A legislação e o Direito da Informática

Fabiano Rabaneda

Resumo: Através da pesquisa da legislação existente, com foco aos aspectos aplicáveis à segurança da informação no Direito Digital, avaliamos a legislação existente, procurando integrar aos principais fatos jurídicos, de forma a apontar as lacunas normativas, apresentando uma exegese ao Direito Comparado Alienígena, tecendo uma síntese das tendências normativas, através do estudo dos projetos de Leis que tramitam na Câmara dos Deputados. Pelo método hipotético-dedutivo proposta por Popper[1], iremos encontrar a resposta para conhecer quais leis regulam os parâmetros da segurança da informação, no conceito computacional e a tendência legislativa para sua regulação.

PALAVRAS-CHAVE: crimes; internet; segurança; legislação penal.

Abstract: Through research of existing legislation, focusing on aspects applicable to information security law in Digital, evaluate existing legislation, seeking to integrate major legal facts in order to identify regulatory gaps, giving an exegesis of Comparative Law Alien, creating a summary of the regulatory trends, through the study of the projects of laws that the Board of Deputies. For the hypothetical-deductive method proposed by Popper, we will find the answer to know which laws governing the parameters of information security concept in computing and legislative trend to its regulation

Keywords: Internet; Law; Security.

1 A EVOLUÇÃO DA COMUNICAÇÃO FRENTE AO MUNDO DAS MAQUINAS ELETRÔNICAS.

Já foi o tempo em que o homem conseguia viver só, tempos remotos de uma época pré-histórica que com o passar dos anos, motivados pela necessidade de garantir sua sobrevivência, passaram a se agrupar em tribos, instalando-se em cavernas e acampamentos.

A partir dessa convivência, surgiu a necessidade de expressão, da transmissão de informações sucintas de modo a permitir a comunicação entre seus membros. Disso, das primeiras pinturas rupestres nas cavernas, até os dias atuais, o homem apenas aprimorou esse processo sinalagmático.

Por esse complexo caminho evolucionário, a informação tomou relevância na organização político-social da humanidade, sendo destaque a partir dos anos sessenta, quando a sociedade passou a caminhar em direção a um novo modelo de organização, no qual o controle e a otimização dos processos industriais eram substituídos pelo manejo da informação como “chave” econômica.

Digamos que este foi o inicio de uma segunda revolução industrial, onde o poder das engrenagens foi sendo substituído por autômatos, afastando a mão de obra humana do processo produtivo.

E, dentro deste novo paradigma, o inútil passa a ter uma nova roupagem, e as informações transformaram-se em posições matemáticas denominadas BITS.

O “BIT” é a menor unidade de transmissão de informações utilizada na computação, seus valores são representados pela carga positiva e negativa, um e zero, o verdadeiro e falso. Fisicamente o bit é armazenado como uma carga - seja ela elétrica, magnética ou luminosa - acima ou abaixo do padrão.

As seqüências dessas cargas compõem o sistema binário, que transformado para a álgebra de George Boole[2], se resume na base de todo o sistema computacional conhecido atualmente.

Por conseqüência desta explanação, em simples raciocínio lógico – o mesmo utilizado na programação dos computadores - , sendo a energia matéria física intangível, podemos dizer que as informações passaram do mundo real (do papel, do livro), para o mundo das essências (dos discos rígidos, das memórias, do hipertexto[3]), como os mundos descritos por Platão – o mundo inteligível, das idéias e o mundo sensível, o real -.

Quando, ao transpor a barreira natural do existir, a informação passou a ser delineada pelas idéias, e as barreiras que antes a limitavam, delineada pelas forças das leis da física, e sem elas, o impossível passou a não mais existir.

Neste contexto grandes transformações culturais foram impostas a essa "nova sociedade" e os pilares que antes sustentavam a base da convivência passaram a ser ditados por regras jamais previstas no ordenamento jurídico.

Se compararmos essa transformação ao filme Matrix[4], onde o jovem Neo - Keanu Reeves – descobre que vive em um mundo não real, homens imersos em casulos ideológicos, e ao tomar a "pílula do conhecimento" é emergido a uma realidade totalmente avessa a singular vivência conhecida, podemos constatar o potencial avassalador que a "nova tecnologia" causa no cotidiano social.

É incontrolável tamanha transformação, que pela liberdade do sistema, esse mundo irreal passou a tomar forma dos desejos reprimidos da sociedade, e o que é torto aqui, do lado de lá pode ser programado a parecer lindo e perfeito. E vice versa.

Contudo, as ações realizadas nesse mundo virtual, muitas vezes, acabam por refletir em conseqüências no mundo de cá, e causa fatos que transformam a maneira do viver e conviver.

Surge, portanto, a necessidade de regular o irregulável. Como pode o mundo dos homens determinar regras de conduta ao mundo das maquinas?

Para entender as implicações dessa regulação é necessário voltarmos ao inicio, pouco antes da criação da internet, como forma de entendermos melhor seu funcionamento.

2 A INTERNET COMO FORMA DE CONEXÃO SOCIAL

Antes de tudo, antes mesmo do advento do primeiro computador pessoal, tínhamos maquinas enormes denominadas de "mainframes". Gigantes que tomavam conta de andares inteiros - consumiam mais energia do que uma faculdade inteira - e passavam quase o tempo todo paradas do que funcionando. Culpa da sujeira. Daí o termo "debug", utilizado por programadores para encontrar possíveis erros nos programas, uma vez que com o calor das válvulas os insetos se alojavam no interior dessas maquinas e constantemente necessitavam os cientistas a "debugar" o equipamento.

Naquele tempo, o que motivava as inovações era a guerra fria, e tudo deveria ser concebido com o fim de defesa da nação. Isso, visto pelo ângulo das inovações, foi bom para o mundo, considerando vultosos investimentos em tecnologia.

Estes investimentos criaram, por volta da década de 60, uma rede idealizada como ferramenta de comunicação militar alternativa, com dispositivos independentes que resistisse a um conflito nuclear mundial[5].

Um grupo de programadores e engenheiros eletrônicos, contratados pelo Departamento de Defesa dos Estados Unidos, desenvolveu o conceito de uma rede de comunicação sem nenhum controle central, por onde as mensagens passariam divididas em pequenas partes, que foram chamadas de "pacotes". Assim, as informações seriam transmitidas com rapidez, flexibilidade e com certa tolerância a erros, em uma rede onde cada computador seria apenas um ponto (ou "nó") que, se impossibilitado de operar, não interromperia o fluxo das informações.

Baseado neste conceito, em outubro de 1969, com uma comunicação entre a Universidade da Califórnia e um centro de pesquisa em Stanford, entrou em operação a ARPAnet (Advanced Research Projects Agency Network), inicialmente ligando quatro computadores.

Posteriormente, mais computadores se juntaram a estes, pertencentes a outras universidades, centros de pesquisa com fins militares e indústrias bélicas.

No início dos anos 80, o desenvolvimento e utilização do TCP/IP (Transmission Control Protocol/Internet Protocol) como protocolo para a troca de informações na ARPAnet possibilitou a conexão entre redes diferentes, aumentando bastante a abrangência da rede.

Em 1990, a ARPAnet foi transformada em NSFnet (National Science Foundation's Network), se ligando a outras redes existentes, inclusive fora dos Estados Unidos, passando a interconectar centros de pesquisa e universidades em todo o mundo.

Estava formada a internet, utilizada principalmente como uma ferramenta de troca de informações entre o meio acadêmico.

Em meados de 1995, devido a evolução dos equipamentos informáticos, a internet foi transferida para a administração de instituições não-governamentais – no Brasil a Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP) -, que se encarregaram, entre outras coisas, de estabelecer padrões de infra-estrutura, registrar domínios[6], enfim, de administrar a operabilidade da rede.

A partir disso a internet começa a se popularizar, e surge o padrão "World Wide Web", desenvolvido no início da década de 1990 pelo cientista inglês Tim Berners-Lee nos laboratórios do CERN (Conselho Europeu para Pesquisa Nuclear), na Suíça.

