estado. Contudo, um dos estudos mais aprofundados e coerentes que versam sob o Estado merece destaque. Hermann Heller, ao analisar o surgimento do Estado, destacou cinco pontos principais que ensejaram o desenvolvimento dessa figura.

O referido autor destaca que o Estado, nos moldes atuais, só surgiu depois da superação do chamado Estado Medieval, ou Estamental. Estabelece ainda, que a ocorrência de alguns fatores contribuíram sobremaneira para o seu desenvolvimento. O primeiro ponto elencado pelo doutrinador foi a ocorrência da chamada reforma protestante que desvinculou o poder dos príncipes, e conseqüentemente do Estado, da dominação eclesiástica:

> *El hecho de que la Iglesia representara durante siglos la única organización monista de autoridad, en un mundo en que el poder estaba disgregado a la manera feudal, no fue la causa menos poderosa de su supremacía. El punto culminante, y a la vez el comienzo de la quiebra de la supremacía papal lo constituyen la bula Unam sanctam, de Bonifacio VIII (1302) y la negación de obediencia por parte de Felipe de Francia, que tuvo lugar al año siguiente. La Reforma trajo como consecuencia la emancipación definitiva y total del poder del Estado respecto a la Iglesia, incluso en los Estados católicos.*[90]

O segundo fator apontado por Heller, como indispensável para a formação do Estado, foi a superação da atomização política existente à época do feudalismo. Assim a pulverização de poder existente nesse período foi concentrada na mão de uma só instância política facilitando a tomada de decisões e a subordinação dos dominados, posto que se dissipou a divisão estamental:

> *La nueva palabra Estado designa certeramente una cosa totalmente nueva porque, a partir Del renacimiento y en el continente europeo, las poliarquías, que hasta entonces tenían un carácter impreciso en lo territorial y cuya coherencia era floja e intermitente, se convierten en unidades de poder continuas y reciamente organizadas, con un solo ejército que era, además, permanente, una única y competente jerarquía de funcionarios y un orden jurídico unitario, imponiendo además a los súbditos el deber de obediencia con carácter general. A consecuencia de la concentración de los instrumentos de política- fenómeno que se produce primeramente en el norte de Italia debido al más temprano desarrollo que alcanza allí la economía monetaria – surge aquel monismo de poder, relativamente estático,*

[90] HELLER, Hermann. **Teoria del Estado**. Argentina: Fondo de Cultura Económica, 1992. p.143

> *que diferencia de manera característica al Estado de la Edad Moderna del Territorio medieval.*[91]

O terceiro fator figura na constituição de uma milícia armada permanente e diretamente vinculada ao governante que mitigou a dependência deste em relação aos demais membros da estrutura feudal:

> *Mediante la creación de un ejército mercenario permanente, cuya existencia depende del pago de la soldada, el señor se hace independiente del hecho aleatorio de la lealtad de sus feudatarios, estableciendo así la unidad de poder del Estado en lo militar... De este modo, la necesidad política de crear ejércitos permanentes dio lugar en muchas partes a una transformación en sentido burocrático, de la administración de las finanzas.*[92]

A manutenção financeira do aparato militar ocasionou a necessidade de organização de um sistema burocrático administrativo de arrecadação e aplicação dos recursos públicos, e foi esse, segundo Heller, um dos fatores mais importantes para a estruturação do Estado, posto que essa organização administrativa possibilitou a centralização do poder político, uma vez que por intermédio da burocratização administrativa eliminou-se a relativização da autoridade estatal feudal e foi possível se criar uma vinculação entre soberano e súdito, de caráter geral e unitária.

Entretanto, Heller afirma que a circunstância deflagradora do surgimento do Estado nos moldes atuais foi a incorporação deste no mundo jurídico:

> *La codificación dispuesta por el príncipe y la burocratización de la función de aplicar y ejecutar el derecho eliminaron, finalmente, el derecho del más fuerte y el desafío, e hicieron posible la concentración del ejercicio legítimo del poder físico en el Estado..... Solo al aparecer las codificaciones oficiales y la jurisdicción burocrático-absoluta y al producirse, en fin, la emancipación del Estado como una unidad de autoridad, se hizo precisa una neta distinción entre derecho de coordinación y derecho de subordinación, entre ley y contrato, entre creación de derecho y jurisdicción. Sólo al surgir la unidad autónoma de poder del Estado moderno se le pudo reclamar, con sentido, como un especial sujeto de derecho caracterizado por su autoridad.*[93]

Assim, após a análise dos elementos que ensejaram o surgimento e o desenvolvimento do Estado verifica-se que a relação do Estado com o Direito revelou-se um dos pontos mais importantes para o surgimento do Estado. A relação entre Estado e Direito pode ser entendida

---

[91] HELLER, Hermann, op. cit., 1992. p.145.
[92] HELLER, Hermann, op. cit., 1992. p.147.
[93] HELLER, Hermann, op. cit., 1992. p.151.

sob o prisma de três concepções. A primeira, a dualística, sustenta que apesar das similitudes, Direito e Estado são duas coisas completamente diferentes, não se confundindo de forma alguma. A segunda corrente, denominada de Paralelismo, defende que Direito e Estado são entidades essencialmente distintas, mas que mantém íntimo grau de relacionamento e interdependência. Já a terceira corrente, nominada de monista, sustenta que Direito e Estado seriam a mesma coisa, não possuindo diferenças entre si. Logo, entende-se que o Estado seria um simples fenômeno jurídico, um ente jurídico.

Definir qual o grau de relação existente entre o Direito e o Estado figura ser uma tarefa aparentemente impossível, contudo analisando o assunto Heller afirma:

> *Mientras se contraponga, sin género alguno de mediación dialéctica entre ambos, el derecho al poder de voluntad del Estado, no podrá comprenderse de modo cabal ni lo específico del derecho ni lo característico del Estado y, por consiguiente, tampoco la relación que existe entre uno e otro. Son, sobre todo, incompresibles la validez y la positividad del derecho sin una correlación entre el Estado y el derecho. Hay que concebir al Derecho como lá condición necesaria del Estado actual y, asimismo, al Estado como la necesaria condición del derecho del presente. Sin el carácter de creador de poder que el derecho entraña no existe ni validez jurídica normativa ni poder estatal; pero sin el carácter de creador de derecho que tiene el poder del Estado no existe positividad jurídica ni estado. La relación entre el estado y el derecho no consiste ni en una unidad indiferenciada ni en una irreductible oposición. Por el contrario, esa relación debe ser estimada como una relación dialéctica, es decir – como relación necesaria de las esferas separadas y admisión de cada polo en su opuesto.*[94]

Analisando o assunto Kelsen, verificou não existir distinção entre o Direito e o Estado. Assevera o autor que o Estado nada mais é que a personificação do ordenamento jurídico de determinada sociedade politicamente organizada, mais ainda, sustenta não haver distinção entre o Direito e o Estado, definindo este como uma "ordem jurídica relativamente centralizada"[95]. Reforçando seu entendimento, Kelsen, procura demonstrar não só a identidade do Direito com o Estado, mas também o caráter ideológico desse dualismo entre Direito e Estado.

> Quando a teoria tradicional do Direito e do Estado contrapõe o Estado ao Direito como uma entidade diferente deste e, apesar disto, o afirma como uma entidade jurídica, ela estrutura esta idéia considerando o estado como sujeito de deveres jurídicos e direito, quer dizer, como pessoa, atribuindo-lhe ao mesmo tempo uma existência independente da ordem jurídica. Assim, como a teoria do direito privado pressupõe originariamente que a personalidade jurídica do indivíduo precede lógica e cronologicamente o direito objetivo, isto é a ordem jurídica, assim também a teoria do Estado pressupõe que o Estado, enquanto unidade coletiva que aparece como

---

[94] HELLER, Hermann, op. cit. 1992. p.209.
[95] KELSEN, Hans. **Teoria pura do direito**. 6. ed. São Paulo: Martins Fontes, 2003. p.318.

> sujeito de uma vontade e de uma atuação, é independente do Direito e até preexistente ao mesmo. Mas o Estado cumpre sua missão histórica – ensina-se- criando o Direito – o seu – Direito, a ordem jurídica objetiva, para depois se submeter ele próprio a ela, quer dizer: para se obrigar e se atribuir direitos através do seu próprio Direito. Assim, o Estado é, como entidade metajurídica, como uma espécie de poderoso macro-ánthropos ou organismo social, pressuposto do Direito e ao mesmo tempo, sujeito jurídico que pressupões o Direito porque lhe está submetido, é por ele obrigado e dele recebe direitos.[96]

Continuando com sua construção doutrinária, Kelsen critica duramente a existência do dualismo entre Direito e Estado, posto que configura-o essencialmente como uma ferramenta ideológica uma vez que o Estado deve ser representado como uma pessoa diferente do direito para que o direito possa justificar o Estado – que cria este direito e se lhe submete. Mais ainda, o Direito só pode justificar o Estado quando é considerado um pressuposto, ou seja, como uma ordem essencialmente diferente do Estado, oposta a sua originária natureza, o poder, e por isso mesmo, reta ou justa em qualquer sentido. Assim o Estado é transformado de um simples fato de poder em Estado de Direito, que se justifica pelo fato de fazer o Direito. Do mesmo passo que uma legitimação metafísica-religiosa do Estado se torna ineficaz, impõe-se a necessidade de esta teoria do Estado de Direito se transformar na única possível justificação do Estado.

Assenta assim Kelsen uma enorme contradição do Dualismo existente entre o Estado e o Direito, posto que, afirma o Estado como uma pessoa jurídica e ao mesmo tempo assenta o Estado como um poder, algo essencialmente diferente do direito, impossível de ser concebido juridicamente. Kelsen defende de forma arraigada a identidade do Direito com o Estado desenvolvendo sua teoria sob o Estado e seus elementos formadores sob o prisma jurídico, evidenciando sempre que o Estado nada mais é que a corporificação da ordem jurídica de uma determinada sociedade politicamente organizada.

Partindo da análise das obras Teoria Pura do Direito e Teoria Geral do Direito e do Estado de Hans Kelsen pode-se traçar um perfil do que o autor prescreve como sendo o Estado, bem como de seus principais componentes.

Kelsen considera o Estado como uma personificação da ordem jurídica nacional, e repudia de forma bastante veemente qualquer relação que possa vir a associar o conceito jurídico de Estado a alguma definição de cunho sociológico. Assim Kelsen procura manter a

---

[96] Ibid., 2003. p.315.

coerência de seu purismo metodológico e afasta de seu estudo qualquer influência da sociologia, notadamente no tocante a conceituação dos institutos ligados ao Estado. Dessa forma o autor discorre:

> O Estado não se identifica com nenhuma das ações que formam o objeto da sociologia, nem com a soma de todos eles. O Estado não é uma ação ou uma quantidade de ações, não mais do que é um ser humano ou uma quantidade de seres humanos. O Estado é aquela ordem da conduta humana que chamamos de ordem jurídica, a ordem à qual se justam as ações humanas, a idéia à qual os indivíduos adaptam sua conduta. Se a conduta humana adaptada a essa ordem forma o objeto da sociologia, então seu objeto não é o Estado. Não existe nenhum conceito sociológico ao lado do conceito jurídico. Tal conceito duplo de Estado é impossível, senão por outro motivo, pelo menos pelo fato de não poder existir mais de um conceito do mesmo objeto. Existe apenas um conceito jurídico de Estado: o Estado como ordem jurídica.[97]

Kelsen, mais uma vez reforçando a pureza metodológica que tanto persegue, estabelece que o conhecimento do Estado deve ser isento de conhecimentos ideológicos, metafísicos e místicos.Assim, procurando um conhecimento do Estado alheio as influências externas à ciência jurídica, Kelsen fundamenta a sua Teoria do Estado na congruência do Direito com o Estado, sendo este a manifestação de uma ordem de conduta humana centralizada. Nesse sentido, os elementos caracterizadores do Estado só podem ser analisados sob o viés jurídico. Ou seja, o povo, o território e o poder soberano só podem ser entendidos conseqüentemente como fenômenos jurídicos:

> Como comunidade social, o Estado – de acordo com a teoria tradicional do Estado – compõe-se de três elementos: a população, o território e o poder, que é exercido por um governo estadual independente. Todos estes três elementos só podem ser definidos juridicamente, isto é, eles apenas podem ser apreendidos como vigência e domínio de vigência – validade – de uma ordem jurídica.[98]

Logo, ao se analisar os elementos formadores do Estado, Kelsen, seguindo seus preceitos metodológicos, verifica ser a população a esfera pessoal de validade de determinada ordem jurídica, ou seja:

> A unidade dos indivíduos que formam a população de um Estado em nada mais pode ver-se do que no fato uma e a mesma ordem jurídica vigora para esses indivíduos, de que a sua conduta é regulada por uma e a mesma ordem jurídica. A população de um Estado é o domínio pessoal de vigência da ordem jurídica estatal.[99]

---

[97] KELSEN, Hans. **Teoria geral do direito e do Estado**. 2. ed. São Paulo: Martins Fontes, 1995. p.190.
[98] KELSEN, Hans, op. cit., 2003. p.318.
[99] KELSEN, Hans, op. cit., 2003. p.319

O povo, no entender de Kelsen, figura como o conjunto de seres humanos, homens, considerados em sua unidade e que se submetem a mesma ordem jurídica nacional. É de forma singela o campo pessoal de incidência de determinada ordem jurídica.

O outro elemento do Estado, o território, pode ser definido sob a ótica kelseniana como a esfera espacial de vigência de determinada ordem jurídica nacional, nas palavras do autor:

> O chamado território do Estado só pode ser definido como o domínio espacial de vigência de uma ordem jurídica estatal, não se vinculando de forma alguma a idéia de unidade territorial. Assim o território configura-se como a esfera territorial de validade da ordem jurídica estatal, onde o Estado pode exercer atos coercitivos.[100]

Repousa justamente nesse ponto uma das grandes controvérsias decorrentes do atual modelo de organização social, econômico e político. O Estado ainda é capaz de fazer valer sua ordem jurídica em seu território? A soberania no seu sentido clássico continua intocada? Kelsen caracterizava o poder soberano como a possibilidade do Estado de fazer valer a sua ordem jurídica nacional, ou seja, na capacidade que o Estado tem de fazer valer, cumprir, a ordem jurídica estabelecida, o que configura-se como a capacidade de valer viger a ordem jurídica estadual.

Em uma análise histórica percebe-se que a soberania tem sido vista como uma qualidade intrínseca e definidora do Estado. Assim, para que um Estado nacional possa ser reconhecido, deve além dos requisitos clássicos estabelecidos (povo, território e finalidade), possuir soberania. "A existência do Estado é caracterizada no plano político-social pela existência de território, população e governo; e no plano jurídico pela soberania. Assim, o Estado deve possuir território, população e um governo soberano."[101]

O conceito de soberania como elemento estrutural e indispensável ao Estado foi primeiramente desenvolvido por Jean Bodin e significava em seu aspecto principal que:

> consistia no poder de fazer e de anular leis, sem o consentimento do maior, semelhante ou menor que ele. Era um poder absoluto e perpétuo, que poderia decretar a guerra e negociar a paz, instituir os principais funcionários, conferir graça aos condenados acima das sentenças e contra o rigor das leis, cunhar moedas,

[100] KELSEN, Hans, op. cit., 2003. p.319
[101] AGUIAR**,** Eduardo Henrique de Almeida. Da soberania do Estado brasileiro frente a OMC. In: GUERRA**,** Sidney; SILVA, Roberto Luis (Org.). **Soberania** – Antigos e novos paradigmas. Rio de Janeiro: Freitas Bastos, 2004. p.125.

> confiscar bens dos condenados, instituir impostos, entre outros. Assim, não era reconhecido ninguém acima do soberano a não ser Deus. Apesar de absoluto encontrava-se limitado pelas leis divinas e naturais.[102]

Originada da palavra latina *superanus*, a soberania tem como significado o grau supremo de poder na hierarquia política. A soberania é "extraída dos livros da filosofia política e da história da afirmação do poder central contra a dispersão do poder provocada pelo modo de produção feudal e contra as tentativas de universalização política (o Sacro Império) e religiosa (o Papado).[103]

Nesse contexto, procedendo a uma análise do desenvolvimento histórico do significado jurídico e político da soberania Albuquerque expõe:

> A soberania passa a adquirir um significado claramente político e jurídico somente com o processo real de centralização do poder, ocorrido nos séculos XV e XVI, decorrentes das necessidades dos altos estamentos feudais, da burguesia que lutava pela extensão dos mercados nacionais e dos próprios interesses da monarquia. É com Bodin, Maquiavel e Hobbes, pensadores e filósofos identificados com a noção absolutista do poder, que se formam as bases doutrinárias de uma adequada fundamentação autônoma do poder secular em relação à igreja. A soberania passa agora a ser compreendida como um conceito vinculado ao poder decisional supremo do monarca sobre todos os outros poderes, a quem de resto não cabe mais questionar sobre o sentido de justiça ou não de seus comandos imperativos. A afirmação da vontade concentrada do monarca absolutista não precisa mais recorrer ao consentimento de outrem, seja ele povo ou o papa, pois ela passa a ser tida como vontade originaria e não mais delegada, sendo assim considerada como fonte imediata de qualquer outra ordem em seu território. [104]

Assim, a soberania pode ser caracterizada dentre outras formas como a capacidade que determinado Estado-nação possui de instituir e aplicar sua ordem jurídica, em suma, fazer valer em seu território, em seu âmbito de validade territorial, seus comandos jurídicos.

Contudo, no atual contexto da sociedade globalizada, as novas tecnologias da comunicação e informação, como *Internet*, aboliram as distâncias físicas reais, e como conseqüência aceleraram a própria noção de realidade. Essa modificação da geofísica global ocasionou uma espécie de desterritorialização dos Estados, e conseqüentemente o enfraquecimento do conceito de soberania.

---

[102] SORIANO, Aldir Guedes**.** Soberania e o direito à liberdade religiosa. In: Ibid., 2004. p.85.
[103] LUPI, André Lipp Basto. Soberania e direito internacional público. In: Ibid., 2004. p.102.
[104] ALBURQUEQUE, N.M apud AGUIAR, Eduardo Henrique de Almeida, op. cit., In: Ibid., 2004. p.142.

Para melhor contextualizar a situação deve-se fazer menção ao caso emblemático dos jogos de azar *online*. "Os Estados Unidos, por exemplo, gostariam de regular o jogo virtual, mas têm problemas em fazê-lo por que os donos de cassinos estabeleceram seus negócios, por precaução, no Caribe"[105]. Outra situação exemplificativa é citada por Érica Ferreira em caso suscitado por Omar Kaminski:

> Duas situações práticas são trazidas por Omar Kaminski, a primeira de conduta ilícita no Brasil e permitida em estado vizinho e a outra no sentido contrário, permitida aqui, mas proibida em outros países: os cassinos *on-line,* citando *site* legalizado na Argentina que possibilita a qualquer brasileiro, utilizando de seu cartão de crédito internacional, realizar conduta que aqui seria ilícita, inclusive informa o autor que, em Liechtenstein, esta atividade é patrocinada e incentivada pelo governo; e ainda a situação de um brasileiro colocar fotos de mulheres nuas, expondo-se a condenações em países islâmicos.[106]

Aproveitando o caso apresentado, e transportando-o para o contexto jurídico brasileiro, percebe-se que apesar da situação em tela configurar ilícito penal o Estado brasileiro nada pode fazer para coibir a prática dos referidos ilícitos em seu território, haja vista que a base eletrônica utilizada para dar suporte as atividades encontra-se fundada em país onde não existe nenhuma restrição as mesmas. Em uma comparação um pouco grosseira, a situação em tela, que pode ser estendida a um sem número de outras situações criminosas, equipara-se a idéia de uma constante invasão do território aéreo brasileiro por traficantes de armas. Ocorre que nessa situação, o Estado brasileiro possui elementos jurídicos hábeis a fundamentar o exercício de atividades que exprimam a sua soberania, como por exemplo, o abate das aeronaves suspeitas. Mas no caso das invasões eletrônicas, como impedir o avanço das atividades ilícitas praticadas por meios eletrônicos, especialmente pela *Internet*? A desconstrução da força do conceito de soberania fica ainda mais evidente quando se percebe os impactos do fenômeno da globalização, posto que segundo Castells:

> O Estado-Nação vem sendo cada vez mais destituído de poder para exercer controle sobre a política monetária, definir orçamento, organizar a produção e o comércio, arrecadar impostos de pessoas jurídicas e honrar seus compromisso visando proporcionar benefícios sociais. Em suma, o Estado-Nação perdeu a maior parte de seu poder econômico, embora detenha ainda certa autonomia par o estabelecimento de regulamentação e relativo controle sobre seus sujeitos.[107]

Assim, associando a perca da capacidade de gerenciamento econômico com a diminuição da capacidade de gestão de sua ordem jurídica, pode-se dizer que o Estado-Nação,

---

[105] MATIAS, Eduardo Felipe P., op. cit., 2005. p.162.
[106] FERREIRA, Érica Lorenço de Lima, op. cit., 2007. p.154.

vai aos poucos perdendo a sua soberania, sua capacidade de imposição perante a ordem econômica e jurídica internacional. "De fato, o crescente desafio à soberania dos Estados em todo o mundo parece advir da incapacidade de o Estado-Nação moderno navegar por águas tempestuosas e desconhecidas entre o poder das redes globais.[108]

Uma das fontes de sustentação do poder do Estado sempre foi a detenção e controle dos instrumentos de informações e entretenimento como forma de possuir o controle indireto sobre a formação e interpretação de opiniões e fatos. Esse mecanismo foi extremamente aperfeiçoado com o desenvolvimento das técnicas midiáticas de publicidade e com o amadurecimento dos meios de comunicação. Contudo, hoje, o Estado-Nação enfrenta três obstáculos inter-relacionados que contribuem sensivelmente para o seu enfraquecimento no contexto mundial: globalização e não exclusividade da propriedade; flexibilidade e a capacidade de penetração da tecnologia; e a autonomia e diversidade da mídia.[109]

> A comunicação via computador também foge ao controle do Estado-Nação, abrindo as portas a uma nova era de comunicação extraterritorial. A maioria dos governos parece estar aterrorizada diante dessa perspectiva. Em janeiro de 1996, o ministro da Tecnologia da Informação da França anunciou a intenção de seu governo de propor à União Européia uma série de medidas de proibição do livre acesso à Internet. O evento que deu origem a tal plano de censura tecnológica engendrado pelo mesmo país que difundiu os ideais revolucionários de liberdade na Europa, bem como a Minitel, foi a última batalha de Mitterrand. Após sua morte, um livro publicado pelo médico de Mitterrand revelou que o ex - primeiro ministro desenvolvera câncer de próstata durante os 14 anos de seu mandado. A pedido da família de Mitterrand, o livro foi retirado de circulação na França, mas podia ser lido na Internet. A indignação do governo francês foi bem além desse assunto em particular. Houvera uma demonstração clara de que atualmente as decisões do governo ou dos tribunais sobre o acesso a informações jamais poderiam ser efetivadas. E a compreensão de que o controle sobre as informações jamais poderiam ser efetivadas. E a compreensão de que o controle sobre as informações vinha sendo, desde bem antes do advento da Era da Informação, o sustentáculo do poder do Estado.[110]

Assim, a soberania do Estado vai sucumbindo ante a recontextualização da sociedade. O molde globalizado mediado pelo vetor tecnológico abrange uma gama de atividades que aos poucos vão erodindo a capacidade instrumental do Estado-Nação, seja no aspecto econômico, no aspecto informacional (mídia e comunicação eletrônica) ou no aspecto criminal, através da globalização do crime.

---

[107] CASTELLS, Manuel. **O poder da identidade** – A era da informação: economia, sociedade e cultura. Tradução. Roneide Venâncio Majer. 3. ed. São Paulo: Paz e Terra, 2001. v.2. p.298.
[108] Ibid., p.287.
[109] Ibid., p.298.
[110] Ibid., p.302.

Vale salientar que a globalização do crime, fenômeno irreversível, subverte de forma profunda o Estado-Nação, modificando seus procedimentos e deixando, como acima foi exemplificado o Estado de mãos atadas. Ressalte-se que o aspecto inovador no que tange a globalização da criminalidade não é a sua penetração junto às esferas econômica ou política, mas sim a sua conexão global, através de um denso entrelaçamento de relações internacionais que dentro de um contexto criminoso transnacional levam a derrocada da eficácia do Estado-Nação enquanto ente responsável por combatê-lo.

Mário Furlaneto Neto e José Augusto Chaves Guimarães[111] analisando publicação da ONU oriunda do Oitavo Congresso sobre Prevenção de Delito e Justiça Penal, celebrado em Havana, Cuba, em 1990, relacionam uma série de condutas que podem ser praticadas por meio de sistemas eletrônicos: 1) Fraudes cometidas mediante manipulação de computadores, caracterizadas por: a) manipulação de dados de entrada; b) manipulação de programas; c) manipulação de dados de saída; d) manipulação informática. 2) Falsificações informáticas: a) como objeto; b) como instrumento. 3) Danos ou modificações de programas ou dados computadorizados: a) vírus; b) gusanos; c) bomba lógica ou cronológica; d) acesso não-autorizado a sistemas de serviços; e) piratas informáticos ou *hackers*; f) reprodução não-autorizada de programas informáticos de proteção legal.

Já em verificando os resultados do Décimo Congresso sobre Prevenção de Delito e Tratamento do delinqüente, realizado em Viena, em abril de 2000, percebem que a ONU majorou a lista de delitos eletrônicos transnacionais acrescentando os ilícitos de: espionagem industrial, sabotagem de sistemas, sabotagem e vandalismo, pesca ou averiguação de senhas secretas, estratagemas, pornografia infantil, jogos de azar, fraude e lavagem de dinheiro.

Percebe-se assim, que a gama de condutas passíveis de serem perpetradas por meio de sistemas eletrônicos e seus efeitos devastadores, no que tange a manutenção da ordem político-jurídica constitucional, reflete a necessidade de estruturação de mecanismos legais aptos a controlarem a práticas desses ilícitos eletrônicos. Assim, ganha importância o estudo do crime eletrônico e dos instrumentos jurídicos de repressão a ele relacionados, o que será alvo de análise no próximo capítulo.

---

[111] FURLANETO NETO, Mário; GUIMARÃES, José Augusto Chaves. Crimes na internet: elementos para uma reflexão sobre a ética informacional. **Centro de Estudos Judiciários: CEJ**, Brasília, v.7, n. 20, p. 67-73, mar. 2003, p.70.

3 ASPECTOS CONSTITUCIONAIS E LEGAIS DO CRIME ELETRÔNICO

A necessidade de proteção aos bens jurídicos surgidos com o advento da sociedade da informação forçou a ordem jurídica penal a intervir de forma direta na regulamentação das condutas nocivas a esse conjunto de bens e valores carente de proteção. O presente capítulo procura analisar os instrumentos constitucionais e penais relacionados ao crime eletrônico.

3.1 Aspectos constitucionais gerais do direito penal

A vida coletiva, ou seja, a vida em sociedade vincula-se diretamente a idéia de um conjunto de regras mínimas que permitam a interação e a convivência dos envolvidos. Assim, a existência do Direito atrela-se a idéia de sociedade. Nesse sentido, Sílvio Rodrigues entende que o Direito "só pode ser imaginado em função do homem vivendo em sociedade"[112].

Dessa forma, o Direito visa estruturar o conjunto de regras necessárias à regulamentação desse ambiente coletivo, procurando conferir segurança e ordem as relações sociais existentes, posto ser a manutenção desses dois fatores indispensáveis para a sobrevivência da ordem social. Nesse contexto, a violação das regras impostas à sociedade pelo Direito, ou seja, regras jurídicas, implica necessariamente na prática de condutas nocivas à coletividade, causando assim, dependendo do valor que se procura proteger, uma ameaça mais elevada ou não a sobrevivência desta.

Os bens e valores jurídicos mais importantes para a manutenção, bem como, para o equilíbrio da sociedade, dentro de uma conotação jurídica, são tutelados, ou seja, protegidos, por um ramo especifico do Direito: o Direito Penal. A violação de uma norma penal

[112] RODRIGUES, Silvio. **Direito civil**. 32. ed. São Paulo: Saraiva, 2001. v. 1. p.3.

incriminadora configura um dos mais graves tipos de ilícitos existentes na ordem jurídica: o ilícito penal. O grau de reprovabilidade dessas condutas, por protegerem bens e valores jurídicos e sociais indispensáveis para a manutenção da sociedade, é tão grande, que às estes ilícitos são aplicadas as sanções mais gravosas existentes na ordem jurídica.

Na contextualização do Estado Democrático de Direito, uma das funções estruturais do Estado é a organização e manutenção de uma sociedade erigida sobre os valores da liberdade, da justiça, da solidariedade e especificamente na ordem constitucional brasileira, da dignidade da pessoa humana. Para o alcance de tão complexo desiderato, o Estado, utilizando de suas ferramentas político-jurídicas procura fixar um conjunto de medidas voltadas tanto à prevenção como à repressão de lesões ou ameaças de gravames aos bens e valores jurídicos afeitos à ordem social e aos cidadãos.

Na organização estrutural do Direito, coube ao Direito Penal a construção de um sistema jurídico que conferisse, aos bens e valores jurídicos que a sociedade elegeu como os mais importantes para a sua própria manutenção, proteção. O descumprimento dessas regras enseja a ocorrência do ilícito penal, denominado pela teoria geral do Direito Penal, de crime.

Ao arcabouço de princípios, regras e normas jurídicas que tem como finalidade a proteção dos bens e valores jurídicos mais importantes para a sociedade, bem como punir às lesões a estes bens e valores, ou seja, que procura regular o crime, denomina-se Direito Penal. Assim, o Direito Penal configura-se como "a reunião de normas jurídicas pelas quais o Estado proíbe determinadas condutas, sob ameaça de imposição de sanção, bem como estabelece os princípios gerais e pressupostos para sua aplicação"[113].

Analisando a constituição e a finalidade do Direito Penal, Miguel Reale entende que "Direito Penal é o sistema de princípios e regras mediante os quais se tipificam as formas de condutas consideradas criminosas, e para as quais são cominadas, de maneira precisa e prévia, penas ou medidas de segurança, visando a objetivos determinados"[114]. Realizando a mesma tarefa Magalhães Noronha entende que "Direito Penal é o conjunto de normas jurídicas que

[113] ARANHA FILHO, Adalberto José Q. T. de Camargo. Crimes na internet e a legislação vigente. São Paulo: **Revista Literária de Direito**, v.9, n.44, p. 23-25, out./dez. 2002. p.23.
[114] REALE, Miguel. **Lições preliminares de direito**. 25. ed. São Paulo: Saraiva, 2001. p.349.

regulam o poder punitivo do Estado, tendo em vista os fatos de natureza criminal e as medidas aplicáveis a quem os pratica"[115].

Tendo como mesmo objetivo, a contextualização conceitual do Direito Penal, Fernando Capez expressa o Direito Penal como:

> Segmento do ordenamento jurídico que detém a função de selecionar os comportamentos humanos mais graves e perniciosos à coletividade, capazes de colocar em risco valores fundamentais para a convivência social, e descrevê-los como infrações penais, cominando-lhes sanções, além de estabelecer todas as regras complementares e gerais necessárias à sua correta e justa aplicação.[116]

Por sua vez, Damásio Evangelista de Jesus[117], Ney Moura Teles[118] e Júlio Fabrini Mirabete[119] concordam com a definição de José Frederico Marques:

> Direito Penal é o conjunto de normas que ligam ao crime, como fato, a pena como conseqüência, e disciplinam também as relações jurídicas daí derivadas, para estabelecer a aplicabilidade das medidas de segurança e a tutela do direito de liberdade em face do poder de punir do Estado.[120]

As definições acima expostas, além de identificar conceitualmente de forma congruente o Direito Penal, permitem a visualização das características desse ramo do Direito, que à luz da ordem constitucional brasileira, compõe um dos segmentos do Direito Público Interno. Partindo dos conceitos acima enumerados, percebe-se que o Direito Penal caracteriza-se por ser normativo, positivo, valorativo, finalista e sancionador. Os elementos normativo e positivo emanam da necessidade do Direito Penal pautar-se na existência de normas jurídicas positivadas, ou seja, o Direito Penal tem como objeto imediato a aplicação de normas de caráter público que são promulgadas pelo Estado no uso de suas funções legislativas: as leis penais; valorativo porque o arcabouço normativo penal procura através das leis penais proteger um conjunto de valores ético-sociais, considerados indispensáveis para a vida em sociedade; finalista porque o Direito Penal tem uma finalidade expressa, qual seja, proteger a sociedade através da tutela dos bens e valores jurídicos mais importantes para a sua manutenção; sancionador porque utiliza como elemento principal de reprimenda, às práticas que procura inibir a sanção.

---

[115] NORONHA, Edgar de Magalhães. **Direito penal**. 20. ed. São Paulo: Saraiva, 1982. p.12.
[116] CAPEZ, Fernando. **Curso de direito penal**. 9. ed. rev. e atual. São Paulo: Saraiva, 2005. v. 1. p.1.
[117] JESUS, Damásio Evangelista de. **Direito penal**. São Paulo: Saraiva, 2005. v.1. p.5.
[118] TELES**,** Ney Moura. **Direito Penal**. 2. ed. São Paulo: Atlas, 2006. p.5.
[119] MIRABETE, Julio Fabrini. **Manual de direito penal**. 23. ed. rev. e atual. São Paulo: Atlas, 2006. p.3.
[120] MARQUES, José Frederico. **Curso de direito penal**. São Paulo: Saraiva, 1954. v.1. p.11.

Como qualquer forma de conhecimento científico o Direito Penal foi estruturado sobre balizas principiológicas que norteiam de forma orgânica toda a sua constituição e aplicação. Vale ressaltar que a concepção do Direito Penal Brasileiro arquiteta-se à luz do perfil constitucional traçado pela Carta de 1988. Nesse esteio deve se destacar que o Estado Democrático de Direito Brasileiro tem como um de seus maiores nortes o princípio da dignidade da pessoa humana.

> A dignidade da pessoa humana é um valor espiritual e moral inerente a pessoa, que se manifesta singularmente na autodeterminação consciente e responsável da vida e que traz consigo a pretensão ao respeito por parte das demais pessoas, constituindo-se em um mínimo invulnerável que todo estatuto jurídico deve assegurar, de modo que apenas excepcionalmente possam ser feitas limitações ao exercício dos direitos fundamentais, mas sempre sem menosprezar a necessária estima que merecem todas as pessoas enquanto seres humanos.[121]

Assim, partindo dessa premissa, os valores insculpidos no princípio da dignidade da pessoa humana serão irradiados a toda à ordem jurídica brasileira, especialmente à ordem jurídica penal, posto que a luz dos preceitos instituídos pelo modelo de organização do Estado brasileiro, o direito de punir do Estado deve ser regulado materialmente e formalmente objetivando a proteção do cidadão. Analisando o conjunto principiológico, informativo, normativo e interpretativo, constitucional-penal pode-se destacar os princípios da legalidade ou da reserva legal, da anterioridade e da taxatividade.

O Princípio da Legalidade e/ou da Reserva Legal. Este princípio "constitui uma efetiva limitação ao poder punitivo estatal"[122] e, além de se configurar como um dos pilares mais importantes na estrutura do Direito Penal moderno, institui-se como uma das maiores garantias conferida ao cidadão contra os eventuais abusos que o Estado possa cometer na aplicação do seu direito;obrigação de punir os infratores de sua ordem jurídica penal.

Em virtude da sua importância na ordem jurídica constitucional-penal o primeiro aspecto que deve ser evidenciado na análise do referido princípio é a sua correta identificação. Boa parte da doutrina nacional considera o princípio da reserva legal sinônimo do princípio da legalidade, entretanto, analisando o assunto José Afonso da Silva expõe que:

> O dispositivo contém uma reserva absoluta de lei formal, que exclui a possibilidade de o legislador transferir a outrem a função de definir o crime e de estabelecer penas.

---

[121] MORAES, Alexandre de. **Constituição do Brasil interpretada**. 6. ed. São Paulo: Atlas, 2006. p.129.
[122] BITTENCOURT, Cezar Roberto. **Tratado de Direito Penal –** Parte geral. 10. ed. São Paulo: Saraiva, 2006. v.1. p.14.

