Brasília, 04 de julho de 2.007.

Exmo. Sr.
Senador Presidente da CCJ-Senado Federal,

Exmo. Sr.
Senador Presidente da CCT-Senado Federal,

Senhores e Senhoras Senadores que integram a presente Audiência Pública,

Primeiramente, gostaríamos de agradecer a honrosa oportunidade que nos concede o convite para participação nesta histórica Audiência Pública.

Nela, o Senado da República tratará de um de seus mais importantes projetos – resumido, hoje, no substutitivo que está apresentado aos Projetos de Lei do Próprio Senado (PLS 76 e 137 de 2.000) e da Câmara Federal (PLC 89 de 2.003) sobre crimes ditos

“informáticos” – ou, ilícitos penais eletrônicos-cibernéticos.

Para que nossa abordagem se resuma a uma objetiva e concreta participação, e com ela busquemos contribuir para o enriquecimento da discussão, estamos dividindo nossa participação para resumi-la a três tópicos principais. São eles:

- <u>Primeiro</u> –

OS DADOS QUE COMPÕEM A ATUAL REALIDADE CIBERNÉTICA BRASILEIRA

- <u>Segundo</u> –

A OPÇÃO DE CRIMINALIZAÇÃO DOS ILÍCITOS CIBERNÉTICOS PELO ESTADO BRASILEIRO

- <u>Terceiro</u> –

BREVE ANÁLISE DOS DISPOSITIVOS SUGERIDOS PELO SUBSTITUTIVO EM DISCUSSÃO

Pedimos permissão, antes de entrarmos propriamente nesses tres temas, para uma breve citação. Com ela esclarecemos nossa ligação com o tema – magistrado de carreira, que somos, do Estado de Minas Gerais, responsável, hoje, por projetos de TI-Tecnologia da Informação do Tribunal de Justiça de MG, pela Assessoria Especial de TI à Presidência daquele Tribunal, pela coordenação dos estudos de implantação do processo eletrônico no TRE-MG, e membro de entidades de TI dentre as quais a ABDI-MG (Associação Brasileira de Direito de Informática e Telecomunicações e o CBTMs-Conselho Brasileiro de Telemedicina/SP) – nosso trabalho, além da atividade jurisdicional, tem intensa ligação com a área de TI.

Nossa citação é, assim, extraída do trabalho "*CRIMES E CYBERCRIMES*", que publicamos recentemente e cujo exemplar anexamos, para análise por esta douta Comissão, como documento do ANEXO II desta abordagem.

Dizíamos, ali, e o repetimos agora:

"....O crime cibernético, tal como o crime físico-comum, tem raízes antigas, humanas; seu traço antropológico não está fora do que marca o "mito do mal". A maldade humana, seu fundamento-básico, é o seu ponto psíquico-comum com o crime físico.
Diferenciar, no tratamento, o criminoso, do crime comum-físico, do delinqüente cibernético é errar profundamente a análise sociológica do crime; é medir equivocadamente sua causação antropológica.
Pior. Equivale diferenciar, por mera sofisticação dos meios usados na execução "do mal", o tratamento do psiquismo delitivo, dispensando, ao melhor preparado (em meios), repercussão criminal menos rigorosa.
A cibernética altera tão só o meio, o instrumento, de execução do crime, não a sua conformação negativa, como fato que atenta contra importantes interesses comunitários. ....."

Com essa filosofia de enfrentamento do tema, passamos a analisar o primeiro ponto proposto.

- <u>Primeiro</u> –

OS DADOS QUE COMPÕEM A ATUAL REALIDADE CIBERNÉTICA BRASILEIRA

Países, como os EUA, estimam, hoje, a rentabilidade atual dos chamados "crimes cibernéticos" em cifras estratosféricas.

Em 2.004, para citar apenas um exemplo, a Conselheira do Tesouro americano, Valeri McNiven, tornou pública uma afirmação de que, com a prática de fraudes, espionagem corporativa, manipulação de ações, pedofilia, extorsão virtual, pirataria, dentre outros ilícitos eletrônicos, o "faturamento" dos chamados crimes cibernéticos havia chegado à impressionante soma de US$ 105 bilhões.

Comparativamente, no Brasil, no período entre 2.004 e 2.005, apenas as fraudes bancárias e financeiras por meio eletrônico saltaram de 5% (2004) para 40% (2005) do total dos incidentes eletrônicos registrados no país naquele período. O dado é do CERT.br ("Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil" – www.cert.br) e informa que as tentativas de fraudes pela rêde mundial cresceram, naquele ano (2.005), 579%.