Em especial, no Mato Grosso, a internet teve inicio com o provedor InterNews BBS, que era responsável pela conexão entre os usuários e o "backbone[7]" central e posteriormente com a InterByte BBS, de propriedade do autor, que fazia a conexão com outros BBS norte-americanos, interligando os usuários através de ligações internacionais à rede mundial de computadores.

Naquele tempo as conexões eram lentas – 1000 vezes menor do que hoje - e o que se podia trafegar eram somente textos e poucas imagens. O custo das ligações, tarifadas em moeda norte-americana e em minutos, inviabilizavam o acesso a massa, estando a "net" restrita a poucas empresas e a usuários com melhor nível social.

Entretanto, mesmo com essas limitações, observamos uma explosão mundial pelo acesso a informação, e posteriormente, com a redução do custo de Telecom, o que antes estava disponível a poucos, passou a ser parte do cotidiano. A grande onda da Internet crescia nos mercados de primeiro mundo, e o Brasil acompanhava essa tendência.

Marilena Chaui[8], retratando o pensador Adam Scaff, e se refere a tecnologia como algo que "mesmo sem darmos conta, estamos rodeados por ela, desde pequenos objetos de uso cotidiano, como o relógio a quartzo, a calculadora de bolso e o telefone celular, até os computadores e os vôos espaciais".

Apontando para uma sociedade contemporânea, Chaui define como sendo os computadores detentores da posse de informações, sejam elas científicas, econômicas, políticas ou militares, relacionando isso ao poder. Surge o conceito do poder informático.

Neste conceito, qual nação estivesse madura em relação a conexão tecnológica gozaria de poder e prestígio.

É esse poder que apontamos à necessidade de regulação.

"A tecnologia humana não determina seu uso: nenhuma técnica pode ser utilizada aleatóriamente, e todo aparelho só permite uma certa gama de aplicações. Por exemplo, os computadores podem ser bem eficazes para promover a comunicação em uma sociedade descentralizada: se escrevo um romance e desejo difundi-lo, devo antes publicá-lo, o que significa ter a aprovação de uma pessoa influente no mundo da edição. Se existisse uma rede de comunicação informatizada, poderia colocar meu romance à disposição dos interessados sem qualquer autorização prévia. Neste sentido a informação ajudará na descentralização, assim como na redução do controle. Mas simultaneamente, os computadores podem ser utilizados por um sensor do governo, a fim de examinar todas as informações difundidas e impedir assim a livre expressão por meio escrito. O mesmo dispositivo, o mesmo computador, poderia ser utilizado com finalidades diferentes e até mesmo contraditórias."[9]

Pessis, em 1993, antes da popularização da internet, já se preocupava, mesmo que nos anseios por uma rede descentralizada, com a utilização contraditória da ferramenta computacional.

Considerando que o homem – mal! Seja por nascido ou por vivido - transformou o utensílio do jantar em arma de morte, do meio de transporte rápido em arma de guerra e da energia fácil em bomba nuclear. Não podia ser diferente com a melhor ferramenta de aprendizado e comunicação já inventada, e passou

a utilizar a rede como forma de violar as garantias e direitos individuais a fim de locupletar-se pelo crime.

A segurança e a privacidade das informações, sejam elas pessoais ou comerciais, nunca estiveram tão ameaçadas e surge a questão: Como estamos preparados para proteger o que temos de mais valioso, nosso petróleo da nova era, a informação?

É dever dos instrumentos sociais acompanhar a evolução tecnológica, e protegê-la, a fim de sanar os vícios do sistema, para que não padeçamos frente ao mundo das essências.

3 A NORMATIZAÇÃO DA "NOVA ERA" FRENTE À ESTRUTURA FUNDAMENTAL DA EXISTÊNCIA JURÍDICA

Paulo Nader[10] define que o homem tem de atender às exigências de um condicionamento de leis da natureza, a fim de construir o seu mundo cultural. Neste processo, mediante constante adaptação, o homem se torna forte, resistente e apto a enfrentar os rigores da natureza. Qualidades que permitem que se viva em sociedade, capaz de desfrutar de justiça e segurança, de conquistar seu mundo cultural.

A necessidade de paz e ordem remete a sociedade para a criação de um organismo responsável pela instrumentalização e regência de tais valores. Ao Direito é conferida tamanha e importante missão.

Devemos destacar que o Direito não corresponde às necessidades individuais, mas uma carência da coletividade. Não um fim, mas um meio para tornar possível a convivência e o progresso social.

Como todos os inventos humanos, as instituições jurídicas sofrem variações no tempo e espaço, adaptando-se a sociedade, e deve, para sua manutenção como ferramenta pacificadora, estar sempre se refazendo.

Durante esse contínuo processo de adaptação, as normas jurídicas – células do direito que fixam os modelos de limites a liberdade do homem, mediante imposição de condutas – devem absorver todos os atos e manifestações humanas, estimuladas por necessidades e em função dos valores de determinada sociedade.

Neste contexto, dizemos que o Direito é o espelho dos anseios sociais de uma coletividade de indivíduos. Fruto de condições sócio-ambientais favoráveis a interação de suas regras à efetividade coercitiva, sempre estimulando a atuação do "querer" coletivo.

Em níveis sociológicos, a constituição física do ser humano revela sua programação a se completar com outro de sua espécie. Sentimentos de afeto e interesse material que movem os ideais para um mesmo objetivo e valor, conjugando o esforço de viver em cooperação mútua entre a espécie.

Por outro lado, existe a competição, uma disputa em que as partes procuram obter o que almejam em detrimento da outra.

Aristóteles, em Ética a Nicômaco, nos ensina que a competição é o ajuste das diferenças. E por mais que os conflitos sejam fenômenos naturais à sociedade, no caminho da complexidade social, pela diversidade de idéias e sentimentos, o resultado é o que se hoje verifica: A dificuldade em viver e conviver.

Sobre isso disse o maior professor das arcadas, Goffredo Telles Junior[11]:

"[...] para viver bem, para bem conviver, é necessário bem se relacionar com o próximo. E isto significa que o relacionamento há de se realizar em consonância com normas, com imperativos que as contingências da vida social vão suscitando e impondo. Significa que a convivência exige disciplina. Sem disciplina para o comportamento das pessoas, a vida em sociedade seria uma permanente guerrilha, e se destruiria a si própria. Tornar-se-ía impossível."

Portanto, conclui-se, por estas palavras, que o Direito está em função da vida social para equilibrar o exagero do conflito, permitindo nexos entre a competição e cooperação, estabelecendo os limites necessários ao equilíbrio justo nas relações.

Mas, como adaptar o Direito a uma universalidade de regras morais, a uma pluralidade de condutas que estão espalhadas pelo emaranhado digital?

Em uma única década romperam-se todas as fronteiras físicas, e o mundo digital (das essências), passou a incorporar a todos os povos, com todas as suas diversidades.

Católicos, mulçumanos, judeus, ricos e plebeus, todos estão na rede, cada qual com suas crenças e suas convicções de moralidade. O que para um é diversão, para outro, se pune com a morte.

Tamanho o grau de complexidade dessa relação que podemos acreditar que as barreiras da soberania foram rasgadas pela capacidade de acesso a informação. E a liberdade está retratada como um procedimento, uma rotina que segue os padrões desenvolvidos pela indústria da tecnologia da informação.

Surge, com isso, o conceito do Direito Comunitário, que visa reunir pontos comuns desta salada de costumes, passando a regular a inter-relação global.

Sustentar o Direito Comunitário é um papel importante as instituições Estatais, uma vez que nem toda norma válida é eficaz. Incorporar a mudança para um meio flexível, que garanta a aceitabilidade é tarefa hercúlea, e que deve ter respaldo das nações, por tratados internacionais, a fim de permitir a execução das ferramentas coercitivas da Lei.

4 A PROBLEMÁTICA DA SEGURANÇA COMPUTACIONAL NA SEARA LEGISLATIVA NACIONAL

Os dados computacionais, como já dissemos, são formados por cargas, positivas ou negativas, esse "status" da a informação capacidades físicas que não foram contempladas na legislação penal existente.