> Demais, a definição legal do crime e a previsão da pena hão que preceder o fato tido como delituoso. Sem lei que o tenha feito não há crime nem pena.[123]

Contextualizando o assunto em nível constitucional, percebe-se que a Constituição Federal de 1988 em seu artigo 5º arrola dois incisos de conteúdo diferentes, mas que ensejam por parte da doutrina a mesma rotulação como princípio da legalidade. O inciso II do artigo 5º da Constituição Federal preceitua que "ninguém será obrigado a fazer ou a deixar de fazer alguma coisa senão em virtude de lei". Já o inciso XXXIX do mesmo artigo estabelece que "não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal", preceito esse reproduzido com a mesma redação no art. 1º do Código Penal Brasileiro.

Os dois preceitos constitucionais referem-se à legalidade, contudo, abarcam conotações significativamente diferentes. Analisando o assunto, Heleno Cláudio Fragoso afirma: "Essa regra básica denomina-se princípio da legalidade dos delitos e das penas ou princípio da reserva legal, e representa importante conquista de índole política, inscrita nas Constituições de todos os regimes democráticos liberais"[124]. Alberto Silva Franco é mais objetivo ao expressar que: "o princípio da legalidade, em matéria penal (CF, art. 5°, XXXIX), equivale à reserva legal."[125]

Apesar da celeuma, percebe-se que, o dispositivo constitucional elencado no inciso XXXIX do artigo 5º, bem como sua reprodução constante no artigo 1º do Código Penal Brasileiro corresponde, após uma análise mais acurada da técnica constitucional, ao princípio da reserva legal. Dessa forma pactua-se com o entendimento firmado por José Afonso da Silva quando este reputa a nominação de Princípio da Legalidade à garantia constitucional estabelecida no inciso II do artigo 5º, enquanto considera o inciso XXXIX do referido artigo como o Princípio da Reserva Legal.

Esta garantia imposta no preceito constitucional capitulado no inciso XXXIX do artigo 5º da Constituição Federal configura-se como um desdobramento lógico dos pilares da ordem político-jurídica brasileira insculpidos nos artigos 1º a 4º da Constituição brasileira.

---

[123] SILVA, José Afonso da. **Curso de direito constitucional positivo.** 21. ed. São Paulo: Malheiros, 2002. p.428.
[124] FRAGOSO, Heleno Cláudio. **Lições de direito penal.** 4. ed. Rio de Janeiro: Forense, 1995. p.89.
[125] SILVA, Alberto Franco. **Código Penal e sua interpretação jurisprudencial.** 5. ed. São Paulo: Revista dos Tribunais, 1995. p.26.

> O princípio da legalidade tem significado político e jurídico: no primeiro caso, é garantia constitucional dos direitos do homem, e no segundo, fixa o conteúdo das normas incriminadoras, não permitindo que o ilícito penal seja estabelecido genericamente sem definição prévia da conduta punível e determinação da *sanctio júris* aplicável.[126]

No mesmo sentido Álvaro Mayrink da Costa expõe que "o princípio da legalidade transcende os limites de uma garantia política modulada no curso da história, e o eleva a condição de princípio científico imprescindível à racionalização de toda atividade punitiva regida pelo direito e não pela força."[127]

Desta forma o princípio da legalidade configura-se como um dos corolários máximos do direito penal e significa que uma conduta só pode ser considerada criminosa, ou seja, um ilícito penal, se ela estiver devidamente enquadrada como tal em uma norma penal incriminadora anterior a prática do fato. Assim, o preceito constitucional dá margem à obtenção de dois outros princípios extremamente importantes: o princípio da anterioridade e o princípio da taxatividade.

Princípio da Anterioridade da Lei Penal. Para que haja crime, e a ele seja cominada uma pena, é preciso que o fato tenha sido cometido depois que a lei que o tipificou entrou em vigor. Esse é um dos princípios constitucionais do Direito Penal, enunciado no art. 5°, XXXIX CF/88 e no art. 1° do Código Penal (CP) pátrios: "Não há crime sem lei anterior que o defina; não há pena sem prévia cominação legal". Decorrência lógica do princípio da reserva legal ou da legalidade funciona como um escudo desse princípio, pois, confere maior eficácia às garantias por ele insculpidas.

O Princípio da Taxatividade impõe que a norma penal incriminadora seja precisa, descreva de forma pormenorizada e detalhada a conduta considerada criminosa. Não se admitindo assim tipos penais lacunosos, vazios ou frouxos, que não confirmem com certeza ao cidadão qual a conduta que é considerada criminosa pelo Estado.

Observados os contornos constitucionais do Direito Penal deve-se, para uma melhor compreensão do objeto de estudo dessa dissertação, passar-se a analisar os aspectos basilares

---

[126] MARQUES, José Frederico, op. cit. 1954. v.1. p.132.
[127] COSTA, Álvaro Mayrink da. **Direito Penal –** parte geral. Rio de Janeiro: Forense, 1982. p.146.

da Teoria do Crime. Hodiernamente a doutrina classifica o crime utilizando-se de três critérios distintos de análise: o material, o formal e o analítico.

O sistema material conceitua o crime utilizando-se dos motivos que levaram o legislador a preceituar determinada conduta humana como criminosa, ou seja, o conteúdo do fato punível. Desta forma considera-se crime "toda ação ou omissão que contraria os valores ou interesses do corpo social, exigindo sua proibição com ameaça de pena."[128].

Manzini [129] conceitua crime como: "a ação ou omissão, imputável a uma pessoa, lesiva ou perigosa a interesse penalmente protegido, constituída de determinados elementos e eventualmente integrada por certas condições, ou acompanhada de determinadas circunstâncias previstas em lei."

A conceituação material visa estabelecer que o conceito de crime está diretamente ligado a idéia de bem ou interesse jurídico protegido por diploma normativo de natureza penal, o que José Frederico Marques sabiamente expressou: "O crime nada mais é que a violação de um bem penalmente protegido."[130]

Sob o aspecto formal conceitua-se crime toda conduta proibida por lei a qual seja cominada sanção penal. "Considera-se infração penal tudo aquilo que o legislador descrever como tal, pouco importando o seu conteúdo".[131]

Sob o aspecto analítico, o crime, na visão clássica, se caracteriza por ser uma conduta típica, antijurídica e culpável[132]. Vale ressaltar que as teorias penais mais modernas entendem que a culpabilidade não se configura como um elemento estrutural do crime, mas sim como elemento que se comporta como pressuposto de aplicabilidade da pena.[133]

---

[128] BITENCOURT, Cezar Roberto, op. cit., 2006. v.1. p.261.
[129] MANZINI apud JESUS, Damásio E. de, op. cit, 2005. v.1. p.151.
[130] MARQUES, José Frederico apud JESUS, Damásio Evangelista de, op. cit., 2005. v.1. p.151
[131] CAPEZ, Fernando, op. cit., 2002. v.1. p.102.
[132] A maior parte da doutrina penal atual exclui a culpabilidade como integrante da definição formal do crime, considerando-a tão somente como elemento da punibilidade. Contudo opta-se por manter a culpabilidade no texto do presente trabalho por força da sua importância para a definição do crime eletrônico na legislação e na doutrina alienígena.
[133] Vide JESUS, Damásio, op. cit., 2005.

A priori para que se possa considerar um fato como crime deve existir uma conduta humana omissiva ou comissiva, que por força do princípio da reserva legal, seja descrita em lei como tal. A conduta criminosa, ou seja, a ação ou omissão delituosa é aquela que se adequa aos elementos descritivos do crime na norma penal. Assim para se caracterizar um fato como delituoso, deve este enquadrar-se ao disposto em uma norma penal incriminadora, tem-se assim o fato típico, que de forma sucinta é a conduta humana delituosa que se subsume a descrição legal contida em norma penal incriminadora.[134]

Ao se verificar a adequação da conduta prática ao descrito em lei penal, surgindo assim a conduta relevante ao direito penal, qual seja a conduta típica, deve-se averiguar ainda se esta foi perpetrada contra a ordem jurídica.

Além do fato ser típico faz-se necessário que este seja antijurídico em suma, contrário ao direito. Em face das inúmeras condutas possíveis, e principalmente do choque de interesses, a lei permite em alguns casos que determinadas condutas típicas proibidas por lei sejam permitidas, não se aplicando a lei penal ao caso. Caracterizada a existência do fato típico é este submetido a juízo de valor, que dirá se o fato assim tipificado está em harmonia ou em antagonismo com a ordem jurídica.[135] Acerca da antijuridicidade Damásio Evangelista de Jesus explana: "A antijuridicidade é a relação de contrariedade entre o fato típico e o ordenamento jurídico. A conduta descrita em norma penal incriminadora será ilícita ou antijurídica quando não for expressamente declarada lícita."[136] Compreende-se desta forma que uma conduta típica é antijurídica quando o ordenamento jurídico não expressamente a estipula como legal.

O terceiro elemento constitutivo do crime consiste na Culpabilidade. N*ullun crimen sine culpa*. O fato lesivo deve necessariamente ser praticado voluntariamente para que se possa configurar um crime. A culpabilidade é um juízo valorativo que serve de ligação da vontade humana a um fato típico e antijurídico, é um juízo de valor porque só se considera culpa a vontade reprovável. A Culpabilidade nos ensinamentos de Aníbal Bruno:

> Consiste na reprovabilidade que vem recair sobre o agente, porque a ele cumpria conformar a sua conduta com o mandamento do ordenamento jurídico, por que tinha

[134] MARQUES, José Frederico. **Tratado de Direito Penal**. São Paulo: Bookseller, 1997. v.2. p.27.
[135] Ibid., 1997. p.27.
[136] JESUS, Damásio E. de, op. cit., 2005. v.1. p.155.

> a possibilidade de fazê-lo e não o fez, revelando no fato de não o ter feito uma vontade contrária àquela obrigação, i.e, no comportamento se exprime uma contradição entre a vontade do sujeito e a vontade da norma. [137]

Assim conceitua-se crime como um fato típico, ou seja, uma conduta humana que se subsume ao descrito em lei penal incriminadora, sob este fato típico deve incidir um juízo de valor que indicará a sua harmonia ou não com o ordenamento jurídico o que consiste na antijuridicidade, além desses dois elementos constitutivos deve o fato ser culpável, devendo incidir um juízo de reprovação social sobre o autor da conduta.

O conceito de crime quando analisado através do sistema material aprecia não o tecnicismo jurídico, mas sim os critérios que levaram o legislador a conceder a determinado bem jurídico a proteção tutelada por normal penal. Deve-se coibir toda ação, positiva ou negativa, que venha prejudicar as condições basilares da convivência em sociedade, tanto nos aspectos materiais como morais, evitando-se assim a perpetração de atos lesivos a valores fundamentais a vida em sociedade.

Da junção dos sistemas de conceituação tem-se que o crime caracteriza-se como um fato típico, antijurídico que se manifesta através de comportamento humano que atente contra bem jurídico, que por força de sua importância para a mantença da ordem social foi objeto da tutela de norma penal.

Nesse sentido, a revolução tecnológica que estruturou a chamada sociedade da informação forjou no contexto social o surgimento de novas relações sociais, econômicas e culturais. Conseqüentemente, ante a valoração social e econômica desse novo contexto, surgiu a necessidade de se conferir, segurança, especialmente segurança jurídica, a essa nova realidade fática.

Surge assim a necessidade de se elaborarem construções jurídicas que respaldassem o surgimento de novos bens e valores jurídicos ligados diretamente a esse novo contexto. Nascem os bens jurídicos informáticos ou eletrônicos, terminologia que possui maior abrangência e acuidade técnica, como sendo o conjunto de bens e valores associados ao contexto social informacional.

---

[137] BRUNO, Aníbal apud JESUS, Damásio E. de, op. cit., 2005. p.155.

"Este novo fenômeno, conseqüência [...] dos avanços dos meios tecnológicos, acabaram modificando por completo a vida na sociedade e criando novos riscos sociais."[138] Esse hodierno conjunto de riscos sociais pode ser melhor visualizado pelo surgimento de inúmeras condutas consideradas lesivas à sociedade, tais como:

a) Segurança nacional (instruções sobre a confecção de bombas, produção de drogas ilegais, atividades de terrorismo);
b) Proteção do menor (formas abusivas de marketing, violência, pornografia);
c)Proteção da dignidade da pessoa humana (incitação ao ódio racial, discriminação racial);
d) Segurança econômica (fraude, instruções para piratear cartões de crédito);
e) Proteção à informação (acesso ilegal e malévolo);
f)Proteção à vida privada (comunicação não autorizada de dados de caráter pessoal);
g) Proteção à reputação (calúnia, injúria e difamação);
h) Propriedade intelectual (comércio de itens não originais).

Ante a situação que se apresentava, surgiu a necessidade do Direito regular as práticas sociais decorrentes do novo modelo de organização social e econômico vigente. Dessa forma, objetivando a tutela dessas novas situações fáticas, estreitaram-se as relações entre o Direito e a Informática e os sistemas eletrônicos.

3.2 As relações entre o direito penal e os sistemas eletrônicos

É inegável a influência da informática e dos sistemas eletrônicos no cotidiano social. A informatização alterou, e vem alterando, de forma sensível a realidade social do mundo pós - industrial. Novas tecnologias criam meios de produção, recriam atividades econômicas, alteram as relações comerciais e de trabalho, em suma criam novas situações jurídicas que devem ser reguladas de forma a minimizar o choque de interesses possibilitando assim a mantença do convívio social.

[138] FERREIRA, Érica Lorenço de Lima, op. cit., 2007. p.86.

Dentro desse contexto inovador carente de regulamentação, surgem dois novos ramos do Direito: O Direito Civil Eletrônico e o Direito Penal Eletrônico.

O Direito Civil Eletrônico trata das relações jurídicas privadas oriundas da utilização ou aplicação da informática e dos sistemas eletrônicos, como por exemplo, o regramento das relações comerciais virtuais, as questões inerentes aos Direitos Autorais, a utilização de *Softwares* entre outros.

O Direito Penal Eletrônico versa sobre normatização necessária a regulamentação da prevenção e repressão de condutas ou fatos que atentem ao uso regular, a exploração, segurança, processamento, armazenamento, transmissão e sigilo de dados ou informações armazenadas ou utilizadas por computadores ou sistemas eletrônicos.

Dentre esses novos ramos do Direito, é o Direito Penal Eletrônico o mais carente de regulamentação, e isto torna a utilização de computadores ou sistema eletrônicos sujeita a um vácuo normativo que fomenta a prática de delitos. Mais ainda, a ausência de regras claras que regulem os aspectos criminais relacionados aos sistemas eletrônicos gera a sensação que o sistema legal é inócuo na repressão desses delitos, o que leva de forma direta a diminuição da utilização desses meios em virtude do aumento do sentimento de insegurança e descrédito dos mecanismos de controle e fiscalização, colocando em risco o desenvolvimento das potencialidades inerentes ao sistema social informacional.

O desenvolvimento tecnológico principalmente no campo da informática modificou de forma irreversível o cotidiano das atividades humanas. A revolução da informação, que gerou uma nova classe de excluídos: os *unplugged*, que constituem um proletariado *off line* ao lado de uma elite *on line,* abalou de forma cabal as estruturas do Direito.

Além de propiciar facilidades e vantagens até então nunca cogitadas, as redes informáticas e eletrônicas também se revelam um extremo facilitador para a perpetração de ilícitos, uma vez que os meios existentes para as práticas de delitos eletrônicos são inúmeros e dada as características dessas infrações os vestígios deixados são mínimos, o que torna a repressão e a persecução a estes atos tarefa árdua.

A informática se tornou fator de suma importância nas relações econômicas, sociais, ou seja, situações jurídicas de natureza diversas. Colocar em risco tais relações que movimentam vultosas quantias é uma afronta à regulamentação social.

É nesse contexto que aflora a importância da relação entre o Direito Penal e a Informática.

> Partindo da premissa que o Direito é a única forma de controle capaz de conter o avanço da criminalidade no mundo virtual, isto porque, de todos os sistemas de controle social, o Direito, possuindo estrutura imperativo atributiva, e [ ] a coercitividade, sancionando assim as condutas ilícitas" qualquer que seja a angulação enfocada, penal, civil ou trabalhista.[139]

Neste sentido, Luiz Flávio Gomes[140] reivindica a criminalização específica dos crimes eletrônicos no Brasil. Na ordem jurídica nacional já existem normas que tipificam algumas condutas, como a Lei 9.983/00 e a Lei 9.504/97, dentre algumas poucas outras. Contudo são tipos penais extremamente específicos, que visam proteger bens jurídicos restritos amparando tão somente a administração pública, o processo eleitoral e a previdência social. Ressalte-se que a existência de legislação específica não serve de óbice à elaboração de legislação penal mais geral.

Nesta linha de pensamento o uso da informática pode ser considerado um fator criminógeno por que:

a) Abre novos horizontes ao delinqüente (que dela pode valer-se para cometer infindáveis delitos – é a instrumentalização da informática);

b) Permite não só o cometimento de novos delitos (p.ex.: utilização abusiva da informação armazenada em detrimento da privacidade, intimidade e imagem das vítimas), mas como a potencialização dos delitos tradicionais (estelionato, racismo, pedofilia, crimes contra a honra etc.);

---

[139] DOUN, Alexandre Jean; BLUM, Renato. Cybercrimes. In: LUCCA, Newton; SIMÃO FILHO, Adalberto (Coord.). **Direito e Internet –** Aspectos jurídicos relevantes. São Paulo: Edipro, 2000. p.119.

[140]GOMES, Luis Flávio apud ELIAS, Paulo Sá. A questão da reserva legal no Direito Penal e as condutas lesivas na área da informática e da tecnologia**. Jus Navigandi**, Ed. 12, out. 2001. Disponível em: < http://www1.jus.com.br/doutrina/texto.asp?id=2038 >. Acesso em: 23 out. 2007.

c) Dá ensejo, de outro lado, não só aos delitos cometidos com o computador, senão também os cometidos contra o computador (contra o *hardware, o software* ou mesmo contra a própria informação – *Computer Crime*);[141]

Pactuando desse entendimento Henry Bosly[142] estabelece a existência de três esferas distintas de relações entre o Direito Penal e a Informática:

- A informatização da documentação penal;
- Informatização dos procedimentos administrativos e judiciais;
- A informática a serviço da delinqüência.

A informatização da documentação penal relaciona-se com os processos informáticos que revolucionaram o tratamento de dados policiais e judiciários. Compreende além dos famosos fichários policiais, os arquivos judiciários e os dos serviços de segurança. É justamente contra essas espécies de documentos eletrônicos que muitas vezes se faz necessário reforçar medidas de proteção às garantias individuais, uma vez que com certa freqüência se verifica uma excessiva ou leviana intromissão dos órgãos estatais reguladores e administradores desta fontes de informação na vida privada do cidadão. Nestes casos a informática funciona como uma ferramenta que agiliza a coleta, a organização, o armazenamento e a manipulação desses bancos de informações indispensáveis as atividades investigatórias. Ressalte-se que visando coibir os abusos praticados na criação e utilização dessas informações, muitas vezes sigilosas, a Constituição Federal instituiu na ordem jurídica brasileira a garantia constitucional do *Habeas Data* que assegura ao impetrante o direito de conhecer e até retificar, as informações constantes nestes bancos de dados relacionadas a sua pessoa.

A informatização dos procedimentos administrativos e judiciais tem como escopo o melhoramento e ao aperfeiçoamento da distribuição da justiça. É através da informatização de emissão de documentos do cotidiano forense, como certidões, alvarás, termos de audiências bem como outros de cunho administrativo que se tem de certa forma aliviado os trabalhos judiciários e ajudado a fiscalização e controle do cumprimento das sentenças e da execução

---

[141] Ibid., 2007.
[142]BOSLY, Henry apud FERREIRA, Ivette Senise. Os crimes da informática. In: BARRA, Rubens Prestes; ANDREUCCI, Ricardo Antunes (Coord.). **Estudos Jurídicos**. São Paulo: RT, 1992. p.143.

das penas. É notório nos grandes centros urbanos brasileiros o nível de modernização dos órgãos da justiça penal, as antigas máquinas de datilografar e os obsoletos fichários manuais vêm sendo substituídos por aparelhos mais modernos e sistemas de processamento automático de dados. O que se tornou não uma conveniência, mas sim uma necessidade em face do grande número de processos que se acumulam nos tribunais. Exemplo cabal das facilidades e segurança geradas pela informatização desses procedimentos na esfera penal é a emissão da certidão de antecedentes criminais exarada através de consulta a banco de informações informatizado que interliga todas as varas criminais. Mais ainda, com a recente edição da Lei 11.419/2006, que institui as regras iniciais do "processo eletrônico" uma nova forma de processamento dos feitos judiciais foi inserida na práxis forense, com frutos já preciosos, como a materialização das garantias da celeridade, economia processual e acesso à justiça, em que pese os exemplos fornecidos pelos Juizados Especiais Federais Virtuais.

A informática a serviço da delinqüência comporta as infrações eletrônicas e as infrações comuns cometidas através de sistemas eletrônicos.

> De fato, esses crimes de informática ora representam novas maneiras de executarem-se as figuras delituosas tradicionais já tipificadas na lei penal, ora apresentam aspectos específicos pouco conhecidos, que não se adaptam á incriminações convencionais e nem seus autores aos modelos criminológicos comuns.[143]

A utilização de meios eletrônicos para a prática de atos ilícitos gera duas situações distintas. A primeira é aquela na qual o uso de sistemas eletrônicos consubstancia-se como ferramenta para a perpetração de conduta já tipificada como crime por lei penal. A segunda se caracteriza pela prática de ato não abarcado no ordenamento jurídico penal, ou seja, condutas ilícitas realizadas através de meios eletrônicos ou contra estes, que não se amoldam a nenhum fato típico descrito em lei, consistindo assim em uma nova figura delitiva.

As formas delituosas são inúmeras e de natureza distintas, tem-se as mais diferentes formas de fraude, furto, apropriação indébita, vandalismo, crimes do colarinho branco, violações autorais, sabotagem, espionagem industrial e diversos outros delitos. Existem ainda as condutas que atentam contra a integridade da própria máquina, como por exemplo, a

[143] FERREIRA, Ivette Senise. Os crimes da informática. In: Ibid., 1992. p. 144.

disseminação intencional dos chamados "vírus de computador"[144] que podem inutilizar todos os dados existentes em uma máquina causando prejuízos incalculáveis ao proprietário.

As facilidades para a prática desses delitos, adicionada à possibilidade de serem praticados em locais distantes de onde se operaram os resultados e a sensação de impunidade reinante no meio eletrônico fazem com que a situação se torne extremamente perigosa beirando tornar-se incontrolável.

Extremamente necessário é o desenvolvimento do Direito Penal Eletrônico para que este discipline a matéria evitando assim a ampliação da situação periclitante que gera a sensação de que os meios eletrônicos, principalmente a Internet, são carentes de regulamentação, sendo territórios anárquicos, férteis para a prática de ilícitos, e isto deve ser coibido.

Entretanto, indispensável o estudo aprofundado do mundo virtual para que se possa disciplinar juridicamente a matéria através da elaboração de mecanismos jurídicos que acompanhem a evolução tecnológica da informação evitando-se dessa forma os perigos de uma inflação legislativa relacionada à matéria. Desta feita a legislação aplicável ao tema estaria revestida de um embasamento doutrinário que evitaria o seu "engessamento" em face do avassalador desenvolvimento tecnológico podendo ser aplicável e eficaz mesmo com o surgimento de inovações alteradoras da realidade fática atinente ao assunto. Assim não cairiam em desuso uma vez que se adequariam as novas realidades vindouras não se tornando "letra morta".[145]

O estudo das condutas lesivas a essa nova ordem social, reputa ser um dos novos desafios do Direito Penal moderno, posto que a análise pormenorizada de todo o contexto social e tecnológico deve ser realizada de forma acurada, a fim de que se possa delinear com contornos sólidos as condutas ilícitas que devam ser criminalizadas através da estruturação dos chamados crimes eletrônicos.

---

[144] Ricardo Cidale define o vírus de computador como "um programa como outro qualquer. Entretanto, enquanto a maioria dos programas visa ao aumento da produtividade no ambiente de trabalho, o programa -vírus quer destruí-la", danificando o sistema informático. CIDALE, Ricardo apud REIS, Maria Helena Junqueira. **Computer crimes**. Belo Horizonte: Del Rey, 1997. p.33.

[145] DOUN, Alexandre Jean; BLUM, Renato, op. cit., In: LUCCA, Newton; SIMÃO FILHO, Adalberto (Coord.). op. cit, 2000. p.121.

3.3 O crime eletrônico

A proliferação da tecnologia da informação no contexto social tornou mais densa a dependência da sociedade dos novos recursos tecnológicos. Passado alguns anos o processo de reorganização social pautado no desenvolvimento tecnológico informacional começa apresentar os primeiros sinais de que alguns ajustes se fazem necessários. Percebe-se nitidamente, que hoje, as palavras de Bill Gates relacionadas ao preço do avanço tecnológico fazem cada vez mais sentido.[146]

As mudanças ocorridas, não se limitaram somente ao campo produtivo, como por exemplo, o receio de que a informatização das cadeias produtivas levasse ao desemprego, mas também propiciaram o surgimento de novas formas de gerar e fazer circular riqueza.

> As informações virtualizadas que podem ser acessadas nos sistemas de rede de computador são riquezas que ampliam o patrimônio material e intelectual dos usuários. Constata-se, historicamente, que a riqueza atrai o crime e, conseqüentemente, o criminoso. O que impressiona é a fragilidade da riqueza das informações uma vez que dados virtuais representam polpudas quantias em dinheiro, que podem ser sonegadas, interceptadas ou subtraídas por simples sinais digitais, quase sempre de identidade anônima. Com as teclas dos computadores (e não com o uso de pistolas automáticas e metralhadoras), os assaltantes virtuais de bancos e de empresas passam a utilizar a riqueza das informações arquivadas nos computadores, servindo-se de sofisticados programas e *softwares* para cometer crimes impunemente. [147]

O surgimento dessa nova forma de circulação de riquezas e poder fomentou o interesse global. Assim os dispositivos, as técnicas e as estruturas utilizadas para viabilizar a comunicação informacional começaram a ser alvo de análises mais aprofundadas, que nem sempre possuíam fins lícitos.

Começaram, dessa forma, a ser diagnosticadas as vulnerabilidades existentes no sistema tecnológico estrutural da sociedade da informação, o que propiciou o surgimento de condutas perniciosas que buscassem explorar essas lacunas em busca de frutos ilícitos. Algo extremamente comum no contexto de desenvolvimento da sociedade humana, posto que tem-se como exemplo o desvirtuamento de inúmeras tecnologias e ferramentas que foram desenvolvidas com finalidades lícitas. Exemplo clássico é a utilização do avião para fins

---

[146] GATES, Bill, op. cit., 1995. p.309.
[147] CORRÊA, Gustavo Testa apud HESPANHA, Benedito, op. cit., v. 1, n. 16, p.29-64, 2002. p. 49.

bélicos, ou o desenvolvimento das chamadas armas biológicas. Analisando o assunto Vander Ferreira de Andrade expõe com clareza que:

> Nesse diapasão, verificamos também que um campo da atividade humana, aquele que é classificado nos registro da Sociologia como sendo resultante de uma humana, individual ou coletiva, mas em qualquer hipótese, de natureza anti-social, a saber, a criminalidade, que tem acompanhado, como efeito acessório e *pari passu*, a própria evolução da sociedade gerando aquilo que denominamos de delitos de informática.[148]

Nesse contexto, a maior parte da doutrina aponta que os primeiros delitos eletrônicos surgiram com a primeira etapa da expansão tecnológica ocorrida na década de 60. Acompanhando o desenvolvimento tecnológico a criminalidade eletrônica desenvolveu-se a níveis tais que se enraizou profundamente no contexto social moderno.

Observando a criminalidade eletrônica moderna Flávio Luiz Gomes[149], entende que ela possui similitude à informatização global: a) *transnacionalidade* – todos os países fazem uso da informatização, independentemente do seu grau de desenvolvimento econômico, social ou cultural, fazendo com que a delinqüência esteja presente em todos os continentes; b) *universalidade* – o acesso aos produtos informáticos está cada vez mais fácil e alcança a todo o contexto social independente de classe; e, por último, c) *ubiqüidade* – a informatização está diluída em todos os campos sociais.

Esse avanço criminoso elevou-se a tal ponto que atualmente coloca em risco os pilares de sustentação da sociedade informacional, o que coloca em risco o desenvolvimento de todo o potencial de utilização das ferramentas tecnológicas modernas. Surge assim na exposição de Gustavo Edurado Aboso e María Florência Zapata:

> *Um nuevo intere social que demanda uma urgente proteccíon jurídica, particularmente la ofrecida por el derecho penal. [...] el avance tecnológico que representa Internet y los problemas presentados por el uso generalizado de los sistemas informáticos disparan necesidades próprias para el derecho penal, que ahora tiene ante si um nuevo interes social digno de protección: la información y su transmisión a través de los sistemas telemáticos.*[150]

---

[148] ANDRADE, Vander Ferreira de. Crimes de informática. **Revista da Faculdade de Direito de Guarulhos**, São Paulo, v.3, p. 281-293, jul/dez. 2001. p.282.

[149] GOMES, Flávio Luiz apud FURLANETO NETO, Mário; GUIMARÃES, José A. Chaves, op. cit., 2003. p.68.

[150] ABOSO, Gustavo Eduardo; ZAPATA, María Florencia. **Cibercriminalidae y derecho penal.** Buenos Aires: B de F, 2006. p.15-16.

Nasce dessa forma à necessidade de intervenção direta do direito penal na realidade criminosa que se avulta e que mina os pilares de sustentação da sociedade informacional. Em busca de tutelar esse novo arcabouço de bens jurídicos indispensáveis para o regular desenvolvimento da sociedade parte o direito penal a estudar e estruturar instrumentos jurídicos relacionados a essa nova criminalidade.

3.3.1 A denominação da matéria

A denominação do objeto de estudo deste trabalho é bastante controversa. Em face das inúmeras possibilidades de ações delituosas o tema tem recebido pelos estudiosos da matéria nomeações distintas.

Criminosos de computador (*Computer Criminals*) é como Aaron M. Konh[151] designa os que praticam essas condutas. Jean Pradel e Cristian Feuiard[152] reportam-se a infrações cometidas por meio de computador.

Visando designar os comportamentos ilegais ou prejudiciais à sociedade realizados pela utilização de um computador Klaus Tiedmann[153] fala em Criminalidade Informática. Na mesma corrente de pensamento, Martine Briat[154] escreve sobre Fraude Informática enquanto J.P Spretels[155] prefere falar sobre infrações ligadas a informática e a uma delinqüência informática.

O direito comparado, através de seus doutrinadores, apesar da variedade de denominações, vem consagrando a expressão *Computer Crime*[156] para nominar o tema. No Brasil afloram novas denominações como *Cybercrimes*, delitos computacionais, crimes de informática, crimes de computador, crimes eletrônicos, crimes telemáticos entre outras.

---

[151] KONH, Aaron M. apud FERREIRA, Ivette Senise, op. cit., In: LUCCA, Newton; SIMÃO FILHO, Adalberto (Coord.), op. cit, 2000. p.209.
[152] PRADEL, Jean; FEUILLARD, Cristian apud FERREIRA, Ivette Senise, op. cit., In: In: LUCCA, Newton; SIMÃO FILHO, Adalberto (Coord.), op. cit, 2000. p.209.
[153] TIEDEMANN, Klaus apud FERREIRA, Ivette Senise, op. cit., In: In: LUCCA, Newton; SIMÃO FILHO, Adalberto (Coord.), op. cit, 2000. p.209.
[154] BRIAT, Martine apud FERREIRA, Ivette Senise, op. cit., In: In: LUCCA, Newton; SIMÃO FILHO, Adalberto (Coord.), op. cit, 2000. p.209.
[155] SPREUTELS, J.P apud FERREIRA, Ivette Senise, op. cit., In: In: LUCCA, Newton; SIMÃO FILHO, Adalberto (Coord.), op. cit, 2000. p.209.
[156] REIS, Maria Helena Junqueira, op. cit, 1997. p.24.

Não há um consenso quanto ao *nomem juris* genérico dos delitos que ofendem interesses relativos ao uso, à propriedade, à segurança ou a funcionalidade de computadores e equipamentos periféricos *(Hardwares)*, redes de computadores e programas de computador *(Softwares)*.[157]

O assunto não é pacífico. A polêmica existente faz com que as denominações sejam citadas de acordo com a preferência dos autores especializados. Ressalte-se, entretanto, a escolha da expressão crime eletrônico para delimitação da matéria ora analisada, porque abarca não só os atos relacionados à utilização da informática ou computadores, mas o conjunto primário e secundário de elementos e sistemas eletrônicos que permitem o acesso e o tratamento de informações.[158]

3.3.2 O Conceito de crime eletrônico

O surgimento e a evolução da informática tem resultado na crescente informatização das atividades rotineiras, reformulando de forma inquestionável o cotidiano mundial. Entretanto esse avanço tecnológico tornou-se uma ferramenta extremamente facilitadora para a perpetração de delitos. Novas formas de praticar crimes já existentes surgiram, bem como condutas criminosas inéditas foram criadas. Nasceram assim os crimes eletrônicos, ou *Computer Crimes* cujo conceito, por se tratar de figura nova no mundo jurídico, vem sendo formulado através de debates doutrinários o que confere a este uma mutabilidade *sui generis*.

Valdir Sznich define Crime de Informática ou Eletrônico "como qualquer ato ilegal onde o conhecimento especial de tecnologia de informática é essencial para a sua execução, investigação e acusação. [159]"

---

[157] ARAS, Vladimir. Crimes de Informática: Uma nova criminalidade. **Jus Navigandi**, Ed. 12, out. 2001. Disponível em: < http://www1.jus.com.br/doutrina/texto.asp?id=2250 >. Acesso em: 23 out. 2007.

[158] Dessa forma, entendemos por Direito Eletrônico o conjunto de normas e conceitos doutrinários, destinados ao estudo e normatização de toda e qualquer relação onde a informática seja o fator primário, gerando direitos e deveres secundários. É, ainda, o estudo abrangente, com o auxílio de todas as normas codificadas de direito, a regular as relações dos mais diversos meios de comunicação, dentre eles os próprios da informática. ALMEIDA FILHO**,** José Carlos. **Processo eletrônico e teoria geral do processo eletrônico:** a informatização judicial no Brasil. Rio de Janeiro: Forense, 2007. p.56.

[159] SZNICH, Valdir apud COSTA, Marco Aurélio Rodrigues da, op. cit., 2001. Disponível em: < http://www1.jus.com.br/doutrina/texto.asp?id=1826 >. Acesso em: 20 out. 2001.

O conceito acima mencionado se caracteriza por ser muito amplo e atrela necessariamente a prática do delito ao conhecimento de técnicas de informática, não mencionando a necessidade do objeto do delito ser um sistema eletrônico ou um conjunto de dados, tornando-se assim, muito amplo e abrangente, não delimitando de forma objetiva o tema alvo de estudo.

João Marcello de Araújo Junior conclui que o Crime Eletrônico consiste em "uma conduta lesiva, dolosa, a qual não precisa, necessariamente corresponder à obtenção de uma vantagem ilícita, porém praticada, sempre com a utilização de dispositivos habitualmente empregados nas atividades de informática" [160].

Apesar de incorrer nos mesmos deslizes da definição supra mencionada. João Marcello Araújo estabelece um novo elemento em sua conceituação: a ausência de obtenção de vantagem ilícita. Em verdade, verifica-se muitas vezes que nos crimes eletrônicos a sua perpetração não corresponde à obtenção de uma vantagem ilegal, mas simplesmente a satisfação do ego ou um teste ao delinqüente que superou os sistemas de segurança da rede eletrônica, por exemplo.