As armadilhas eletrônicas – a "pescaria" eletrônica de incautos (o "phishing scam", por exemplo, ou, os "hoax" – as piadas de má-intenção voltadas para a obtenção de

vantagem ilícita-patrimonial) – cunharam uma nova "aplicação" da "engenharia do mal", ou, a "engenharia social", entendida como o rol de práticas implementadas por "experts" para engodo, engano, indução a erro, de pessoas e corporações não habilitadas à lida técnica com recursos sofisticados de TI.

O que surgiu como ataque e defesa de caráter puramente tecnológico – "hackers" que, sofisticalizando o abandono dos rigores técnicos de seu ofício profissional, tornaram-se "crackers", e avançaram sobre sistemas e redes eletrônicos não adequadamente estruturados – passou à velha e milenar característica humana, que é o abuso do homem-pelo-homem.

A chamada "engenharia social" não passa de uma vergonhosa disputa, no meio eletrônico, da superioridade cultural-técnica dos maus "experts" sobre a limitada capacidade popular de conhecimento técnico dos recursos das rêdes.

Onde há o desconhecimento técnico, navega, livre, o abuso, o ímpeto cruel da exploração, da indução a erro, com ele o desejo do proveito fácil, como ocorre com as senhas secretas obtidas, hoje, por "e-mails" falsos, falsos anúncios de cancelamentos de títulos eleitorais, convites para entrada em sites de premiação, simulação de websites para coleta de logs secretos, etc., enfim um arsenal de fraudes, simulações, que passaram a ter na sofisticação do meio e no desconhecimento humano-generalizado de suas potencialidades um novo "ar" de atuação.

Estamos juntando a esta abordagem, Senhores Senadores, três publicações, todas recentes – de 2.006, uma, e de abril/maio-2007, as duas outras –especializadas em segurança da informação eletrônica no Brasil. Foram todas editadas pela conceituada empresa "MÓDULO TECHNOLOGY FOR RISK MANAGEMENT", que, hoje, inicia processo de exame dos recursos tecnológicos-eletrônicos do TJMG para prestação de serviços de mapeamento e planejamento de segurança da informação eletrônica interna e

externa, e que vem prestando serviços a outros importantes órgãos públicos da União e dos Estados.

Poderão ver Vvs. Exas., nesses volumes, dados impressionantes do crescimento da demanda por serviços eletrônicos no Brasil – e, com eles, por segurança mínima contra fraudes e crimes cibernéticos já implementados.

São eles:

1 – O Serviço de declaração do IR pela Internet, que acaba de completar 10 anos de existência, foi usado, agora em 2.007, por 99% dos contribuintes-declarantes, isto é, das 23,270 milhões de declarações recebidas pela SRF, 22,900 foram enviadas pela Internet, numa mostra do volume quase absoluto da adesão da população contribuinte a sistemas eletrônicos convencionais (pág. 13 do vol. 12, da rev. "Risk Management Review", em anexo);

2 – Por outro lado, ou, em paralelo com esta crescente adesão voluntária-popular ao meio eletrônico público e privado,

registrou o país número expressivo de incidentes de segurança na internet no mesmo ano do exercício fiscal declarado (197 mil em 2006, ou, um crescimento de 191% em relação aos 68 mil registrados em 2.005). Desses números, apenas a prática do "phishing scam" – a "pescaria eletrônica" de incautos pela Internet, usualmente, por e-mails não-autorizados, uma característica da tal "engenharia social" – respondeu por 21% destas ocorrências. O "phishing scam" para obtenção de senhas bancárias e de números de cartões de crédito cresceu, em 2006, 53% (pág. 14 do vol. 12, da rev. "Risk Management Review", em anexo).

3 – As empresas de grande porte estão investindo crescentes somas de seus orçamentos na tentativa de proteção a clientes, consumidores, e a seus próprios ativos. Cita-se, como exemplo recente, a ocorrência de tentativa de fraude em sistema de pedágio capixaba de grande porte – ocorreram acessos indiretos à base de dados e procedimentos manuais na coleta de informações consolidadas sobre o movimento de

veículos passantes pelo pedágio (portanto, uma atividade supostamente atribuível ao próprio corpo funcional-interno da empresa concessionária, ou indícios de atuação humana conjugada a acessos livres a base eletrônica de dados). Este fato demandou investimentos em reforço de tecnologia da informação, com custos repassáveis aos usuários do próprio sistema público de transporte (caso citado à pág. 32 do vol. 12, da ver. "Risk Management Review").