Para se ter uma idéia, quando retiramos um arquivo de um meio de armazenamento para outro, o que fazemos é uma cópia idêntica de seu conteúdo. E assim, podemos transportar a informação.

Para nossa legislação penal, o furto é caracterizado pelo traslado do objeto com ânimo de assenhoramento. Como pode o invasor de um sistema computacional, que "remove" o arquivo, com o "ctrl+c e ctrl+v", responder por furto?

Embora tenha sido esse o "animo", subtração da coisa, prevalece a atipicidade na conduta, uma vez que não houve a remoção do física do arquivo, e sim sua cópia e posterior deleção.

A empresa, quando muito, conseguirá eventuais indenizações por danos sofridos. E ainda terá que provar quais foram os danos.

Não obstante a isso, temos a dificuldade de punição dos invasores computacionais que fogem para o Brasil.

É que a Lei 6.815/80, que regula a extradição no Brasil, pelo principio da dupla tipicidade, em seu artigo 77, determina que não se conceda a extradição quando o fato que motivar o crime não seja considerado crime no Brasil.

Assim, como no exemplo do EXT1029/PT-Portugal/STF, o cidadão português que comete os crimes tipificados no Código Penal português de Falsidade Informática fica impune, uma vez que a justiça não encontra respaldo na legislação pátria. Neste sentido, versou o relatório do pedido de extradição, relator Min. Cezar Peluso:

"[..] in casu não se faz presente tal requisito no que diz respeito ao crime de falsidade de informática.

A legislação portuguesa define o crime na Lei nº 109/91, nos seguintes termos:

'Falsidade Informática – Art. 4º: Quem, com intenção de provocar engano nas relações jurídicas, introduzir, modificar, apagar, suprimir dados ou programas informáticos ou, por qualquer outra forma, interferir num tratamento informático de dados, quando esses dados ou programas sejam susceptíveis de servirem como meio de prova, de tal modo que a sua visualização produza os mesmos efeitos de um documento falsificado, ou bem assim, os utilize para os fins descrito, será punido com pena de prisão

até cinco anos ou multa de 120 a 600 dias' (grifado) Apesar de inúmeras tentativas, o Brasil ainda não aprovou uma legislação própria de crimes de informática, tendo sido promulgada unicamente a Lei nº 9.983/2000, que diz respeito a crimes praticados por funcionário público contra a Administração em geral, situação diversa da descritas nos autos. A especificidade dos elementos normativos que compõe o delito penal de falsidade informática é tamanha que impossibilita o encontro correspondente na legislação nacional, ou seja, ainda que se perquirisse sobre os crimes de falsidade documental, não se conseguiria obter tal intento."

A extradição foi concedida em parte, porque houve a possibilidade, pela analogia do crime de Burla Informática (art. 221 do CP Português) ao crime de Estelionato (art. 171 do CP), de tipificar a conduta de um outro crime praticado, mas de fosse somente aquele, teria o réu se beneficiado.

Neste campo de estudo, o Brasil engatinha na regulação dos crimes de informática, e nos remete a um estudo dos tipos penais, que descrevem crimes de informática, já existentes:

- Lei 8.137/90: Art. 2º, inciso V, que considera crime "utilizar ou divulgar programa de processamento de dados que permita ao sujeito passivo da obrigação tributária possuir informação contábil daquela que é, por lei, fornecida à Fazenda Pública", punível com reclusão de 2 a 5 anos, e multa;

O crime previsto nesta lei é definido como crime contra a ordem tributária, sendo praticado por quem utiliza (o comerciante, o empresário, o funcionário – que sabe da existência da artimanha -) ou quem divulga (o produtor, programador) o software de processamento de dados. Pode haver o concurso de sócios, mas a conduta de cada um deve ser descrita, sobre pena de infringir o exercício do direito a ampla defesa[12].

O sujeito passivo é a Fazenda Pública, pois é ela a prejudicada com a alteração nas informações contábeis.

Embora a jurisprudência traga que a materialidade dos crimes contra a ordem tributária necessite diretamente da relação com o lançamento definitivo do crédito tributário[13], entendemos que o inciso V não seja assim, sendo crime formal, tanto na primeira quanto na segunda modalidade, uma vez que a conduta típica é o simples uso ou divulgação.

É exigido o dolo na conduta, o ânimo de burlar o sistema de processamento a fim de emitir informações contábeis diversas à realidade da empresa, não importando a finalidade.

A consumação do crime não depende de um resultado, basta o uso, ou a divulgação, do sistema adulterado que permita a diferença entre a informação contábil do sujeito passivo da obrigação – denominada de contabilidade gerencial – com a fornecida à Fazenda Pública – denominada de contabilidade fiscal -. É permitida a tentativa somente para a segunda conduta - a divulgação -, uma vez que o agente pode ser surpreendido no momento, e com os materiais para a consumação. Já na primeira, a conduta de utilizar esta relacionada diretamente a entrega das informações ao fisco, ou seja, o programa computacional é o meio para a burla.

Trata-se de crime de difícil prova, uma vez que é necessária a comprovação de que as informações divergentes foram geradas pelo sistema computacional, exigindo perícia técnica que promova a engenharia reversa do executável[14] a fim de se obter o código fonte com a burla.

- Lei 9.296/96: Art. 10, que considera crime, punível com reclusão de 2 a 4 anos e multa, "realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo de Justiça, sem autorização judicial ou com objetivos não autorizados em lei".

A Lei citada é utilizada para regular o inciso XII do Art. 5º da CF, que trata sobre o sigilo das comunicações.

Na primeira parte da norma, qualquer pessoa pode ser o sujeito ativo, já na segunda parte – realizar sem autorização judicial – o delito é próprio, só podendo ser cometido por quem tem obrigação de guardar sigilo: Juiz de Direito, Promotor de Justiça, Delegado de Policia, Escrivão ou Escrevente, enfim, todos que manipulam a prova.

O sujeito passivo são os interlocutores, de dupla subjetividade, contudo havendo o consentimento de um dos sujeitos passivos, exaure-se o delito.

O delito se configura quando, sem autorização judicial, ou com objetivos não expressos na Lei, o agente realiza interceptação telefônica ou telemática (informática), ou quebra o segredo desta, expondo seu conteúdo a terceiro.

Em se tratando de interceptação telemática, considerando as características dos sistemas computacionais, comete o crime quem faz a captura dos "pacotes" enviados pela rede de comunicação.

A ausência de autorização judicial configura o elemento normativo do tipo penal[15], exigindo-se o dolo, a vontade de interceptar a comunicação ou quebrar segredo, com fins diversos dos estabelecidos pela Lei.

A sua consumação dá-se por mera conduta, independente de qualquer resultado, e é aceita a tentativa para o primeiro tipo penal – interceptar -, uma vez que o sujeito pode ser surpreendido no momento em que vai realizar a interceptação, contudo o segundo tipo não a admite.

Esta norma é extremamente polêmica, uma vez que o art. 5º da CF, XII, diz que somente as comunicações telefônicas, nas hipóteses e na forma que a lei estabelecer, podem ter seu sigilo quebrado.

Desta forma, a interceptação do fluxo de informações, contido no parágrafo único desta Lei, é inconstitucional.

Na ADI-MC 1.448/DF/STF/Relator: Min. Néri da Silveira, a Associação dos Delegados de Policia do Brasil aflora que o tema foi discutido e o entendimento predominante no Senado Federal é no sentido de que o art. 5º garantiu o sigilo das comunicações privadas em geral, excetuando apenas os das comunicações telefônicas, e o parágrafo único foi considerado inconstitucional e suprimido.

Senador Jefferson Peres[16]: "Fica claro que a C.F. só abre exceção para a interceptação no caso de comunicação telefônica. Não encontramos justificativa razoável para que a norma constitucional tenha mantido inviolável, em qualquer caso, outras formas de comunicações diversas da telefonia. Não obstante essa é a norma a ser cumprida."

Incongruente a Câmara dos Deputados, mesmo após a aprovação, em revisão do Senado, eliminando a inconstitucionalidade referida, a Emenda foi rejeitada e o texto anterior foi votado.