Na mesma linha de pensamento Dom Parker afirma que "Abuso de computador é amplamente definido como qualquer incidente ligado à tecnologia do computador, no qual uma vítima sofreu, ou poderia ter sofrido, um prejuízo, e um agente teve, ou poderia ter tido vantagens." [161]

Carla Rodrigues Araújo de Castro conceitua crime informático como "aquele praticado contra sistema de informática ou através deste, compreendendo os crimes praticados contra o computador e seus acessórios e os perpetrados através do computador.[162]"

Os conceitos suso mencionados se caracterizam ora por sua grande abrangência, ora por limitarem-se a alguns aspectos dos Crimes Eletrônicos. Nessa esteira a OECD – Organização para Cooperação Econômica e Desenvolvimento define o Crime Eletrônico como "qualquer

---

[160] ARAÚJO JUNIOR, João Marcello apud MELO, Aline Mary M. de. **Os Crimes de Informática**. Suas formas de punição e o Direito. Manaus: Instituo Luterano de Ensino Superior, 2000. 38p. Monografia.
[161] PARKER, Dom apud REIS, Maria Helena Junqueira, op. cit, 1997. p.25.
[162]CASTRO, Carla Rodrigues Araújo de. **Crimes de informática e seus aspectos processuais.** 2 ed. Rio de Janeiro: Lúmen Juris, 2003. p.9.

conduta ilegal, não ética, ou não autorizada, que envolva processamento automático de dados e/ou transmissão de dados".[163] Verifica-se que as definições acerca do que seja um Crime Eletrônico não satisfazem a necessidade de identificar de maneira objetiva o que seja esta espécie de delito e qual o seu objeto.

Michael Gemignani com muita ironia levanta questionamentos sobre o tema: "Se uma secretária cansada de ser desfalcada pelo computador, deliberadamente jogasse café na máquina, isto seria um crime informático ou um ato de vandalismo contra a propriedade da empresa?"[164]

Apesar dos inúmeros entendimentos colacionados pode-se concluir que a definição de Crime de Eletrônico deve estar intriscitamente relacionada ao bem jurídico que se almeja proteger. Ao contrário dos delitos tradicionais que podem ser perpetrados contra os sistemas de eletrônicos ou contra os *softwares* (como o furto), o crime eletrônico é aquele perpetrado contra bens jurídicos eletrônicos ou informacionais que se materializam no conjunto de dados/informações contidos nos sistemas eletrônicos, estando estes armazenados, sob manipulação ou em transmissão. Nesse sentido María de La Luz Lima explicita que:

> Delito eletrônico, em sentido amplo, é qualquer conduta criminógena ou criminal em cuja realização haja o emprego da tecnologia eletrônica como método, meio ou fim, em um sentido estrito, qualquer ato ilícito penal em que os computadores, suas técnicas e funções desempenham um papel como método, meio ou fim[165].

Desta feita a célula básica para uma definição do crime eletrônico parte da análise do bem jurídico a ser tutelado pela lei penal incriminadora, o que culmina com a conclusão de que a proteção estatal deve recair sob a proibição de condutas que atentem contra o estado natural dos dados e recursos oferecidos por um sistema de tratamento de dados, seja pela inserção, manipulação, compilação, armazenamento, processamento e transmissão de dados/informações. A análise dos entendimentos apresentados permite-se depreender a existência de dois pressupostos necessários para a caracterização do crime eletrônico:

---

[163] REIS, Maria Helena Junqueira, op. cit, 1997. p.25.
[164] GEMIGNANI, Michael apud REIS, Maria Helena Junqueira, op. cit, 1997. p.25.
[165] LIMA, María de la Luz apud FURLANETO NETO, Mário; GUIMARÃES, José A. Chaves, op. cit., mar. 2003. p. 70.

- O crime deve ser perpetrado contra bens jurídicos eletrônicos ou informacionais (como a segurança, ou a integridade do sistema eletrônico ou das informações por ele tratadas);

- Sejam perpetrados através da utilização de alguma ferramenta eletrônica no transcorrer do *iter criminis*.

Considerando a moderna doutrina penal para a conceituação de crime, se verifica a necessidade de adequar o conceito de crime eletrônico ao conceito moderno de crime ao qual a ordem jurídica brasileira se filia.

Assim o fazem Ivette Senise Ferreira[166] e Alexandre Jean Doun[167] : "Constitui crime de informática toda ação típica, antijurídica e culpável cometida contra ou pela utilização de processamento automático de dados ou pela sua transmissão."

Abrangendo uma ampla gama de relações sociais e individuais abarcada pela utilização dos sistemas eletrônicos e suscetíveis a prática delituosa, essa definição consagra ainda os elementos necessários à criminalização de condutas nos termos da teoria adotada pelos legisladores pátrios.

Qualquer comportamento humano quer comissivo, quer omissivo, encontra-se abrangido pelo conceito de ação. Ressalte-se que a conduta deva ser típica, correspondendo a um modelo previsto em lei como crime, sempre respeitando o princípio basilar do direito penal *nullun crimem nulla poena sine lege.*

É com base nos comentários acima tecidos que o Secretário Executivo da Associação de Direito e Informática do Chile, Claudio Libano Manzur conseguiu captar os elementos necessários a definir com clareza o crime eletrônico como:

> *Todas aquellas aciones u omissiones típicas, antijurídicas y dolosas, trátase de hechos aislados o de una série de ellos, cometidos contra personas naturales o jurídicas, realizadas en uso de un sistema de tratamiento de la infromación y*

[166] FERREIRA, Ivette Senise. A criminalidade informática. In: LUCCA, Newton; SIMÃO FILHO, Adalberto (Coord.), op. cit, 2000. p. 210.
[167] DAOUN, Alexandre Jean. Crimes Informáticos. In: BLUM, Renato Opice (Coord.). **Direito Eletrônico** – A Internet e os Tribunais. São Paulo: Edipro, 2001. p.206.

> *destinadas a producir un perjuicio en la victema a tráves de atentados a la sana técnica infrormática, lo cual generalmente, producirá de manera colateral lesiones a distintos valores jurídicos, repontándose, muchas veces, un beneficio ilícito en el agente, sea no se caracter patrimonial, actúe com o sin ánimo de lucro.* [168]

Apesar da clareza do doutrinador chileno, uma nova discussão deve ser levantada visando uma conceituação mais técnica. A maioria dos conceitos formulados revela a existência de uma bipolarização acerca do objetivo dos crimes eletrônicos, de um lado existe a corrente que pugna pela proteção dos dados e das informações contidas no sistema computacional, do outro requer-se tão somente a proteção aos sistema informáticos.

A escolha de um só desses objetivos como sendo o único a ser alvo dos delitos eletrônicos criará lacunas que tornarão insustentável a regulamentação jurídica do tema, pois surgiram vácuos carentes de proteção legal propiciando a prática de inúmeros delitos. Neste sentido defende-se que o objetivo do crime eletrônico deve recair sob os sistemas eletrônicos e sob os dados e informações nestes contidos. Desta feita, os bens jurídicos a serem protegidos por meio de normas penais incriminadoras possuiriam aspecto mais amplo abarcando uma série de condutas a serem prevenidas.

Após se estabelecer as considerações supra colacionadas se pode compor um conceito de crime eletrônico que se coadune com as preposições doutrinárias seguidas bem como preencha os requisitos formais estabelecidos pela ordem jurídica constitucional vigente no Brasil.

Assim o crime eletrônico pode ser conceituado como toda ação típica, antijurídica perpetrada contra bens jurídicos eletrônicos ou informacionais (como a segurança, ou a integridade do sistema eletrônico ou das informações por ele tratadas), através da utilização de alguma ferramenta eletrônica no transcorrer do *iter criminis,* não importando se o ato ocorre na introdução, no tratamento, no armazenamento ou na transmissão dos dados.

Nos delitos eletrônicos a conduta típica atentará contra um sistema de eletrônico, contra o tratamento automático de dados ou em sua transmissão. Consiste na utilização de um meio de eletrônico para lesar sistemas de eletrônicos ou, os dados contidos nestes.

---

[168]MANZUR, Cláudio Libano apud PINHEIRO, Reginaldo Cesár. Os Cybercrimes na esfera jurídica brasileira. **Jus Navigandi**, set., 2001. Disponível em: <http://www.jus.com.br/doutrina/cybercri.html >. Acesso em: 10 set. 2001.

Com base no bem juridicamente ofendido se tece a classificação da ação ilícita em categorias distintas, surgindo assim novos problemas específicos que desafiam os aplicadores do direito. Em face disto sustenta-se a necessidade de elaboração de uma nova construção doutrinária aplicada ao Direito Penal Eletrônico dos dados e dos bens intangíveis, que são as bases dos sistemas eletrônicos e dos ilícitos praticados sob a égide de Crimes eletrônicos.

3.3.3 O sistema de classificação dos crimes eletrônicos

Por se tratar de matéria nova no cenário jurídico, não possuindo ainda bases doutrinárias sólidas, afluem diversos formas de classificações acerca dos Crimes Eletrônicos. Estes sistemas se utilizam de vários critérios para efetuarem suas classificações, dentre os existentes destacam-se os abaixo mencionados.

Partindo da forma de atuação do autor, Sieber[169] estabelece a seguinte classificação:

- Fraude por manipulação de um computador contra um sistema de processamento de dado;
- Espionagem informática e furto de software;
- Sabotagem Informática;
- Furto de tempo;
- Acesso não autorizado;
- Ofensas tradicionais

A fraude por manipulação de um computador contra um sistema de processamento de dados consiste na modificação de dados dentro de um sistema eletrônico com intuito de se obter vantagem ilícita. Pode ocorrer através da introdução de dados falsos ou também por meio da alteração dos resultados.

Os delitos capitulados sob a classificação de Espionagem Informática consistem nos ilícitos que possuem como objetivo a obtenção de dados ou informações sigilosas por meio de sistemas de informática, um exemplo de espionagem informática oferecido pelo autor é a coleta de dados através da radiação eletrônica emitida por um terminal informático que pode

[169] SIEBER, Ulrich apud REIS, Maria Helena Junqueira, op. cit., 1997. p.29.

ser captada e armazenada até aproximadamente um quilômetro de onde está situado o terminal. Já o furto de *software*, que pode ser realizado pelo modo descrito anteriormente se restringe não a apropriação do meio físico de suporte do programa, mas sim a apropriação de elementos formadores da estrutura do *software*, elementos imateriais basilares da composição do programa, que servem para elaboração de programas similares concorrentes ao *software* espionado.

A sabotagem informática é um dos mais danosos delitos praticados através 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 através 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 principais.

O furto de tempo é a modalidade ilícita mais comum e mais difundida dos crimes eletrônicos. Essa modalidade ocorre quando pessoas sem autorização se utilizam de sistemas eletrônicos para fins particulares. Normalmente ocorre em empresas quando o funcionário sem possuir autorização para acessar a rede informática burla os sistemas de segurança e utiliza o computador e seus recursos para fins alheios aos interesses ao do empregador. O acesso não autorizado pode render ao infrator vantagens ilícitas como dinheiro e informações. Algumas legislações estrangeiras já consideram como propriedade da empresa o tempo de uso do computador, incriminando o seu uso não autorizado.

O acesso não autorizado a sistema eletrônico configura-se de longe como o crime eletrônico que mais se desenvolveu com o surgimento da Internet. É através da rede mundial de computadores que os *Hackers e Crackers* encontram meios para as invasões em massa a sistemas eletrônicos particulares. Consiste de maneira simples em um acesso por pessoa não autorizado a um sistema informatizado restrito onde o invasor, de maneira ilegal, pode ter acesso a informações sigilosas manipulando-as, de forma a destruí-las, alterá-las ou praticar outras ações delituosas.

A última categoria elencada por Sieber em sua classificação refere-se às ofensas tradicionais que podem ser praticadas por meio de um sistema de eletrônico ou que tenha a

sua parte tangível como objeto. Consubstancia-se na utilização de um sistema eletrônico para a prática de ilícitos comuns, onde o computador ou o sistema computacional não passa de novo meio de execução, como por exemplo, a falsificação de documentos.

Utilizando como base o trabalho do Dr. Sieber, Martine Briat[170] estabelece uma classificação um pouco mais específica, mas que pouco difere da anterior disposta:

- Manipulação de dados e/ou programas a fim de cometer uma infração já prevista pelas incriminações tradicionais;
- Falsificação de dados, de programas e entrave a sua utilização;
- Divulgação, utilização ou reprodução ilícita de dados e de programas;
- Uso não autorizado de sistema de informática;
- Acesso não autorizado a sistema de informática.

O sistema de classificação proposto por Briat não possui diferenças palpáveis em relação ao elaborado por Sieber, uma vez que a essência da classificação é a mesma alterando-se tão somente o nome das classes de delitos.

Rompendo com a linha de pensamento inicialmente disposta, Marc Jaeger[171] ao revés de utilizar a expressão crime informático utiliza em sentido amplo o termo Fraude Informática para designar as ações ilícitas ou anti-sociais ligadas ao uso de sistemas eletrônicos, classificando tais ações em:

- Fraudes propriamente ditas;
- Atentados à vida privada.

Os atentados à vida privada se compõem por condutas que apesar de serem perpetrados através de meio eletrônico, lesam interesses jurídicos distintos dos que formam o conjunto de bens que devem ser tutelados especificamente pelas normas penais eletrônicas, o que caracteriza a prática de crime comum. O conjunto de condutas danosas aos bens eletrônicos

[170] BRIAT, Martine apud FERREIRA, Ivette Senise. A Criminalidade Informática. In: LUCCA, Newton; SIMÃO FILHO, Adalberto (Coord.), op. cit, 2000. p.213.
[171] JAEGER, Marc apud FERREIRA, Ivette Senise. A Criminalidade Informática. In: LUCCA, Newton; SIMÃO FILHO, Adalberto (Coord.), op. cit, 2000. p.214.

ou informacionais configura o que se denomina de fraudes propriamente ditas. Estas comportam uma ampla gama de condutas lesivas aos sistemas eletrônicos e se subdividem ainda em:

- Fraudes no nível da matéria corporal;
- Fraudes no nível do *input;*
- Fraudes no nível do tratamento;
- Fraudes no nível do *output*.

As fraudes no nível da matéria corporal são aquelas que atingem a integridade física do sistema eletrônico, danificando-o ou inutilizando-o. As fraudes no nível de *input* são as perpetradas através da inserção de dados alterados em um sistema informacional. Quando as fraudes são perpetradas em nível de processamento ocorre uma modificação no programa responsável pelo tratamento dos dados o que altera significativamente os resultados do processamento destes. Já as fraudes em nível de *output* consubstanciam-se quando o autor altera dados corretos que passaram por um processamento adequado estando aptos a serem externados, logo é uma fraude ocorrida no intervalo de envios dos dados processados aos dispositivos de saída do sistema eletrônico.

Neste mesmo sentido Romeo Casabona[172] estabelece que os crimes eletrônicos podem ser classificados em quatro categorias:

- Manipulação de entrada de dados (*input*);
- Manipulações no programa;
- Manipulações na saída de dados (*output*);
- Manipulações à distância.

A manipulação de entrada de dados perpetra-se através da manipulação de dados quando de sua introdução no sistema informacional, quer seja pela introdução de dados falsos, quer pela alteração destes, ressaltando-se a possibilidade da manipulação ocorrer em face da omissão do registro de dados que deveriam compor toda a informação. As manipulações no programa acontecem através de modificações ou eliminação de etapas do programa que fazem

[172] CASABONA, Carlos M. Romeo apud REIS, Maria Helena Junqueira, op. cit, 1997. p. 31.

com que o processamento conduza a resultados errôneos, mesmo quando os dados inseridos no sistema são corretos. As manipulações na saída de dados ocorrem quando dados verdadeiros são tratados por programas inalterados, mas os dados obtidos pelo processamento são alterados na saída do equipamento, como por exemplo, quando estes estão sendo enviados a impressora. As manipulações à distância ocorrem quando o computador manipulado encontra-se conectado com outros formando assim uma rede. As alterações acontecem à distância sendo efetuadas por máquina distinta a que está sendo manipulada.

Mudando o parâmetro de classificação para a finalidade do delito, e excluindo os crimes já enquadrados nos ordenamentos jurídicos, Pradel[173] assim os delimita:

- Manipulações para obtenção de dinheiro;
- Manipulações para obtenção de informações.

A manipulação para obtenção de dinheiro deve ser entendida em sentido amplo, qual seja de qualquer proveito econômico, comportando todas as atividades ilícitas que importem de alguma maneira em uma vantagem econômica para o autor. A manipulação em busca de informações paira sob um só aspecto, a utilização do sistema eletrônico para a obtenção de informações as quais o autor não possui direito, violando assim o sigilo das mesmas.

A classificação confeccionada por Pradel é uma das mais bem elaboradas, uma vez que exclui os delitos já abarcados pelo ordenamento jurídico, classificando tão somente os verdadeiros delitos eletrônicos. Contudo a mesma não abraça todos os possíveis ilícitos cometidos contra sistemas informacionais, uma vez que estes novos crimes muitas vezes são praticados sem o intuito de obtenção de vantagem, mas simplesmente com o objetivo de causar prejuízo danificando o equipamento, como na sabotagem informática.

Em outro contexto vem se consagrando na doutrina internacional o sistema binário de conceituação proposta por Hervé Croze e Yves Bismuth[174] :

---

[173] PRADEL, Jean; FEUILLARD, Cristian apud FERREIRA, Ivette Senise. A criminalidade informática. In: LUCCA, Newton; SIMÃO FILHO, Adalberto (Coord.), op. cit, 2000. p.214.

[174] BISMUTH, Yves e CROZE, Hervé apud FERREIRA, Ivette Senise. A criminalidade informática. In: LUCCA, Newton; SIMÃO FILHO, Adalberto (Coord.), op. cit, 2000. p. 215.

- Atos dirigidos contra um sistema de informática, independentemente da motivação do autor;

- Atos que atentam contra outros valores sociais através de um sistema informático.

Da classificação acima estabelecida obtêm-se o entendimento da existência de duas situações fático-jurídicas distintas. Existem condutas praticadas por meio de sistemas eletrônicos contra outros bens jurídicos, funcionando o sistema informacional como instrumento da ação, e existem atos que são praticados contra dados ou informações armazenados, em processamento ou em transmissão, ou contra a integridade do próprio sistema, sendo estes objetos materiais da ação.

São os atos praticados contra um sistema informacional os delitos eletrônicos autênticos, pois o sistema funciona como instrumento e objetivo da ação, sendo meio e meta do ato, podendo esta recair sob os dados e informações armazenados, bem como sob a própria máquina, seu suporte lógico e até os periféricos. Nos atos que lesam outros valores sociais, o sistema eletrônico é apenas a ferramenta executória do crime fim.

Absorvendo os avanços doutrinários internacionais os autores nacionais passaram a acatar com quase unanimidade os elementos básicos da classificação suso exposta. Luis Flávio Gomes divide os crimes informáticos em duas categorias semelhantes as proposta por Croze & Bismuth, quais sejam os crimes praticados contra o computador em sentido amplo e crimes por meio de computador.[175]

Nesta mesma corrente de pensamento Damásio Evangelista de Jesus classifica os crimes informáticos em duas categorias, os Crimes informáticos puros ou próprios e os crimes informáticos impuros ou impróprios. Os delitos próprios são aqueles praticados por meio de um sistema eletrônico onde o resultado da conduta se opera em meio eletrônico, sendo o sistema informacional o bem jurídico protegido (segurança do sistema e titularidade das informações, integridade da máquina e dos periféricos e etc.), os crimes impróprios são aqueles em que o sistema funciona como ferramenta para a prática de condutas lesivas a bem

[175] GOMES, Luis Flávio apud ELIAS, Paulo Sá. A questão da reserva legal no Direito Penal e as condutas lesivas na área da informática e da tecnologia. **Jus Navigandi**, Ed. 12, out. 2001. Disponível em: < http://www1.jus.com.br/doutrina/texto.asp?id=2038 >. Acesso em: 23 out. 2001.

jurídicos já protegidos por outras normas penais incriminadoras, não relacionados com a os bens informacionais.[176]

Verifica-se que a maioria dos sistemas de classificação podem ser condensados nas duas categorias elencadas por Damásio ou por Croze & Bismuth, resumindo-se em condutas que atentem contra o sistema eletrônicos ou a atos que lesem outros bem jurídicos já penalmente protegidos. Compreende-se a importância da discussão doutrinária acerca da correta classificação dos crimes eletrônicos, bem como a necessidade de produção científica embasadora da matéria, contudo ao proceder-se análise à cerca das classificações propostas se percebe que o objetivo alcançado por esta foi tão somente distinguir o crime eletrônico do crime tradicional cometido por meio de um sistema informatizado. O uso do sistema eletrônico para a perpetração de condutas ilícitas já tipificadas como o furto ou o estelionato não se faz capaz de conferir a natureza de crime eletrônico à conduta praticada. Isto porque o sistema eletrônico funcionou como um novo meio de execução de conduta já descrita em norma penal incriminadora protetiva de outro valor social alheio aos bens informacionais ou eletrônicos. E isso em uma sociedade cada vez mais informatizada passará a ser mais comum, uma vez que a delinqüência, vislumbrando o surgimento de inúmeras oportunidades também se informatizará passando a utilizar em maior escala os sistemas eletrônicos para a prática de delitos comuns.

O simples surgimento de um novo meio de execução de uma conduta já tipificada não altera o seu núcleo nem o objeto protegido, não alterando sua classificação nem sua natureza. Exemplo cabal disso foi o surgimento da arma de fogo que apesar de ter sido um novo meio de execução do homicídio não alterou a sua figura típica, pois o cerne do fato típico ficou inalterado uma vez que a descrição: matar alguém; permite a prática do delito por inúmeros meios, inclusive com uso de arma de fogo.

Desta feita percebe-se que os esforços em busca da classificação dos crimes eletrônicos não alcançaram o seu desiderado de forma completa, pois tão somente ajudaram a sedimentar a distinção entre crime eletrônico e crime comum, ressaltando-se a importância do caráter didático destas classificações.

---

[176] JESUS, Damásio E. de apud ARAS, Vladimir. Crimes de Informática: Uma nova criminalidade. **Jus Navigandi**, Ed. 12, out. 2001. Disponível em: < http://www1.jus.com.br/doutrina/texto.asp?id=2250 >. Acesso em: 02 out. 2001.

Neste sentido faz-se necessário a reformulação dos sistemas de classificação extirpando-se dos seus conteúdos os crimes já abarcados por normas penais protetoras de outros interesses jurídicos que não os eletrônicos, como por exemplo:

Quantos aos efeitos dos crimes eletrônicos:

- Crimes eletrônicos de efeitos tangíveis;
- Crimes eletrônicos de efeitos intangíveis.

Classificam-se como crimes eletrônicos de efeitos tangíveis aquelas condutas que apesar de serem perpetradas em meio eletrônico produzem também efeitos diretos no mundo real, exemplo cabal destes ilícitos é a ação de sabotagem informática que além de danificar ou inutilizar os dados efetua danos muitas vezes irreparáveis na máquina. As ações que debelam crimes eletrônicos intangíveis lesam tão somente os elementos imateriais formadores do sistema informacional com os dados armazenados, em processamento ou em transmissão.

Quanto aos objetivos:

- Crimes eletrônicos de mero acesso;
- Crimes eletrônicos de dano ou lesão.

Os crimes eletrônicos de mero acesso consubstanciam-se com o simples acesso ao sistema informacional, não necessitando que do referido ato resulte algum dano a dados ou ao próprio sistema. Por outro lado os crimes eletrônicos de dano ou lesão são aqueles que de maneira direta danificam o sistema computacional sem necessidade da obtenção de alguma vantagem econômica ilícita para o autor, é o que ocorre na sabotagem informática ou na disseminação de vírus.

São classificações neste sentido que devem ser elaboradas, pois facilitam o estudo e divisão da matéria, não se desmerecendo o valor doutrinário e didático dos sistemas classificatórios enunciados neste trabalho. Deve-se ressaltar que estes sistemas serviram para evidenciar a distinção entre crimes comuns (tradicionais) e crimes eletrônicos, uma vez que o uso do sistemas eletrônicos para praticar condutas já incriminadas por tipos penais não pode

ser considerado um crime eletrônico, pois o sistema informacional não passou de um meio de execução, e isto no máximo pode render a tal prática a qualificação da conduta alterando-lhe a pena pois o núcleo do tipo penal permaneceu inalterado.

Nesses casos cabe ao legislador a criação de qualificadoras e elementos majorantes genéricos para as condutas perpetradas por computador que atentem contra bens juridicamente já protegidos, evitando-se a criação de tipos penais extremamente específicos unicamente pelo surgimento de um novo meio de execução.

3.4 O criminoso eletrônico

O mundo supostamente complexo da informática, suas expressões e linguagens peculiares, bem como a especificidade de conhecimentos virtualmente exigidos fazem crer que o criminoso eletrônico, ou seja, o agente ativo das condutas ilícitas, venha a ser um exímio perito na operação de computadores e sistemas de eletrônicos.

Passou-se o tempo em que o perfil do criminoso eletrônico era esse. Atualmente com as facilidades ocasionadas pelo desenvolvimento de *Softwares e Hardwares*, bem como as inúmeras informações disponíveis na própria rede à cerca do assunto, qualquer indivíduo que possua as mínimas noções de como operar um computador pode ser considerado um criminoso eletrônico em potencial.

Ao contrário do que se apresentava nos anos 70 e 80, quando o criminoso eletrônico possuía conhecimentos específicos e detalhados chegando a ser contratado, após o cumprimento de suas penas, por empresas especializadas em segurança de sistemas, os crimes informáticos ou os cometidos através da Internet passaram a ser conhecidos como os *"Special Oportunity Crime*", Crimes de Oportunidade. Normalmente os criminosos também são de oportunidade, não sendo afeitos a prática de condutas ilícitas, mas em face das facilidades e da oportunidade que surge praticam o fato. Na maioria das vezes são profissionais que laboram na área de informática e com freqüência praticam os delitos contra seus empregadores.

Os meios de comunicação divulgaram no correr dos anos um perfil extremamente romântico do criminoso eletrônico, o que gerou dentro da sociedade uma sensação de aceitabilidade equivocada em relação a estes, pois acreditava-se que os delitos perpetrados

possuíam menor potencial lesivo, não passando de brincadeiras de estudantes de classe média altamente especializados em informática, com boa escolaridade, inteligentes e normalmente afeitos pela síndrome de *Robin Wood,* criando em favor de si certa simpatia social. O que muito os distinguiam dos criminosos ditos comuns, pertencentes as classes D e E.

O perfil criado e divulgado pela mídia tem o criminoso eletrônico como sendo, em regra, indivíduo do sexo masculino, que trabalha de alguma forma com a utilização de computadores e sistemas eletrônicos, com idade entre 16 e 33 anos de idade, avessos a violência e que possuem inteligência acima da média. São extremamente audaciosos e aventureiros, movidos acima de tudo pelo desejo de conhecimento e de superação à máquina.

Hoje tais delinqüentes são, em geral, pessoas que trabalham no ramo ligado a utilização de sistemas eletrônicos, não tão jovens nem inteligentes; são *insiders*, vinculados a empresas (em regra); sua característica central consiste na pouca motivabilidade em relação à norma (raramente se sensibilizam com a punição penal); motivos para delinqüir: ânimo de lucro, perspectiva de promoção, vingança, apenas para chamar a atenção etc.

Escondem-se normalmente atrás do sentimento de anonimato, que permeia o ambiente eletrônico, que serve para bloquear os parâmetros de entendimento da conduta que praticam como ilegal, alegando ainda o desconhecimento do crime que praticaram escondem-se atrás do fato de praticarem o ato simplesmente por "brincadeira".

Notavelmente podem-se dividir as condutas ilícitas praticadas em três estágios de motivação (objetivos do criminoso). A primeira fase surge com seu instinto aventureiro; movidos pelo desafio de superação da máquina perpetram condutas criminosas. Uma vez superada a máquina e satisfeito o ego, percebem um meio fácil, e sob sua óptica seguro, de ganhar dinheiro extra, este é o segundo estágio. O terceiro caracteriza-se como um prolongamento do segundo, uma vez que passam a praticar infrações com o intuito de sustentarem seus altos custos de vida que se resumem a compra de equipamentos eletrônicos de última geração.

A questão é extremamente alarmante e perigosa, para ilustrar tal situação experimente pensar em um jovem brilhante estagiário de informática do centro de processamento de dados de uma Universidade, que altera as notas e as freqüências dos alunos, ou um promissor

programador de computador de uma empresa multinacional, ávido por reconhecimento, que rompe os sistemas de segurança para depois apresentar-se como solução.

Verifica-se de maneira assustadora que o perfil do criminoso eletrônico difere em muito do criminoso comum, e isto embaça de sobremaneira o trabalho de investigação e repressão a estes delitos.

Contudo, a figura mais associada à prática de ilícitos por intermédio de sistemas eletrônico é a do *Hacker*. Termo lendário e gerador de inúmeras polêmicas o *Hacker* está ligado diretamente ao surgimento dos primeiros sistemas informatizados e de forma genérica pode ser definido como aquele que burlam os sistemas de segurança de redes de computadores ou sistemas eletrônicos obtém acesso não autorizado ao sistema ou aos recursos por ele disponibilizados.

A origem da palavra *Hacker* é bastante controvertida, indo desde o simples fato de dar um golpe cortante, até o indivíduo que viola sistemas de informática. Procurando esclarecer o assunto David Casacuberta e José Luis Martín Más afirmam que:

> *Según la leyenda, el primer uso no 'tradiciona' del términp se debe a alguien que sabía donde dar el puntapié ('hack') exacto en una máquina de refrescos para conseguir una botella gratis. Ya sea en ese sentido o en el de cortar algo en pedazos, lo cierto es que el primer uso genuino de hacker en el mundo de la informática era el de alguien que conocá de forma tan detallada un sistema operativo (lo habáia 'cortado en pedazos' por así decirlo) que podía obtner de él lo que quisiera (como el señor de la leyenda urbana acerca de una máquina de refrescos). Así, en el sentido originario, un hacker es simplemente alguien que conoce los sistemas operativos (y por tanto los ordenadores) como la palma de su mano.* [177]

Apesar de possuir origem conturbada, o vocábulo *Hacker* popularizou-se, principalmente por força dos meios de comunicação, como o criminoso eletrônico. Contudo, no submundo virtual a terminologia hacker dificilmente é associada a fins criminosos, sendo correlacionada tão somente a um indivíduo extremamente hábil no campo informático.

Dentro desse grupo, criou-se uma nova denominação, os *Crackers*. No seio da comunidade informática repousa quase que sagrada a divisão entre *Hackers e Crackers,* posto

---

[177] CASACUBERTA, David; MARTÍNS MÁS, José Luis. **Diccionario de ciberderechos**. Disponível em: <http://www.kriptopolis.com/dicc.html>. Acesso em: 5 jan. 2000.

que os primeiros invadem sistemas computacionais com o objetivo tidos, por eles, como nobres, como por exemplo verificar a segurança de determinada rede, ou somente para aprimorar suas técnicas. Os *Crackers*, tidos como os *Hackers* não éticos, ou "maus", são aqueles que enveredam pela criminalidade eletrônica invadindo sistemas com interesses patrimoniais ou danosos.

A bem da verdade, independentemente dos objetivos ou das motivações pessoais *Hackers e Crackers* invadem sistemas informáticos e invariavelmente violam a privacidade e o sigilo dos dados contidos nesses sistemas, o que por si só já configura crime na maioria dos países de primeiro mundo.

Inúmeros estudos tentaram classificar os diversos tipos de *Hackers*. Dentre eles pode-se destacar Landreth[178], Hollinger[179] e Rogers[180]. Contudo, é a classificação formulada por Túlio Lima Vianna[181] a que mais se destaca. Para o autor os criminosos eletrônicos se classificam da seguinte forma:

- *Crackers* de Servidores – *Hackers* que invadem computadores ligados em rede;

---

[178] Landreth classificou os *hackers* em seis níveis: Os novatos (Novice) que possuiam menor capacidade técnica e lesiva; Os estudantes (Student) que ao revés de se dedicar a seus afazeres acadêmicos passa seu tempo invadindo sistemas; O turista (Tourist) que invade sítios pela sensação de aventura; O estilhaçador (Crasher) que invade sistemas com objetivos de danificá-los, e o Ladrões(Thief) que possuem objetivos econômicos). LANDRETH, B. Out of the inner circle. Redmond: Microsoft Books, 1985 apud ROGERS. Disponível em: <http://www.escape.ca/~mkr/hackerdoc.pdf>. Acesso em: 10 fev. 2003.

[179] Hollinger efetuou criterioso estudo dentro da comunidade universitária e classificou os Hackers em três grandes grupos: Piratas (Pirates), Navegadores (Browsers) e os Crackers. Os piratas seriam menos desenvolvidos tecnicamente resumindo suas atividades as violações de direitos autorais sobre *softwares.* Os navegadores, por se encontrarem em um nível intermediário de conhecimento possuem habilidades para invadir sistemas, mas não causam qualquer espécie de lesão a integridade dos dados ali contidos. Já os *Crackers* são aqueles que possuem nível de conhecimento técnico mais elevado e os responsáveis pelos maiores prejuízos as vítimas.

[180] O professor da Universidade de Manitoba e criminólogo Marc Rogers diferencia os *Hackers* em sete categorias distintas: *Newbie/tool kit(NT), Cyberpunk(CP), Internals(IT), Coders(CD), Old guard hackers(OG), Professional Criminal(PC) e Cyber-terrorists(CT).* Os NT são os invasores que possuem o menor nível técnico, utilizando-se de programas prontos que adquirem da própria *Internet*. Os CP possuem bom conhecimento de informática e de programação sendo capazes de desenvolver seus próprios programas. Contudo envolvem-se em atividades mal intencionadas como alteração de sítios e fraudes com cartões de crédito e de telefonia. Já os IT e CD, que segundo Rogers são responsáveis por mais de 70% da atividade ilícita envolvendo computadores, são na sua grande maioria empregados descontentes ou ex-funcionários que utilizam-se dos conhecimentos adquiridos na empresa para atacá-las como forma de vingança. O grupo formado pelos OG não possui intenções criminosas e incorporam a filosofia romântica da primeira geração *hacker,* contudo não respeitam a privacidade de terceiros. Entretanto, as categorias mais perigosas são as que englobam os PC e os CT, posto que estas classes são formadas por criminosos profissionais e ex-agentes de inteligência que especializaram-se em espionagem corporativa e atacam por dinheiro. ROGERS apud VIANNA, Túlio Lima. **Hackers**: um estudo criminológico da subcultura cyberpunk. **Jus Navegandi**. Disponível em: <http://www.jus.com.br>. Acesso em: 10 fev. 2003.

[181] Ibid., 2003.

- *Crackers* de Programas – *Hackers* que quebram proteções de *softwares* cedidos a título de demonstração para usá-los por tempo indeterminado;
- *Phreakers – Hackers* especialistas em telefonia móvel ou fixa;
- Desenvolvedores de Vírus, *Worms* e *Trojans* – Programadores que criam pequenos *softwares* que causam algum dano ao usuário;
- Piratas – Indivíduo que clonam programas fraudando direitos autorais;
- Distribuidores de *Warez – Webmaters* que disponibilizam em suas páginas *softwares* sem autorização dos detentores dos direitos autorais.

Dentro desses vários grupos de criminosos eletrônicos deve-se destacar que tudo se originou com os chamados *Crackers* de Servidores, sendo estes os responsáveis tecnicamente pelas invasões de computadores e de sistemas eletrônicos. Essa categoria do gênero *hacker* se subdivide, segundo o entendimento de Túlio Lima Vianna[182] , nas seguintes subcategorias:

- Curiosos – Movidos por curiosidade, não causam danos aos dados armazenados ou em tráfego pelas redes informáticas, restringindo-se somente a violar a privacidade das vítimas, e o sigilo dos dados em trânsito pelos sistemas computacionais;
- Pichadores Digitais – Procuram auto-afirmação dentro da rede agindo com o único objetivo de serem reconhecidos e famosos no universo virtual;
- Revanchistas – Formados por ex-funcionários ou empregados descontentes que utilizam-se dos conhecimentos auferidos na empresa para sabotá-la;
- Vândalos – Agem simplesmente pelo prazer de causar danos as vítimas;
- Espiões – Agem com a finalidade de adquirirem informações confidencias armazenadas nos sistemas computacionais das vítimas, as informações podem ter caráter comercial ou não;
- Ciberterroristas – Possuem motivações políticas ou religiosas e utilizam-se do meio digital para realizarem atividades criminosas que possibilitem a divulgação de suas crenças;
- Ladrões e Estelionatários – Têm objetivos de lesar o patrimônio das vítimas.