4 – A maior empresa brasileira de distribuição de petróleo e derivados anuncia, à pág. 34 da mesma revista citada, que, "*....possuindo uma força de trabalho com mais de cinco mil pessoas espalhadas por todo o Brasil...*", teve que fazer significativos investimentos em segurança (interna) da informação eletrônica, pois, acentua, "*...a informação é um dos ativos mais preciosos da companhia, sendo, portanto, fundamental, que todos estejam conscientes da sua preservação...*" (pág. 35).

5. Igualmente, as empresas de cartões de crédito informam um salto nas

dimensões do mercado com uso desta sistemática: transações eletrônicas, com cartões de crédito, passaram, em somatória total, de R$ 4,3 bilhões/2006 para R$ 4,9 bilhões/2007 (pág. 41 da rev.Citada). São informações eletronicamente trocadas pela população usuária dos serviços com prestadores da garantia de pagamento e fornecedores de bens e serviços.

6. Comparativamente a este crescimento, pesquisa do Gartner Group – citada à pág. 22 do vol. 11 da revista "Security Review" (anexa) – sustenta que as compras de softwares "de defesa" corporativa (destinados à segurança da informação eletrônica processada e armazenada) atingirão aumento de 10,7% em 2.007, sendo que, em todo o mundo, a cifra deverá atingir US$ 9,1 bilhões contra US$ 8,2 bilhões em 2.006 e, principalmente, que mais da metade deste mega-investimento, ou o equivalente a 53,8%, será destinada à compra de programas "anti-vírus"., que responderão, sozinhos, por US$ 4,9 bilhões. O "Gartner Group" estima que, em 2.007, em razão da crescente demanda de ataques cibernéticos às

rêdes corporativas, 3 em cada 4 organizações serão atacadas por códigos eletrônicos maliciosos. No Brasil, a venda de programas de computador destinados à proteção eletrônica foi estimada, pelo IDC-International Data Corporation Brasil (http://www.idclatin.com/default2.asp?ctr=bra), em US$ 144 milhões em 2.006, mais que o dobro do volume notado no ano anterior (2.005) (página 22 do vol. 11 da Revista "Security Review", em anexo).

7. Uma das maiores e mais conhecidas empresas de prestação de serviço medico do país – indicada às fls. 45 da revista mencionada – está investindo, apenas no Estado de SP, somas expressivas em segurança da informação, direcionando-as especificamente a sistemas de identificação biométrica para reconhecimento de seus segurados por impressões digitais. Anuncia que o faz porque "*...20% das despesas do atendimento médico no país em 2006 são fraudes*...", chegando à conclusão, por isso, que o investimento em sistemas eletrônicos, e em defesa desses, através de recursos tecnológicos de

segurança da informação que a resguarde contra fraudes humanas-eletrônicas, prestigiará a redução de seus custos operacionais, resultando na busca de melhores tarifas de serviços ao consumo (págs. 45 e 46 do vol. 11 da Revista mencionada – em anexo).

8. O BACEN-Banco Central, em nota publicada à pág. 51 da mesma Revista, anuncia que, até o dia 31.12.2007, todos os bancos brasileiros deverão cumprir a Resolução 3380/BACEN, de 29.06.2006, no sentido de otimizarem seus sistemas eletrônicos para redução de riscos operacionais (reportagem da pág. 51 da Revista mencionada).

9. À pág. 52, o Secretário Geral do CNJ-Conselho Nacional de Justiça, detalha o que será a Justiça brasileira com a completa integração-informatização dos 91 Tribunais brasileiros (a implantação do sistema eletrônico que irá eliminar o papel como matriz física do processo judicial brasileiro, em todas as instâncias, para todas as jurisdições – a questão está prevista na Lei 11.419/2006, e detalhada à

pág. 52/53 da Revista anexa). Sobre este projeto, diria, mega-projeto brasileiro – em nada inferior, talvez até superior, ao porte da transformação do processo eleitoral brasileiro em sistema eletrônico de eleições – há números significativos: 42 milhões de processos judiciais, contendo os dados da população brasileira, serão tornados eletrônicos. Suas peças, petições, provas, decisões, pareceres, serão, todos, transformados em "bits" digitais eletrônicos, que se incumbirão, ao invés do papel, da nova estruturação estatal do mecanismo de solução de conflitos do país. Em MG, na Justiça Estadual, há, hoje, 3.500.000 processos judiciais em papel; em SP, são 12.000.000 de processos judiciais na Justiça Estadual. Eles se tornarão eletrônicos. Os Tribunais estão implantando pilotos de experimentação desses processos sem papel. Em SP, foi recentemente inaugurado, na Freguesia do Ó, o primeiro Juizado Especial eletrônico da maior metrópole da AL. Nele, não há papel. Não há papel na Justiça Estadual de Florianópolis – Vara de Família virtual – nem na Vara Federal do JEF de São Gonçalo, no RJ; nem,