Após requisitar informações a Presidência da Republica, o Procurador Geral aduz tese de que o termo "dados informáticos" estaria se referindo ao termo "comunicação", e o sigilo reputado está na defesa do interesse da privacidade.

Por fim, se faz uma análise gramátical no texto constitucional, numa tentativa teratoscópica de encontrar explicação teleológica plausível.

Essa linha de raciocínio não tem cabimento!

Como já estudamos, em relação aos dados computacionais, as informações são combinações de "bits", e ao realizar qualquer tipo de interceptação, o agente não tem, a priori modo, estabelecer o que é comunicação, análoga a correspondência, e o que são dados diversos.

Ao decodificar o protocolo de comunicação computacional, a fim de conhecer o seu conteúdo, se houver dados de derivam de uma correspondência, já cometeria, em tese, o crime.

E tamanha a probabilidade disso ocorrer, uma vez que o uso do e-mail é cada vez maior, e os dados não escolhem momentos especificos para trafegar em rede.

Ainda que fosse possível sinalizar o pacote de dados com a informação de que se trata de correspondência, analisar uma lei por simetria entre seus blocos é jogar na sorte. A difícil tarefa de entender a tutela que o Poder Constituinte quis resguardar vai ser sufocada pela evolução tecnológica, uma vez que as comunicações analógicas de voz serão substituídas pela digital, e o que se ouvirá serão ruídos.

Tudo estará transformados em "bits", encapsulados dentro dos "pacotes IP", como dados.

Desta maneira, por mais que existam Leis infra-constitucionais que venham a regular essa interceptação de dados, sempre se esbarrará no confuso texto do pétreo artigo 5º, XII, e em analogia a tese da pena de morte, é redundante querer discutir isso hoje. Precisaríamos de uma nova redação constitucional.

- Lei 9.504/97: O Art. 72 da Lei n° 9504/97 define que 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 evitar 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 suas pastas."

Esta Lei é conhecida como Lei Eleitoral, e tem insculpidos três tipos penais, sendo que no inciso I está descrita a conduta de obter o acesso ao sistema com o fim de evitar a apuração dos votos. Trata-se de crime formal, consumando com o simples acesso, independente do resultado. Exige o dolo, vontade de evitar a apuração dos votos.

Por sua vez, o inciso II trata dos "vírus[17]" e "cavalos de tróia[18]", que são programas com capacidade de destruir, apagar, eliminar, alterar, gravar ou transmitir instrução, provocando com isso, resultado diverso ao esperado. Como no inciso anterior, trata-se de crime formal, basta que o agente desenvolva ou introduza o programa nos sistemas do serviço eleitoral. Exige o dolo de adulterar os dados computacionais.

Já o inciso III, trata de crime de dano às urnas eletrônicas, com conduta material, ou seja, espera-se um resultado - que o equipamento seja danificado -. Exige dolo, vontade de causar propositadamente o dano físico.

O sujeito ativo é qualquer pessoa, e o passivo será a administração pública. Admite-se a tentativa para os três tipos penais, uma vez que observado ao agente possuir instrumentos capazes de produzir os resultados tipificados.

- Lei 9.609/98: Art. 12, caput, § 1° e 2°, que tipifica o crime de violação de direitos de autor de programa de computador, punindo-o com detenção de 6 meses a 2 anos, ou multa; ou com pena de reclusão de 1 a 4 anos e multa, se agente visa lucro;

Definida como Lei Anti-Pirataria, a Lei 9.609/98 dispõe sobre a propriedade intelectual dos programas computacionais.

Punindo quem viola os direitos de autoria, faz referência a Lei 9.610/98, e constitui um marco regulatório no direito digital no Brasil, substituindo a fraquíssima Lei 8.248/91. Define claramente o conceito de programa de computador[19], e assinala os direitos e deveres dos usuários e empresas que produzem e comercializam os programas computacionais.

Em seu texto, exclui como infração ao direito do autor do programa de computador:

• Ter uma cópia do programa de computador (Art. 6º, I, 9.609/98);

• Citar, para fins didáticos, trechos do programa, desde que identificados o programa e o titular dos direitos respectivos;

• Ter semelhança com outro programa, quando se der por força das características funcionais de sua aplicação, da observação de preceitos normativos e técnicos;

• Integrar um programa, mantendo-se suas características essenciais, a um sistema aplicativo ou operacional, tecnicamente indispensável às necessidades do usuário, desde que para uso exclusivo de quem a promoveu.

De outra forma, pune quem viola os direitos de autor, ou seja, quem efetua engenharia reversa no intuito de obter o código fonte e assim utilizar da inovação tecnológica.

Neste tipo penal, o sujeito ativo pode ser qualquer pessoa, de outra forma o sujeito passivo será sempre o detentor do direito autoral do software. Trata-se de conduta típica, exige a violação do direito autoral.

È necessário a vontade de violação, a consciência da infração, e admite a tentativa.

Nos § 1º e § 2º, temos tipificados as condutas de reprodução de programa de computador para fins de comércio sem autorização expressa do autor, ou quem vende, expõe a venda, introduz no País, adquire, oculta ou tem deposito, para fins de comércio, original ou cópia de programa de computador, produzido com violação de direito autoral.

Assim, trata-se de crime subsidiário, havendo a necessidade de que ocorra, inicialmente a violação do direito autoral.

O legislador pune, no caso, a comercialização do programa "pirata", tendo como sujeito ativo qualquer um que se encaixe nas condutas descritas. O sujeito passivo será o detentor do direito autoral.

O crime é de mera conduta, bastando que se copie, que se venda, que se exponha, que se introduza, que se deposite o software. Contudo o elemento subjetivo é o intuito de comercialização.

Assim, o cidadão, que em sua casa, copia o software, com fins de salvaguarda dos arquivos, não comete crime algum.

O tipo subjetivo é o dolo, e admite-se a tentativa, uma vez constatado instrumentos capazes da realização do crime, e que sua execução não se deu por condições alheias a vontade do agente.

- Código Penal: Art. 153, § 1°-A, com a redação dada pela Lei n° 9.983/2000, que tipifica o crime de divulgação de segredo: "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", punindo-o com detenção de 1 a 4 anos.

No intuito de promover resguardo a informação da base de dados pública, a Lei 9.983/00 promoveu grandes, e importantes, alterações no código penal, tipificando os crimes eletrônicos no serviço público.

O crime deste artigo é caracterizado como crime comum, ou seja, pode o sujeito ativo ser qualquer pessoa, funcionário público ou não. De sentido diametralmente oposto, o sujeito passivo será, sempre, a administração pública.

A tipicidade da conduta é caracterizada por divulgar informações sigilosas, sendo necessário para a caracterização do crime que as informações estejam protegidas por Lei. Assenta Mirabette[20]: "não bastando, portanto, que a proibição provenha de outras regras jurídicas, como portarias, regulamentos".

O tipo subjetivo é o dolo, a vontade de divulgar o segredo, e deixa de ser típico se houver justa causa para a divulgação.

A tentativa é permitida quando a divulgação é não é transmitida oralmente, e por circunstâncias alheia a vontade do agente, não se consumou.

- Código Penal: Art. 313-A, introduzido pela Lei n° 9983/2000, que tipificou o crime de inserção de dados falsos em sistemas de informações, com a seguinte redação: "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", punindo-o com pena de reclusão, de 2 a 12 anos e multa;

Este artigo prevê três modalidades de execução criminosa: inserir, alterar ou excluir dados nos sistemas da Administração Pública. O agente deve manipular os dados de forma a alterar a verdade dos dados, ou quando exclui indevidamente dados que deviam constar no sistema ou do banco de dados.

O sujeito ativo é o funcionário público autorizado, que por conseqüência, tem acesso a base de informações, mas nada impede o concurso de terceiro, uma vez que a norma prevê a facilitação por estranho ao acesso. O sujeito passivo será a administração pública.

Trata-se de crime doloso, exigindo a vontade e a ciência de que se esta inserindo dados falsos, alterando os existentes ou excluindo-os indevidamente. O elemento subjetivo de obtenção de vantagem indevida é necessário, ou de causar dano a administração pública.