O *modus operandi* dos agentes criminosos é bastante variado, e possui respaldo na gama de técnicas e ferramentas desenvolvidas por estes com a finalidade de perpetrarem os

[182] Ibid., 2003.

ilícitos eletrônicos. Túlio Lima Vianna[183], em análise pormenorizada dos métodos utilizados pelo Cr*ackers* enumera as seguintes formas:

a) Dedução: é o método mais simples para se conseguir uma senha. Para que o acesso seja liberado, o servidor requer do usuário sempre um *login* e uma senha. O *login* em geral é público e na maioria dos casos é muito fácil de descobri-lo. Por exemplo: no caso de acesso a Internet, o *login* do usuário é a parte do *email* anterior ao caráter "@". Conhecendo o *login* do usuário, o *cracker* procura, a partir dele, deduzir a senha correspondente. Não é difícil deduzir-se corretamente porque um grande número de usuários cria as suas senhas baseando-se numa relação com o respectivo *login*, proporcionando facilmente o acesso não autorizado.

b) Engenharia social: a utilização desse método para a prática de crimes é uma forma de dedução mais elaborada, onde o *cracker* utiliza de conhecimentos prévios a respeito da vítima para tentar usá-los como senha, por exemplo: data de nascimento, nomes de esposo(a), namorado (a) e filhos do usuário. No dizer de José Antônio Milagre, engenharia social é "a arte de enganar pessoas"[184]. Viviane Zandonadi[185], diz que, para investigar crimes eletrônicos, é preciso mergulhar no conhecimento técnico e na engenharia social.

c) Tentativa e erro: aqui o *cracker* tenta todas as combinações de letras e números possíveis até encontrar a correta. Seria um método inviável se fosse preciso digitar uma por uma todas as combinações, mas existem programas que poupam o trabalho braçal de digitação das possibilidades. Embora lento, é um procedimento cem por cento viável.

d) Invasão do servidor: dos métodos analisados acima, este é o único que exige um conhecimento avançado por parte dos *crackers*. Nele o *cracker* consegue forçar sua conexão a um servidor e então copia os arquivos em que ficam armazenadas as senhas dos usuários. Depois, já desconectado da rede, o *cracker* descriptografa as senhas.

A realidade social e cultural que permeia o ambiente digital torna extremamente complexa a confecção de um perfil do chamado criminoso eletrônico. Contudo, a

[183] Ibid., 2003.
[184] MILAGRE, José Antonio. Riscos do uso inadequado dos recursos de TI: tele-trabalho e boas práticas de direito digital. **Imasters**, Espírito Santo. a.1, p. 58-65, jul. 2007. p.62.
[185] ZANDONADI, Viviane. Na cola dos crackers. **Info Exame**, São Paulo, v. 19, n. 221, p. 66-67, ago. 2004.

complexidade de relações ilícitas potencializadas pela utilização das redes informacionais, bem como as inúmeras possibilidades de classificação desses criminosos, o que torna essa atividade muito mais *sui generis,* fazem com que a criminologia cada vez mais se interesse pelo tema e busque, dentro de seus pressupostos científicos, erigir um conceito científico a ser adotado pelo direito penal.

3.5 Os crimes eletrônicos previstos na ordem jurídica brasileira

Inseridas no conjunto de normas legais formadoras do ordenamento jurídico nacional, encontram-se de maneira esparsa alguns tipos penais de natureza eletrônica contidos em normas específicas de determinado ramo do direito, como por exemplo, o Direito Eleitoral.

Neste sentido a Lei Federal 8.137 de 27 de dezembro de 1990, que define os crimes contra a ordem tributária, econômica e contra as relações de consumo, entre ouras providências estabelece:

> Artigo 2º - Constitui crime da mesma natureza:
>
> V - utilizar ou divulgar programa de processamento de dados que permita ao sujeito passivo da obrigação tributária possuir informação contábil diversa daquela que é, por lei, fornecida à Fazenda Pública.
> Pena - detenção, de 6 (seis) meses a 2 (dois) anos, e multa

Além de constituir violação contra a ordem tributária, se trata de crime eletrônico, pois o programa utilizado para o processamento dos dados inseridos no sistema altera o correto tratamento dos dados e faz com que o resultado do processo seja maculado, uma vez que dados corretos são processados por um programa alterado que, objetivando fraudar as informações processadas, modifica o resultado. Verifica-se ademais, que se trata de tipo penal extremamente específico, uma vez que só ocorre quando se viola interesse da fazenda pública. Contudo, tal conduta, qual seja, a utilização de programa modificado para alteração dos resultados do processamento, pode ser perpetrada contra inúmeros sujeitos passivos distintos do fisco, e nestes casos, por falta de regulação legal são condutas carentes de punição, apesar do juízo reinante de reprovabilidade social.

Regulando inciso XII, parte final, do art. 5° da Constituição Federal[186], a Lei Federal 9.296 de 24 de julho de 1996 estabelece em seu bojo um crime de natureza informática:

> Artigo 10 - 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.

O dispositivo legal acima colacionado estabelece como crime o ato de interceptar comunicações, mas não é qualquer tipo de comunicação, até porque o ser humano possui inúmeras formas de se comunicar. Assim, a supra mencionada lei enumera quais os tipos de interceptação são passíveis de punição em face de serem consideradas ilícitas. Dentre os tipos dispostos na lei está a interceptação de comunicação eletrônica. Logo qualquer interceptação não autorizada de comunicação realizada entre sistemas computacionais e eletrônicos, constitui ato ilícito tipificado pelo artigo 10 da Lei Federal 9.296/96. Exemplo singular da interceptação da comunicação informática, ou seja, da troca de informações ou de dados feitas por meios informáticos, é a violação de *e-mails*.

Visando proteger os sistemas informáticos utilizados pela Justiça Eleitoral, a Lei Federal 9.504 de 30 de setembro de 1997 prevê a criação de três delitos eletrônicos:

> Artigo 72. Constituem crimes, puníveis com reclusão, de cinco a dez anos:
>
> 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;
>
> II - 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;
>
> III - causar, propositadamente, dano físico ao equipamento usado na votação ou na totalização de votos ou a suas partes.

Apesar da especificidade dos delitos, ou seja, só podem ser perpetrados contra sistemas eletrônicos utilizados pela Justiça Eleitoral, tratam-se de condutas que de forma genérica podem ser praticadas contra qualquer sistema informacional, contudo, em face do "engessamento" cometido pelo legislador, estas situações ficaram desprotegidas uma vez que

[186] Constituição Federal de 1988. Artigo 5º inciso XII – "É inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal".

somente o caso específico foi regulamentado.

No delito tipificado no inciso I, tem-se a ocorrência de duas situações ilícitas. A primeira é o acesso não autorizado a sistema eletrônico, que por si só já se configura como fato punível como crime eletrônico. Entretanto, o tipo penal atrela ao acesso o intuito de alteração de dados relativos a contagem dos votos. Só quando verificadas essas duas condições a conduta se torna punível. O ato lesa interesses jurídicos distintos dos bens eletrônicos, mas opera-se por meio de lesão a estes, uma vez que a segurança do sistema foi violada e a integridade dos dados foi deturpada em face de sua manipulação.

No crime capitulado no inciso II, tem-se um conjunto de condutas lesivas a bens eletrônicos tais como apagar ou transmitir dados e informações. O tipo penal visa proteger a corrupção do tratamento correto de dados utilizados pelo serviço eleitoral, quer seja pelo desenvolvimento ou pela introdução de comando, instrução ou programa, quer por qualquer meio que altere o correto processamento e o resultado dos dados inseridos no sistema eletrônico a serviço do pleito eleitoral.

No inciso III verifica-se, apesar de seu espectro de incidência reduzido, a tipificação da conduta intitulada pela doutrina como dano eletrônico, ou seja, efetuar dolosamente dano ao equipamento utilizado na votação com objetivo de evitar o acesso aos dados nele contidos ou a própria destruição do suporte físico de armazenamento dos dados.

Os delitos tipificados pela Lei 9.504/97 possuem aspecto extremamente restrito pois somente se aplicam a atos que atentem contra sistemas eletrônicos ou equipamentos envolvidos no processo eleitoral, o que causa uma enorme lacuna no ordenamento jurídico penal, pois deixa sem punição condutas perfeitamente adequadas aos elementos incriminadores dispostos na norma penal, mas por não atingirem sistemas eletrônicos a serviço da Justiça Eleitoral não são puníveis. Tal constatação demonstra à necessidade de repensar-se o modo de elaboração das normas legais aplicáveis a matéria.

Com a escalada da criminalidade eletrônica a Lei Federal 9.983 de 14 de junho de 2000 visando proteger e coibir a prática de ilícitos contra os sistemas eletrônicos utilizados pela Administração Pública, estabeleceu nova redação e introduziu artigos no Código Penal brasileiro. As modificações operaram-se da seguinte forma:

> § 1º-A do artigo 153 do Código Penal - 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 ;
>
> Artigo 313-A do Código Penal - 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;
>
> Artigo 313-B do Código Penal - 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 a modificação ou alteração resulta dano para a Administração Pública ou para o administrado.
>
> § 1º do artigo 325 do Código Penal Brasileiro - Nas mesmas penas deste artigo incorre quem:
>
> I - permite ou facilita, mediante atribuição, fornecimento e empréstimo de senha ou qualquer outra forma, o acesso de pessoas não autorizadas a sistema de informações ou banco de dados da Administração Pública;
>
> II - se utiliza, indevidamente, do acesso restrito:
>
> § 2º Se da ação ou omissão resulta dano à Administração Pública ou a outrem:
>
> Pena - reclusão, de 2 (dois) a 6 (seis) anos, e multa.

O delito capitulado no § 1º - A do artigo 153 do Código Penal, denomina-se de violação de segredo. Só adquire a natureza de crime eletrônico quando as informações sigilosas estiverem contidas em meios eletrônicos como os bancos de dados computacionais, pois somente assim um bem eletrônico seria lesado pela prática do ilícito, ou seja, seria violado o sigilo dos dados computacionais existentes no sistema.

O artigo 313 – A, tipificou a conduta de manipulação de dados em sistema eletrônico pertencente à Administração Pública. Dentre as peculiaridades do fato típico encontra-se mais uma vez a restrição da prática da conduta a determinados sistemas eletrônicos, ou seja, aqueles a serviço da Administração Pública, bem como a necessidade de que o mesmo seja praticado por funcionário público, amputando-se assim o campo de incidência do tipo penal o que por força de sua extrema especificidade deixa uma série de condutas ilícitas carentes de sanção legal. O crime em análise visa coibir de forma direta que um funcionário público manipule ou facilite a manipulação de dados contidos em sistema de informacional ou banco de dados da Administração Pública. A manipulação pode consistir na inserção de dados falsos

no sistema, na alteração ou exclusão de dados corretos, não importando se o interesse do autor da conduta era a obtenção de alguma vantagem econômica ilícita ou se apenas causar dano.

Estabelece o artigo 313 – B do Código Penal, o crime que só pode ser praticado por funcionário público, consistindo a conduta típica na alteração ou modificação sistema de informações ou programa de computador sem a devida autorização.

Ressalte-se que os delitos capitulados nos artigos 313-A e 313-B do Código Penal nacional são considerados pela maioria da doutrina como crimes de mão própria, ou seja, só podem ser cometidos por funcionários públicos, restringindo-se, desta forma, ainda mais o campo de aplicação da lei incriminadora.

O inciso I do § 1º do artigo 325 do Código Penal pune o funcionário que de alguma forma possibilita a terceiro não autorizado o acesso a banco de dados ou sistemas de informação da Administração Pública, não importando qual o meio utilizado pelo agente para facilitar o acesso indevido. Trata-se de dispositivo legal extremamente importante que busca coibir a facilitação dos acessos indevidos. Entretanto este crime adquire aspecto peculiar, pois em virtude da ausência de dispositivos legais reguladores da matéria aplicáveis a todos os agentes, somente o funcionário público seria punido, não recaindo nenhuma punição sob quem acessou o banco de dados ou o sistema de informações.

Já o inciso II do parágrafo 1º do artigo 325 do Código Penal, procura punir o funcionário que dotado de autorização para acessar informações ou para realizar atividades de cunho restrito no sistema eletrônico, arbitrariamente extrapola os limites de sua autorização, acessando dados não permitidos ou praticando atividades indevidas.

Além das condutas acima impostas, que já possuem certo nível de repressão penal na ordem jurídica brasileira, lista-se abaixo um quadro que enumera os tipos penais já existentes que podem facilmente serem potencializados pela utilização de meios eletrônicos:

Crimes contra a pessoa	
Induzimento, instigação ou auxílio a suicídio	Art. 122, CP: Induzir ou instigar alguém a suicidar-se ou prestar-lhe auxílio para que o faça. Parágrafo único. A pena é duplicada: I – se o crime é praticado por motivo egoístico;

	II – se a vítima é menor ou tem diminuída, por qualquer causa, a capacidade de resistência.
Ameaça	Art. 147, CP: Ameaçar alguém, por palavra, escrito ou gesto, ou qualquer outro meio simbólico, de causar-lhe mal injusto e grave. A pena é de detenção, de um a seis meses, ou multa.
Violação de correspondência	Art. 151, CP: Devassar indevidamente o conteúdo de correspondência fechada, dirigida a outrem. A pena é detenção, de um a seis meses.
Divulgação segredo	Art. 153, CP: Divulgar alguém, sem justa causa, conteúdo de documento particular ou de correspondência confidencial, de que é destinatário ou detentor, e cuja divulgação possa produzir dano a outrem. A pena é de detenção, de um a seis meses, ou multa.

Crimes contra o patrimônio	
Estelionato	Art. 171, CP: Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento. A pena aplicada ao tipo simples é de reclusão, de um a cinco anos, e multa.

Crimes contra a propriedade imaterial	
Violação de direito autoral	Art. 184, CP: Violar direito autoral. § 1º. Se a violação consistir em reprodução, por qualquer meio, com intuito de lucro, de obra intelectual, no todo ou parte, sem autorização expressa do autor ou de que o represente, ou consistir na reprodução de fonograma ou videofonograma, sem a autorização do produtor ou de quem o represente. A pena aplicada ao tipo simples (*caput*) é de detenção, de três meses a um ano, ou multa.
Usurpação de nome ou pseudônimo alheio	Art. 185, CP: Atribuir falsamente a alguém, mediante o uso de nome, pseudônimo ou sinal por ele adotado para designar seus trabalhos, a autoria de obra literária, científica ou artística. A pena é de detenção, de seis meses a dois anos.

Crimes contra o sentimento religioso	
Ultraje a culto e impedimento ou perturbação de ato a ele relativo	Art. 208, CP: Escarnecer de alguém publicamente, por motivo de crença ou função religiosa; impedir ou perturbar cerimônia ou prática de culto religioso; vilipendiar publicamente ato ou objeto de culto religioso. (grifou-se) A pena para o tipo simples é de detenção, de um mês a uma ano, ou multa.
Crimes contra os costumes	
Corrupção de menores	Art. 218, CP: Corromper ou facilitar a corrupção de pessoa maior de 14 (catorze) e menor de 18 (dezoito) anos, com ela praticando ato de libidinagem, ou induzindo-lhe a praticá-lo ou presenciá-lo. (grifou-se) A pena é de reclusão, de um a quatro anos.

Favorecimento da prostituição	Art. 228, CP: Induzir ou atrair alguém à prostituição, facilitá-la ou impedir que alguém a abandone. A pena é de reclusão, de dois a cinco anos.
Escrito ou objeto obsceno	Art. 234, CP: Fazer, importar, exportar, adquirir ou ter sob sua guarda, para fim de comércio, de distribuição ou de exposição pública, escrito, desenho, pintura, estampa ou qualquer objeto obsceno. A pena é de detenção, de seis meses a dois anos.

Crimes contra a paz pública	
Incitação ao crime	Art. 286, CP: Incitar, publicamente, a prática de crime. A pena é de detenção, de três a seis meses, ou multa.
Apologia de crime ou criminoso	Art. 287, CP: Fazer, publicamente, apologia de fato criminoso ou de autor de crime. A pena á de detenção, de três a seis meses, ou multa.

Crimes contra a fé pública	
Falsa identidade	Art. 307, CP: Atribuir-se ou atribuir a terceiro falsa identidade para obter vantagem, em proveito próprio o alheio, ou para causar dano a outrem. A pena é de detenção, de três meses a um ano, ou multa.

Crimes contra a administração pública	
Exercício arbitrário das próprias razões	Art. 345, CP: Fazer justiça pelas próprias mãos, para satisfazer pretensão, embora legítima, salvo quando a lei o permite. A pena é de detenção, de quinze dias a um mês, ou multa.

Crimes previstos na legislação extravagante	
Tráfico de drogas	Lei nº. 11.343 de 23 de agosto de 2006, que dispõe sobre medidas de prevenção e repressão ao tráfico ilícito e uso indevido de substâncias entorpecentes ou que determinem dependência física ou psíquica
Contra a segurança nacional	Lei nº. 7.170 de 14 de dezembro de 1983, que define os crimes contra a segurança nacional, a ordem política e social: estabelece seu processo e julgamento: Art. 13. Comunicar, entregar ou permitir a comunicação ou a entrega, a governo ou a grupo estrangeiro, ou a organização ou grupo de existência ilegal, de dados, documentos ou cópias de documentos, planos, códigos, cifras ou assuntos que, no interesse do Estado brasileiro, são classificados como sigilosos. Art. 15. Praticar sabotagem contra militares contra instalações militares, meios de comunicações, meios e vias de transporte, estaleiros, portos, aeroportos, fábricas, usinas, barragens, depósitos e outras instalações congêneres. Art. 23. Incitar: I – à subversão da ordem política ou social; II – à animosidade entre as Forças Armadas ou entre estas e classes sociais ou as instituições civis;

	III – à luta com violência entre as classes sociais; IV – à pratica de qualquer dos crimes previstos nesta lei. A pena para o crime do art. 13 é de detenção, de um a cinco anos; para o crime do art. 15, reclusão, de três a dez anos; e para o crime do art. 23, reclusão, de um a quatro anos.
Pedofilia e divulgação de pornografia infantil	Lei nº. 8.069 de 13 de julho de 1990, que dispõe sobre o Estatuto da Criança e do Adolescente: Art. 241. Apresentar, produzir, vender, fornecer, divulgar ou publicar, por qualquer meio de comunicação, inclusive rede mundial de computadores ou internet, fotografias ou imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente.
Contra a ordem tributária	Lei nº. 8.137 de 27 de dezembro de 1990, que define crimes contra a ordem tributária, econômica e contra as relações de consumo: Art. 1º. Constitui crime contra a ordem tributária suprimir ou reduzir tributo, ou contribuição social e qualquer acessório, mediante as seguintes condutas: III – falsificar ou alterar nota fiscal, fatura, duplicata, nota de venda, ou qualquer outro documento relativo à operação tributável; IV – elaborar, distribuir, fornecer, emitir ou utilizar documento que saiba ou deva saber falso ou inexato; A pena para os crimes elencados no art. 1º é de reclusão, de dois a cinco anos, e multa. Para os crimes do art. 2º é de detenção, de seis meses a dois anos, e multa.
Tráfico de armas	Lei nº. 10.826 de 22 de dezembro de 2003, que institui o Estatuto do Desarmamento.

Os exemplos colacionados demonstram que apesar do surgimento de legislação correlacionada com a matéria, a regulamentação existente é dispersa e extremamente específica aplicando-se a determinados temas. Em conseqüência disto uma gama de condutas ilícitas encontram-se carentes de punição em face da ausência de normas legais atinentes ao assunto como um todo. Deve-se então elaborar diploma legal que trate a matéria de forma técnica, criminalizando as condutas que atentem contra os sistemas eletrônicos e seus dados, independentemente do seu proprietário, não importando se ente público ou privado, se a Administração Pública ou particular, ressaltando-se que uma vez escalonado os graus de importância dos mais variados sistemas eletrônicos, deve-se estipular algumas qualificadoras para condutas que atentem contra os mais importantes.

Logo, em virtude do vácuo normativo existente, o que ocasiona a falta de punição penal a esse novo conjunto de ilícitos (novos crimes e novos meios de execução), deve-se com urgência elaborar mecanismos jurídicos aptos à tratarem a matéria.

3.6 As perspectivas de regulação dos crimes eletrônicos

A carência de regras jurídicas a nortearem a proteção dos sistemas eletrônicos, vem causando inúmeros prejuízos a manutenção da ordem informacional. Dessa forma, verifica-se a existência de laguna legislativa que expõe a perigo efetivo os bens e valores eletrônicos que foram albergados pela ordem constitucional.

Logo para sanar a situação faz-se necessário o preenchimento desse vazio normativo, através da criação de mecanismos legais que permitam a incriminação das condutas tidas como lesivas. Nesse diapasão, resta ao Estado brasileiro optar pela elaboração de normas internas, ou aderir ao esforço internacional de regulamentação da matéria.

3.6.1 A regulação interna

A construção jurídica constitucional brasileira, por força do princípio da reserva legal, formalmente inserido no inciso XXXIX do artigo 5º da Constituição Federal, veda a utilização da interpretação analógica na seara penal sempre que esta forma seja utilizada para ampliar o rol de incidência de alguma figura típica. Ou seja, a analogia só pode ser utilizada no direito penal em situações que comportem alguma vantagem apara o acusado, nunca em sentido contrário.

Dessa maneira, na busca de tutelar penalmente a nova realidade criminosa que surge ante a evolução tecnológica, faz-se indispensável a construção de tipos penais incriminadores através do sistema formal de expressão penal, qual seja, a lei. A ausência de dispositivos legais específicos que ensejem a criminalização das condutas criminosas eletrônicas configura-se um problema complexo e de difícil solução técnica. Entretanto, como único detentor do poder punitivo penal, cabe ao Estado a tarefa de zelar pelos direitos dos cidadãos, e acima de tudo reprimir as condutas nocivas a manutenção da sociedade.

> Se na era da informática, com a transformação tecnológica da sociedade, surgiu a prática do crime virtual, conseqüentemente se impõe a existência de limites legais a tipificação regulamentadora dessas condutas antijurídicas universalmente praticadas pelos usuários da internet[187].

[187] HESPANHA, Benedito, op. cit., v. 1, n. 16, p.29-64, 200. p.50-53.

Atento a essa nova realidade o Congresso Nacional sediou debates sobre o assunto, o que fomentou o surgimento de inúmeras proposições legislativas. Do conjunto de projetos de lei que versam sobre o tema da criminalidade nas áreas da informática, das telecomunicações e da Internet pode-se destacar três como os mais importantes e de maior acuidade técnica. São eles: Projeto de Lei da Câmara nº. 89 de 2003 (PLC 89/03); Projeto de Lei do Senado nº. 137 de 2000 (PLS 137/00); e, Projeto de Lei do Senado nº. 76 de 2000 (PLS 76/00).

O Projeto de Lei da Câmara 89/03 possuía como origem o Projeto de Lei da Câmara 84/99. O referido projeto, de autoria do Deputado Luiz Piauhylino, teve como processo inicial de construção o trabalho de um grupo de juristas que aperfeiçoou o PLC nº. 1.713/96, de autoria do Deputado Cássio Cunha Lima, arquivado em decorrência do término de sua legislatura. Após muita discussão, o projeto inicial foi sensivelmente alterado, principalmente pelo abandono da estruturação de uma lei extravagante que tratasse exclusivamente de crimes eletrônicos e conteve-se coma proposta de alteração do Decreto-Lei nº. 2.848, de 07 de dezembro de 1941 (Código Penal), e a Lei nº. 9.296, de 24 de julho de 1996, além de estabelecer outras providências.

Busca o projeto em análise inserir a Seção V, no Capítulo VI do Título I do Código Penal, onde seriam definidos os crimes contra a inviolabilidade dos sistemas informatizados, a saber: a) acesso indevido a meio eletrônico (art. 154-A); b) manipulação indevida de informação eletrônica (art. 154-B); c) dano eletrônico (art. 163, §3º); d) pornografia infantil (art. 218-A); e) atentado contra a segurança de serviço de utilidade pública; f) interrupção ou perturbação de serviço telegráfico e telefônico; g) falsificação de cartão de crédito; h) falsificação de telefone celular (art. 298-A); i) divulgação de informações pessoais ou de empresas.

O Projeto de Lei do Senado 137/00, de autoria do Senador Leomar Quintanilha, arquiteta-se em cima de apenas um artigo. O projeto disciplina as condutas ilícitas que utilizem ou danifiquem sistemas de computador e estabelece como circunstância majorante da pena (aumenta em até o triplo) quando o crime praticado contra a pessoa, o patrimônio, a propriedade imaterial ou intelectual, os costumes, e a criança e o adolescente for cometidos por meio da utilização da tecnologia de informação e telecomunicações.

De autoria do senador Renam Calheiros, o Projeto de Lei do Senado 76/00, procura tipificar os delitos praticados com o uso de computadores, e lhes atribuir as respectivas penas, sem modificar o Código Penal. Assim, classifica os crimes eletrônicos em sete categorias: a) crimes contra a inviolabilidade de dados e sua comunicação; b) crimes contra a propriedade e o patrimônio; c) crimes contra a honra e a vida privada; d) crimes contra a vida e a integridade física das pessoas; e) crimes contra o patrimônio fiscal; f) crimes contra a moral pública e opção sexual, e g) crimes contra a segurança nacional.

Ademais, o PLS 76/00 inovou ao acrescentar o termo "telecomunicação" ao tipo penal do crime de atentado contra a segurança de serviço de utilidade pública (art. 265), e ao do crime de interrupção ou perturbação de serviço telegráfico ou telefônico (art. 266); Mais ainda, utilizando a similitude com o regramento jurídico do furto de energia elétrica (art. 155, parágrafo 4º do Código Penal) estendeu a definição de "dano" do art. 163 para incluir elementos de informática, bem como, equiparou o cartão de crédito a documento particular no tipo de falsificação de documento particular (art. 298). Procura ainda, através de norma penal explicativa definir para fins penais o que seja "meio eletrônico" e "sistema informatizado", e por último, autoriza a interceptação do fluxo de comunicações em sistema de informática ou telemática, para a investigação de crimes punidos com pena de detenção, o que é vedado pela lei que regula a matéria (art. 2º,§ 2º, da Lei nº. 9.296, de 24 de julho de 1996).

Em 2005, em decorrência do requerimento 847/05 de autoria do Senador Renan Calheiros, o três projetos acima expostos passaram a tramitar conjuntamente posto que versavam sobre a mesma matéria: crimes eletrônicos. Contudo, atualmente, tramita no Congresso Nacional, especificamente na Comissão de Constituição e Justiça uma versão substitutiva do PLS 76/00 aprovada pela Comissão de Educação do Senado, que considerou as propostas pertinentes, votando pela aprovação do PLS 76/00, incorporando parcialmente o PLC 89/03 e o PLS 137/00 na forma do substitutivo. Acompanha o substitutivo um parecer elaborado pelo Senador Eduardo Azeredo[188], que ressalta a importância do tema tratado, bem como procede a minuciosa analise dos projetos aglutinados.

Para isso, o Projeto de Lei Substitutivo do PLC 89/03, PLS 137/00 e PLS 76/00 altera o Decreto-Lei nº. 2848, de 07 de dezembro de 1940 (Código Penal); o Decreto-Lei nº. 1.001, de

[188] AZEREDO, Eduardo. A tipificação de crimes na internet. **Ciência Jurídica,** Belo Horizonte, v.20, n.132, p.336-358, nov./dez. 2006. p. 338.

21 de outubro de 1969 (Código Penal Militar); o Decreto-Lei nº. 3.689, de 3 de outubro de 1941 (Código de Processo Penal); a Lei nº. 8.078, de 11 de setembro de 1990 (Código do Consumidor); a Lei nº. 9.296, de 24 de julho de 1996 (Lei de Interceptação Telefônica); e, por fim, a Lei nº. 10.446, de 8 de maio de 2002.

Em sua estrutura o Projeto Substitutivo[189] compõe-se de dezesseis artigos, dentre os quais podem-se destacar a tipificação das seguintes condutas:

Conduta delituosa	Sugestão do substitutivo ao Código Penal
Acesso indevido a dispositivo de comunicação	Art. 154-A. Acessar indevidamente, ou sem autorização, dispositivo de comunicação. Pena: reclusão, de 2 (dois) a 4 (quatro) anos, e multa. § 1º Nas mesmas penas incorre quem fornece a terceiro meio indevido ou não autorizado a dispositivo de comunicação ou sistema informatizado. ... § 3º A pena é aumentada de sexta parte, se o agente se vale de anonimato, de nome suposto ou da utilização de identidade de terceiros para a prática de divulgação.
Manipulação indevida de informação eletrônica	Art. 154-B. Manter consigo, transportar ou fornecer indevidamente ou sem autorização, dado ou informação obtida em dispositivo de comunicação ou sistema informatizado. Pena: detenção, de 2 (dois) a 4 (quatro) anos, e multa.
Divulgação de informações depositadas em banco de dados	Art. 154-D. Divulgar, ou tornar disponíveis, para finalidade daquela que motivou a estruturação do banco de dados, informações privadas, direta ou indiretamente, a dados econômicos de pessoas físicas ou jurídicas, ou a dados de pessoas físicas referentes a raça, opinião política, religiosa, crença, ideologia, saúde física ou mental, orientação sexual, registros policiais, assuntos familiares ou profissionais, além de outras de caráter sigiloso, salvo por decisão de autoridade competente, ou mediante expressa anuência da pessoa a que se refere, ou de seu representante legal. Pena: detenção, de 1 (um) a 2 (dois) anos, e multa. Parágrafo único. A pena é aumentada de sexta parte, se o agente se vale de anonimato, de nome suposto ou da utilização de identidade de terceiros para a prática de divulgação.
Deixar de manter dados e conexões realizadas	Art. 154-E. Deixar de manter, aquele que torna disponível o aceso a rede de computadores, os dados de conexões e comunicações realizadas por seus equipamentos, aptas a identificação do usuário, endereços eletrônicos de origem e destino no transporte dos registros de dados e informações, data e horário de início e término da conexão, incluindo protocolo de internet ou mecanismo de identificação equivalente, pelo prazo de cinco anos.

[189] O texto do projeto encontra-se no Anexo A.

	Pena: detenção, de 2 (dois) a 6 (seis) meses, e multa.
Permitir acesso por usuário não identificado e não autenticado	Art. 154-F. Permitir, aquele que torna disponível o acesso a rede de computadores, a usuário, sem a devida identificação e autenticação, qualquer tipo de acesso ou uso pela rede de computadores. Pena: detenção, de 1 (um) a 2 (dois) anos, e multa.
Dano por difusão de vírus eletrônico	Art. 163-A. Criar, inserir ou difundir vírus em dispositivo de comunicação ou sistema informatizado, com a finalidade de destruí-lo, inutilizá-lo ou dificultar-lhe o funcionamento. Pena: reclusão, de 1 (um) a 3 (três) anos, e multa. Parágrafo único. A pena é aumentada de sexta parte, se o agente se vale de anonimato, de nome suposto ou da utilização de identidade de terceiros para a prática de divulgação.
Atentado contra a segurança de serviço de utilidade pública	Art. 265. Atentar contra a segurança ou o funcionamento de serviço de água, luz, força, calor, informação ou telecomunicação, ou qualquer outro de utilidade pública.
Interrupção ou perturbação de serviço telegráfico ou telefônico	Art. 266. Interromper ou perturbar serviço telegráfico, radiotelegráfico, telefônico, telemático ou de telecomunicação, impedir ou dificultar-lhe o restabelecimento.
Difusão maliciosa de código	Art. 266-A. Difundir, por qualquer meio, programa, conjunto de instruções ou sistema informatizado com o propósito de induzir alguém a fornecer, espontaneamente e por qualquer meio, dados ou informações que facilitem ou permitam o acesso indevido ou sem autorização, a dispositivo de comunicação ou a sistema informatizado, ou a obtenção de qualquer vantagem ilícita. Pena: detenção, de 1 (um) a 2 (anos). Parágrafo único. A pena é aumentada de sexta parte, se o agente se vale de anonimato, de nome suposto ou da utilização de identidade de terceiros para a prática de divulgação.
Falsificação de telefone celular ou meio de acesso a sistema eletrônico	Art. 298-A. Criar ou copiar, indevidamente ou sem autorização, ou falsificar código; seqüência alfanumérica; cartão inteligente; transmissor ou receptor de rádio freqüência ou telefonia celular; ou qualquer instrumento que permita o acesso a dispositivo de comunicação ou sistema informatizado. Pena: reclusão, de 1 (um) a 5 (cinco) anos, e multa.

3.6.2 A regulação supranacional – A Convenção de Budapeste

Apesar do esforço do Estado brasileiro em buscar estabelecer uma regulamentação penal eficaz que coíba e puna os crimes eletrônicos através da edição de leis específicas que tipifiquem essas condutas, boa parte da doutrina, especialmente a estrangeira, entende que pelas características da criminalidade eletrônica, especialmente a ausência de barreiras espaciais, a reprimenda a essas condutas dificilmente será eficaz quando realizada isoladamente por um Estado.

> Desta forma, os últimos anos demonstram claramente a nova visão e característica da criminalidade mundial; uma criminalidade transnacional com interesses à superação dos limites territoriais, possibilidade cada vez mais tranqüila com o advento da internet, acarretando a desconstituição dos Estados Nações que impede ou dificulta a detecção, o processamento e a punição de tais crimes que integram esta macrocriminalidade. [...] Podem-se citar como exemplos de crimes da macrocriminalidade, os delitos informáticos, econômicos, tributários, ambientais, criminalidade no comércio exterior, contrabando internacional de armas, drogas, órgãos, entre outros, todos permeados por características comuns, sendo que as principais são: geralmente a ausência de vítimas individualizadas; pouca visibilidade dos danos causados; bens jurídicos supra-individuais, universais ou vagos; novo e específico modus operandi; ausência de violência física e muita organização.[190]

A disparidade entre as características do espaço criado pela rede mundial de computadores e as do Estado como instituição é ironizada por Liliana Minardi Paesani:

> A *internet* foi programada para funcionar e distribuir informações de forma ilimitada. Em contrapartida, as autoridades judiciárias estão presas às normas e instituições do Estado e, portanto, a uma Nação e a um território limitado. Configura-se o conflito e a dificuldade de aplicar controles judiciais na rede e surge o problema da aplicação de regras. [...] A rede é dotada de características absolutamente próprias e conflitantes: ao mesmo tempo em que se tornou um espaço livre, sem controle, sem limites geográficos e políticos, e, portanto, insubordinado a qualquer poder, revela-se como um emaranhado perverso, no qual se torna possível o risco de ser aprisionado por uma descontrolada elaboração eletrônica[191].

Ante as dificuldades à repressão dessas condutas por parte do Estado, que foram devidamente apresentadas no capítulo 2 do presente trabalho, ganhou força a idéia de regulação supranacional. Nesse escopo o Comitê Europeu para os Problemas Criminais (CDPC), fundamentado na deliberação CDPC/103/21196 de novembro de 1996, formou uma comissão de especialistas para realizar estudo aprofundado sobre as questões relacionadas à cibercriminalidade.

Após cinco anos de debates aprofundados, entre 1997 e 2000, o Comitê responsável pelo estudo realizou 10 sessões plenárias e 15 assembléias que culminara com a elaboração de um memorando explicativo e de um projeto de uma convenção que procurava regular os crimes eletrônicos.

Em junho de 2001, na 50ª Sessão plenária da CDPC, o projeto de convenção e seu memorando explicativo foram aprovados e encaminhados ao Comitê de Ministro da União Européia a fim de ser aberto o prazo para assinatura.

---

[190] FERREIRA, Érica Lorenço de Lima, op. cit., 2007. p.70.
[191] PAESANI, Liliana Minardi, op. cit., 2006. p.36-37.

Estruturalmente a Convenção é formada por quatro capítulos: o primeiro que trata do aspecto conceitual e terminológico; o segundo, que versa sobre as medidas políticas a serem empreendidas a nível interno pelos Estados pactuantes; o terceiro, que trata das condutas criminosas e das medidas processuais cabíveis e por último, o quarto que trata das disposições finais.[192]

A Convenção de Budapeste, ou a Convenção Européia de Cibercriminalidade, tem como objetivos principais a harmonização dos ordenamentos jurídicos penais dos países signatários no que tange à cibercriminalidade e áreas conexas, bem como uniformizar e fomentar o desenvolvimento nas ordens processuais penais estatais de mecanismos processuais eficazes à investigação e repressão do cibercrimes. Por último procura estabelecer um regime eficaz de cooperação internacional no que tange à prevenção e ao combate do cibercrime a nível internacional.