tampouco, no Fórum virtual (criminal, cível-de-família) de Manaus, e noutros tantos. Em MG, instalaremos, no Juizado Especial de Telefonia de Belo Horizonte, um dos maiores e mais movimentados do país, em agosto próximo, nosso primeiro experimento estadual de Justiça completamente eletrônica. Isto tem tomado dos Tribunais, particularmente das Diretorias de TI e dos magistrados que ocupam funções de TI, cuidados intensos com a segurança da informação (externa e interna), pois dados sensíveis da população, como os inerentes aos conflitos de família, os criminais, os que dizem respeito à intimidade das pessoas, aos segredos industriais, às cláusulas contratuais "non-disclosure", e tantos outros, não podem ser abertos ao público por sistemas eletrônicos desguarnecidos, ou fornecidos-comercializados desautorizadamente. Investimentos em TI, em mapeamento de pontos de vulnerabilidade eletrônica das rêdes internas e externas dos Tribunais, estão sendo alocados e previstos em "budgets" orçamentários.

10. Ainda assim, há riscos intensos – que precisam ser cuidados. Nos EUA, o sistema PACER, que coordena o programa de processo judicial eletrônico da Secretaria de Justiça norteamericana (mais de 25.000.000 de processos judiciais sem papel, das Côrtes Federais dos EUA), impede acessos a dados de intimidade dos litigantes processuais e responsabiliza, inclusive criminalmente, fraudes na obtenção não-autorizada desses dados. No Brasil, não dispomos de normas legais específicas que autorizem providências incriminadoras ou de criminalização específica, como esta, do acesso indevido a dados eletrônicos-processuais não-autorizados.

11. Não podemos deixar também de mencionar importante trabalho de pesquisa realizado pela empresa MÓDULO TECHNOLOGY FOR RISK MANAGEMENT – com mais de 600 profissionais brasileiros, atuantes nas áreas de Segurança e Tecnologia da Informação de organizações privadas, públicas, e de economia mista do país, nos segmentos de Governo, Financeiro, Informática, Indústria,

Prestação de Serviços, Telecomunicações, Comércio, Educação, Energia Elétrica, Saúde, Mineração, dentre outros. O trabalho – juntado, igualmente, a esta abordagem (entitulado "10ª. Pesquisa Nacional de Segurança da Informação", pág. 6) – mostra, como principais problemas relatados por estas corporações e como causas diretas de perdas financeiras, as seguintes:

a) ataques eletrônicos por vírus (15%);

b) ataques eletrônicos por spam (10%);

c) fraudes eletrônicas (8%);

d) vazamento de informações sensíveis (7%);

e) acesso remoto indevido (6%)

f) divulgação/roubo de senhas eletrônicas (5%);

g) invasão de sistemas internos (4%);

h) furto de informações proprietárias (2%);

i) sabotagem eletrônica (2%);

j) pirataria (2%);

l) espionagem (1%).

12. Estes dados estão refletidos na própria estruturação institucional da inteligência custodiada pelo Estado brasileiro. A ABIN-Agência Brasileira de Inteligência salienta – em reportagem com o Sr. Márcio Buzzanelli, que a dirige com "expertise" de ex-chefe de divisões de crime organizado e terrorismo no Oriente Médio (pág. 8 da Revista "Security Review", vol. 11, anexo) – instituiu o PNPC-Programa Nacional de Proteção ao Conhecimento, desenvolvendo trabalho no CEPESC_Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações, adotando metodologia denominada "risk@Gov" e usando o DSIC-Departamento de Segurança das Informações e Comunicações, criado pelo Presidente Lula especialmente para coordenação das atividades de segurança da

informação do governo federal. Isto, ou este arsenal público destinado à Segurança da Informação, decorre do fato de que, no dizer do referido gestor, "*...o setor público é responsável por uma série de serviços ao cidadão e, em última análise, um ataque à rede de dados de alguma instituição da Administração Pública Federal irá...prejudicar o fornecimento desses serviços, prejudicando o bem-estar do cidadão*...".