É cabível a tentativa, uma vez se constante todos os meios para a execução do crime, que não se consuma por fatos alheios a vontade do agente.

- Código Penal: Art. 313-B, introduzido pela Lei n.° 9.983/2000, que tipificou o crime de modificação ou alteração não autorizada de sistema de informações, com a seguinte redação: "Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente", cominando-lhe pena de detenção, de 3 meses a 2 anos, e multa;

Quem não se lembra do incidente de violação do painel do Senado, crime imputado a participação de Antonio Carlos Magalhães[21], este é uma conduta típica descrita no Art. 313-B. Naquele tempo, não havia tipicidade para essa conduta e o Tribunal por unanimidade reconheceu a extinção da punibilidade do crime, já que havia sido denunciado pelo artigo 305 CP.

Trata o 313-B de crime próprio, praticado por funcionário público, mas permite a participação de terceiro, por instigação material ou moral. O sujeito passivo será o Estado.

A tipicidade da conduta dá-se pela ação de modificar o sistema de informática - o agente substitui o sistema existente por outro -, ou quando altera o sistema já existente. O elemento normativo do tipo exige que não se tenha autorização para a modificação ou alteração.

Consuma-se o crime com a alteração ou modificação sem autorização, não exigindo resultado de dano para a Administração Pública.

O dolo é necessário, onde o agente deve ter consciência de que não está autorizado, mas mesmo assim modifica ou altera o sistema. Admite-se tentativa.

- Código Penal: Art. 325, §1°, incisos I e II, introduzidos pela Lei n.° 9983/2000, tipificando novas formas de violação de sigilo funcional, nas condutas de quem "I - permite ou facilita, mediante atribuição, fornecimento e empréstimo de senha ou qualquer outra forma, o acesso de pessoas não autorizadas a sistemas de informações ou bancos da Administração Pública" e de quem "II - se utiliza, indevidamente, do acesso restrito", ambos sancionados com penas de detenção de 6 meses a 2 anos, ou multa;

Tendo como sujeito ativo o funcionário público, que mediante atribuição, ou seja, com ordem de superior hierárquico, permite ou facilita o acesso de pessoas não autorizadas a sistemas de informações da Administração Pública, ou se utiliza do acesso restrito indevidamente. Deve, portanto, o funcionário púbico ter acesso ao sistema de informação. O sujeito passivo será o Estado.

Trata-se de crimes formais, é irrelevante que tenha ocorrido qualquer dano a Administração Pública, bastando para a consumação do crime, para o primeiro tipo penal, mediante o acesso indevido de pessoas não autorizadas a operar o sistema computacional, a simples atribuição, fornecimento, empréstimo de senha ou, no caso do segundo tipo penal, a mera utilização indevida do acesso e dos proveitos que ele concedeu ao agente. É possível a tentativa.

5 AS INOVAÇÕES PROPOSTAS PELOS PROJETOS DE LEI.

Neste tempo são inúmeros os Projetos de Lei que tramitam nas casas legislativas visando regulamentar a matéria penal cibernética, haja vista a preocupação da sociedade em criar meios institucionais aptos a reprimir os crimes digitais.

Dentre esses Projetos, o que representa grandes e profundas transformações no conceito desses crimes, está o CD.PL-84/1999, de autoria do Deputado Luiz Piauhylino.

Com redação substitutiva aprovada no Senado em 09 de julho de 2008, o projeto foi remetido a Câmara para votação.

Os pontos principais desse PL é que no artigo 16, esclarece, para efeitos penais, as terminologias técnicas que são utilizadas no meio cibernético.

Ainda, altera significativamente o Decreto-Lei 2.848/40 – Código Penal -, de forma a acrescentar um capitulo especial para crimes contra a segurança dos sistemas informatizados. São eles:

- Art. 285-A: Tipifica o crime de acesso não autorizado a rede de computadores, realizado por violação de segurança: "Acessar, mediante violação de segurança, rede de computadores, dispositivo de comunicação ou sistema informatizado, protegidos por expressa restrição de acesso", punindo o agente com reclusão de 1 (um) a 3 (três) anos, e multa.

O sujeito ativo é qualquer pessoa – crime comum - que acessa, mediante violação de segurança expressa, rede de computador. Entende-se por violação de segurança expressa como a não concordância de uma regra de conduta de acesso, proposta pelo administrador do sistema computacional.

O tipo subjetivo de acessar uma rede segura, com restrição expressa, é requisito essencial para o crime, devendo, portanto, a rede ter um nível mínimo de segurança.

Considerando que este nível não é estipulado, devendo apenas ter uma regra de conduta expressa – tal qual um termo de uso -, se abre a questionamentos de cunho subjetivo, uma vez que dependendo do ângulo pode se considerar típico, ou não, o fato delituoso.

O simples ato de inserir uma mensagem de que a rede é protegida, sem ao menos se importar com requisitos fundamentais são armadilhas ao usuário, que pode acessar o sistema computacional sem esforço algum.

Logo, seguindo que a Lei penal deve ser clara e precisa, em concordância ao principio da taxatividade, podemos considerar que ao não estipular corretamente a conduta, a Lei abrirá discussões que comprometerá sua eficácia.

Portando, percebemos que a conduta tipificada neste artigo, é caracterizada como norma penal branca, fazendo menção genérica ao termo segurança, sem especificar os requisitos mínimos do que pode ser seguro.

O sujeito passivo será sempre o proprietário do sistema invadido. O tipo objetivo é o dolo, ou seja, deve o agente ter a vontade de acessar o sistema, mas pode não ter ciência de que seja não seja protegido.

Para piorar a situação o parágrafo único traz uma qualificadora – utilização de nome falso ou da utilização de identidade de terceiros para a prática do crime -. Todo acesso, tanto em redes locais, como na internet, é feito através de um apelido. Este apelido, na maioria das vezes é criado com base em um pseudônimo, um ser inexistente, transmutado nos desejos sociais do internauta – pode ser SuperHomem, Robocop, Gato_Gostoso, enfim -. O Projeto de Lei, neste caso, pune quem acessa o sistema utilizando estas informações. Um absurdo.

O crime é de mera conduta, não esperando por qualquer resultado, basta acessar o sistema e já temos a materialidade do fato criminoso. Não admite a tentativa.

Por força do Art. 285-C a ação penal procede mediante representação, salvo se o crime é cometido contra o setor público.

- Art. 285-B: Tipifica como crime quem obtém ou transfere, "sem autorização ou em desconformidade com autorização do legítimo titular da rede de computadores, dispositivo de comunicação ou sistema informatizado, protegidos por expressa restrição de acesso, dado ou informação neles disponível", punindo com pena de reclusão de 1 (um) a 3 (três) anos e multa.

Voltamos a ter problemas com mais este polêmico artigo, uma vez que a conduta versa novamente sobre a expressa restrição de acesso.

Segundo o sitio do “abaixo assinado” que pede o veto desse PL[22], os autores consideraram o projeto como “uma séria ameaça à diversidade da rede, às possibilidades recombinantes, além de instaurar o medo e a vigilância”.

Diz ainda, que se aprovado for – como foi – “o simples ato de acessar um site já seria um crime por ‘cópia sem pedir autorização’ na memória ‘viva’ (RAM) temporária do computador. Deveríamos considerar todos os browsers ilegais por criarem caches de páginas sem pedir autorização, e sem mesmo avisar ao mais comum dos usuários que eles estão copiando. Citar um trecho de uma matéria de um jornal ou outra publicação on-line em um blog, também seria crime. O projeto, se aprovado, colocaria a prática do ‘blogging’ na ilegalidade, bem como as máquinas de busca, já que elas copiam trechos de sites e blogs sem pedir autorização de ninguém!”

Ainda, se formos analisar a estrutura organizacional da internet, avaliando a forma que uma rede se liga a outra, não possuindo uma ordem pré-estabelecida, trafegando essa informação por cada “roteador[23]” ligado no backbone, conforme a necessidade e congestionamento da rede serão impossíveis colecionar todas as autorizações do titular de cada rede por onde trafegará essa informação.