[192] O texto da convenção figura no Anexo B.

CONCLUSÃO

O desenvolvimento de novas tecnologias sempre influenciaram a sociedade, seja, em suas estruturas, seja em seus valores. Os avanços decorrentes da explosão tecnológica ocorrida na última metade do século XX modificaram completamente o contexto social mundial. Como conseqüência da adoção de valores econômicos e sociais pautados na importância da informação e a utilização de mecanismos tecnológicos na mediação dessas relações se organizou as bases da "Sociedade da Informação"

O processo de transformação social informacional moderno baliza-se por dois grandes paradigmas: o fenômeno globalizante; e a disseminação nas estruturas e práticas sociais de instrumentos tecnológicos relacionados à informação. As potencialidades oriundas do desenvolvimento desse modelo de organização social impactaram diretamente os modos de produção, as relações sociais, econômicas e culturais.

Essas modificações foram tão profundas que exigiram, na busca de proteger os interesses envolvidos, a regulamentação jurídica das novas relações econômicas, sociais e culturais surgidas com o advento da "Sociedade da Informação". Notadamente, o primeiro âmbito de influência normativa dessa nova situação fática foi na seara constitucional. A Constituição, enquanto elemento normativo-político estruturante e organizador do Estado assimilou os nuances da nova realidade social e principiou a tutelar em seu âmbito esse novo contexto.

Dessa forma, as ordens constitucionais modernas, dentre as quais se inclui a brasileira, procuram estabelecer um conjunto de regras mínimas que procurassem resguardar às novas relações surgidas do novo modelo de organização social, econômico e cultural. Assim, além de estabelecer normas asseguradoras ao direito de informação, entendido esse como um direito binário, ou seja, englobando o direito de se informar e de informar, o que inclui o

direito de se comunicar, a carta constitucional de 1988, de forma inovadora, em seu artigo 220, reconhece a liberdade informacional eletrônica, que significa a garantia que todo cidadão tem de utilizar qualquer meio para obter informações ou se comunicar, inclusive os oriundo das novas tecnologias: os meios eletrônicos.

Assim, a carta de 1988, reconheceu a necessidade de se conferir ao cidadão proteção contra os avanços da utilização dos meios eletrônicos informacionais em práticas que além de infringir direitos e garantias fundamentais como a intimidade e a privacidade, violavam de forma direta um dos pilares da ordem político-jurídica brasileira: a dignidade da pessoa humana, uma vez que a mediação tecnológica das relações econômicas, sociais e culturais, transformam o homem em um simples dado, relegando-se a segundo plano toda sua essência subjetiva.

Ao tutelar essas novas relações, a constituição reconhece o surgimento de novos bens jurídicos que precisavam ser protegidos a nível infraconstitucional. Dentre as novas concepções protetivas necessárias, destaca-se de forma evidente a necessidade de coibir as práticas criminosas surgidas com o advento do modo informacional de organização da sociedade.

As atividades decorrentes da utilização desvirtuada das tecnologias da informação começaram a colocar em risco a própria estrutura de organização social que estava surgindo. Em decorrência das fragilidades diagnosticadas nas estruturas de funcionamento dos meios eletrônicos utilizados para a mediação das relações econômicas e sociais a base de funcionamento da sociedade da informação ficou vulnerável à pratica de condutas lesivas aos novos bens e valores jurídicos nascidos com a sociedade da informação.

Dessa forma, a tutela penal dos interesses jurídicos oriundos das relações econômicas e sociais informacionais, fez-se extramente necessária, uma vez que a ausência de mecanismos jurídicos que coibissem, por meio do senso de prevenção, e punissem, através da aplicação de sanções mais densas, torna bastante instável a base de sustentação do novo modelo de organização social vigente.

A necessidade de regulamentação penal encontra duas grandes barreiras: uma de ordem normativa teórica; outra de natureza normativa prática. No primeiro caso, existe, por força dos

preceitos constitucionais estabelecidos no inciso XXXIX do artigo 5º da Constituição Federal, princípio da reserva legal, a necessidade de estabelecimento de normas penais incriminadoras específicas à realidade eletrônica, uma vez que a estrutura normativa penal não permite a utilização da interpretação analógica para a incriminação de condutas. Logo, amiúde a não existência de normas penais aplicáveis a matéria instala-se um verdadeiro "velho oeste eletrônico", onde a ausência e normas incriminadoras torna as condutas atípicas o que cria um ambiente sem lei. Em um segundo momento, mesmo que existam normas incriminadoras, as características dessas novas práticas criminosas, como a pluralidade de locais, ensejam óbices a aplicação das normas penais por parte do Estado. Normalmente os crimes praticados por meios eletrônicos são considerados "crimes à distância", o que significa que a ação se deu em um local (país) e o resultado em outro (país), e cuida de agentes criminosos de nacionalidade distinta do local onde a conduta foi consumada. Assim, mesmo que o fato seja típico e antijurídico, o Estado onde a conduta se concretizou terá enorme dificuldade em fazer valer o seu direito de punir o agente infrator, posto que somente em situações extremamente específicas, a norma local poderá ser aplicada de forma eficiente.

Assim, mesmo diante da existência de normas incriminadoras surge a possibilidade da conduta não ser punida ante a impossibilidade do Estado aplicar de forma concreta suas normas. A idéia de Estado soberano dessa forma sofre uma mitigação, pondo assim em risco a própria idéia de soberania. A construção do sistema repressivo nacional a condutas eletrônicas vincula-se necessariamente, como uma resposta a essa forma de criminalidade globalizada, a construção de uma rede de colaboração internacional.

Logo, por mais que no contexto atual da ordem jurídica brasileira seja evidente a necessidade de implementação de diploma normativo incriminador, para de modo primário inibir e reprimir as práticas delitivas eletrônicas, tais como a aprovação do Projeto de Lei Substitutivo de autoria do Senador Luiz Azeredo, deve-se sobre maneira, estruturar-se uma rede mundial de combate a criminalidade eletrônica baseada em pactos internacionais que além de estabelecerem condutas típicas comuns, possam firmar mecanismos jurídicos de colaboração entre os Estados para efetivar de forma concreta a punição dos infratores.

A interação entre globalização e tecnologia gerou modificações drásticas na sociedade. A busca por novos modelos de organização econômica alterou de forma significativa os instrumentos sociais e culturais que moldavam as estruturas organizativas da sociedade. Essa

reorganização trouxe consigo um conjunto de aspectos antagônicos. De um lado produziu avanços que facilitaram inúmeras atividades humanas, tornando mais simples e eficientes atividades antes consideradas complexas. De outro lado, o desvirtuamento da utilização dessas novas tecnologias ocasionou o surgimento de inúmeras condutas lesivas aos bens jurídicos oriundos da recontextualização da sociedade. A inércia estatal na busca de prevenir e reprimir essas condutas lesivas, pode de forma concreta colocar em risco os elementos fundadores de uma nova era.

Dessa forma, figura-se indispensável a organização de mecanismos de cooperação internacional para a estruturação de um sistema de proteção aos bens e valores jurídicos inseridos na ordem constitucional brasileira oriundos ou influenciados pela reorganização social informacional.

REFERÊNCIAS

ABOSO, Gustavo Eduardo; ZAPATA, María Florencia. **Cibercriminalidae y derecho penal.** Buenos Aires: B de F, 2006.

AGUIAR, Eduardo Henrique de Almeida. Da soberania do estado brasileiro frente a OMC. In: GUERRA**,** Sidney; SILVA, Roberto Luis (Org.). **Soberania** – Antigos e novos paradigmas. Rio de Janeiro: Freitas Bastos, 2004.

ALMEIDA FILHO, José Carlos. **Processo eletrônico e teoria geral do processo eletrônico:** a informatização judicial no Brasil. Rio de Janeiro: Forense, 2007.

_____; CASTRO**,** Aldemário Araújo. **Manual de informática jurídica e Direito da informática**. Rio de Janeiro: Forense, 2005.

ANDRADE, Vander Ferreira de. Crimes de informática. **Revista da Faculdade de Direito de Guarulhos**, São Paulo, v.3, p. 281-293, jul/dez. 2001.

ARANHA FILHO, Adalberto José Q. T. de Camargo. Crimes na internet e a legislação vigente. **Revista Literária de Direito**, São Paulo, v.9, n.44, p. 23-25, out./dez. 2002.

ARAS, Vladimir. Crimes de Informática: Uma nova criminalidade. **Jus Navigandi**, Ed. 12, out. 2001. Disponível em: < http://www1.jus.com.br/doutrina/texto.asp?id=2250 >. Acesso em: 25 fev. 2008.

ARISTÓTELES. **A política.** Tradução de Nestor Silveira Chaves. Rio de Janeiro: Ediouro, [s.d.].

AZEREDO, Eduardo. A tipificação de crimes na internet. **Ciência Jurídica**, Belo Horizonte, v.20, n.132, p.336-358, nov./dez. 2006. p. 338.

BRETON**,** Philippe. **História da informática**. Tradução de Elcio Fernandes. São Paulo: Universidade Estadual Paulista, 1991.

BENAKOUCHE, Rabah (Org.). **A informática e o Brasil**. São Paulo: Polis, 1985.

BASSO, Maristela; ALMEIDA, Guilherme A. É preciso difundir mentalidade digital nas empresas. In: KAMINSKI**,** Omar. (Org.). **Internet legal –** O Direito na tecnologia da informação: Doutrina e jurisprudência. Curitiba: Júrua, 2007.

BENEYTO, Juan. **Informação e sociedade:** os mecanismos sociais da atividade informática. Petrópolis: Vozes, 1997.

BITTENCOURT, Cezar Roberto. **Tratado de Direito Penal –** Parte geral. 10. ed. São Paulo: Saraiva, 2006. v.1.

BOBBIO, Norberto. **A era dos direitos**. Tradução de Carlos Nelson Coutinho. 10. ed. Rio de Janeiro: Campus, 1992.

BONAVIDES, Paulo. **Curso de direito constituciona**l. 6. ed. Rio de Janeiro: Forense, 1996.

BRANCO, Paulo Gustavo Gonet. **Hermenêutica constitucional e direitos fundamentais**. Brasília: Brasília Jurídica, 2002.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. 28. ed. São Paulo: Saraiva, 2008.

_____. **Decreto – l ei 2.848**, de 7 de dezembro de 1940. **Código Penal brasileiro**. 46. ed. São Paulo: Saraiva, 2008.

_____. **Lei 8.137**, de 27 de dezembro de 1990. Define crimes contra a ordem tributária, econômica e contra as relações de consumo, e dá outras providências. Disponível em:< http://www.senado.gov.br>. Acesso em: 10. fev. 2008.

_____. **Lei 9.296**, de 24 de julho de 1996. Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal. Disponível em: <http://www.senado.gov.br>. Acesso em: 10. fev. 2008.

_____. L**ei 9.504**, de 30 de setembro de 1997. Estabelece normas para as eleições. Disponível em: <http://www.senado.gov.br>. Acesso em: 11 fev. 2008.

_____. **Lei 9.983**, de 14 de julho de 2000. Altera o Decreto-lei n.º 2.848, de 7 de dezembro de 1940 - Código Penal e dá outras providências. Disponível em: <http://www.senado.gov.br>. Acesso em: 12 fev. 2008.

BRASIL, Angela Bittencourt. **Informática jurídica**: O ciber direito. Rio de Janeiro: Juris Doctor, 2000.

BLUM, Renato Opice (Coord). **Direito Eletrônico** – A Internet e os Tribunais. São Paulo: Edipro, 2001.

CALHEIROS, Renan. Uma legislação contra os crimes de informática. **Consulex**, Brasília, v. 10, n. 233, p. 19, abr. 2006.

CASACUBERTA, David; MARTÍNS MÁS, José Luis. **Diccionario de ciberderechos.** Disponível em: <http://www.kriptopolis.com/dicc.html>. Acesso em: 5 jan. 2000.

CAPEZ, Fernando. **Curso de direito penal**. 9. ed. rev. e atual. São Paulo: Saraiva, 2005. v. 1.

CASTELLS**,** Manuel. **A sociedade em rede – A era da informação**: economia, sociedade e cultura. Tradução de Roneide Venâncio Majer. São Paulo: Paz e Terra, 1999. v.1.
_____. **O poder da identidade – A era da informação**: economia, sociedade e cultura. Tradução de Roneide Venâncio Majer . 3ed. São Paulo: Paz e Terra, 2001. v.2.

CASTRO, Carla Rodrigues Araújo de. **Crimes de informática e seus aspectos processuais.** 2. ed. Rio de Janeiro: Lúmen Juris, 2003.

CARVALHO, Ademir. **Centro de informações:** a descentralização da informática. São Paulo: Érica, 1991.

CONCERINO, Arthur José. Internet e segurança são compatíveis? In: LUCCA, Newton de; SIMÃO FILHO, Adalberto (Coord.). **Direito e Internet:** aspectos jurídicos relevantes. Bauru: Edipro, 2000.

COSTA, Marcelo Antônio Sampaio Costa. **Computação forense**. Campinas: Millennium, 2003.

COSTA, Marco Aurélio Rodrigues da. Crimes de Informática. **Jus Navigandi**. Disponível em: < http:// www1. Jus.com.br/doutrina/texto.asp?id=1826>. Acesso em: 20 jan. 2007.

COSTA, Álvaro Mayrink da. **Direito Penal –** parte geral. Rio de Janeiro: Forense, 1982.

CUNHA JÚNIOR**,** Eurípede Brito. Os Contratos eletrônicos e o novo Código Civil. **Revista do Centro de Estudos Judiciários - CEJ**, Brasília, n. 19, p.62-77, out./dez, 2002.

DALLARI, Dalmo de Abreu. **Elemento de teoria geral do Estado**. 19. ed. São Paulo: Saraiva, 1995.

DELPUPO**,** Poliana Moreira. O consumo na Internet e a responsabilidade civil do provedor. In: ROVER**,** Aires José (Org.). **Direito e informática**. Barueri: Manoele, 2004.

DUPAS, Gilberto. **Ética e poder na sociedade da informação –** De como a autonomia das novas tecnologias obriga a rever o mito do progresso. São Paulo: UNESP, 2000.

DAOUN, Alexandre Jean. Crimes informáticos. In: BLUM, Renato Opice (Coord.). **Direito eletrônico**.São Paulo: Edipro, 2001.

_____; BLUM, Renato. Cibercrimes. In: LUCCA, Newton; SIMÃO FILHO, Adalberto (Coord.). **Direito e Internet –** Aspectos jurídicos relevantes. São Paulo: Edipro, 2000.

ELIAS, Paulo Sá. A questão da reserva legal no Direito Penal e as condutas lesivas na área da informática e da tecnologia. **Jus Navigandi**, Ed. 12, out. 2001. Disponível em: < http://www1.jus.com.br/doutrina/texto.asp?id=2038 >. Acesso em: 23 out. 2007.

FERREIRA, Ivette Senise. Os crimes da informática. In: BARRA, Rubens Prestes; ANDREUCCI, Ricardo Antunes (Coord.) **Estudos Jurídicos**. São Paulo: RT, 1992.

_____. A criminalidade informática. In: LUCCA, Newton; SIMÃO FILHO, Adalberto (Coord.). **Direito e Internet –** Aspectos jurídicos relevantes. São Paulo: Edipro, 2000.

FERREIRA, Aluízio. **Direito à informação, direito à comunicação:** direitos fundamentais na constituição brasileira. São Paulo: Celso Bastos editor, 1997.

FERREIRA, Érica Lorenço de Lima. **Internet –** Macrocriminalidade e jurisdição internacional. Curitiba: Júrua, 2007.

FERNANDES**,** Ângela Silva et al. Tecnologia e comunicação. In: Antônio Miranda; Elmira Simeão (Org.). **Informação e Tecnologia**: Conceitos e recortes. Brasília: Universidade de Brasília, Departamento de Ciência da Informação e Documentação, 2005.

FRAGOSO, Heleno Cláudio. **Lições de direito penal**. 4. ed. Rio de Janeiro: Forense, 1995.

FURLANETO NETO, Mário; GUIMARÃES, José Augusto Chaves. Crimes na internet: elementos para uma reflexão sobre a ética informacional. **Centro de Estudos Judiciários: CEJ**, Brasília, v.7, n. 20, p. 67-73, mar. 2003.

GATES, Bill. **A estrada do futuro.** Tradução de Beth Vieira et al. São Paulo: Companhia das Letras, 1995.

HELLER, Hermann. **Teoria del Estado**. Argentina: Fondo de Cultura Económica, 1992.

HESPANHA, Benedito. O poder normativo da internet e a regulamentação dos crimes virtuais: uma análise crítica à legislação penal brasileira. **Justiça do Direito**, Rio Grande do Sul, v. 1, n. 16, p.29-64, 2002.

JESUS, Damásio Evangelista de. **Direito penal.** São Paulo: Saraiva, 2005. v.1.

KAMINSKI**,** Omar. Aspectos jurídicos que envolvem a rede das redes. In: _____ (Org.). **Internet legal –** O Direito na tecnologia da informação: Doutrina e jurisprudência. Curitiba: Júrua, 2007.

KANT, Immanuel. **Crítica da razão prática.** Tradução de Rodolfo Schaefer. São Paulo: Martin Claret, 2006.

KELSEN, Hans. **Teoria geral do direito e do Estado**. 2. ed. São Paulo: Martins Fontes, 1995.

_____. **Teoria pura do direito**. 6. ed. São Paulo: Martins Fontes, 2003.

LIMBERGER, Têmis. Direito e informática: os desafios de proteger os direitos do cidadão. In: SARLET, Ingo Wolfgang (Org.). **Direitos fundamentais, informática e comunicação e algumas aproximações**. Porto Alegre: Livraria do Advogado, 2007.

LOPES, Ana Maria D´Ávila. **Direitos fundamentais como limites ao poder de legislar**. Porto Alegre: Sergio Antonio Fabris Júnior editor, 2001.

LUPI**,** André Lipp Basto**.** Soberania e direito internacional público. In: GUERRA, Sidney; SILVA, Roberto Luis (Org.). **Soberania** – Antigos e novos paradigmas. Rio de Janeiro: Freitas Bastos, 2004.

MARQUES, José Frederico. **Curso de direito penal.** São Paulo: Saraiva, 1954. v.1.

_____. **Tratado de Direito Penal**. São Paulo: Bookseller, 1997. v.2.

MATIAS**,** Eduardo Felipe P. **A humanidade e suas fronteiras** – do Estado soberano à sociedade global. São Paulo: Paz e Terra, 2005.

MATTELART**,** Armand. **História da sociedade da informação**. Tradução de Nicolas Nyimi Campanário. São Paulo: Loyola, 2002.

MELO, Aline Mary M. de. **Os crimes de Informática**. Suas formas de punição e o Direito. Manaus: Instituo Luterano de Ensino Superior, 2000. 38p. Monografia.

MILAGRE, José Antonio. Riscos do uso inadequado dos recursos de TI: tele-trabalho e boas práticas de direito digital.**Imasters**, Espírito Santo. a.1, p. 58-65, jul. 2007. p. 62.

MIRABETE, Julio Fabrini. **Manual de direito penal**. 23. ed. rev. e atual. São Paulo: Atlas, 2006.

MORAES, Alexandre de. **Constituição do Brasil interpretada**. 6. ed. São Paulo: Atlas, 2006.

MORIN, Edgard. **Os sete saberes necessários à educação do futuro**. Tradução de Catarina Eleonora F. da Silva. 11. ed. São Paulo: Cortez, 2006.

NORONHA, Edgar de Magalhães. **Direito penal.** 20. ed. São Paulo: Saraiva, 1982.

PAESANI, Liliane. **Direito de informática.** 3. ed. São Paulo: Atlas, 2006.

PINTO, Agerson Tabosa. **Teoria geral do Estado.** Fortaleza: Imprensa Universitária - UFC, 2002.

PRETTO, Nelson; BONILLA, Maria Helena. **Sociedade da informação:** democratizar o quê? Salvador. Disponível em: <http://www.faced.ufba.br/not/83.htm>. Acesso em: 11 out. 2007.

PINHEIRO, Reginaldo Cesár. Os Cybercrimes na esfera jurídica brasileira. **Jus Navigandi**, set., 2001. Disponível em: <http://www.jus.com.br/doutrina/cybercri.html >. Acesso em: 25 out. 2005.

REALE, Miguel. **Lições preliminares de direito.** 25. ed. São Paulo: Saraiva, 2001.

REINALDO FILHO, Demócrito. **Direito da informática**: temas polêmicos. Bauru: Edipro, 2002.

REIS, Maria Helena Junqueira Reis. **Computer crimes –** A Criminalidade na Era dos Computadores. Belo Horizonte, Del Rey, 1997.

RODRIGUES, Silvio. **Direito civil.** 32. ed. São Paulo: Saraiva, 2001. v. 1.

ROHRMANN, Carlos Alberto. **Curso de direito virtual**. Belo Horizonte: Del Rey, 2005.

ROSA, Fabrízio. **Crimes de informática**. Campinas, Bookseller, 2005.

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

_____. **Informática, telemática e Direito Penal**. São Paulo:Memória Jurídica, 2004.

ROVER, Aires José (Org). **Direito, sociedade e informática** – Limites e perspectivas da vida digital. Florianópolis, Fundação Boiteux, 2000.

_____ (Org.). **Direito e informática**. Barueri: Manoele, 2004.

SANTOS, José Luiz dos. **O que é cultura.** 14. ed. São Paulo: Brasiliense, 1994.

SARLET, Ingo Wolfgang (Org.). **Direitos fundamentais, informática e comunicação e algumas aproximações.** Porto Alegre: Livraria do Advogado, 2007.

_____. **Eficácia dos diretos fundamentais**. Porto Alegre: Livraria do Advogado, 2004.

SCHAFF, Adam. **A sociedade informática.** Tradução de Carlos Eduardo Jordão Machado e Luís Arturo Obojes. 4. ed. São Paulo: UNESP, 1995.

SILVA, Alberto Franco. **Código Penal e sua interpretação jurisprudencial.** 5. ed. São Paulo: Revista dos Tribunais, 1995.

SILVA, José Afonso da. **Curso de direito constitucional positivo.** 21. ed. São Paulo: Malheiros, 2002.

SILVA, Rita de Cássia Lopes. **Direito penal e sistema informático**. São Paulo: Revista dos Tribunais, 2003

SORIANO, Aldir Guedes**.** Soberania e o direito à liberdade religiosa. In: GUERRA**,** Sidney; SILVA, Roberto Luis (Org.). **Soberania** – Antigos e novos paradigmas. Rio de Janeiro: Freitas Bastos, 2004.

TELES, Ney Moura. **Direito Penal.** 2. ed. São Paulo: Atlas, 2006.

VIANNA, Túlio Lima. **Fundamentos de Direito Penal informático**: do acesso não autorizado a sistemas computacionais. Rio de Janeiro: Forense, 2003.

_____. Hackers: um estudo criminológico da subcultura cyberpunk. **Jus Navegandi**. Disponível em: <http://www.jus.com.br>. Acesso em: 10 fev.2003.

VICENTINO, Cláudio. **História geral.** 8. ed. São Paulo: Scipione, 1997.

VEIGA**,** Luiz Adolfo Olsen da; ROVER**,** Aires José. Dados e informações na internet: é legítimo o uso de robôs para a formação de base de dados de clientes? In: ROVER**,** Aires José (Org.). **Direito e informática**. Barueri: Manoele, 2004.

VERZELLO, Robert; REUTTER III, John. **Processamento de dados:** sistemas e conceitos. Tradução de Regina Szwarcfiter. São Paulo: McGraw-Hill, 1984.

WARNIER, Jean Pierre. **A mundialização da cultura.** Tradução de Viviane Ribeiro. São Paulo: EDUSC, 2003.

WIERNER, Norbert. **Cibernética e sociedade** – O uso humano de seres humanos. São Paulo: Cultrix, 1950

ZANDONADI, Viviane. Na cola dos crackers. **Info Exame**, São Paulo, v. 19, n. 221, p. 66-67, ago. 2004.

GLOSSÁRIO*

Hardware – Configura-se como a parte física do equipamento. São as partes eletrônicas e mecânicas de um computador, seja de forma individualizada, seja em conjunto. São exemplos de Hardware o teclado, o mouse, o monitor, o disco rígido;

Software ou Programa de Computador – "É a expressão de um conjunto organizado de instruções em linguagem natural ou codificada, contido em suporte físico de qualquer natureza, de emprego necessário em máquinas automáticas de tratamento da informação, dispositivos, instrumentos ou equipamentos periféricos (...) para fazê-los funcionar de modo e para fins determinados".[193]

Disco Rígido ou Disco Fixo – Consiste em um disco magnético de metal (bronze), que serve como suporte físico para os dados/informações gravados de forma serial na superfície do disco por meio de pontos magnetizados. É no disco rígido onde são armazenados os dados ou as informações para que posteriormente possam ser utilizadas, alteradas ou até mesmo apagadas.

Mouse – Trata-se de dispositivo fundamental em ambientes gráficos (como o Windows), por propiciar a movimentação nas janelas e a substituição de comando antes executas por intermédio do teclado.

Processador – Compõe-se de um circuito integrado de silício onde são colocados milhares ou milhões de transistores ligados aos componentes externos por finos fios de alumínio. Normalmente, o processador possui duas partes principais: a) a unidade lógico-aritmética e b) a unidade de controle. A primeira, como a denominação indica, executa as operações matemáticas e os comandos do computador. A segunda, controla o ciclo da máquina.

Memória – Dispositivo responsável pelo armazenamento de dados e informações. Os microcomputadores possuem dois tipos de memória para tal fim. A memória ROM (Read Only Memory) e a memória RAM (Random Access Memory). A primeira, somente de leitura, não é modificada com o desligamento da máquina e tem como função primordial ser usada nas rotinas de inicialização do computador (boot). A memória RAM é vinculada tanto a leitura quanto a gravação, fazendo parte da memória principal.

Dado – O significado do termo dado varia de acordo com a acepção que o mesmo é utilizado. Dentro da informática pode possuir uma acepção singela como sendo o elemento basilar da informação. Pode ainda se configurar como uma representação de fatos ou assume ainda o

---

* O presente glossário foi construído utilizando-se informações da Lei 9.609/98; REIS, Maria Helena Junqueira. **Computer Crimes.** Belo Horizonte: Del Rey, 1997; e ALMEIDA FILHO, José Carlos & CASTRO, Aldemário Araújo. **Manual de informática jurídica e direito da informática**. Rio de Janeiro: Forense, 2005.

caráter de instruções, em formas apropriadas para o armazenamento processamento ou transmissão por meios automáticos. Assim um dado pode ser entendido como um fragmento de uma informação ou como algo capaz de trazer uma informação. Além disso, o dado pode revestir-se sob a forma de uma informação de cunho numérico possuidora de formato que permite a cognição, o processamento, o armazenamento ou a transmissão da mesma por um sistema informático.

Informação – Partindo-se de uma abordagem mais ampla que engloba o conhecimento sob algo, temos que é por meio da informação que se adquire conhecimento. De forma genérica pode-se definir uma informação como um conjunto de dados que integra um corpo de conhecimento qualquer. Quando se analisa a informação sob a ótica da informática, verifica-se que qualquer dado, quer seja como instrução, quer como registro, é considerado uma informação.

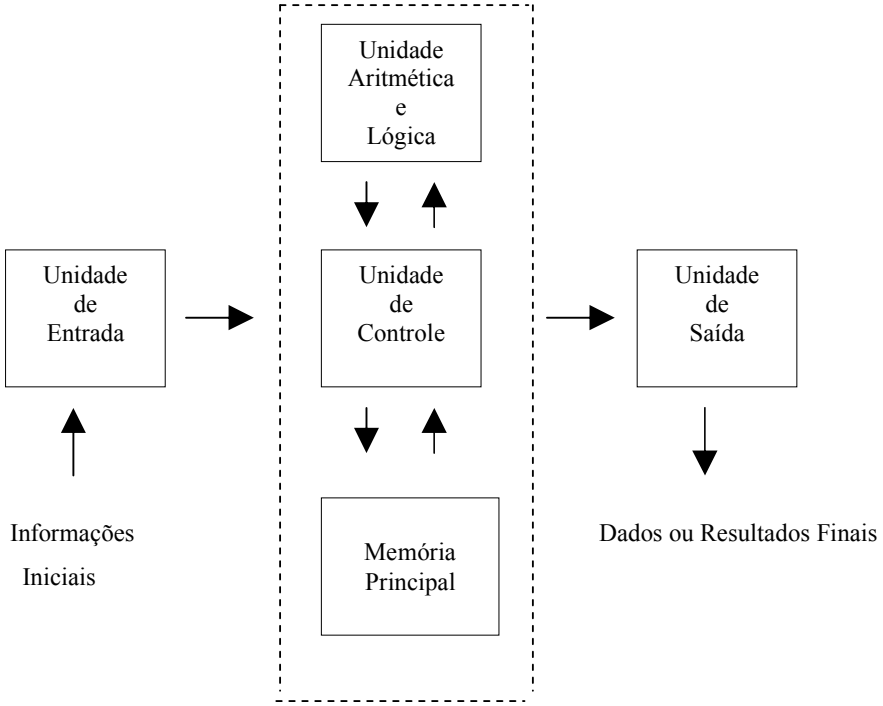
Processamento de Dados – Todo homem, voluntariamente ou sem percepção à cerca do fato, realiza o que conceitua-se processamento de dados, pois os dados compõem a estrutura das informações e no cotidiano humano tem-se contato com os mais diversos dados/informações como sons, cheiros, imagens, textos, etc. O processamento de dados. pode assumir as mais diversas formas e manusear os mais diversos tipos de instrumentos ou ferramentas auxiliares. Assim, podemos falar em processamento: a) não mecânico ou manual (utilizando sinais e gestos); b) mecânico (com a presença de engrenagens e mecanismos) e c) eletrônico (relacionado com circuitos eletrônicos compostos por elementos específicos, tais como transistores, resistores e capacitores, responsáveis pela execução das tarefas solicitadas).Para se chegar ao resultado da mais singela expressão matemática como:

$$3 \times 3 = 9$$

Utiliza-se um processo onde os dados foram captados. No processamento computacional os dados devem ser inseridos na máquina através de uma Unidade de Entrada, o teclado. Nos homens a unidade de entrada corresponde aos cinco sentidos responsáveis pela percepção sensorial por meio dos quais recebesse dados para processamento, no exemplo acima citado a Unidade de Entrada dos dados são os olhos. A Unidade de Entrada é o meio de inserção dos dados aptos a processamento em um sistema computacional e pode ser efetivada pelo teclado, por um disco flexível ou outro meio apto a fornecer dados ao sistema.No exemplo da equação matemática a Unidade de Entrada humana são os olhos, ao se retirar a figura 1 do campo sensorial visual, pode-se claramente dizer seu conteúdo, pois os dados inseridos foram transferidos para o cérebro e armazenados na memória, sendo memorizados. Esse mesmo procedimento ocorre no processamento de dados em um computador. A Unidade de Entrada capta os dados, sob suas mais diversas formas, e através do sistema binário transforma-os em códigos aptos ao processamento que a máquina armazena em sua memória. Codificados de forma a serem processados os dados/informações são armazenados na Memória. O homem para efetuar os cálculos necessários a resolução da equação utiliza tabuadas, o que corresponde a Unidade Aritmética. É nesta unidade onde são efetuadas as operações necessárias a solução da equação. No homem tais operações ocorrem no cérebro, no computador são realizadas em circuitos elétricos específicos por meio de impulsos elétricos. Efetivados os cálculos pela Unidade Aritmética os resultados são remetidos a Memória. Contudo os resultados estão expressos em linguagem binária, ininteligível aos seres humanos. Nesse momento a Unidade Lógica entra em ação e converte o resultado para um meio pré determinado que torne capaz a sua percepção pelo homem. A Unidade Lógica equiparasse aos neurônios humanos que controlam e decodificam os impulsos elétricos cerebrais. Após realizadas as operações procedimentais para obtenção do resultado do processamento dos

dados, estes precisam ser externados. No homem isto ocorre, por exemplo, por meio da fala da escrita, do desenho e etc. É o que se chama de Unidade de Saída, porque ela é responsável pela saída dos dados/informações processados de forma que possam ser captados e entendidos, no computador as Unidades de Saída principais são a tela de vídeo e a impressora. No transcorrer de todo o processamento existiu uma coordenação dos procedimentos integrantes do processo. Assim como no ser humano, o computador possui uma Unidade de Controle que é responsável pela manutenção da ordem correta e coerente dos procedimentos. É a unidade de controle que efetiva a execução das etapas do processo indicando o momento adequado para a prática de determinado ato regulando todo o processo de acordo com parâmetros pré definidos contido no programa utilizado no processamento. Assim se verifica que a operação de processamento de dados nada mais é que a transformação de dados ou informações iniciais recebidas, em resultados desejados, com a utilização de procedimentos predefinidos, tais procedimentos são conhecidos como programas, anteriormente já definidos.

Esquema ilustrativo:



ANEXO A

PARECER Nº , DE 2006

Da COMISSÃO DE EDUCAÇÃO, sobre o Projeto de Lei da Câmara nº 89, de 2003, e Projetos de Lei do Senado nº 137, de 2000, e nº 76, de 2000, todos referentes a crimes na área de informática. RELATOR: Senador **EDUARDO AZEREDO**

I – RELATÓRIO

Chegam a esta Comissão, para parecer, o Projeto de Lei da Câmara (PLC) n° 89, de 2003 (n° 84, de 1999, na origem), e os Projetos de Lei do Senado (PLS) n° 137, de 2000, e n° 76, de 2000, todos referentes a crimes na área de informática. Tramitam em conjunto, em atendimento ao Requerimento n° 847, de 2005, do Senador Renan Calheiros. Em decorrência do Requerimento n° 848, de 2005, foi extinta a urgência na tramitação do PLC n° 89, de 2005, que havia sido declarada em decorrência da aprovação do Requerimento n° 599, de 2005, de autoria da Senadora Ideli Salvatti. Os projetos de lei do Senado perdem o caráter terminativo nas comissões.

O PLS n° 137, de 2000, de autoria do Senador Leomar Quintanilha, consiste em apenas um artigo, além da cláusula de vigência, e visa a aumentar em até o triplo as penas previstas para os crimes contra a pessoa, o patrimônio, a propriedade imaterial ou intelectual, os costumes, e a criança e o adolescente na hipótese de tais crimes serem cometidos por meio da utilização da tecnologia de informação e telecomunicações.

O PLS n° 76, de 2000, de autoria do Senador Renan Calheiros, apresenta tipificação de delitos cometidos com o uso de computadores, e lhes atribui as respectivas penas, sem entretanto alterar o Código Penal. Classifica os crimes cibernéticos em sete categorias: contra a inviolabilidade de dados e sua comunicação; contra a propriedade e o patrimônio; contra a honra e a vida privada; contra a vida e a integridade física das pessoas; contra o patrimônio fiscal; contra a moral pública e opção sexual, e contra a segurança nacional. Tramitou em conjunto com o PLS n° 137, de 2000, por força da aprovação do Requerimento n° 466, de 2000, de autoria do Senador Roberto Freire, por versarem sobre a mesma matéria.

O PLC n° 89, de 2003, de iniciativa do Deputado Luiz Piauhylino, altera o Decreto-Lei n° 2.848, de 7 de dezembro de 1941 (Código Penal), e a Lei n° 9.296, de 24 de julho de 1996, e dá outras providências. Resulta do trabalho do grupo de juristas que aperfeiçoou o PLC n° 1.713, de 1996, de autoria do Deputado Cássio Cunha Lima, arquivado em decorrência do término da legislatura. As alterações propostas visam a criar os seguintes tipos penais, cometidos contra sistemas de computador ou por meio de computador: acesso indevido a

meio eletrônico (art. 154-A); manipulação indevida de informação eletrônica (art. 154-B); pornografia infantil (art. 218-A); difusão de vírus eletrônico (art. 163, § 3°); e falsificação de telefone celular ou meio de acesso a sistema informático (art. 298-A).