13. **Os riscos dos ataques à informação e aos dados sensíveis – corporativos públicos e privados – brasileiros têm crescido a ponto de os Estados internamente se organizarem para a dotação de organismos investigatórios-policiais especializados na coleta de indícios da prática de delitos eletrônicos (como a técnica do rastreamento dos endereçamentos IP). É uma realidade que retrata a que se nota fora do país[1]. Vejam exemplos brasileiros:**

---

[1] Anti-Phishing Working Group
CardCops
Corporate Investigator, The,
Cybercrime - Computer Crime and Intellectual Property Section
Delitos Informáticos (Espanha)
Delitos Informáticos (México)
Digicrime Inc.
The Fake Detective

A - Coordenadoria de Investigações Eletrônicas - MP/RJ
B - Delegacia Virtual - Rio de Janeiro
C - Delegacia de Repressão aos Crimes de Informática - DRCI
Delegacia Eletrônica - São Paulo
D - Delegacia Online - Rio Grande do Sul
E - Ministério Público Federal - Digi-Denúncia
F - Hotline Br - denuncie a pornografia infantil
G - Brasil Telecom - denúncias de fraude
H – Delegacia Especializada em Crimes Informáticos/BH-MG

14 – Outras particularidades da vida eletrônica brasileira têm chamado a atenção de organismos internacionais. Um exemplo é o das comunidades relacionais do "Orkut". Um programa gerado e concebito como

---

FBI
FraudWatch International
Incident Response, Electronic Discovery, and Computer Forensics
Internet Fraud Complaint Center
Internet Identity
Internet Safety - The Police Notebook
Interpol
Newsfactor - Cybercrime & Security
P2P Patrol
Perverted-Justice
Polícia Judiciária - criminalidade informática (Portugal)
US-Cert: Cyber Security Tips
Web Police
ZNet - News - Ecrime, Law & You

Hacking: (voltar)

AdvICE - database of information security
Hackers' Hall of Fame
Hacktivismo
MIT Hack Gallery
Zone-H

Mecanismos de bloqueio e filtros: (voltar)

Cybersitter
Net Nanny
SurfWatch - Internet Filtering Software
SurfControl
http://www.internetlegal.com.br/links/crimes.htm

um sistema relacional via Internet, destinado, conceitualmente, à formação de grupos – científicos, acadêmicos, relacionais familiares, afetivos, etc. – e criado, há três anos, nos EUA, por uma empresa norteamericana ("Google Inc"), tem, como sua maior comunidade mundial, a de jovens brasileiros, que compõe, hoje, mais de cinqüenta por cento do universo das comunidades "Orkut"de todo o globo. Pois o "Orkut" tem provocado, ao lado de seu incomensurável efeito benéfico-relacional, atentados brasileiros os mais variados, como páginas de ataque à honra de personalidades públicas, de corporações privadas, de formação (eletrônica) de comunidades voltadas para o crime financeiro, comercialização internacional e nacional de entorpecentes e, mais recentemente, organização de ataques físicos e cibernéticos coletivos, fatos que começam a chegar às barras dos criminais sob intensa discussão de tipicidade penal. As regras de extraterritorialidade da lei penal-convencional brasileira não têm conseguido inibir este crescente nível de criminalidade eletrônica e um dos

motivos tem sido a alegação do fato de que a estrutura física de armazenamento das páginas Orkut estaria situada em território norteamericano, sem possibilidade de atuação jurisdicional brasileira. O Ministério Público Estadual, de Minas Gerais, acaba, inclusive, de firmar acordo diretamente com a empresa "Google Inc." via do qual a empresa disponibilizará uma página/Internet direta e especialmente para acesso por Promotores de Justiça e Policiais de MG, a fim de que obtenham estes, ali, informações eletrônicas de praticantes de pedofilia eletrônica, promoção eletrônica de venda de armas e entorpecentes (vide http://www.mp.mg.gov.br/extranet/internet.action#o9gDPnwAHrvzTbhBHrxzifMBKXwzY5ICLnwDWvMCHjhkJ9MB0vwDK92qH9glXmdm5idl1Gtk7a).