De fim, o artigo põe sérias restrições a forma coletiva e compartilhada de tráfego de informações na Internet, servindo para bloquear práticas criativas e liquidar com o avanço das redes abertas.

Comete o crime – sujeito ativo – qualquer um que obtém, ou transfere dados de dispositivo de comunicação ou sistema informatizado. O tipo subjetivo é que esta transferência seja sem autorização ou em desconformidade com a autorização do legitimo titular da rede, e ainda que estes dados estejam protegidos pro expressa restrição de acesso.

O sujeito passivo será o legitimo titular da rede de computadores. Trata-se de crime formal, ou seja, basta que se obtenha, ou transfira o dado para sua consumação, não sendo esperado nenhum outro resultado.

A vontade deve estar presente – crime doloso -, e é admitido a tentativa, uma vez que a transferência pode se interromper por vontade alheia do agente, e com isso não se realiza a obtenção.

A qualificadora do parágrafo único aumenta a pena em um terço se a informação obtida for fornecida a terceiros.

Por força do Art. 285-C, sendo a vitima de caráter privado, procede a ação penal somente representação.

- Art. 154-A: Tipifica a divulgação, comercialização ou disponibilização de “dados e informações pessoais contidas em sistema informatizado com finalidade distinta da que motivou seu registro, salvo nos casos previstos em lei ou mediante expressa anuência da pessoa a que se referem, ou de seu representante legal”, punindo a conduta com detenção de 1(um) a 2 (dois) anos e multa.

Trata-se de crime de violação de segredo, tipificando três condutas: divulgar, comercializar ou disponibilizar informações pessoais.

O tipo subjetivo é a divulgação com finalidade diversa da que motivou seu registro, porem se houver previsão legal, ou mediante expressa anuência da pessoa a que se referem a tipicidade será afastada.

Comete o crime qualquer pessoa que esteja insculpida nos tipos penais, e o sujeito passivo é a quem interessa preservar o segredo.

O dolo é requerido. O crime consuma-se com a pratica dos tipos penais envolvidos, tendo o agente conhecimento de que usa de forma diversa ao fim que se deu o cadastro.

A ação penal é publica condicionada – procede mediante representação – e se admite a tentativa, uma vez que pode o agente não consumar o crime por força alheia a sua vontade.

- Art. 163: Acrescenta ao art. 163 do CP a complementação “ou dado eletrônico alheio”, mantendo a punição de 1(um) a 6(seis) meses, ou multa.

Neste sentido, o legislador compara o dado eletrônico – bem incorpóreo - a um bem patrimonial, de natureza corpórea.

O sujeito ativo é qualquer pessoa que destrói, inutiliza, ou deteriora dado eletrônico alheio.

Considera dado eletrônico "qualquer representação de fatos, de informações ou de conceitos sob forma suscetível de processamento numa rede de computadores ou dispositivo de comunicação"[24].

O sujeito passivo é o proprietário dos dados e a reparação do dano não é causa extintiva de punibilidade.

Exige a vontade de praticar as condutas previstas, e a conduta aguarda a produção do resultado tipificado, consumando-se, ainda que parcial. É admissível a tentativa.

- Art. 163-A: Tipifica a inserção ou difusão de "código malicioso em dispositivo de comunicação, rede de computadores, ou sistema informatizado", com pena de reclusão de 1(um) a 4(quatro) anos, e multa e qualifica, "se do crime resulta destruição, inutilização, deterioração, alteração, dificultação do funcionamento, ou funcionamento desautorizado pelo legítimo titular, de dispositivo de comunicação, de rede de computadores, ou de sistema informatizado", punindo o agente com reclusão de 2 (dois) a 4 (quatro) anos, e multa e com agravante "se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime", com aumento de pena de sexta parte.

Este tipo penal visa tutelar a inserção ou difusão de "vírus", "trojans", "pishing" e outros códigos maliciosos, que podem resultar em destruição, inutilização, deterioração, alteração, dificultação do funcionamento, ou funcionamento desautorizado pelo legítimo titular.

Aparece, portanto, oito condutas típicas.

As duas primeiras, tratando do caput do artigo, versam sobre a ação de inserção ou difusão do código malicioso, e as demais tutelam as conseqüências do ato em si.

O sujeito ativo será sempre quem insere ou difunde o código, mas atente-se, exige o dolo, a vontade de difusão do código malicioso. Logo, o funcionamento desautorizado pelo legitimo titular – retratando que o "vírus" assume a maquina do usuário para se disseminar – acabará sendo excludente de culpabilidade.

Entretanto, podemos considerar o dolo eventual, que consiste quando o usuário sabe que sua maquina esta infectada pelo código malicioso, e que a utiliza para disseminar entre outras maquinas da rede, e não faz nada para impedir, assumindo o risco de produzi-lo.

O sujeito passivo será o prejudicado pelo ato, o proprietário do dado, o titular da rede que teve sua performance reduzida (dificultação de funcionamento) ou o proprietário do sistema informatizado "zumbi".

É admitido a tentativa, uma vez que considerando as características do crime, é possível encontrar o agente pronto a inserir ou disseminar o código malicioso, e não teve sucesso por força externa a sua vontade.

Agrava a pena se o agente se vale de nome falso, ou da utilização de identidade de terceiros.

Aqui, voltamos a discussão dos apelidos, mas a visão do legislador é permitir a rastreabilidade do vilão. Será ponto de discussão nos tribunais.

- Art. 171: Inclui a modalidade de estelionato eletrônico, tipificando a conduta de difusão, por qualquer meio, de "código malicioso com intuito de facilitar ou permitir acesso indevido à rede de computadores, dispositivo de comunicação ou sistema informatizado", punindo com reclusão de 1 (um) a 5 (cinco) anos, e multa. Agrava a pena se o agente "se vale de nome falso ou da utilização de identidade de terceiros" aumentando a pena de sexta parte.

O sujeito ativo é qualquer pessoa que difunde, por qualquer meio, "código malicioso". Exige o dolo de facilitar ou permitir acesso indevido a rede de computadores.

O sujeito passivo é a pessoa que sofre o acesso indevido.

O crime é agravado pela utilização do nome falso ou de utilização de identidade de terceiros. Entendemos que esta agravante acaba punindo o agente duas vezes – bis in idem – uma vez que a utilização de nome falso ou de identidade de terceiro é prevista no caput (induzindo ou mantendo alguém em erro, mediante artifício ardil), assim, a agravante não encontrará respaldo nos princípios penais.

O crime se consuma com a difusão do código malicioso, não exigindo necessariamente que o acesso não autorizado seja realizado. É permitido a tentativa.

- Art. 265: Acrescenta os tipos penais de atentar contra serviços de informação ou telecomunicação, mantendo a pena de reclusão de 1(um) a 5 (cinco) anos e multa.

Trata-se de crime comum, sendo praticado por qualquer um que atente contra os tipos penais insculpidos. O sujeito passivo é a coletividade, o Estado, bem como o particular proprietário do serviço de Telecom ou de informação.

Exige dolo, vontade de atacar os serviços tipificados, e o crime se consuma com a ação capaz de produzir os resultados. É possível a tentativa.

- Art. 266: Insere as condutas típicas de interromper ou perturbar serviço telemático, informático de dispositivo de comunicação, de rede de computadores, de sistema informatizado ou de telecomunicação.

Trata-se de crime comum, onde qualquer pessoa pode-o praticar. Exige o dolo de praticar a conduta, não exigindo qual seja a finalidade da interrupção, devendo o agente apenas ter consciência que pode produzir o resultado.

Elenco um perigo para o técnico de informática, ou do funcionário do provedor de internet, que numa eventual manutenção, com desligamento dos sistemas, pode incorrer no tipo penal, uma vez que por ação ou omissão deveria agir para evitar o resultado.

O sujeito passivo é o Estado, a coletividade que se utiliza dos serviços.

Trata-se de crime de perigo abstrato, uma vez que sem destruir ou diminuir o bem jurídico tutelado, o representa em ameaça de dano. É admissível a tentativa.