Além dessas modificações, o referido projeto acrescenta o termo *telecomunicação* ao tipo penal de atentado contra a segurança de serviço de utilidade pública (art. 265) e ao de interrupção ou perturbação de serviço telegráfico ou telefônico (art. 266), estende a definição de dano do art. 163 para incluir elementos de informática, equipara o cartão de crédito a documento particular no tipo de falsificação de documento particular (art. 298), define meio eletrônico e sistema informatizado, para efeitos penais (art. 154-C), e permite a interceptação do fluxo de comunicações em sistema de informática ou telemática, mesmo para crimes punidos apenas com detenção (art. 2°, § 2°, da Lei n° 9.296, de 24 de julho de 1996). Tendo estado à disposição dos senhores Senadores, o PLC n° 89, de 2003 não recebeu emendas.

II – ANÁLISE

Muitas são as proposições legislativas já produzidas e debatidas no Congresso Nacional a respeito do tema da criminalidade nas áreas da informática, das telecomunicações e da Internet, a rede mundial de computadores. A evolução das tecnologias relacionadas à produção, ao processamento, ao armazenamento e à difusão da informação tem ocorrido com muita velocidade, gerando lacunas no ordenamento jurídico vigente.

A existência dessas lacunas tem motivado a proliferação de casos de fraudes e de danos ao patrimônio e danos morais de agentes públicos e privados. Estima-se que bilhões de reais já foram desviados de contas bancárias de pessoas físicas ou jurídicas em decorrência da atuação indevida de especialistas da área. Além disso, a violação de bases de dados mantidas em meio eletrônico tem provocado danos de grande monta pelo roubo de informações pessoais. Não bastasse isso, há evidências de ligação entre o cibercrime e o financiamento do terrorismo internacional, e o crescimento do tráfico de seres humanos e de drogas. E 2004 foi apontado como o ano em que os crimes cibernéticos passaram a gerar lucros superiores aos do tráfico de drogas. De acordo com pesquisa realizada pela firma de consultoria americana *Computer Economics*, em 2004 as perdas totais chegam a 18 bilhões de dólares, com uma taxa de crescimento anual próxima de 35%.

A sociedade clama por medidas eficazes no combate ao crime cibernético. Não é mais possível que divergências hermenêuticas acerca da possível aplicabilidade das nossas normas jurídicas a esse tipo de conduta continuem a impedir a punição de condutas extremamente nocivas ao País. A imprensa nacional destaca recentemente que alguns internautas já começam a fazer denúncias contra usuários pedófilos ou terroristas do sítio *Orkut*, denunciando-os ao provedor. O *Orkut*, um serviço da multinacional americana *Google*, imediatamente retira aqueles usuários do sistema mas não consegue detectar e impedir a sua reinclusão, face á liberalidade, inerente à rede mundial de computadores.

Estabelece-se assim o círculo da denúncia e da punição responsável. Esse círculo, entretanto, tem como resposta novo círculo vicioso com o reinício dos delitos por novos usuários não identificados, tudo isto sem que se perceba um fim próximo.

O teor do PLS nº. 137, de 2000, reflete preocupação idêntica àquela que conduziu o legislador na formulação dos dois outros projetos que acompanha, qual seja: a de disciplinar as condutas perniciosas que utilizem ou danifiquem sistemas de computador. Não obstante, é de abrangência e precisão mais restrita que aqueles, que o englobam integralmente.

O projeto limita-se a estabelecer que os crimes contra a pessoa, o patrimônio, a propriedade imaterial e intelectual, os costumes, bem como contra a criança e o adolescente, cometidos com a utilização de meios de tecnologia de informação e telecomunicações, terão suas penas triplicadas. Ou seja, a pena seria agravada em razão do meio utilizado pelo agente para perpetrar o crime.

A alteração legislativa proposta pelo PLS nº. 137, de 2000, não é conveniente por duas razões. Em primeiro lugar, tornaria superlativo o desvalor do meio utilizado pelo agente, que prevaleceria tanto sobre o desvalor do resultado quanto sobre o desvalor da intenção (genericamente considerada) – aquele, inspirador da teoria clássica da ação; este, da teoria finalista da ação, ambas adotadas de forma alternada pelo Código Penal a partir da reforma da sua Parte Geral, empreendida pela Lei nº. 7.209, de 11 de julho de 1984. A segunda razão, que decorre da anterior, é a desproporcionalidade na aplicação das penas, haja vista que um delito menos grave poderia ser apenado mais severamente do que outro mais reprovável, apenas por ter sido cometido por meio da Internet.

O PLC nº. 89, de 2003, pretende inserir a Seção V no Capítulo VI do Título I do Código Penal, onde seriam definidos os crimes contra a inviolabilidade dos sistemas informatizados. São nove as condutas delituosas por meio de acesso a sistema eletrônico de que trata o PLC:

- o acesso indevido a meio eletrônico;

- a manipulação indevida de informação eletrônica;

- o dano eletrônico;

- a pornografia infantil;

- o atentado contra a segurança de serviço de utilidade pública;

- a interrupção ou perturbação de serviço telegráfico e telefônico;

- a falsificação de cartão de crédito;

- a falsificação de telefone celular;

- a divulgação de informações pessoais ou de empresas.

Vejamos cada um desses tipos.

a) Arts. 154-A, 154-B e 154-C do CP, ou seja, o acesso indevido, a manipulação indevida de informação e a definição de meio eletrônico e sistema informatizado.

A redação pode ser aperfeiçoada para registrar que o meio eletrônico ou sistema informatizado é protegido contra as hipóteses em que o agente consegue o acesso mediante a violação desse sistema de proteção. Já a pena, que seria aplicada ao *hacker*, nome dado ao usuário que tenta violar ou viola o sistema de proteção, deveria ser mais severa.

Ademais, embora os três artigos possam ser reunidos em um só, preferimos manter a redação dada pelo PLC nº. 89 de 2003, que define com maior clareza os delitos que se

pretende tipificar. Entretanto propomos a alteração da pena original de detenção de 3 (três) meses a 1 (um) ano, e multa para detenção, de 1 (um) a 4 (quatro) anos, e multa, mantendo os mesmos parágrafos.

Ainda, quando este PLC nº. 89 de 2003 estava sendo relatado nesta Comissão, o atento Senador Hélio Costa fez algumas sugestões de emendas que os membros da Comissão entenderam necessárias, mas que deveriam fazer parte de um novo Projeto de Lei a fim de que aquele projeto em discussão, uma vez aprovado, pudesse ir à sanção presidencial. Estando ele apensado ao PLS nº. 76 de 2000 entendemos que é hora de acatar aqui algumas sugestões.

A primeira sugestão aqui acatada trata da definição e tipificação da Fraude Eletrônica, conhecida pelos profissionais de Tecnologia de Informação e Comunicação (TIC) como *phishing* ou *port fishing*, incluindo-a no Código Penal como segue:

"Fraude Eletrônica".

Art. 154 - D. Difundir, por qualquer meio, sistema informatizado com o propósito de induzir alguém a fornecer, espontaneamente e por qualquer meio, dados ou informações que facilitem ou permitam o acesso indevido ou sem autorização, a dispositivo de comunicação ou a sistema informatizado:

Pena – reclusão de dois a quatro anos e multa.

Parágrafo único. Somente se procede mediante representação, salvo se o crime é cometido contra a União, Estado, Município, empresa concessionária de serviços públicos, agências, fundações, autarquias, empresas públicas ou sociedade de economia mista e suas subsidiárias, ou se o sistema informatizado fraudador tiver potencial de propagação ou alastramento."

Aqui acolhemos contribuição valiosa, de advogado especialista e com vasta experiência na defesa contra os crimes de informática, de que deveríamos evitar o nome "fraude", em seu título, para não haver confusão com a "fraude material" ou com o "furto mediante fraude". Nossa proposta é que o crime seja nominado "difusão maliciosa de código" ou "disseminação de armadilha eletrônica".

Se mantivéssemos a nomenclatura "fraude eletrônica", olvidando a confusão de natureza dos tipos, estaríamos engendrando, na verdade, uma hipótese aberta de "tentativa de fraude", pois a conduta do agente difusor, a partir de um eventual resultado, pode ser qualquer uma. A partir do fornecimento espontâneo de dados, o agente pode praticar fraude, dano, furto, chantagem ou qualquer outro crime, inclusive fora da esfera digital (mundo atômico).

Nossa proposta, finalmente, é no sentido de que a redação do caput seja a seguinte, com sua inclusão no Título VIII (Dos crimes Contra a Incolumidade Pública), Capítulo II (Dos Crimes Contra a Segurança Dos Meios de Comunicação e Transporte e Outros Serviços Públicos):

"Difusão Maliciosa de Código".

Art. 266 -A. Difundir, por qualquer meio, sistema informatizado com o propósito de induzir alguém a fornecer, espontaneamente e por qualquer meio, dados ou informações que facilitem ou permitam o acesso indevido ou sem autorização, a dispositivo de comunicação ou a sistema informatizado, ou a obtenção de qualquer vantagem ilícita:

Pena – reclusão de um a dois anos.

"Parágrafo único - A pena é aumentada de sexta parte, se o agente se vale de anonimato, de nome suposto ou da utilização de identidade de terceiros para a prática de acesso."

Outra sugestão do Senador refere-se à inclusão de alteração ao art. 46 do Decreto-Lei nº. 2.848, de 7 de dezembro de 1940, Código Penal, mediante a inclusão a ele do § 5º dando a opção ao juiz a aplicação de pena alternativa, sugestão não acatada por entendermos que as penas alternativas já estão bem definidas no Código Penal. Ademais, a aplicação desta espécie de pena alternativa aumentará exponencialmente os riscos e as vulnerabilidades dos sistemas de informática das instituições públicas, que ficarão ainda mais expostas aos ataques de *hackers* e organizações cibernéticas criminosas, tendo em vista a possibilidade de instalação de *backdoors* e outros dispositivos fraudulentos nos *softwares* manipulados durante o cumprimento da pena.

Finalmente o Senador sugeriu a mudança do termo "meio eletrônico" por "dispositivo de comunicação" no art. 154-C, à qual acatamos e no substitutivo promovemos sua atualização e complementação:

"Dispositivo de Comunicação e Sistema Informatizado".

Art. 154-C Para os efeitos penais, considera-se:

I – dispositivo de comunicação: o computador, o processador de dados, o disquete, o CD-ROM ou qualquer outro meio capaz de armazenar ou transmitir dados de maneira magnética, ótica, ou eletronicamente.

"II – sistema informatizado: a rede de computadores, a base de dados, o programa de computador ou qualquer outro sistema capaz de armazenar ou transmitir dados eletronicamente."

b) Arts. 163, §§ 2ºe 3º

A equiparação feita pelo § 2º (equiparação à coisa do dado, informação ou a base de dados; a senha ou qualquer meio de identificação) é pertinente, mas poderia estar posicionada no Capítulo VIII do Título II (Disposições Gerais), pois dessa forma a regra seria válida para todos os tipos de crimes contra o patrimônio.

Por contribuição valiosa de vários advogados especialistas em crimes de informática, quanto à conduta do § 3º, entendemos que a pena deva ser mais severa, tendo em conta a potencialidade do dano material que se pode causar, por isso sugerimos a criação de um tipo autônomo com pena mais agravada do que a prevista no *caput* e parágrafo único do art. 163 e mais ainda se praticada no anonimato. Em vista disso, sugerimos a seguinte redação:

"Dano por Difusão de Vírus Eletrônico".

Art. 163-A. Criar, inserir ou difundir vírus em dispositivo de comunicação ou sistema informatizado, com a finalidade de destruí-lo, inutilizá-lo ou dificultar-lhe o funcionamento.

Pena: detenção, de 1 (um) a 3 (três) anos, e multa.

"Parágrafo único - A pena é aumentada de sexta parte, se o agente se vale de anonimato, de nome suposto ou da utilização de identidade de terceiros para a prática de acesso."

c) Art. 167 do CP

Por sua vez, a alteração proposta para o art. 167 do CP não é conveniente, pois proceder-se mediante queixa, quando o dado ou informação não tiver potencial de propagação ou alastramento, é um tratamento diferenciado para uma conduta por si só inaceitável e que justamente por isso ganha tipo penal autônomo no art. 163-A.

d) Art. 218-A do CP (Pornografia Infantil)

O delito descrito nesse dispositivo já está previsto, de modo mais abrangente, nos arts. 240 e 241 do Estatuto da Criança e do Adolescente (ECA).

e) Arts. 265 e 266 do CP, respectivamente "atentado contra a segurança de serviço de utilidade pública" e "interrupção ou perturbação de serviço telegráfico ou telefônico":

As alterações propostas para esses dispositivos são convenientes.

f) Arts. 298 e 298-A do CP

A redação que se propõe para o art. 298 é conveniente (falsificação de cartão de crédito); quanto ao art. 298-A procedemos a pequenas modificações de forma a melhorar sua clareza e compreensão, (falsificação de telefone celular ou meio de acesso a sistema eletrônico).

g) Art. 2º, § 2º, da Lei nº. 9.296, de 1996.

A alteração prevista no art. 2º da Lei nº. 9.296, 24 de julho de 1996, é conveniente conforme o art. 15 do Substitutivo. Não há que se falar em inconstitucionalidade da medida proposta, pois a reserva legal expressa e qualificada prevista no inciso XII do art. 5º da Constituição Federal estabeleceu apenas dois requisitos a serem observados pelo legislador ordinário no momento da regulamentação da restrição ao direito fundamental à privacidade das comunicações, quais sejam: existência de autorização judicial prévia à interceptação e 'para fins de investigação criminal ou instrução processual penal'.

O constituinte não estabeleceu o requisito de os 'crimes serem apenados com pena de reclusão'. Esta foi uma decisão do legislador ordinário, da Lei nº. 9.296, de 1996, decisão que pode ser alterada a qualquer momento sem que isto signifique qualquer afronta à Lei Maior.

Há que se frisar, ainda, que referida alteração será importante para apuração de crimes punidos com detenção praticados com o uso de sistemas informatizados, tais como:

- calúnia (aplicação do art. 138 à conduta de falar falsamente em *chat* ou comunidade *online* que alguém cometeu crime),

- difamação (aplicação do art. 139 à conduta de difamar alguém através de boato eletrônico ou *hoax*),

- injúria (aplicação do art. 140 à conduta de enviar *e-mail* com ofensas pessoais ao destinatário),

- violação de direito autoral (aplicação do art. 184 à conduta de copiar conteúdo de página da Internet sem citar a fonte),

- falsa identidade (aplicação do art. 307 à conduta de enviar *spam* com remetente falso),

- exercício arbitrário das próprias razões (aplicação do art. 345 à conduta de atacar emissário de *spam* ou vírus para evitar novos danos).

Todos esses delitos são praticados por meio dos sistemas informatizados, mas seriam punidos, conforme a proposta aqui endossada, com pena de detenção, o que impede a interceptação para fins de instrução criminal, dificultando sua comprovação pelos ofendidos e pelo Ministério Público.

Essa medida, ademais, viabilizará a possibilidade de manter a apenação de crimes informáticos com pena de detenção, afastando a necessidade de se estipularem penas de reclusão para esses delitos, ferindo o princípio da proporcionalidade da pena. Se, para viabilizar a apuração e a investigação criminal, estabelecêssemos pena de reclusão para esses crimes, ao invés de viabilizar a quebra legal do sigilo para crimes apenados com detenção, estaríamos provocando severa e injustificada distorção do sistema penal.

h) Art. 10 do PLC nº. 89, de 2003.

O dispositivo é necessário, com as inclusões propostas no substitutivo, análogas aos artigos incluídos no Código Penal, para tipificar os crimes no Código Penal Militar, usando ferramentas de tecnologia da informação e comunicações.

Por fim, o art. 11 do projeto mostra-se adequado, enquanto o art. 12 não é conveniente, sendo preferível manter o sistema de crimes estabelecido nos arts. 240 e 241 do ECA. A Lei nº. 10.764, de 12 de novembro de 2003, alterou o art. 241 do Estatuto da Criança e do Adolescente (Lei nº. 8.069, de 13 de julho de 1990), para tipificar e punir de forma mais severa a pornografia infantil.

O PLS nº. 76, de 2000, revestido de norma autônoma, afigura-se o projeto mais abrangente entre os que estão sendo aqui analisados. Os crimes informáticos estão divididos, no projeto, em crimes contra a inviolabilidade de dados e sua comunicação, contra a propriedade e o patrimônio, contra a honra e a vida privada, contra a vida e a integridade física das pessoas, contra o patrimônio fiscal, contra a moral pública e opção sexual e contra a segurança nacional.

Realmente a visão ampla que se tem dos crimes de informática é o grande mérito deste projeto inovador proposto pelo eminente Senador Renan Calheiros. Seus dispositivos mostram a gravidade crescente dos delitos praticados com instrumentos informatizados, cujas punições ainda não contam com o necessário suporte legal. Isto vem trazendo enorme insegurança a toda a sociedade pois crimes são praticados no anonimato da internet sem que haja a mínima possibilidade de defesa para o usuário.

Entretanto, a descrição de algumas das condutas deixa dúvidas em relação aos elementos dos respectivos delitos, o que pode prejudicar sua compreensão. Vale lembrar que a Lei Complementar nº. 95 de 1998 determina que havendo legislação em vigor deve-se preferir a sua alteração à criação de nova norma e desta forma o substitutivo proposto promove alterações ao Decreto-Lei nº. 2.848, de 7 de dezembro de 1940, o Código Penal. Comentamos, a seguir, sobre as disposições do PLS nº. 76, de 2000.

a) Art. 1º, § 1º – crimes contra a inviolabilidade de dados e sua comunicação.

Os incisos I, IV e V são espécies de crime de dano, descrito no art. 163 do CP; além disso, o inciso V deveria tipificar não a mera programação de instruções, mas a sua efetiva utilização, pois o nosso direito, via de regra, não pune os atos meramente preparatórios. Pode-se, alternativamente, prever, no art. 163 do CP, a equiparação dos dados informatizados à coisa, como o fez o PLC nº. 89, de 2003, ou fazê-lo ao final do Título II do CP.

O inciso II pode ser tido como furto (art. 155 do CP), se houver subtração da coisa, ou como apropriação indébita (art. 168 do CP), se o agente tinha a posse ou a detenção da coisa. Quanto ao inciso III, melhor seria punir o uso indevido dos dados em razão da finalidade do agente: se atenta contra a intimidade da pessoa, contra o patrimônio, contra a fé pública, etc. Entretanto, há que se ter em conta que a maioria desses crimes já existe, e que a informática é apenas um meio para realização da conduta delituosa. A equiparação à coisa que se pode fazer ao final do Título II do CP resolveria o problema.

Além disso, as penas propostas são muito brandas em face da gravidade das condutas equiparadas que acima citamos.

b) Art. 1º, § 2º

Os incisos I e II são espécies de furto, crime definido no art. 155 do CP, cuja pena é bem mais severa do que a proposta no PLS nº. 76, de 2000.

c) Art. 1º, § 3º

O inciso I está incluso no crime de injúria, descrito no art. 140 do CP; a conduta do inciso II, por sua vez, poderia ser inserida no Código Penal, mediante acréscimo do art. 154 D. Cabe observar que, se a informação for lesiva à honra, sua divulgação importará em um dos crimes tipificados no Capítulo V do Código Penal (calúnia, difamação ou injúria). Para desestimular o anonimato permitido pela internet, normalmente o caminho usado pelos autores dos crimes aqui tipificados, incluímos o artigo 154-F criando a obrigatoriedade de cadastramento identificador, além de estabelecermos, nos crimes em que tal conduta é especialmente perversa (Art. 154-A, § 3º, 154-D, parágrafo único e 266-A, parágrafo único), causas de aumento de pena a serem aplicadas pelo juiz, no momento de fixação da pena.

Todos os atos e fatos que se materializam através destes meios chegam, fácil e rapidamente, ao conhecimento de milhões de pessoas, causando um considerável prejuízo aos bens jurídicos tutelados. Em vista disso o potencial lesivo da conduta que ofende a honra da pessoa é incomensuravelmente maior quando o agente o faz por meio eletrônico como acontece nas redes de computadores. Isso já é bastante para justificar uma resposta penal mais severa, para que o agente sinta-se seriamente desestimulado a cometer o delito contra a honra por esse meio. É necessário, portanto, maior força penal coercitiva para evitá-los e assim fizemos incluir o art. 141-A conforme o art. 8º do substitutivo, estabelecendo causa especial de aumento de pena, com acréscimo de dois terços quando o meio utilizado é um dispositivo de comunicação ou sistema informatizado.

Novamente, em relação ao crime de ameaça, conduta que chega a ser banal no sítio do Orkut, por exemplo, a coibição do anonimato permitido pela internet, normalmente o caminho usado pelo agente da ameaça, entendemos suficiente a inclusão do artigo 154-F e dos parágrafos incluídos nos artigos 154-A, 154-D e 266-A.

d) Art. 1º, § 4º

O inciso I, a depender do resultado da conduta, será crime de lesão corporal ou homicídio, ambos já tipificados no Código Penal (arts. 129 e 121, respectivamente). O inciso II traz a incriminação de ato meramente preparatório.

Além disso, os artefatos explosivos têm ampla utilização na indústria, não sendo conveniente definir como crime o trabalho intelectual de elaboração de um sistema informatizado de detonação.

e) Art. 1º, § 5º

As condutas descritas nos incisos I e II configuram crime contra a ordem tributária, definidos de forma mais abrangente e adequada nos arts. 1º e 2º da Lei nº. 8.137, de 27 de dezembro de 1990.

f) Art. 1º, § 6º

O inciso I já está definido no art. 218 do CP (corrupção de menores).

Os incisos II e III estão inclusos no art. 234 do CP (escrito ou objeto obsceno).

Novamente, com o anonimato coibido pelo artigo 154-F e pelos parágrafos incluídos nos artigos 154-A, 154-D e 266-A do substitutivo, os autores destes crimes estarão desestimulados a cometê-los.

g) Art. 1º, § 7º

Os crimes definidos nesse parágrafo já estão contemplados na Lei nº. 7.170, de 14 de dezembro de 1983 (Lei de Segurança Nacional), especificamente nos seus arts. 13, 15 e 23.

Recentemente em Audiência Pública sobre o PLS nº. 279 de 2003, do qual também sou relator, de autoria do nobre Senador Delcídio Amaral e que propõe a criação de um cadastro de titulares de correio eletrônico na internet, ficou evidente que, para fins de investigação, é necessário estabelecer um prazo legal de armazenamento dos dados de conexões e comunicações realizadas pelos equipamentos componentes da internet, o que será feito pelos seus provedores de acesso. Os serviços de telefonia e transmissão de dados mantêm por cinco anos os dados de conexões e chamadas realizadas por seus clientes para fins judiciais, mas na internet brasileira inexiste procedimento análogo.

Registre-se que naquela audiência foram ouvidos representantes do Comitê Gestor da Internet no Brasil (CGIBr) do Ministério da Ciência e Tecnologia; da Fundação de Amparo à Pesquisa de São Paulo (FAPESP) que representa no Brasil o ICANN (*Internet Corporation for Assigning Names and Numbers)*, gestora do registro de nomes e números IP (*Internet Protocol),* ou seja, os endereços na internet; da– Associação Brasileira dos Provedores de Internet (ABRANET); do Instituto de Criminalística em Informática da Polícia Federal, do Ministério da Justiça (PF); da Agência Nacional de Telecomunicações (ANATEL).

Há apenas uma recomendação do Comitê Gestor da Internet Brasil (CGIBr) aos provedores nacionais: que mantenham, por no mínimo três anos, os dados de conexões e comunicações realizadas por seus equipamentos – a saber, identificação dos endereços de IP (protocolo de internet) do remetente e do destinatário da mensagem, bem como a data e

horário de início e término da conexão, sem registrar o conteúdo da mensagem, preservando assim o sigilo da comunicação. É clara a necessidade de se transformar tal recomendação em imposição legal, razão por que apresentamos a inclusão no Código Penal do art.154-E conforme o art. 2º do substitutivo.

Além disso, também para fins de investigação, na mesma Audiência Pública, registrou-se a necessidade de estabelecer a obrigatoriedade de identificação positiva do usuário que acesse a Internet, ou qualquer rede de computadores, perante seu provedor ou junto a quem lhe torne disponível o acesso a dispositivo de comunicação ou sistema informatizado, muito embora todos tenham reconhecido as dificuldades técnicas, econômicas e culturais que a regra possa oferecer. Incluem-se aqui os *cyber-cafe* ou *hot zones*.

Vêm à memória os episódios danosos que ocorreram no início da operação com os celulares pré-pagos, o que obrigou o seu cadastramento obrigatório pelas operadoras, contra todos os argumentos então apresentados, ou seja, a sociedade brasileira mostrou o seu bom senso e mudou seu comportamento.

Desde já, alertamos que tal identificação e cadastramento necessitam serem necessariamente presenciais, com cópias de documentos originais, mas admite-se a alternativa de se utilizarem os certificados digitais, cuja emissão já é presencial conforme definido em Lei.

Outras formas alternativas de identificação e cadastramento podem ser usadas a exemplo do que os bancos, operadoras de telefonia, operadores de *callcenter* e o comércio eletrônico em geral já vêm fazendo, usando cadastros disponíveis mediante convênios de cooperação ou simples colaboração.

Dados como nome de acesso (*login* ou *username*), nome completo, filiação, endereço completo, data de nascimento, números de telefone e senha criteriosa (número de caracteres, mistura de letras e números etc) devem ser requeridos no momento do cadastramento de um novo usuário. Este, ao solicitar um acesso posterior, usará seu nome de acesso e sua senha e outros procedimentos de validação e conferência automáticas realizados pelo sistema do provedor de acesso, procedimentos que têm o nome de "autenticação do usuário".

Conforme já citado em parágrafo anterior, a identificação e conseqüente cadastramento já acontecem com os serviços de telefonia, transmissão de dados e rádio-transmissão, onde cada operador já é obrigado por regulamento a manter um cadastro de proprietários de telefones fixos, móveis ou de aparelhos transmissores e receptores de rádio - cadastro usado exclusivamente para fins de investigação ou judiciais. Novamente, procedimento obrigatório análogo não existe na internet brasileira.

Novas tecnologias de transmissão, como a conexão sem fio, conhecida como *wireless* ou *Wi-Fi,* estão cada vez mais disponíveis. Como são padronizadas internacionalmente, tendem a se tornar extremamente baratas e a serem disseminadas largamente por todas as cidades, distritos ou aglomerações urbanas ou rurais, libertando o usuário de internet do local físico a que hoje está obrigado. Com o advento próximo da televisão digital tal disseminação será ainda mais efetiva.

Ainda, em qualquer outro serviço privado que se utilize da internet, seja instituição financeira, operadoras de cartões de crédito, empresas de comércio ou indústria, ou nas redes internas das instituições públicas e privadas, a autenticação do usuário mediante senha

acompanhada, ou não, de outros requisitos de identificação, como certificado digital, tabela de códigos alfanuméricos e assim por diante, são requeridos para que o usuário acesse os serviços ou as informações.

Em outro caso, em decisão recente, o Tribunal Superior do Trabalho (TST) deu ganho de causa a um banco contra um funcionário que divulgava informações incorretas sobre as aplicações em um fundo de investimentos. O referido agente fora denunciado por uma cliente que tivera prejuízos com as informações e, em razão disso, foi demitido por justa causa, já que usou equipamento do banco, em horário de trabalho funcional, distribuindo informes não-verdadeiros na internet.

Assim, não é demais lembrar, principalmente para esses casos de difamação e injúria ou de prejuízos pessoais, o que dispõe a Carta Magna no seu art. 5º inciso IV que diz "é livre a manifestação do pensamento, sendo vedado o anonimato", o que por si só já justificaria a identificação, o cadastramento e a respectiva autenticação do usuário pelo provedor de acesso à internet brasileira.

Para tanto, transformamos a identificação, o cadastro e respectiva autenticação do usuário em imposição legal, conforme o caput do Art. 13 do substitutivo e incluindo no Código Penal o artigo 154-F e os parágrafos incluídos nos artigos. 154-A, 154-D e 266-A, conforme o art. 2° do substitutivo.

A fim de preservar a intimidade dos usuários, o cadastro somente poderá ser fornecido a terceiros mediante expressa autorização judicial ou em casos que a Lei determinar, conforme o § 2º do art. 14 do substitutivo. Mas reconhecendo a existência de ferramentas de segurança mais potentes, previmos, conforme o § 3º do art. 14 do substitutivo, a troca opcional, pelo provedor, da identificação e do cadastro do usuário, pelo certificado digital.

Este requer, de maneira presencial quando da sua emissão, todas as informações cadastrais, inclusive a constituição tecnicamente adequada de senha. A regra é condizente com a Medida Provisória número 2.200-2, de 24 de agosto de 2001, mantida em vigor conforme a Emenda Constitucional número 32, de 12 de setembro de 2001. Como toda tecnologia inovadora o certificado digital inicialmente se restringiu às trocas interbancárias, a Transferência Eletrônica Disponível (TED), instituída pelo Sistema de Pagamentos Brasileiro (SPB), implantado em 2002 pelo Banco Central do Brasil. Estatísticas recentes mostram a ocorrência de quase 100 milhões de transações e mais de R$ 5 trilhões de reais transferidos com toda segurança em tempo real.

É público o fato de que o custo de cada certificado digital e seu suporte físico, (cartão de plástico, CD-ROM, ou outro dispositivo de comunicação), tende a cair em proporção geométrica, à medida que se dissemine o seu uso, uma característica conhecida das inovações tecnológicas. Ao dispor sobre o uso do certificado digital como opcional, a presente norma permite a sua própria evolução, aguardando que a sociedade se adapte à nova realidade transformada a cada dia pela tecnologia, sem obrigar o usuário ou os provedores a novos custos ou a novos hábitos e comportamentos.

Por fim, mantendo a necessária segurança e respeitando os pressupostos de uma rede de computadores, naturalmente ágil, compatível, interoperável, colaborativa e cooperativa, previmos, conforme o § 4º do art. 14 do substitutivo, a substituição opcional do cadastro de identificação, a critério daquele que torna disponível o acesso, por cadastro que poderá ser

obtido mediante instrumento público de convênio de cooperação ou colaboração com aqueles que já o tenham constituído na forma prevista no substitutivo.

III – VOTO

Diante do exposto, e considerando a pertinência e importância da solução proposta, somos pela aprovação do Projeto de Lei do Senado nº. 76, de 2000, incorporando parcialmente o Projeto de Lei da Câmara n° 89, de 2003 (n° 84, de 1999, na Câmara dos Deputados) e o Projeto de Lei do Senado n° 137, de 2000, na forma do substitutivo que apresentamos.

SUBSTITUTIVO (ao PLS 76/2000, PLS 137/2000 e PLC 89/2003)

Altera o Decreto-Lei nº. 2.848, de 7 de dezembro de 1940 (Código Penal) e o Decreto-Lei nº. 1.001, de 21 de outubro de 1969 (Código Penal Militar), para tipificar condutas realizadas mediante uso de rede de computadores ou internet, ou que sejam praticadas contra sistemas informatizados e similares, e dá outras providências.

O CONGRESSO NACIONAL decreta:

Art. 1º O Capítulo IV do Título II da Parte Especial do Decreto-Lei nº. 2.848, de 7 de dezembro de 1940 (Código Penal) fica acrescido do art. 163-A, assim redigido:

"Dano por Difusão de Vírus Eletrônico"

Art. 163-A. Criar, inserir ou difundir vírus em dispositivo de comunicação ou sistema informatizado, com a finalidade de destruí-lo, inutilizá-lo ou dificultar-lhe o funcionamento.

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

Parágrafo único - A pena é aumentada de sexta parte, se o agente se vale de anonimato, de nome suposto ou da utilização de identidade de terceiros para a prática de acesso. "(NR)

Art. 2º O Título I da Parte Especial do Código Penal fica acrescido do Capítulo VII-A, assim redigido:

"Capítulo VII-A DA VIOLAÇÃO DE DISPOSITIVO DE COMUNICAÇÃO OU SISTEMA INFORMATIZADO".

Acesso indevido a dispositivo de comunicação

Art. 154-A. Acessar indevidamente, ou sem autorização, dispositivo de comunicação ou sistema informatizado:

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

§ 1º Nas mesmas penas incorre quem fornece a terceiro meio indevido ou não autorizado de acesso a dispositivo de comunicação ou sistema informatizado.

§ 2º Somente se procede mediante representação, salvo se o crime é cometido contra a União, Estado, Município, empresa concessionária de serviços públicos, agências, fundações, autarquias, empresas públicas ou sociedade de economia mista e suas subsidiárias.

§ 3º A pena é aumentada de sexta parte, se o agente se vale de anonimato, de nome suposto ou da utilização de identidade de terceiros para a prática de acesso.

Manipulação indevida de informação eletrônica

Art. 154-B. Manter consigo, transportar ou fornecer indevidamente ou sem autorização, dado ou informação obtida em dispositivo de comunicação ou sistema informatizado:

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

Parágrafo único - Somente se procede mediante representação, salvo se o crime é cometido contra a União, Estado, Município, empresa concessionária de serviços públicos, agências, fundações, autarquias, empresas públicas ou sociedade de economia mista e suas subsidiárias.

Dispositivo de comunicação, sistema informatizado, identificação de usuário e autenticação de usuário.

Art. 154-C. Para os efeitos penais, considera-se:

I – dispositivo de comunicação: o computador, o computador de mão, o telefone celular, o processador de dados, os meios de armazenamento de dados digitais, ou qualquer outro meio capaz de processar, armazenar ou transmitir dados utilizando-se de tecnologias magnéticas, óticas ou qualquer outra tecnologia digital.

II – sistema informatizado: a rede de computadores, o equipamento ativo da rede de comunicação de dados com ou sem fio, a rede de telefonia fixa ou móvel, a rede de televisão, a base de dados, o programa de computador ou qualquer outro sistema capaz de processar, armazenar ou transmitir dados eletronicamente.

III – identificação de usuário: os dados de nome de acesso, senha criteriosa, nome completo, filiação, endereço completo, data de nascimento, numero da carteira de identidade ou equivalente legal, que sejam requeridos no momento do cadastramento de um novo usuário de dispositivo de comunicação ou sistema informatizado.

IV – autenticação de usuário: procedimentos de validação e conferência da identificação do usuário, quando este tem acesso ao dispositivo de comunicação ou sistema informatizado, realizados por quem os torna disponíveis ao usuário.

Divulgação de informações depositadas em banco de dados

Art. 154-D. Divulgar, ou tornar disponíveis, para finalidade distinta daquela que motivou a estruturação do banco de dados, informações privadas referentes, direta ou indiretamente, a dados econômicos de pessoas físicas ou jurídicas, ou a dados de pessoas físicas referentes a raça, opinião política, religiosa, crença, ideologia, saúde física ou mental, orientação sexual, registros policiais, assuntos familiares ou profissionais, além de outras de caráter sigiloso, salvo por decisão da autoridade competente, ou mediante expressa anuência da pessoa a que se referem, ou de seu representante legal.

Pena – detenção, de um a dois anos, e multa.

Parágrafo único: A pena é aumentada de sexta parte, se o agente se vale de anonimato, de nome suposto ou da utilização de identidade de terceiros para a prática de divulgação.

Dados de conexões e comunicações realizadas

Art. 154-E. Deixar de manter, aquele que torna disponível o acesso a rede de computadores, os dados de conexões e comunicações realizadas por seus equipamentos, aptas à identificação do usuário, endereços eletrônicos de origem e destino no transporte dos registros de dados e informações, data e horário de início e término da conexão, incluindo protocolo de internet ou mecanismo de identificação equivalente, pelo prazo de cinco anos.

Pena – detenção, de dois a seis meses, e multa.

Permitir acesso por usuário não identificado e não autenticado

Art. 154-F. Permitir, aquele que torna disponível o acesso a rede de computadores, a usuário, sem a devida identificação e autenticação, qualquer tipo de acesso ou uso pela rede de computadores.

Pena – detenção, de um a dois anos, e multa.

Parágrafo único. Na mesma pena incorre, o responsável por provedor de acesso a rede de computadores, que deixa de exigir, como condição de acesso à rede, a necessária, identificação e regular cadastramento do usuário.