- Art. 297: Inclui o tipo penal dado eletrônico no caput do artigo.

Neste contexto, o legislador compara o dado eletrônico ao documento em papel.

Não altera a essência do crime, sendo o sujeito ativo qualquer pessoa e o passivo será o Estado. Exige que haja imitação da verdade, o que é muito fácil em meios eletrônicos, considerando a volatilidade dos dados, porem se o não pode enganar, não haverá crime de falsidade.

Isso é importante quando o documento é assinado digitalmente, onde sua autenticidade é verificada por uma entidade certificadora, na podendo o “diligens pater familia” se iludir.

Trata-se de crime material, devendo ser comprovado por perícia. Exige dolo, vontade de falsificar. É permitido a tentativa.

- Art. 298: Trata-se do mesmo crime previsto no artigo 297, mas é realizado em documento particular.

Ainda, o PL em discussão altera o Código Penal Militar, conferindo a mesma tutela do Código Penal.

Revoluciona quando altera o inciso II do §3º do art. 20 da Lei nº 7.716/89 – Lei do Racismo – oferecendo poder ao juiz, em caso de crime, a cessação das respectivas transmissões eletrônicas, ou da publicação por qualquer meio. Inclui neste caso as paginas de comunidades e sítios eletrônicos diversos.

Na matéria de proteção a criança e o adolescente, altera a Lei 8.069/90 – ECA – de modo a punir as condutas de receptar ou armazenar consigo fotos, imagens com pornografia ou cenas de sexo explicito envolvendo criança ou adolescente. Antes disso, somente era punido o transmissor e não o receptor das fotografias.

Trata-se de crime de mera conduta, ou seja, não importa o fim, havendo busca de apreensão judicial, encontrando por perícia imagens, comete o agente crime, punível com reclusão de 2 (dois) a 6 (seis) anos, e multa.

Por fim, no art. 22 do PL, trata da responsabilidade dos provedores de acesso a rede de computadores, obrigando-os a:

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

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

III - informar, de maneira sigilosa, à autoridade competente, denúncia que tenha recebido e que contenha indícios da prática de crime sujeito a acionamento penal público incondicionado, cuja perpetração haja ocorrido no âmbito da rede de computadores sob sua responsabilidade"[25].

Acontece que a matéria tem sido alvo de duras criticas por parte das entidades sociais que resguardam os interesses dos provedores.

Enquanto o PL tenta resguardar as provas dos crimes cometidos, transferindo aos provedores a responsabilidade de manter os dados de acesso por três anos – culpa da lentidão do judiciário -, os provedores chamam a Convenção de Budapeste, documento internacional ratificado por 22 países que regula os crimes internacionais na rede, que determina a guarda por 90 dias.

Segundo a ABRANET[26] – Associação Brasileira dos Provedores de Internet – o custo dessa guarda está estimado entre 14 e 15 milhões.

Outro ponto polemico trata sobre a obrigatoriedade é o inciso III desse artigo, que determina que os provedores devem informar a autoridade competente as denuncias que recebem e que contenham indícios da prática de crime.

Determinar que os provedores investiguem indícios de crime é transferir para os provedores o papel que compete exclusivamente ao Estado.

Esta atitude, alem de ser infame, vai gerar uma onda de denuncismo que vai levar a criminalização de milhares de pessoas.

CONCLUSÃO

Após todos os levantamentos feitos, concluímos que a legislação vigente possui lacunas graves ao não tipificar condutas que já são parte do Direito Penal em outros países, gerando desconforto e insegurança aos detentores de informações computacionais.

O Brasil avança quando, em pesquisa no site da Câmara dos Deputados, encontramos inúmeros Projetos de Lei que versam para uma possível regulação da matéria.

Considerando que o Direito Penal não permite a analogia, é dever das casas legislativas aprovar, em regime de urgência, os projetos em tramitação.

Contudo, como podemos perceber no substitutivo PL89/2003, a legislação enfrentará problemas, se na Câmara não for corrigido os pontos polêmicos e incongruentes.

Neste tempo, considerando o potencial ofensivo dos crimes cibernéticos e a branda legislação penal existente, iremos observar a prática crescente dos ciber-crimes, que evoluem de forma tão rápida a tal ponto que, quando for sancionado qualquer Lei que verse sobre o tema, corremos o risco dela já ser obsoleta e perder sua eficácia no controle social.

Deve os organismos sociais estar atentos a esses problemas, e exigir uma resposta mais rápida do Legislativo. Corremos sério risco de perdermos a luta para os ignóbeis que se locupletam neste deserto de regras.

Referência:

____, Telefônica Espanha. **Conceito de Sociedade da Informação**, 2002, Disponível em: <http://www.telefonica.es/sociedaddelainformacion/pdf/informes/brasil_2002/parte1_1.pdf>. Acesso em 20 julho 2008.

____, Colégio Web. **Evolução da Sociedade**, Disponível em <http://www.colegioweb.com.br/geografia/evolucao-da-sociedade>. Acesso em 20 julho 2008a.

____. **Pelo veto ao projeto de cibercrimes - Em defesa da liberdade e do progresso do conhecimento na Internet Brasileira**. Disponível em: < http://www.petitiononline.com/veto2008/petition.html>. Acesso em 21 julho 2008q.

____, Consultor Juridico. **Crimes cibernéticos Itamaraty ainda estuda adesão à Convenção de Budapeste**. Disponível em: < http://www.jusbrasil.com.br/noticias/17355/crimes-ciberneticos-itamaraty-ainda-estuda-adesao-a-convencao-de-budapeste>. Acesso em 21 julho 2008r.

____, **Diga Não a Erotização Infantil. Lei sobre crimes virtuais transfere ação do Estado para a sociedade, diz Abranet**. Disponível em: <http://diganaoaerotizacaoinfantil.wordpress.com/2008/07/11/lei-sobre-crimes-virtuais-transfere-acao-do-estado-para-a-sociedade-diz-abranet/>. Acesso em 21 julho 2008n.

BRASIL. Constituição (1988). **Constituição da República do Brasil**. Brasília, DF: Senado, 1988.

BRASIL. Lei 6.815 (1980). **Define a situação jurídica do estrangeiro no Brasil, cria o Conselho Nacional de Imigração**. Disponível em: <http://www.planalto.gov.br/Ccivil_03/Leis/L6815.htm>. Acesso em 21 julho 2008.

BRASIL. Lei 8.137 (1990). **Define crimes contra a ordem tributária, econômica e contra as relações de consumo, e dá outras providências**. Disponível em: <http://www.planalto.gov.br/Ccivil_03/Leis/L8137.htm>. Acesso em 21 julho 2008e.

BRASIL. Lei 9.296 (1996). **Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal**. Disponível em: <http://www.planalto.gov.br/Ccivil_03/Leis/L9296.htm>. Acesso em 21 julho 2008f.

BRASIL. Lei 9.504 (1997). **Estabelece normas para as eleições**. Disponível em: <http://www.planalto.gov.br/Ccivil_03/Leis/L9504.htm>. Acesso em 21 julho 2008k.

BRASIL. Lei 9.609 (1998). **Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências**. Disponível em: <http://www.planalto.gov.br/Ccivil_03/Leis/L9609.htm>. Acesso em 21 julho 2008l.

BRASIL. DEC-Lei 2.848 (1940). **Código Penal**. Disponível em: < http://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del2848.htm>. Acesso em 21 julho 2008c.

BRASIL. Câmara dos Deputados. Projeto de Lei 84 (1999). Autor Luiz Piauhylino – PSDB-PE. **Dispõe sobre os crimes cometidos na área de informática, suas penalidades e dá outras providências**. Situação em 21 julho 2008p: MESA. Aguardando Retorno.

BRASIL. Lei 7.716 (1989). **Define os crimes resultantes de preconceito de raça ou de cor**. Disponível em: < http://www.planalto.gov.br/ccivil_03/Leis/L7716.htm>. Acesso em 21 julho 2008o.

BRASIL. Lei 8.069 (1990). **Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências**. Disponível em: < http://www.planalto.gov.br/ccivil_03/Leis/L8069.htm>. Acesso em 21 julho 2008.

BRASIL. Superior Tribunal Federal. EXT 1029-PT-Portugal. Requerente: Governo de Portugal. Extraditado: Jorge Campilho Pereira. Relator: Min. Cezar Peluso. Brasília, 13 setembro 2006d.

BRASIL. Superior Tribunal Federal. Inq 1656/SP. Autor: Ministério Público Federal. Denunciado: Odeval José Gonçalves. Relator: Min. Ellen Gracie. Brasília, 18 dezembro 2003g.

BRASIL. Superior Tribunal Federal. HC 86032. Impetrante: Paulo Alfredo De Souza Silva E Outro(A/S). Coator: Superior Tribunal de Justiça. Relator: Min. Celso de Melo. Brasília, 04 setembro 2007h.

BRASIL. Superior Tribunal Federal. ADI 1448/DF. Requerente: Associação dos Delegados de Policia do Brasil. Requerido: Congresso Nacional. Relator: Min. Neri da Silveira, 09 março 2001i.

BRASIL. Superior Tribunal Federal. Inq 1879. Autor: Ministério Público Federal. Denunciado: Antônio Carlos Magalhães. Relator: Min. Ellen Gracie, 10 setembro 2003m.

CHAUI, Marilena. **Convite a Filosofia**. São Paulo: Ed. Ática, 2000.

CUNHA, Marcio Soares. **Aplicação da Lei Penal na Internet**. Universidade Católica de Goiás, 2002, Disponível em: <http://agata.ucg.br/formularios/ucg/institutos/nepjur/pdf/aplicacaodaleipenalnainternet.pdf>. Acesso em: 21 julho 2008.

DIZARD Jr., Wilson. **A nova mídia: a comunicação de massa na era da informação**. Rio de Janeiro : Jorge Zahar Ed., 2000.

MAIA, Felipe. Folha On-Line. **Lei sobre crimes virtuais transfere ação do Estado para a sociedade, diz Abranet**. Disponível em <http://www1.folha.uol.com.br/folha/informatica/ult124u421234.shtml>. Acesso em 21 julho 2008.
MARQUES, José Frederico. Curso de Direito Penal. São Paulo: Edit. Saraiva, 1956.
MILAGRES, Francisco Gomes. **Uso de Informações de Contexto em segurança computacional**, 2004, Disponível em: <http:// http://milagres.com/papers/milagres_msc.pdf>. Acesso em: 04 julho 2008.
MIRABETTE, Julio Fabrini. **Código Penal Interpretado**. São Paulo: Ed. Atlas, 2005.
PECK, Patrícia Peck. **Direito Digital**. São Paulo: Ed. Saraiva 2002.
RENAULT, Leonardo Vasconcelos. **PARADIGMAS E MODELOS: proposta de análise epistemológica para a Ciência da Informação**, 2007, Disponível em: <http://www.ies.ufpb.br/ojs2/index.php/ies/article/view/636>. Acesso em: 12 julho 2008.
WIKIPÉDIA. Desenvolvido pela Wikimedia Foundation. Apresenta conteúdo enciclopédico. Disponível em: <http://pt.wikipedia.org/w/index.php?title=Bit&oldid=11459028>. Acesso em: 20 Jul 2008b.
WIKIPÉDIA. Desenvolvido pela Wikimedia Foundation. Apresenta conteúdo enciclopédico. Disponível em: <http://pt.wikipedia.org/w/index.php?title=Bin%C3%A1rio&oldid=6173346>. Acesso em: 24 Jul 2008j.
WIKIPÉDIA. Desenvolvido pela Wikimedia Foundation. Apresenta conteúdo enciclopédico. Disponível em: < http://pt.wikipedia.org/wiki/V%C3%ADrus_de_computador>. Acesso em: 21 Jul 2008.
WIKIPÉDIA. Desenvolvido pela Wikimedia Foundation. Apresenta conteúdo enciclopédico. Disponível em: < http://pt.wikipedia.org/wiki/Trojan>. Acesso em: 21 Jul 2008.

Notas:

[1] Consiste na adoção da seguinte linha de raciocínio: “quando os conhecimentos disponíveis sobre determinado assunto são insuficientes para a explicação de um fenômeno, surge o problema. Para tentar explicar a dificuldades expressas no problema, são formuladas conjecturas ou hipóteses. Das hipóteses formuladas, deduzem-se conseqüências que deverão ser testadas ou falseadas. Falsear significa tornar falsas as conseqüências deduzidas das hipóteses. Enquanto no método dedutivo se procura a todo custo confirmar a hipótese, no método hipótetico-dedutivo, ao contrário, procuram procuram-se evidências empíricas para derrubá-la (SILVA, Edna Lucia, p. 27).

[2] George Boole nasceu em 2 de Novembro de 1814 em Lincoln , na Inglaterra. O desenvolvimento natural do que Boole começou, transformou-se em uma das mais importantes divisões da matemática pura. Disse Bertrand Russell: “a matemática pura foi descoberta por Boole em seu trabalho “Leis do Pensamento”, publicado em 1854 (Wikipédia).

[3] Conjunto de textos estruturados ou organizados dessa forma, e ger. implementado em meio eletrônico computadorizado, no qual as remissões correspondem a comandos que permitem ao leitor passar diretamente aos elementos associados (Dicionário Aurélio Eletrônico).

[4]Andy Wachowski e Larry Wachowski.

[5] DIZARD, 2000, p. 24.

[6] Numa rede como a Internet, o segmento final de um endereço eletrônico (q. v.), que identifica a rede local, a instituição, ou o provedor de acesso do servidor (Aurélio Eletrônico).

[7] A parte de uma rede de computadores, ou sua estrutura física, que suporta o maior tráfego de informações (Aurélio Eletrônico).

[8] Convite a Filosofia, 2000, p. 302.

[9] PESSIS, Do caos à inteligência artificial, UNESP, 1993, p. 242.

[10] Introdução ao Estudo do Direito, Forense, 2001, p. 15.

[11] RABANEDA, Discurso a Ordem, Apud Goffredo Telles Júnior em sessão de abertura da semana de recepção dos calouros na Faculdade Largo do São Francisco, em São Paulo, 26 de fevereiro de 2007.

[12] Inq.1656/SP/STF/Relatora: Min. Ellen Gracie.

[13] HC 86.032/RS/STF/Relator: Min. Celso de Melo, HC 91.542/RJ/STF/Relator: Min. Cezar Peluso, HC 89.227/CE/STF/Relator: Min. Eros Grau.

[14] Diz-se de programa que pode ser executado diretamente por computador, por encontrar-se codificado em linguagem de máquina (Aurélio Eletrônico).

[15] Marques, Curso de Direito Penal, p. 81.

[16] Na ADI citada.

[17] Em informática, um vírus de computador é um programa malicioso desenvolvido por programadores que, tal como um vírus biológico, infecta o sistema, faz cópias de si mesmo e tenta se espalhar para outros computadores, utilizando-se de diversos meios (Wikipédia).

[18] Trojan Horse ou Cavalo de Tróia é um programa que age como a lenda do cavalo de Tróia, entrando no computador e liberando uma porta para um possível invasor (Wikipédia).

[19] Art. 1º Programa de computador é a expressão de um conjunto organizado de instruções em linguagem natural ou codificada, contida em suporte físico de qualquer natureza, de emprego necessário em máquinas automáticas de tratamento da informação, dispositivos, instrumentos ou equipamentos periféricos, baseados em técnica digital ou análoga, para fazê-los funcionar de modo e para fins determinados.

[20] Código Penal Interpretado, Atlas, 2005, p. 1214.

[21] Inq. 1879/DF/STF/Relator: Ellen Gracie.

[22] http://www.petitiononline.com/veto2008/petition.html

[23] Aparelho designado para determinação da rota (ou direção imediata) de um bloco de informações enviado numa rede de computadores em que há comutação de pacotes (q. v.) (Aurélio Eletrônico).
[24] Art. 16 PL cit.
[25] PL cit.
[26] http://www1.folha.uol.com.br/folha/informatica/ult124u421234.shtml.