Art. 3º O Código Penal passa a vigorar acrescido do seguinte art. 183-A:

Art. 183-A. Equiparam-se à coisa o dado ou informação em meio eletrônico, a base de dados armazenada em dispositivo de comunicação e o sistema informatizado, a senha ou qualquer meio que proporcione acesso aos mesmos.

Art. 4º Os arts. 265 e 266 do Código Penal passam a vigorar com as seguintes redações:

"Atentado contra a segurança de serviço de utilidade pública"

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

..... (NR)"

"Interrupção ou perturbação de serviço telegráfico ou telefônico"

Art. 266. Interromper ou perturbar serviço telegráfico, radiotelegráfico, telefônico, telemático ou de telecomunicação, impedir ou dificultar-lhe o restabelecimento:

..... (NR)"

Art. 5º O Capitulo II do Título VIII do Código Penal passa a vigorar acrescido do seguinte artigo:

"**Difusão Maliciosa de Código".**

Art. 266-A. Difundir, por qualquer meio, programa, conjunto de instruções ou sistema informatizado com o propósito de induzir alguém a fornecer, espontaneamente e por qualquer meio, dados ou informações que facilitem ou permitam o acesso indevido ou sem autorização, a dispositivo de comunicação ou a sistema informatizado, ou a obtenção de qualquer vantagem ilícita:

Pena – detenção de um a dois anos.

Parágrafo único - A pena é aumentada de sexta parte, se o agente se vale de anonimato, de nome suposto ou da utilização de identidade de terceiros para a prática de acesso.(NR)"

Art. 6º O art. 298 do Código Penal passa a vigorar acrescido do seguinte parágrafo único:

"**Art. 298.** .....

Falsificação de cartão de crédito ou débito ou qualquer dispositivo eletrônico portátil de armazenamento e processamento de informações

Parágrafo único. Equipara-se a documento particular o cartão de crédito ou débito ou qualquer dispositivo eletrônico portátil de armazenamento ou processamento de informações. (NR)"

Art. 7º O Código Penal passa a vigorar acrescido do seguinte art. 298-A:

"Falsificação de telefone celular ou meio de acesso a sistema eletrônico".

Art. 298-A. Criar ou copiar, indevidamente ou sem autorização, ou falsificar código; seqüência alfanumérica; cartão inteligente; transmissor ou receptor de rádio freqüência ou telefonia celular; ou qualquer instrumento que permita o acesso a dispositivo de comunicação ou sistema informatizado:

Pena – reclusão, de um a cinco anos, e multa."(NR)

Art. 8º O Código Penal passa a vigorar acrescido do seguinte art. 141-A:

Art. 141-A. As penas neste Capítulo aumentam-se de dois terços caso os crimes sejam cometidos por intermédio de dispositivo de comunicação ou sistema informatizado.

Art. 9º O Capítulo VII do Título V da Parte Especial do Livro I do Decreto-Lei nº. 1.001, de 21 de outubro de 1969 (Código Penal Militar) fica acrescido do art. 262-A, assim redigido:

"Dano por Difusão de Vírus Eletrônico".

Art. 262-A. Criar, inserir ou difundir vírus em dispositivo de comunicação ou sistema informatizado, com a finalidade de destruí-lo, inutilizá-lo ou dificultar-lhe o funcionamento.

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

Parágrafo único - A pena é aumentada de sexta parte, se o agente se vale de anonimato, de nome suposto ou da utilização de identidade de terceiros para a prática de acesso."(NR)

Art. 10 O Título VII da Parte Especial do Livro I do Código Penal Militar, Decreto-Lei, nº. 1.001, de 21 de outubro de 1969, fica acrescido do Capítulo VII-A, assim redigido:

"Capítulo VII-A DA VIOLAÇÃO DE DISPOSITIVO DE COMUNICAÇÃO OU SISTEMA INFORMATIZADO".

Acesso indevido a dispositivo de comunicação

Art. 339-A. Acessar indevidamente, ou sem autorização, dispositivo de comunicação ou sistema informatizado:

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

§ 1º Nas mesmas penas incorre quem fornece a terceiro meio indevido ou não autorizado de acesso a dispositivo de comunicação ou sistema informatizado.

§ 2º A pena é aumentada de sexta parte, se o agente se vale de anonimato, de nome suposto ou da utilização de identidade de terceiros para a prática de acesso.

Manipulação indevida de informação eletrônica

Art. 339-B. Manter consigo, transportar ou fornecer indevidamente ou sem autorização, dado ou informação obtida em dispositivo de comunicação ou sistema informatizado:

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

Dispositivo de comunicação, sistema informatizado, identificação de usuário e autenticação de usuário.

Art. 339-C. Para os efeitos penais, considera-se:

I – dispositivo de comunicação: o computador, o computador de mão, o telefone celular, o processador de dados, os meios de armazenamento de dados digitais, ou qualquer outro meio capaz de processar, armazenar ou transmitir dados utilizando-se de tecnologias magnéticas, óticas ou qualquer outra tecnologia digital.

II – sistema informatizado: a rede de computadores, o equipamento ativo da rede de comunicação de dados com ou sem fio, a rede de telefonia fixa ou móvel, a rede de televisão, a base de dados, o programa de computador ou qualquer outro sistema capaz de processar, armazenar ou transmitir dados eletronicamente.

III – identificação de usuário: os dados de nome de acesso, senha criteriosa, nome completo, filiação, endereço completo, data de nascimento, numero da carteira de identidade ou equivalente legal, que sejam requeridos no momento do cadastramento de um novo usuário de dispositivo de comunicação ou sistema informatizado.

IV – autenticação de usuário: procedimentos de validação e conferência da identificação do usuário, quando este tem acesso ao dispositivo de comunicação ou sistema informatizado, realizados por quem os torna disponíveis ao usuário.

Divulgação de informações depositadas em banco de dados

Art. 339-D. Divulgar, ou tornar disponíveis, para finalidade distinta daquela que motivou a estruturação do banco de dados, informações privadas referentes, direta ou indiretamente, a dados econômicos de pessoas físicas ou jurídicas, ou a dados de pessoas físicas referentes a raça, opinião política, religiosa, crença, ideologia, saúde física ou mental, orientação sexual, registros policiais, assuntos familiares ou profissionais, além de outras de caráter sigiloso, salvo por decisão da autoridade competente, ou mediante expressa anuência da pessoa a que se referem, ou de seu representante legal.

Pena – detenção, de um a dois anos, e multa.

Parágrafo único: A pena é aumentada de sexta parte, se o agente se vale de anonimato, de nome suposto ou da utilização de identidade de terceiros para a prática de divulgação.

Dados de conexões e comunicações realizadas

Art. 339-E. Deixar de manter, aquele que torna disponível o acesso a rede de computadores, os dados de conexões e comunicações realizadas por seus equipamentos, aptas à identificação do usuário, endereços eletrônicos de origem e destino no transporte dos registros de dados e informações, data e horário de início e término da conexão, incluindo protocolo de internet ou mecanismo de identificação equivalente, pelo prazo de cinco anos.

Pena – detenção, de dois a seis meses, e multa.

Permitir acesso por usuário não identificado e não autenticado

Art. 339-F. Permitir, aquele que torna disponível o acesso a rede de computadores, a usuário, sem a devida identificação e autenticação, qualquer tipo de acesso ou uso pela rede de computadores.

Pena – detenção, de um a dois anos, e multa.

Parágrafo único. Na mesma pena incorre, o responsável por provedor de acesso a rede de computadores, que deixa de exigir, como condição de acesso à rede, a necessária, identificação e regular cadastramento do usuário.(NR)"

Art. 11 O Capítulo I do Título VI da Parte Especial do Livro I do Decreto-Lei nº. 1.001, de 21 de outubro de 1969 (Código Penal Militar) fica acrescido do art. 281-A, assim redigido:

"Difusão Maliciosa de Código"

Art. 281-A. Difundir, por qualquer meio, programa, conjunto de instruções ou sistema informatizado com o propósito de induzir alguém a fornecer, espontaneamente e por qualquer meio, dados ou informações que facilitem ou permitam o acesso indevido ou sem autorização, a dispositivo de comunicação ou a sistema informatizado, ou a obtenção de qualquer vantagem ilícita:

Pena – detenção de um a dois anos.

Parágrafo único - A pena é aumentada de sexta parte, se o agente se vale de anonimato, de nome suposto ou da utilização de identidade de terceiros para a prática de acesso.(NR)"

Art. 12 O Título V da Parte Especial do Livro I do Código Penal Militar, Decreto-Lei, nº. 1.001, de 21 de outubro de 1969, fica acrescido do Capítulo VIII-A, assim redigido:

"Capítulo VIII-A DISPOSIÇÕES GERAIS".

Art. 267-A. Equiparam-se à coisa o dado ou informação em meio eletrônico, a base de dados armazenada em dispositivo de comunicação e o sistema informatizado, a senha ou qualquer meio que proporcione acesso aos mesmos. (NR)"

Art. 13 Todo aquele que desejar acessar uma rede de computadores, local, regional, nacional ou mundial, deverá identificar-se e cadastrar-se naquele que torne disponível este acesso.

Parágrafo único. Os atuais usuários terão prazo de cento e vinte dias após a entrada em vigor desta Lei para providenciarem ou revisarem sua identificação e cadastro junto a quem, de sua preferência, torne disponível o acesso aqui definido.

Art. 14 Todo aquele que torna disponível o acesso a uma rede de computadores somente admitirá como usuário pessoa ou dispositivo de comunicação ou sistema informatizado que for autenticado conforme validação positiva dos dados cadastrais previamente fornecidos pelo contratante de serviços.

A contratação dar-se-á exclusivamente por meio formal, vedado o ajuste meramente consensual.

§1º O cadastro mantido por aquele que torna disponível o acesso a uma rede de computadores conterá obrigatoriamente as seguintes informações prestadas por meio presencial e com apresentação de documentação original: nome de acesso; senha de acesso ou mecanismo similar; nome completo; endereço completo com logradouro, número, complemento, código de endereçamento postal, cidade e estado da federação; número de registro junto aos serviços ou institutos de identificação das Secretarias de Segurança Pública Estaduais ou conselhos de registro profissional; número de inscrição no Cadastro de Pessoas

Físicas (CPF), mantido pelo Ministério da Fazenda ou o Número de Identificação do Trabalhador (NIT), mantido pelo Ministério da Previdência Social.

§ 2º O cadastro somente poderá ser fornecido a terceiros mediante expressa autorização da autoridade competente ou em casos que a Lei venha a determinar.

§ 3º A senha e o cadastro de identificação, a critério daquele que torna disponível o acesso, poderão ser substituídos por certificado digital emitido dentro das normas da Infra-estrutura de Chaves Públicas Brasileira (ICP–Brasil), conforme determina a MP 2.200-2 de 24 de agosto de 2001.

§ 4º O cadastro de identificação, a critério daquele que torna disponível o acesso, poderá ser obtido mediante instrumento público de convênio de cooperação ou colaboração com aqueles que já o tenham constituído na forma deste artigo.

§ 5º Para assegurar a identidade e a privacidade do usuário a senha de acesso poderá ser armazenada criptografada por algoritmo não reversível.

Art. 15. O art. 2º da Lei nº. 9.296, de 24 de julho de 1996, passa a vigorar acrescido do seguinte § 2º, renumerando-se o parágrafo único para § 1º:

§ 2º O disposto no inciso III do caput não se aplica quando se tratar de interceptação do fluxo de comunicações em dispositivo de comunicação ou sistema informatizado.” (NR)

Art. 16 Esta Lei entra em vigor sessenta dias após a data de sua publicação.

ANEXO B

CONVENÇÃO SOBRE O CIBERCRIME

Budapeste, 23.XI.2001

Preâmbulo

Os Estados membros do Conselho da Europa e os seguintes Estados signatários,

Considerando que o objectivo do Conselho da Europa é realizar uma união mais estreita entre os seus membros;

Reconhecendo a importância de intensificar a cooperação com os outros Estados Partes da presente Convenção;

Convictos da necessidade de prosseguir, com carácter prioritário, uma política criminal comum, com o objectivo de proteger a sociedade contra a criminalidade no ciberespaço, designadamente, através da adopção de legislação adequada e da melhoria da cooperação internacional;

Conscientes das profundas mudanças provocadas pela digitalização, pela convergência e pela globalização permanente das redes informáticas;

Preocupados com o risco de que as redes informáticas e a informação electrónica, sejam igualmente utilizadas para cometer infracções criminais e de que as provas dessas infracções sejam armazenadas e transmitidas através dessas redes;

Reconhecendo a necessidade de uma cooperação entre os Estados e a indústria privada no combate à cibercriminalidade, bem como a necessidade de proteger os interesses legítimos ligados ao uso e desenvolvimento das tecnologias da informação;

Acreditando que uma luta efectiva contra a cibercriminalidade requer uma cooperação internacional em matéria penal acrescida, rápida e eficaz;

Convictos de que a presente Convenção é necessária para impedir os actos praticados contra a confidencialidade, integridade e disponibilidade de sistemas informáticos, de redes e dados informáticos, bem como a utilização fraudulenta de desses sistemas, redes e dados, assegurando a incriminação desses comportamentos tal como descritos na presente Convenção, e da adopção de poderes suficientes para combater eficazmente essas infracções, facilitando a detecção, a investigação e o procedimento criminal relativamente às referidas infracções, tanto ao nível nacional como internacional, e estabelecendo disposições materiais com vista a uma cooperação internacional rápida e fiável;

Tendo presente a necessidade de garantir um equilíbrio adequado entre os interesses da aplicação da lei e o respeito pelos direitos fundamentais do ser humano, tal como garantidos pela Convenção para a Protecção dos Direitos do Homem e das Liberdades Fundamentais do Conselho da Europa de 1950, pelo Pacto Internacional sobre os Direitos Civis e Políticos das Nações Unidas de 1966, bem como por outros tratados internacionais aplicáveis em matéria de direitos do Homem, que reafirmam o direito à liberdade de opinião sem qualquer ingerência, o direito à liberdade de expressão, incluindo a liberdade de procurar, de receber e transmitir informações e ideias de qualquer natureza sem considerações de fronteiras e, ainda, o direito ao respeito pela vida privada;

Tendo igualmente presente o direito à protecção de dados pessoais, tal como é conferido, por exemplo, pela Convenção do Conselho da Europa de 1981, para a Protecção das Pessoas relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal;

Considerando a Convenção das Nações Unidas sobre os Direitos da Criança de 1989, e a Convenção da Organização Internacional do Trabalho sobre as Piores Formas do Trabalho Infantil de 1999;

Tendo em conta as convenções existentes do Conselho da Europa sobre a cooperação em matéria penal, bem como outros tratados similares celebrados entre os Estados membros do Conselho da Europa e outros Estados, e sublinhando que a presente Convenção tem por finalidade complementar as referidas convenções, de modo a tornar mais eficazes as investigações e as acções penais relativas a infracções penais relacionadas com sistemas e dados informáticos, bem como permitir a recolha de provas em forma electrónica de uma infracção penal;

Saudando os recentes desenvolvimentos destinados a aprofundar o entendimento e cooperação internacionais no combate à criminalidade no ciberespaço, nomeadamente, as acções empreendidas pelas Nações Unidas, pela OCDE, pela União Europeia e pelo G8;

Recordando as Recomendações do Comité de Ministros N.º R (85) 10 relativa à aplicação prática da Convenção Europeia sobre Auxílio Judiciário Mútuo em Matéria Penal quanto às cartas rogatórias para a intercepção de telecomunicações, N.º R (88) 2 sobre as medidas destinadas a combater a pirataria no domínio do direito de autor e dos direitos conexos, N.º R (87) 15 que regula a utilização de dados de carácter pessoal no sector da polícia, N.º R (95) 4 relativa à protecção dos dados de carácter pessoal no sector das telecomunicações, tendo em conta, designadamente os serviços telefónicos e a N.º R (89) 9 sobre a criminalidade informática que estabelece directrizes para os legisladores nacionais respeitantes à definição de certos crimes informáticos e, ainda, a N.º R (95) 13 relativa a problemas processuais penais relacionados com as tecnologias da informação;

Tendo em conta a Resolução n.º 1 adoptada pelos Ministros Europeus da Justiça na sua 21ª Conferência (Praga, 10 e 11 de Junho de 1997), que recomenda ao Comité de Ministros para apoiar o trabalho desenvolvido pelo Comité Europeu para os Problemas Criminais (CDPC) sobre a cibercriminalidade a fim de aproximar as legislações penais nacionais e de permitir a utilização de meios de investigação eficazes em matéria de crimes informáticos, bem como a Resolução n.º 3, adoptada na 23ª Conferência dos Ministros Europeus da Justiça (Londres, 8 e 9 de Junho de 2000), que incentiva as partes intervenientes nas negociações a prosseguirem os seus esforços para encontrar soluções apropriadas que permitam o maior número possível de

Estados a tornarem-se Partes da Convenção e reconhece a necessidade de dispor de um mecanismo rápido e eficaz de cooperação internacional, que tenha devidamente em conta as exigências específicas da luta contra a cibercriminalidade;

Tendo igualmente em conta o Plano de Acção adoptado pelos Chefes de Estado e de Governo do Conselho da Europa, por ocasião da sua Segunda Cimeira (Estrasburgo, 10 e 11 de Outubro de 1997), para procurar respostas comuns face ao desenvolvimento das novas tecnologias da informação, com base nas normas e princípios do Conselho da Europa;

Acordaram no seguinte:

Capítulo I – Terminologia

Artigo 1º - Definições

Para os fins da presente Convenção:

a) "Sistema informático" significa qualquer dispositivo isolado ou grupo de dispositivos relacionados ou interligados, em que um ou mais de entre eles, desenvolve, em execução de um programa, o tratamento automatizado dos dados;

b) "Dados informáticos" significa qualquer representação de factos, de informações ou de conceitos sob uma forma susceptível de processamento num sistema de computadores, incluindo um programa, apto a fazer um sistema informático executar uma função;

c) "Fornecedor de serviço" significa:

(i) Qualquer entidade pública ou privada que faculte aos utilizadores dos seus serviços a possibilidade de comunicar por meio de um sistema informático e (ii) Qualquer outra entidade que processe ou armazene dados informáticos em nome do referido serviço de comunicação ou dos utilizadores desse serviço.

d) "Dados de tráfego" significa todos os dados informáticos relacionados com uma comunicação efectuada por meio de um sistema informático, gerados por este sistema como elemento de uma cadeia de comunicação, indicando a origem da comunicação, o destino, o trajecto, a hora, a data, o tamanho, a duração ou o tipo do serviço subjacente.

Capítulo II – Medidas a tomar a nível nacional

Secção 1 – Direito penal material

Título 1 – Infracções contra a confidencialidade, integridade e disponibilidade de sistemas informáticos e dados informáticos.

Artigo 2º - Acesso ilegítimo

Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, no seu direito interno, o acesso intencional e ilegítimo à totalidade ou a parte de um sistema informático. As Partes podem exigir que a infracção seja cometida com a violação de medidas de segurança, com a intenção de obter dados

informáticos ou outra intenção ilegítima, ou que seja relacionada com um sistema informático conectado a outro sistema informático.

Artigo 3º - Intercepção ilegítima

Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, no seu direito interno, a intercepção intencional e ilegítima de dados informáticos, efectuada por meios técnicos, em transmissões não públicas, para, de ou dentro de um sistema informático, incluindo emissões electromagnéticas provenientes de um sistema informático que veicule esses dados. As Partes podem exigir que a infracção seja cometida com dolo ou que seja relacionada com um sistema informático conectado com outro sistema informático.

Artigo 4º - Interferência em dados

1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, no seu direito interno, o acto de intencional e ilegitimamente danificar, apagar, deteriorar, alterar ou eliminar dados informáticos.

2. Uma Parte pode reservar-se o direito de exigir que a conduta descrita no n.º 1 provoque danos graves.

Artigo 5º - Interferência em sistemas

Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, no seu direito interno, a obstrução grave, intencional e ilegítima, ao funcionamento de um sistema informático, através da introdução, transmissão, danificação, eliminação, deterioração, modificação ou supressão de dados informáticos.

Artigo 6º - Uso abusivo de dispositivos

1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracções penais, em conformidade com o seu direito interno, quando cometidas intencional e ilegitimamente:

a) A produção, a venda, a obtenção para utilização, a importação, a distribuição, ou outras formas de disponibilização de:

i. Um dispositivo, incluindo um programa informático, concebido ou adaptado essencialmente para permitir a prática de uma das infracções definidas em conformidade com os artigos 2º a 5º;

ii. Uma palavra-passe, um código de acesso ou dados informáticos semelhantes que permitam aceder a todo, ou a parte de um sistema informático com a intenção de serem utilizados para cometer qualquer uma das infracções definidas nos Artigos 2º a 5º; e

b) A posse de um elemento referido nos alínea a), i. ou ii., com a intenção de ser utilizado com o objectivo de cometer qualquer uma das infracções referidas nos artigos 2º a 5º. As Partes podem exigir que no direito interno se reuna um certo número desses elementos para que seja determinada a responsabilidade criminal.

2. O presente artigo não deve ser interpretado como impondo responsabilidade criminal quando a produção, a venda, a aquisição para utilização, a importação, a distribuição, ou outra forma de disponibilização ou posse, mencionadas no n.º1 do presente artigo não tenham por objectivo cometer uma infracção estabelecida em conformidade com os artigos 2º a 5º da presente Convenção, como é o caso de ensaios autorizados ou de protecção de um sistema informático.

3. (Cada Parte pode reservar-se o direito de não aplicar o disposto no n.º 1 do presente artigo desde que essa reserva não diga respeito à venda, distribuição, ou a qualquer outra forma de disponibilização dos elementos referidos no n.º 1, a), ii.

Título 2 – Infracções relacionada com computadores

Artigo 7º - Falsidade informática

Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, em conformidade com o seu direito interno, a introdução, a alteração, a eliminação ou a supressão intencional e ilegítima de dados informáticos, produzindo dados não autênticos, com a intenção de que estes sejam considerados ou utilizados para fins legais como se fossem autênticos, quer sejam ou não directamente legíveis e inteligíveis. Uma Parte pode exigir no direito interno uma intenção fraudulenta ou uma intenção ilegítima similar para que seja determinada a responsabilidade criminal.

Artigo 8º - Burla informática

Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, em conformidade com o seu direito interno, o acto intencional e ilegítimo, que origine a perda de bens a terceiros através:

a) Da introdução, da alteração, da eliminação ou da supressão de dados informáticos,

b) De qualquer intervenção no funcionamento de um sistema informático, com a intenção de obter um benefício económico ilegítimo para si ou para terceiros.

Título 3 – Infracções relacionadas com o conteúdo

Artigo 9º -Infracções relacionadas com pornografia infantil

1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, em conformidade com o seu direito interno, as seguintes condutas, quando cometidas de forma intencional e ilegítima:

a) Produzir pornografia infantil com o objectivo da sua difusão através de um sistema informático;
b) Oferecer ou disponibilizar pornografia infantil através de um sistema informático;

c) Difundir ou transmitir pornografia infantil através de um sistema informático;

d) Obter pornografia infantil através de um sistema informático para si próprio ou para terceiros;

e) Possuir pornografia infantil num sistema informático ou num meio de armazenamento de dados informáticos.

2. Para efeitos do n.º 1, a expressão "pornografia infantil" inclui qualquer material pornográfico que represente visualmente:

a) Um menor envolvido num comportamento sexualmente explícito;

b) Uma pessoa que aparente ser menor envolvida num comportamento sexualmente explícito;

c) Imagens realísticas que representem um menor envolvido num comportamento sexualmente explícito;

3. Para efeitos do n.º 2, a expressão "menor" inclui qualquer pessoa com idade inferior a 18 anos. Uma Parte, pode, no entanto, exigir um limite de idade inferior, que não será menos que 16 anos.

4. Cada Parte pode reservar-se o direito de não aplicar, no todo ou em parte, o disposto nos n.ºs 1, alínea d), e., 2, alíneas b) e c).

Título 4 – Infracções relacionadas com a violação do direito de autor e direitos conexos

Artigo 10º -Infracções relacionadas com a violação do direito de autor e dos direitos conexos

1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, em conformidade com o seu direito interno, a violação do direito de autor definido pela legislação dessa Parte, em conformidade com as obrigações que a mesma assumiu em aplicação da Convenção Universal sobre o Direito de Autor, revista em Paris, em 24 de Julho de 1971, da Convenção de Berna para a Protecção das Obras Literárias e Artísticas, do Acordo sobre os Aspectos dos Direitos de Propriedade Intelectual Relacionados com o Comércio, e do Tratado da OMPI sobre o Direito de Autor, com excepção de quaisquer direitos morais conferidos por essas Convenções, quando esses actos forem praticados intencionalmente, a uma escala comercial e por meio de um sistema informático.

2. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, em conformidade com o seu direito interno, a violação dos direitos conexos definidos pela legislação dessa Parte, em conformidade com as obrigações assumidas por força da Convenção Internacional para a Protecção dos Artistas Intérpretes ou Executantes, dos Produtores de Fonogramas e dos Organismos de Radiodifusão (Convenção de Roma) do Acordo sobre Aspectos dos Direitos de Propriedade Intelectual Relacionados com o Comércio, e do Tratado da OMPI sobre Interpretações, Execuções e Fonogramas, com excepção de qualquer direito moral conferido por essas Convenções, quando esses actos forem praticados intencionalmente, a uma escala comercial e por meio de um sistema informático.
3. Uma Parte pode, em circunstâncias bem delimitadas, reservar-se o direito de não determinar a responsabilidade penal nos termos dos n.ºs 1 e 2 do presente artigo, na condição

de estarem disponíveis outros meios eficazes e essa reserva não prejudique as obrigações internacionais que incumbem a essa Parte, em aplicação dos instrumentos internacionais mencionados nos n.ºs 1 e 2 do presente artigo.

Título 5 – Outras formas de Responsabilidade e Sanções

Artigo 11º -Tentativa e cumplicidade

1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, em conformidade com o seu direito interno, a cumplicidade, quando cometida intencionalmente, na prática de qualquer uma das infracções estabelecidas de acordo com os artigos 2º a 10º da presente Convenção, com a intenção de que essa infracção seja cometida.

2. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, em conformidade com o seu direito interno, a tentativa de cometer uma das infracções estabelecidas nos artigos 3º, 5º, 7º, 8º, 9º, 1., alínea a) e 9, 1. alínea c) da presente Convenção.

3. Cada Parte pode reservar-se o direito de não aplicar, no todo ou em parte, o disposto no n.º 2 do presente artigo.

Artigo 12º -Responsabilidade de pessoas colectivas

1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para assegurar que as pessoas colectivas possam ser consideradas responsáveis por infracções estabelecidas de acordo com a presente Convenção, quando cometidas em seu benefício por uma pessoa singular agindo quer individualmente, quer como membro de um órgão da pessoa colectiva que exerça no seu seio uma posição de direcção, com base no seguinte:

a) Poder de representação da pessoa colectiva;

b) Autoridade para tomar decisões em nome da pessoa colectiva;

c) Autoridade para exercer controlo no seio da pessoa colectiva.

2. Além dos casos já previstos no n.º 1 deste artigo, cada Parte adoptará as medidas necessárias para assegurar que uma pessoa colectiva possa ser considerada responsável quando a ausência de supervisão ou de controlo por parte de uma pessoa singular, mencionada no n.º 1 tornou possível a prática de infracções previstas na presente Convenção, em benefício da referida pessoa colectiva por uma pessoa singular agindo sob a sua autoridade.

3. De acordo com os princípios jurídicos da Parte, a responsabilidade de uma pessoa colectiva pode ser criminal, civil ou administrativa.

4. Essa responsabilidade deve ser determinada sem prejuízo da responsabilidade criminal das pessoas singulares que cometeram a infracção.

Artigo 13º -Sanções e medidas

1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para assegurar que as infracções penais verificadas em aplicação dos Artigos 2º a 11º sejam passíveis de sanções eficazes, proporcionais e dissuasivas, incluindo penas privativas da liberdade.

2. Cada Parte assegurará que as pessoas colectivas consideradas responsáveis nos termos do artigo 12º, fiquem sujeitas à aplicação de sanções ou medidas, penais ou não penais eficazes, proporcionais e dissuasivas, incluindo sanções pecuniárias.

Secção 2 – Direito Processual

Título 1 – Disposições comuns

Artigo 14º -Âmbito das disposições processuais

1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias, para instituir os poderes e os procedimentos previstos na presente Secção, para fins de investigação ou de procedimento penal.

2. Salvo disposição em contrário constante do artigo 21º, cada Parte aplicará os poderes e procedimentos referidos no n.º 1:

a) Às infracções penais em conformidade com o disposto nos artigos 2º a 11º da presente Convenção;

b) A outras infracções penais cometidas por meio de um sistema informático; e

c) À recolha de prova em suporte electrónico provas electrónicas de qualquer infracção penal.

3. (a) Cada Parte pode reservar-se o direito de apenas aplicar as medidas referidas no artigo 20º às infracções ou categorias de infracções especificadas na reserva, desde que o conjunto dessas infracções ou categorias de infracções não seja mais reduzido do que o conjunto de infracções às quais aplica as medidas referidas no artigo 21º. Cada Parte procurará limitar essa reserva de modo a permitir a aplicação mais ampla possível da medida referida no Artigo 20º.

b) Nos casos em que uma Parte, devido a restrições impostas pela sua legislação em vigor no momento da adopção da presente Convenção, não puder aplicar as medidas referidas nos Artigos 20º e 21º às comunicações transmitidas num sistema informático de um fornecedor de serviços, que:

i. Esteja em funcionamento para benefício de um grupo fechado de utilizadores, e

ii. Não utilize redes públicas de telecomunicações e não esteja em conexão com outro sistema informático, quer seja público ou privado, essa Parte pode reservar-se o direito de não aplicar essas medidas às referidas comunicações. Cada Parte procurará limitar essa reserva de modo a permitir a aplicação mais ampla possível das medidas referidas
nos Artigos 20º e 21º.

Artigo 15º -Condições e salvaguardas

1. Cada Parte assegurará que o estabelecimento, a entrada em vigor e a aplicação dos poderes e procedimentos previstos na presente Secção são sujeitos às condições e salvaguardas estabelecidas pela legislação nacional, que deve assegurar uma protecção adequada dos direitos do Homem e das liberdades, designadamente estabelecidas em conformidade com as obrigações decorrentes da aplicação da Convenção do Conselho da Europa para a Protecção dos Direitos do Homem e das Liberdades Fundamentais dos Cidadãos (1950), do Pacto Internacional das Nações Unidas sobre os Direitos Civis e Políticos, (1966), bem como de outros instrumentos internacionais aplicáveis relativos aos Direitos do Homem e que deve integrar o princípio da proporcionalidade.

2. Quando for apropriado, tendo em conta a natureza do poder ou do procedimento em questão, as referidas condições e salvaguardas incluirão, designadamente, um controlo judicial ou outras formas de controlo independente, os fundamentos que justificam a sua aplicação, bem como a limitação do âmbito de aplicação e a duração do poder ou procedimento em causa.

3. Na medida em que seja do interesse público, em particular da boa administração da justiça, cada Parte examinará o efeito dos poderes e dos procedimentos da presente Secção sobre os direitos, responsabilidades e interesses legítimos de terceiros.

Título 2 – Conservação expedita de dados informáticos armazenados

Artigo 16º -Conservação expedita de dados informáticos armazenados

1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para permitir às suas autoridades competentes exigir ou obter de uma outra forma a conservação expedita de dados informáticos específicos, incluindo dados relativos ao tráfego, armazenados por meio de um sistema informático, nomeadamente nos casos em que existem motivos para pensar que os mesmos são susceptíveis de perda ou alteração.

2. Sempre que a Parte aplique o disposto no n.º 1, através de uma injunção ordenando a uma pessoa que conserve os dados informáticos específicos armazenados que estão na sua posse ou sob o seu controlo, esta Parte adoptará as medidas legislativas e outras que se revelem necessárias para obrigar essa pessoa a conservar e proteger a integridade dos referidos dados durante um período de tempo tão longo quanto necessário, até um máximo de 90 dias, de modo a permitir às autoridades competentes obter a sua divulgação. Uma Parte pode prever que essa injunção seja subsequentemente renovada.

3. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para obrigar o responsável pelos dados, ou outra pessoa encarregada de os conservar a manter segredo sobre a execução dos referidos procedimentos durante o período previsto pelo seu direito interno.
4. Os poderes e procedimentos referidos no presente artigo devem estar sujeitos aos artigos 14º e 15º.

Artigo 17º -Conservação expedita e divulgação parcial de dados de tráfego

1. A fim de assegurar a conservação de dados relativos ao trafego em aplicação do artigo 16º, cada Parte adoptará as medidas legislativas e outras que se revelem necessárias, para:

a) Assegurar a conservação rápida desses dados de tráfego, quer tenham participado na transmissão dessa comunicação um ou vários fornecedores de serviços; e

b) Assegurar a divulgação rápida à autoridade competente da Parte ou a uma pessoa designada por essa autoridade, de uma quantidade de dados de tráfego, suficiente para permitir a identificação dos fornecedores de serviços e da via através do qual a comunicação foi efectuada.

2. Os poderes e procedimentos referidos no presente artigo devem estar sujeitos aos artigos 14º e 15º.

Título 3 – Injunção

Artigo 18º -Injunção

1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para habilitar as suas autoridades competentes para ordenar:

a) A uma pessoa que se encontre no seu território que comunique os dados informáticos específicos, na sua posse ou sob o seu controlo e armazenados num sistema informático ou num outro suporte de armazenamento de dados informáticos; e

b) A um fornecedor de serviços que preste serviços no território da Parte, que comunique os dados na sua posse ou sob o seu controlo, relativos aos assinantes e respeitantes a esses serviços;

2. Os poderes e procedimentos referidos no presente artigo devem estar sujeitos aos artigos 14º e 15º.

3. Para os fins do presente artigo, a expressão "dados relativos aos assinantes" designa qualquer informação, contida sob a forma de dados informáticos ou sob qualquer outra forma, detida por um fornecedor de serviços e que diga respeito aos assinantes dos seus serviços, diferentes dos dados relativos ao tráfego ou ao conteúdo e que permitam determinar:

a) O tipo de serviço de comunicação utilizado, as medidas técnicas tomadas a esse respeito e o período de serviço;

b) A identidade, a morada postal ou geográfica e o número de telefone do assinante, e qualquer outro número de acesso, os dados respeitantes à facturação e ao pagamento, disponíveis com base num contrato ou acordo de serviços;
c) Qualquer outra informação sobre a localização do equipamento de comunicação, disponível com base num contrato ou acordo de serviços.

Título 4 – Busca e Apreensão de dados informáticos armazenados

Artigo 19º -Busca e apreensão de dados informáticos armazenados

1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para habilitar as suas autoridades competentes para proceder a buscas ou aceder de modo semelhante:

a) A um sistema informático ou a uma parte do mesmo, bem como a dados informáticos que nele se encontrem armazenados; e

b) A um suporte que permita armazenar dados informáticos.

2. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para assegurar que, nos casos em que as suas autoridades procedam a buscas ou acedam de forma semelhante a um sistema informático específico ou a uma parte do mesmo, em conformidade com o disposto no n.º 1, a), e tenham razões para pensar que os dados procurados se encontram armazenados noutro sistema informático ou numa parte do mesmo situado no seu território, e que esses dados são legalmente acessíveis a partir do sistema inicial ou obteníveis a partir desse sistema inicial, as referidas autoridades estejam em condições de estender de forma expedita a busca, ou o acesso de forma semelhante ao outro sistema.

3. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para habilitar as suas autoridades competentes para apreender ou para obter de forma semelhante os dados informáticos relativamente aos quais o acesso foi realizado em aplicação dos n.ºs 1 ou 2. Essas medidas incluem as prerrogativas seguintes:

a) Apreender ou obter de forma semelhante um sistema informático ou uma parte deste ou um suporte de armazenamento informático;

b) Realizar e conservar uma cópia desses dados informáticos;

c) Preservar a integridade dos dados informáticos pertinentes armazenados; e

d) Tornar inacessíveis ou eliminar esses dados do sistema informático acedido.

4. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para habilitar as suas autoridades competentes a ordenar a qualquer pessoa que conheça o funcionamento do sistema informático ou as medidas utilizadas para proteger os dados informáticos nele contidos, que forneça na medida do razoável as informações razoavelmente necessárias, para permitir a aplicação das medidas previstas nos n.ºs 1 e 2.

5. Os poderes e procedimentos referidos no presente artigos devem estar sujeitos aos artigos 14º e 15º.

Título 5 – Recolha em tempo real de dados informáticos

Artigo 20º -Recolha em tempo real de dados relativos ao tráfego

1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para habilitar as suas autoridades competentes a:

a) Recolher ou registar, através da aplicação de meios técnicos existentes no seu território, e

b) Obrigar um fornecedor de serviços, no âmbito da sua capacidade técnica existente, a:

i. Recolher ou registar por meio da aplicação de meios técnicos no seu território, ou

ii. Prestar às autoridades competentes o seu apoio e assistência para recolher ou registar, em tempo real, dados de tráfego relativos a comunicações específicas no seu território transmitidas através de um sistema informático.

2. Quando uma Parte, em virtude dos princípios estabelecidos pela sua ordem jurídica interna, não pode adoptar as medidas descritas no nº. 1, alínea a), pode, em alternativa, adoptar as medidas legislativas e outras que se revelem necessárias para assegurar a recolha ou o registo em tempo real dos dados de tráfego associados a comunicações específicas transmitidas no seu território através da aplicação de meios técnicos existentes nesse território.

3. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para obrigar um fornecedor de serviços a manter secreto o facto de qualquer um dos poderes previstos ter sido executado, bem como qualquer informação a esse respeito.

4. Os poderes e procedimentos referidos no presente artigo devem estar sujeitos aos artigos 14º e 15º.

Artigo 21º -Intercepção de dados relativos ao conteúdo

1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para habilitar as suas autoridades competentes relativamente a um leque de infracções graves, a definir em direito interno, a:

a) Recolher ou registar, através da aplicação de meios técnicos existentes no seu território, e

b) Obrigar um fornecedor de serviços, no âmbito da sua capacidade técnica existente, a:

i. Recolher ou registar através da aplicação de meios técnicos no seu território, ou

ii. Prestar às autoridades competentes o seu apoio e a sua assistência para recolher ou registar, em tempo real, dados relativos ao conteúdo de comunicações específicas no seu território, transmitidas através de um sistema informático.

2. Quando a Parte em virtude dos princípios estabelecidos pela sua ordem jurídica interna, não pode adoptar as medidas descritas no n.º 1, alínea a), pode, em alternativa, adoptar as medidas legislativas e outras que se revelem necessárias, para assegurar a recolha ou o registo em tempo real dos dados relativos ao conteúdo associados a comunicações específicas transmitidas no seu território através da aplicação de meios técnicos existentes nesse território.

3. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias, para obrigar um fornecedor de serviços a manter secreto o facto de qualquer um dos poderes previstos no presente artigo ter sido executado, bem como qualquer informação a esse respeito.

4. Os poderes e procedimentos referidos no presente artigo devem estar sujeitos aos artigos 14º e 15º.

Secção 3 – Competência

Artigo 22º -Competência

1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer a sua competência relativamente a qualquer infracção penal definida em conformidade com os artigos 2º a 11º da presente Convenção, sempre que a infracção seja cometida:

a) No seu território; ou

b) A bordo de um navio arvorando o pavilhão dessa Parte;

c) A bordo de uma aeronave matriculada nessa Parte e segundo as suas Leis; ou

d) Por um dos seus cidadãos nacionais, se a infracção for punível criminalmente onde foi cometida ou se a infracção não for da competência territorial de nenhum Estado.

2. Cada Parte pode reservar-se o direito de não aplicar ou de apenas aplicar em casos ou em condições específicas, as regras de competência definidas no n.º1, alínea b) a alínea d) do presente artigo ou em qualquer parte dessas alíneas.

3. Cada Parte adoptará as medidas que se revelem necessárias para estabelecer a sua competência relativamente a qualquer infracção referida no artigo 24º, n.º1 da presente Convenção, quando o presumível autor da infracção se encontre no seu território e não puder ser extraditado para outra Parte, apenas com base na sua nacionalidade, após um pedido de extradição.

4. A presente Convenção não exclui qualquer competência penal exercida por uma Parte em conformidade com o seu direito interno.

5. Quando mais que uma Parte reivindique a competência em relação uma presumível infracção prevista na presente Convenção, as Partes em causa, se for oportuno, consultar-se-ão a fim de determinarem qual é a jurisdição mais apropriada para o procedimento penal.

Capítulo III – Cooperação Internacional

Secção 1 – Princípios gerais

Título 1 – Princípios gerais relativos à cooperação internacional

Artigo 23º -Princípios gerais relativos à cooperação internacional

As Partes cooperarão entre si, em conformidade com as disposições do presente capítulo, em aplicação dos instrumentos internacionais pertinentes sobre a cooperação internacional em matéria penal, de acordos celebrados com base nas legislações uniformes ou reciprocas, e do seu direito nacional, na medida mais ampla possível, para efeitos de investigações ou de procedimentos relativos a infracções penais relacionadas com sistemas e dados informáticos, ou para recolher provas sob a forma electrónica de uma infracção penal.

Título 2 – Princípios relativos à extradição

Artigo 24º -Extradição

1. a) O presente artigo aplica-se à extradição entre as Partes relativamente a infracções penais definidas em conformidade com os artigos 2º a 11º da presente Convenção, desde que sejam puníveis na legislação de duas Partes envolvidas, por uma pena privativa de liberdade por um período máximo de, pelo menos um ano ou através de uma pena mais grave.

b) Quando for exigida uma pena mínima diferente, com base num tratado de extradição aplicável entre duas ou mais Partes, incluindo a Convenção Europeia de Extradição (STE Nº 24), ou num acordo baseado em legislações uniformes ou recíprocas, é a pena mínima prevista por esse tratado ou acordo que se aplica.

2. As infracções penais descritas no n.º 1 do presente artigo são consideradas como infracções passíveis de extradição em qualquer tratado de extradição existente ou que venha a existir entre as Partes. As Partes comprometer-se-ão a incluir essas infracções como infracções passíveis de extradição em qualquer tratado de extradição que possa ser firmado entre as Partes.

3. Quando uma Parte condicionar a extradição à existência de um tratado e receba um pedido de extradição de outra Parte com a qual não tenha celebrado qualquer tratado de extradição, pode considerar a presente Convenção como base jurídica para a extradição relativamente a qualquer infracção penal referida no n.º 1 do presente artigo.

4. As Partes que não condicionem a extradição à existência de um tratado, reconhecerão entre si as infracções penais referidas no n.º 1 do presente artigo como infracções passíveis de extradição.

5. A extradição ficará sujeita às condições previstas pelo direito interno da Parte requerida ou pelos tratados de extradição aplicáveis, incluindo os fundamentos com base nos quais a Parte requerida pode recusar a extradição.

6. No caso de a extradição por uma infracção penal mencionada no n.º 1 do presente artigo ser recusada unicamente com base na nacionalidade da pessoa procurada, ou pelo facto de a Parte requerida se considerar competente relativamente a essa infracção, a Parte requerida remeterá o processo, a pedido da Parte requerente, às suas autoridades competentes para fins de procedimento criminal e comunicará em tempo útil o resultado do processo à Parte requerente. As autoridades em questão tomarão a sua decisão e conduzirão a investigação e o procedimento do mesmo modo que em relação a qualquer outra infracção de natureza comparável, em conformidade com a legislação desta Parte.

7. a) Cada Parte comunicará ao Secretário Geral do Conselho da Europa, no momento da assinatura ou do depósito do seu instrumento de ratificação, aceitação, aprovação ou adesão, o nome e morada de cada autoridade responsável pelo envio ou pela recepção de um pedido de extradição ou de detenção preventiva, no caso de ausência de tratado.

b) O Secretário Geral do Conselho da Europa constituirá e manterá actualizado um registo das autoridades assim designadas pelas Partes. Cada Parte deve assegurar com permanência a exactidão dos dados que constam do registo.

Título 3 – Princípios Gerais relativos ao auxílio mútuo .

Artigo 25º -Princípios gerais relativos ao auxílio mútuo.

1. As Partes concederão entre si o auxílio mútuo mais amplo possível para efeitos de investigações ou de procedimentos relativos a infracções penais relacionadas com sistemas e dados informáticos, ou para efeitos de recolha de provas sob a forma electrónica de uma infracção penal.

2. Cada Parte adoptará igualmente as medidas legislativas e outras que se revelem necessárias para darem cumprimento às obrigações estabelecidas nos artigos 27º a 35º.

3. Em caso de urgência, cada Parte pode formular os pedidos de auxílio mútuo ou comunicações com ele relacionadas, através de meios de comunicação rápidos, tais como o fax ou o correio electrónico, desde que esses meios ofereçam condições de segurança e de autenticação (incluindo, se necessário, o uso da encriptação) com posterior confirmação oficial sempre que o Estado requerido o exigir. O Estado requerido aceitará o pedido e responderá através de qualquer desses meios de comunicação rápidos.

4. Salvo disposição em contrário expressamente prevista nos artigos do presente Capítulo, o auxílio mútuo será sujeito às condições fixadas pelo direito interno da Parte requerida ou pelos tratados de auxílio mútuo aplicáveis, incluindo os fundamentos com base nos quais a Parte requerida pode recusar a cooperação. A Parte requerida não deve exercer o seu direito de recusar o auxílio mútuo relativamente às infracções previstas nos artigos 2º a 11º apenas com fundamento em que o pedido se refere a uma infracção que considera ser de natureza fiscal.

5. Quando em conformidade com as disposições do presente capítulo, a Parte requerida estiver autorizada a subordinar o auxílio mútuo à existência de dupla incriminação, esta condição será considerada como satisfeita se o comportamento que constitui a infracção relativamente à qual foi efectuado o pedido de auxílio, for qualificado como infracção penal pelo seu direito interno, quer o direito interno classifique ou não a infracção na mesma categoria de infracções ou a designe ou não pela mesma terminologia que o direito da Parte requerente.

Artigo 26º -Informação espontânea

1. Uma Parte pode, dentro dos limites da sua legislação nacional e na ausência de pedido prévio, comunicar a outra Parte informações obtidas no quadro das suas próprias investigações, sempre que considerar que isso pode ajudar a Parte destinatária a iniciar ou a levar a cabo investigações ou procedimentos relativos a infracções penais, estabelecidas em conformidade com a presente Convenção, ou sempre que essas informações possam conduzir a um pedido formulado por essa Parte, nos termos do presente Capítulo.

2. Antes de comunicar essas informações, a Parte que as fornece pode solicitar que as mesmas permaneçam confidenciais ou apenas sejam utilizadas em determinadas condições. Caso a Parte destinatária não puder dar satisfação a esse pedido, deve informar a outra Parte desse facto que determinará se as informações devem contudo ser fornecidas. Se a Parte destinatária aceitar a informação nas condições estipuladas, fica obrigada a observar essas condições. Título 4 – Procedimentos relativos aos pedidos de auxílio mútuo na ausência de acordos internacionais aplicáveis

Artigo 27º -Procedimentos relativos aos pedidos de auxílio mútuo na ausência de acordos internacionais aplicáveis

1. Na ausência de tratado de auxílio mútuo ou de acordo de que se baseie em legislação uniforme ou recíproca em vigor entre a Parte requerente e a Parte requerida, serão aplicáveis as disposições dos n.ºs 2 a 9 do presente artigo. Não serão aplicáveis se existir um tratado, um acordo, ou legislação deste tipo, a menos que as Partes em causa decidam aplicar em sua substituição o presente artigo no todo ou em parte.

2. a) Cada Parte designará uma ou mais autoridades centrais encarregadas de enviar os pedidos de auxílio mútuo ou de lhes responder, de os executar ou de os transmitir às autoridades competentes para a sua execução;

b) As autoridades centrais comunicarão directamente entre si;

c) Cada Parte, no momento da assinatura ou do depósito dos seus instrumentos de ratificação, aceitação, aprovação ou adesão, comunicará ao Secretário Geral do Conselho da Europa os nomes e moradas das autoridades designadas em aplicação do presente parágrafo.

d) O Secretário Geral do Conselho da Europa constituirá e manterá actualizado um registo das autoridades centrais designadas pelas Partes. Cada Parte assegurará em permanência a exactidão dos dados constantes do registo.

3. Os pedidos de auxílio ao abrigo do presente artigo serão executados em conformidade com os procedimentos especificados pela Parte requerente, excepto se forem incompatíveis com a legislação da Parte requerida.
4. Além das condições ou fundamentos de recusa previstos no artigo 25º, n.º 4, o auxílio pode ser recusado pela Parte requerida:

a) Se o pedido respeitar a infracções consideradas pela Parte requerida como infracções políticas ou com elas conexas; ou

b) Se a Parte considerar que o cumprimento do pedido pode atentar contra a sua soberania, segurança, ordem pública ou qualquer outro interesse essencial do seu país.

5. A Parte requerida pode adiar a execução de um pedido, se isso puder prejudicar as investigações criminais ou os procedimentos levados a cabo pelas suas autoridades.

6. Antes de recusar ou adiar a cooperação, a Parte requerida examinará após ter consultado, se for caso disso, a Parte requerente, se pode satisfazer o pedido no todo ou em parte ou sujeitá-lo às condições que considere necessárias.

7. A Parte requerida informará rapidamente a Parte requerente do seguimento que entende dar ao pedido de auxílio mútuo. Deve ser fundamentada a eventual recusa ou adiamento do pedido. A Parte requerida informará igualmente a Parte requerente de qualquer fundamento que torne impossível a execução do pedido ou que seja susceptível de o retardar significativamente.

8. A Parte requerente pode solicitar que a Parte requerida mantenha confidenciais os factos e o objecto de qualquer pedido formulado ao abrigo do presente Capítulo, excepto na medida

necessária à execução do referido pedido. Se a Parte requerida não puder dar satisfação a esse pedido de confidencialidade, deve informar prontamente a Parte requerente, a qual determinará então se o pedido deve contudo ser executado.

9. a) Em caso de urgência, as autoridades judiciárias da Parte requerente podem enviar directamente às suas homólogas da Parte requerida os pedidos de auxílio mútuo ou as comunicações que lhes digam respeito. Nesses casos, uma cópia será dirigida às autoridades centrais da Parte requerida por intermédio da autoridade central da Parte requerente.

c) Qualquer pedido ou comunicação ao abrigo do presente parágrafo pode ser efectuado através da Organização Internacional de Polícia Criminal (Interpol).

d) Quando um pedido tiver sido efectuado em aplicação da alínea a) do presente parágrafo e a autoridade não for competente para o tratar, transmiti-lo-á à autoridade nacional competente e informará desse facto directamente a Parte requerente.

e) Os pedidos ou comunicações efectuados em aplicação do presente parágrafo, que não impliquem uma acção coerciva, podem ser directamente transmitidos pelas autoridades competentes da Parte requerente às autoridades competentes da Parte requerida.

f) Cada Parte pode informar o Secretário Geral do Conselho da Europa, no momento da assinatura ou do depósito do seu instrumento de ratificação, aceitação, aprovação ou adesão que, por razões de eficácia, os pedidos efectuados em conformidade com o presente número devem ser dirigidos à sua autoridade central.

Artigo 28º -Confidencialidade e restrição de utilização

1. Na ausência de tratados ou acordos de auxílio judiciário mútuo celebrados com base em legislações uniformes ou recíprocas em vigor entre a Parte requerente e a Parte requerida, serão aplicáveis as disposições do presente Artigo. Estas não serão aplicáveis quando exista um tratado, um acordo ou legislação daquele tipo, excepto se as Partes envolvidas decidirem aplicar em sua substituição o presente Artigo no todo ou em parte.

2. A Parte requerida pode sujeitar a comunicação da informação ou de material em resposta a um pedido à condição de que:

a) Seja mantida confidencial quando o pedido de auxílio judiciário mútuo não puder ser satisfeito na ausência dessa condição, ou

b) Não seja utilizada para fins de outra investigação ou de procedimento diferente dos indicados no pedido.

3. Se a Parte requerente não puder satisfazer uma das condições mencionadas no n.º 2, informará prontamente a Parte requerida, a qual determinará então se a informação deve, ainda assim, ser fornecida. Se a Parte requerente aceitar esta condição, ficará vinculada pela mesma.

4. Qualquer Parte que forneça informações ou material sujeita a uma das condições referidas no n.º2, pode exigir à outra Parte que lhe forneça esclarecimentos relativos a essa condição, quanto à utilização dessa informação ou desse material.

Secção 2 – Disposições específicas

Título 1 – Auxílio mútuo em matéria de medidas provisórias

Artigo 29º -Conservação expedita de dados informáticos armazenados

1. Uma Parte pode pedir a outra Parte que ordene ou obtenha de outra forma a conservação rápida dos dados armazenados por meio de um sistema informático, que se encontre no território dessa outra Parte, e relativamente aos quais a Parte requerente pretenda apresentar um pedido de auxílio mútuo para fins de busca ou de acesso similar, apreensão ou obtenção por meio similar, ou divulgação dos dados.

2. Um pedido de conservação efectuado nos termos do n.º 1 deve especificar:

a) A autoridade que pede a conservação;

b) A infracção que é objecto de investigação criminal ou de procedimento e uma breve exposição dos factos relacionados;

c) Os dados informáticos armazenados a conservar e a sua relação com a infracção;

d) Todas as informações disponíveis que permitam identificar o responsável pelos dados informáticos armazenados ou a localização do sistema informático;

e) A necessidade da medida de conservação; e

f) Que a Parte tenciona apresentar um pedido de assistência mútua com vista à busca ou outra forma de acesso, apreensão ou obtenção semelhante, ou divulgação dos dados informáticos armazenados.

3. Após ter recebido o pedido de outra Parte, a Parte requerida deve tomar as medidas apropriadas a fim de proceder, de forma expedita, à conservação dos dados especificados, em conformidade com o seu direito interno. Para poder responder a esse pedido, a dupla incriminação não é exigida como condição prévia à conservação.

4. Uma Parte que exija a dupla incriminação como condição necessária para responder a um pedido de auxílio mútuo para fins de busca ou acesso semelhante, apreensão ou obtenção por meio semelhante, ou a divulgação dos dados, pode, no que diz respeito a outras infracções diferentes das estabelecidas em conformidade com os artigos 2º a 11º da presente Convenção, reservar-se o direito de recusar o pedido de conservação ao abrigo do presente artigo, se tiver razões para crer que no momento da divulgação, a condição de dupla incriminação não pode ser preenchida.

5. Além disso, um pedido de conservação só pode ser recusado se:

a) O pedido respeitar a infracções consideradas pela Parte requerida como infracções políticas ou com elas conexas; ou

b) A Parte requerida considerar que o cumprimento do pedido pode atentar contra a sua soberania, segurança, ordem pública ou qualquer outro interesse essencial.

6. Quando a Parte requerida considerar que a simples conservação não é suficiente para garantir a disponibilidade futura dos dados, e comprometerá a confidencialidade da investigação da Parte requerente, ou prejudica de outra forma a mesma, informará prontamente disso a Parte requerente que decidirá, então, se o pedido deve, ainda assim, ser executado.

7. Qualquer conservação efectuada em resposta a um pedido referido no n.º 1 será válida por um período não inferior a 60 dias, a fim de permitir à Parte requerente apresentar um pedido para fins de busca ou acesso semelhante, apreensão ou obtenção semelhante, ou divulgação dos dados. Após a recepção desse pedido, os dados devem continuar a ser conservados até à adopção de uma decisão respeitante ao pedido.

Artigo 30º -Divulgação expedita dos dados de tráfego conservados

1. Se ao executar um pedido de conservação de dados relativos ao tráfego relacionados com uma comunicação específica efectuada em aplicação do artigo 29º, a Parte requerida descobrir que um fornecedor de serviços noutro Estado participou na transmissão dessa comunicação, a Parte requerida divulgará rapidamente à Parte requerente uma quantidade suficiente de dados relativos ao tráfego que permita identificar esse fornecedor de serviços e a via através da qual a comunicação foi transmitida.

2. A divulgação de dados de tráfego nos termos do disposto no n.º 1 apenas pode ser recusada se:

a) Se o pedido respeitar a uma infracção considerada pela Parte requerida como infracção de natureza política ou com ela conexa; ou

b) Se a Parte requerida considerar que o cumprimento do pedido pode atentar contra a sua soberania, segurança, ordem pública ou qualquer outro interesse essencial.

Título 2 – Auxílio mútuo relativamente a poderes de investigação

Artigo 31º -Auxílio mútuo relativamente ao acesso a dados informáticos armazenados

1. Uma Parte pode pedir a outra Parte para investigar ou aceder de forma semelhante, apreender, ou obter de forma semelhante, e divulgar dados armazenados por meio de sistema informático que se encontre no território dessa outra Parte, incluindo os dados conservados em conformidade com o artigo 29º.

2. A Parte requerida dará satisfação ao pedido aplicando os instrumentos internacionais, acordos e legislação referida no artigo 23º, e dando cumprimento às disposições pertinentes do presente Capítulo.

3. O pedido deve ser satisfeito o mais rapidamente possível nos casos em que:

a) Existam motivos para crer que os dados relevantes são especialmente vulneráveis à perda ou modificação; ou

b) Os instrumentos, acordos e legislação referida no n.º 2 prevejam uma cooperação rápida.

Artigo 32º - Acesso transfronteiríço a dados informáticos armazenados, com consentimento ou quando são acessíveis ao público Uma Parte pode, sem autorização de outra Parte:

a) Aceder a dados informáticos armazenados acessíveis ao público (fonte aberta), seja qual for a localização geográfica desses dados; ou

b) aceder ou receber, através de um sistema informático situado no seu território, dados informáticos armazenados situados no território de outra Parte, se obtiver o consentimento legal e voluntário da pessoa legalmente autorizada a divulgar esses dados, através deste sistema informático.

Artigo 33º -Auxílio mútuo relativamente à recolha de dados de tráfego em tempo real

1. As Partes concederão entre si o auxílio mútuo no que diz respeito à recolha, em tempo real, de dados de tráfego associados a comunicações específicas transmitidas no seu território por meio de um sistema informático. Sem prejuízo do disposto no n.º2, esse auxílio regular-se-à pelas condições e procedimentos previstos em direito interno.

2. Cada Parte concederá o auxílio pelo menos no que diz respeito às infracções penais relativamente às quais seria possível a recolha ao nível interno a recolha em tempo real dos dados de tráfego em caso semelhante. Artigo 34º -Auxílio mútuo em matéria de intercepção de dados de conteúdo As Partes concederão auxílio judiciário mútuo, na medida em que é permitido pelos tratados e pelas legislações aplicáveis no que diz respeito à recolha ou ao registo, em tempo real, de dados relativos ao conteúdo de comunicações específicas transmitidas por meio de um sistema informático.

Título 3 - Rede 24/7

Artigo 35º - Rede 24/7

1. Cada Parte designará um ponto de contacto disponível 24 horas sobre 24 horas, 7 dias por semana, a fim de assegurar a prestação de assistência imediata a investigações ou procedimentos respeitantes a infracções penais relacionadas com dados e sistemas informáticos, ou a fim de recolher provas, sob forma electrónica, de uma infracção penal. O auxílio incluirá a facilitação, ou se o direito e práticas internas o permitirem, a aplicação directa das seguintes medidas:

a) A prestação de aconselhamento técnico;

b) A conservação de dados em conformidade com os artigos 29º e 30º; e

c) A recolha de provas, informações de carácter jurídico e localização de suspeitos.

2. a) O ponto de contacto de uma Parte deve ter capacidade técnica para corresponder-se com o ponto de contacto de outra Parte de uma forma rápida;

b) Se o ponto de contacto designado por uma Parte não depender da autoridade ou autoridades dessa Parte responsáveis pela cooperação internacional ou extradição dessa Parte, o ponto de contacto assegurará que pode agir em coordenação com essa ou essas autoridades de forma rápida.

3. Cada Parte assegurará que pode dispor de pessoal formado e equipado a fim de facilitar o funcionamento da rede.

Capítulo IV – Disposições Finais

Artigo 36º -Assinatura e entrada em vigor

1. A presente Convenção está aberta à assinatura dos Estados membros do Conselho da Europa e dos Estados não membros que participaram na elaboração da mesma.

2. A presente Convenção é submetida a ratificação, aceitação ou aprovação. Os instrumentos de ratificação, aceitação ou aprovação serão depositados junto do Secretário Geral do Conselho da Europa.

3. A presente Convenção entrará em vigor no primeiro dia do mês seguinte ao termo de um período de três meses após a data na qual cinco Estados, incluindo pelo menos três Estados membros do Conselho da Europa, tenham manifestado o seu consentimento em ficar vinculados pela Convenção, em conformidade com as disposições dos n.ºs 1 e 2.

4. Em relação a qualquer Estado signatário que posteriormente exprima o seu consentimento em vincular-se à Convenção, esta entrará em vigor no primeiro dia do mês seguinte ao termo de um período de três meses após a data em que tenha sido expresso o seu consentimento em vincular-se à Convenção, em conformidade com as disposições dos n.ºs 1 e 2.

Artigo 37º -Adesão à Convenção

1. Após a entrada em vigor da presente Convenção, o Comité de Ministros do Conselho da Europa pode, depois de ter consultado os Estados contratantes da Convenção e de ter obtido o acordo unânime, convidar qualquer Estado não membro do Conselho e que não tenha participado na sua elaboração, a aderir à presente Convenção. A decisão é tomada pela maioria prevista no artigo 20º, alínea d), dos Estatutos do Conselho da Europa e por unanimidade dos representantes dos Estados contratantes com direito de voto no Comité de Ministros.

2. Em relação a qualquer Estado aderente à Convenção, em conformidade com o n.º 1, a Convenção entrará em vigor no primeiro dia do mês seguinte ao termo de um período de três meses após a data do depósito do instrumento de adesão junto do Secretário Geral do Conselho da Europa.

Artigo 38º -Aplicação territorial

1. Qualquer Estado pode, no momento da assinatura ou no momento do depósito do seu instrumento de ratificação, aceitação, aprovação ou adesão, designar o, ou os territórios aos quais se aplicará a presente Convenção.

2. Qualquer Estado pode, em qualquer momento posterior, mediante declaração dirigida ao Secretário Geral do Conselho da Europa, tornar extensível a aplicação da presente Convenção a qualquer outro território designado na declaração. A Convenção entrará em vigor em relação a esse território no primeiro dia do mês seguinte ao termo de um período de três meses após a data de recepção da declaração pelo Secretário Geral.

3. Qualquer declaração feita nos termos dos dois parágrafos anteriores pode ser retirada, no que diz respeito a qualquer território designado na declaração, mediante notificação dirigida ao Secretário Geral do Conselho da Europa. Essa declaração produzirá efeitos no primeiro dia do mês seguinte ao termo de um período de três meses após a data de recepção da referida notificação pelo Secretário Geral.

Artigo 39º -Efeitos da Convenção

1. O objectivo da presente Convenção é complementar os tratados ou acordos multilaterais ou bilaterais aplicáveis existentes entre as Partes, incluindo as disposições:

- Da Convenção Europeia de Extradição, aberta para assinatura em Paris a 13 de Dezembro de 1957 (STE Nº 24);

- Da Convenção Europeia de Auxílio Mútuo em Matéria Penal, aberta para assinatura em Estrasburgo, a 20 de Abril de 1959 (STE n.º 30);

- Do Protocolo Adicional à Convenção Europeia de Auxílio Mutuo em Matéria Penal, aberta para assinatura em Estrasburgo, a 17 de Março de 1978 (STE n.º 99).

2. Se duas ou mais Partes tiverem já celebrado um acordo ou tratado relativo às matérias tratadas pela presente Convenção ou se, de outra forma, tiverem estabelecido relações a este respeito, ou se vierem a fazê-lo no futuro, terão a possibilidade de aplicar o referido acordo ou tratado ou estabelecer essas relações em substituição da presente Convenção. Todavia, sempre que as Partes estabeleçam relações respeitantes a matérias objecto da presente Convenção de forma diferente daquela que é prevista pela mesma, fa-lo-ão de uma forma que não seja incompatível com os princípios e objectivos da presente Convenção.

3. Nada na Convenção prejudicará outros direitos, restrições, obrigações e responsabilidades de uma Parte.

Artigo 40º -Declarações

Qualquer Estado pode, mediante notificação por escrito dirigida ao Secretário Geral do Conselho da Europa no acto da assinatura ou do depósito do seu instrumento de ratificação, aceitação, aprovação ou adesão, declarar que fará uso da faculdade de exigir, se for caso disso, um ou mais elementos suplementares, tal como previsto nos artigos 2º, 3º, 6º, n.º 1, alínea b), 7º, 9º, n.º 3 e 27º, n.º 9, alínea e).

Artigo 41º -Cláusula federal

1. Um Estado federal pode reservar-se o direito de assumir as obrigações nos termos do capítulo II da presente Convenção na medida em que sejam compatíveis com os princípios fundamentais que governam as relações entre o seu Governo central e os Estados federados,

ou outras entidades territoriais análogas, desde que esteja em condições de cooperar com base no Capítulo III.

2. Quando tiver feito uma reserva prevista no n.º1, não pode utilizar essa reserva para excluir ou diminuir de forma substancial as suas obrigações nos termos do Capítulo II. Em qualquer caso, dotar-se-á de meios amplos e eficazes que permitam a aplicação das medidas previstas no referido capítulo.

3. No que se refere às disposições da presente Convenção, cuja execução seja da competência legislativa dos Estados federados ou de outras entidades territoriais análogas que não são, nos termos do sistema constitucional da federação obrigados a tomar medidas legislativas, o governo federal levará com parecer favorável as referidas disposições ao conhecimento das autoridades competentes dos Estados federais incitando-os a adoptar as medidas adequadas para as executar.

Artigo 42º -Reservas

Qualquer Estado pode, mediante notificação por escrito dirigida ao Secretário Geral do Conselho da Europa no momento da assinatura ou do depósito do seu instrumento de ratificação, aceitação, aprovação ou adesão, declarar a sua intenção de fazer uso da(s) reserva(s) previstas nos artigos 4º, n.º 2, 6º, n.º 3, 9º, n.º 4, 10º, n.º 3, 11º, n.º 3, 14º, n.º 3, 22º, n.º 2, 29º, n.º 4, e 41, n.º 1. Nenhuma outra reserva poderá ser formulada.

Artigo 43º -Estatuto e levantamento das reservas

1. Uma Parte que tenha formulado uma reserva em conformidade com o artigo 42º pode retirá-la no todo ou em parte, mediante notificação dirigida ao Secretário- Geral do Conselho da Europa. A declaração produzirá efeitos na data de recepção da referida notificação pelo Secretário Geral. Se a notificação indicar que o levantamento da reserva deve produzir efeitos numa data precisa e essa data for posterior à da recepção da notificação pelo Secretário Geral, a declaração produz efeitos nessa data posterior.

2. Uma Parte que tenha formulado uma reserva nos termos do artigo 42º retirará essa reserva no todo ou em parte, logo que as circunstâncias o permitam.

3. O Secretário-Geral do Conselho da Europa pode, periodicamente, pedir às Partes que formularam uma ou mais reservas nos termos do artigo 42º, informações sobre as perspectivas de levantamento dessas reservas.

Artigo 44º - Aditamentos

1. Quaisquer aditamentos à presente Convenção podem ser propostas por qualquer uma das Partes e serão comunicadas pelo Secretário Geral do Conselho da Europa aos Estados membros do Conselho da Europa, aos Estados não membros que participaram na elaboração da presente Convenção, bem como a qualquer Estado que tenha aderido, ou sido convidado a aderir em conformidade com as disposições do artigo 37º.

2. Qualquer aditamentos proposta por uma Parte deve ser comunicada ao Comité Europeu para os Problemas Criminais (CDPC), que submeterá ao Comité de Ministros o seu parecer relativamente à alteração proposta.

3. O Comité de Ministros examinará o aditamento proposto e o parecer submetido pelo Comité Europeu para os Problemas Criminais (CDPC) e, após consulta dos Estados não membros, Partes na presente Convenção, pode adoptar o referido aditamento.

4. O texto de qualquer aditamento adoptado pelo Comité de Ministros em conformidade com o n.º 3 do presente artigo será comunicado às Partes para aceitação.

5. Qualquer aditamento adoptado em conformidade com o n.º 3 do presente artigo entrará em vigor no trigésimo dia após todas Partes terem informado o Secretário Geral acerca da sua aprovação.

Artigo 45º -Resolução de litígios

1. O Comité Europeu para os Problemas Criminais (CDPC) será mantido informado sobre a interpretação e a aplicação da presente Convenção.

2. No caso de litígio entre as Partes sobre a interpretação ou a aplicação da presente Convenção, as mesmas esforçar-se-ão por encontrar uma solução para o litígio através da negociação ou de qualquer outro meio pacífico à sua escolha, incluindo submeter o litígio ao Comité Europeu para os Problemas Criminais (CDPC), a um tribunal arbitral, cujas decisões vincularão as Partes no litígio, ou ao Tribunal Internacional de Justiça, de comum acordo entre as Partes envolvidas.

Artigo 46º -Consulta entre as Partes

1. As Partes consultar-se-ão periodicamente, se necessário, a fim de facilitar:

a) A utilização e a execução efectiva da presente Convenção, incluindo a identificação de qualquer problema na matéria, bem como os efeitos de qualquer declaração ou reserva feita em conformidade com a presente Convenção;

b) A troca de informações sobre os desenvolvimentos jurídicos, políticos ou técnicos importantes verificados no domínio da cibercriminalidade e a recolha de provas sob forma electrónica;

c) A análise de eventuais complementos ou aditamentos à Convenção.

2. O Comité Europeu para os Problemas Criminais (CDPC) será mantido periodicamente informado do resultado da consulta referida no n.º 1.

3. O Comité Europeu para os Problemas Criminais (CDPC) facilitará, se necessário, as consultas referidas no n.º 1 e adoptará as medidas necessárias para ajudar as Partes nos seus esforços destinados a complementar ou a fazer aditamentos à Convenção. O mais tardar no final de um prazo de três anos a contar da entrada em vigor da presente Convenção, o Comité Europeu para os Problemas Criminais (CDPC) procederá em cooperação com as Partes a um reexame de todas as disposições constantes da Convenção e, se necessário, proporá os aditamentos adequados.

4. Salvo quando o Conselho da Europa assuma as despesas ocasionadas pela aplicação do disposto no n.º 1, as mesmas serão suportadas pelas Partes.

5. As Partes são assistidas pelo Secretariado do Conselho da Europa no exercício das suas funções decorrentes do presente artigo.

Artigo 47º -Denúncia

1. Qualquer Parte pode, em qualquer momento, denunciar a presente Convenção através de notificação dirigida ao Secretário Geral do Conselho da Europa.

2. A denúncia produzirá efeitos no primeiro dia do mês seguinte ao termo de um período de três meses após a data de recepção da notificação pelo Secretário Geral.

Artigo 48º -Notificação

O Secretário Geral do Conselho da Europa notificará os Estados membros do Conselho da Europa, os Estados não membros que participaram na elaboração da presente Convenção, bem como qualquer Estado aderente, ou que tenha sido convidado a aderir à presente Convenção de:

a) Todas as assinaturas;

b) O depósito de qualquer instrumento de ratificação, aceitação, aprovação ou adesão;

c) Todas as datas de entrada em vigor da presente Convenção, em conformidade com os artigos 36º e 37º;

d) Todas as declarações efectuadas em aplicação do(s) artigo(s) 40º, 41º, ou as reservas formuladas em aplicação do artigo 42º:

e) Qualquer outro acto, notificação ou comunicação relacionados com a presente Convenção.

Em fé do que os abaixo assinados, devidamente autorizados para este efeito, assinaram a presente Convenção.

Feito em Budapeste, em 23 de Novembro de 2001, em francês e inglês, ambos os textos fazendo igualmente fé, num único exemplar, que será depositado nos arquivos do Conselho da Europa. O Secretário Geral do Conselho da Europa enviará cópias autenticadas a cada um dos Estados membros do Conselho da Europa, aos Estados não membros que participaram na elaboração da presente Convenção, e a qualquer Estado que tenha sido convidado a aderir à Convenção.