15. Por último, estatísticas têm demonstrado que os ataques a rêdes corporativas de telecomunicações – intranets, extranets, internets – provêm, em percentuais significativos (acima de 24%), de iniciativas dos próprios empregados-colaboradores internos, bem como a eles tem sido em grande parte atribuída a ação

criminosa de comercialização de senhas, logs computacionais, e até códigos alfa-numéricos de telefonia móvel celular. Quem não se lembra da extensão da "clonagem celular" ? Começou com um singelo ato de cunho tecnológico – o uso de um scanner de radiofreqüência em regiões/antenas em que a emissão do sinal telefônico se fazia no modo analógico. Depois, passou para outro nível, o da fraude humana e não tecnológica, quando então, ao invés de equipamentos, foram subtraídos dados significativos (códigos alfa-numéricos) de bancos de dados das empresas de telefonia para comercialização em praça pública, o que passou a explicar a razão pela qual CDs de baixo custo, com milhares de números de telefones, tornaram-se comercializáveis, ilegalmente, em regiões centrais as mais variadas, como as de São Paulo, Rio de Janeiro, Belo Horizonte, e outras.

Em suma, Senhores Senadores, podemos resumir esses dados em objetivas conclusões. São elas:

A – O nível do envolvimento crescente da população – das pessoas naturais e

das corporações – com os sistemas eletrônicos em geral (rêdes corporativas internas, externas, Internet, telefonia móvel, fixa) atinge, na atualidade, volume majoritário do interesse nacional (cem milhões de telefones celulares, 50 milhões de telefones fixos, 20 milhões de usuários/Internet);

B- Os serviços públicos eletrônicos brasileiros – dos Poderes Executivo, Legislativo, Judiciário – cresceram e crescerão, significativamente, de agora em diante, de modo a exigirem cautelas e cuidados especiais por parte do Estado brasileiro quanto à Segurança da Informação relativamente aos dados sensíveis custodiados no âmbito de cada Poder;

C – Os ataques e condutas lesivas, contrárias a uma mínima visão de razoabilidade social, denotam crescente tendência delitiva por parte de usuários de sistemas eletrônicos de comunicação. Estes fatos arriscam interesses da majoritária parcela de usuários, formada por inocentes, gerando uma desigualdade prática que tem cunhado expressões as mais

inaceitáveis para o convívio harmônico como o da "engenharia social";

D – As ações criminosas eletrônicas, por razões de sofisticação, massificação, e alto poder ofensivo-humano, rompem o poder de defesa gerado por emprego de meros softwares ou medidas paliativas de proteção. A ação produtiva do injusto eletrônico reclama contra-ação estatal minimamente preventiva, que contenha a necessidade de emprego de grandes somas de recursos financeiros, grandes contingentes estratégicos, na defesa de dados sensíveis de interesse público, a portes administráveis;

E – Finalmente, o grau de interesses lesados ou sujeitos a risco de lesão potencial já sobe ao porte dos interesses tuteláveis pelo Estado através do emprego de medidas penais, especificamente de criminalização destas condutas.

Passamos, assim, a tratar do segundo ponto.

- Segundo –

A OPÇÃO DE CRIMINALIZAÇÃO DOS ILÍCITOS CIBERNÉTICOS PELO ESTADO BRASILEIRO

O moderno Direito Penal e os estudos de criminologia editados, no mundo contemporâneo – especialmente na Europa – após a fase do Iluminisno repugnam a primitiva idéia, que vigorou até à Idade Média, "da lei de Talião", do uso da pena, do Direito Penal, como meio de retribuição "pelo mal causado".

A criminalização não pode derivar de ímpeto estatal-retributivo.

A decisão do Estado de tornar determinada conduta crime deve ser a última "ratio", a última providência, tomada diante de indicadores ético-sociais mínimos que a justifiquem, com foco no resguardo das garantias fundamentais sobre as quais estruturado o próprio Estado.

Preserva-se, com isso, a idéia de mínima intervenção do Estado-sancionador na

vida comunitária que é própria do Estado de Direito. Este, o princípio da intervenção mínima, que se alia ao da fragmentariedade, no gerenciamento de uma visão moderna do Direito Penal que deve habitar um Estado Social de Direito, ambos indicando a necessidade de seleção de condutas que sejam efetivamente exorbitantes da razoabilidade do convívio, para que se sujeitem à criminalização.

Uma vez decidida a adoção da via penal como solução para dada tendência social de produção do injusto, deve-se respeitar, ainda, o derradeiro princípio gerenciador do moderno Direito Penal, que é o da proporcionalidade entre a criminalização, a pena e o fim buscado por ela.

O fim buscado pela pena, pela sanção penal, não pode ser outro, por sua vez, que não o estrito intuito de educação. A pena deve educar, a criminalização deve educar, limitativamente, a tendência social quanto à prática do crime (chama-se a esta finalidade de princípio da prevenção geral-limitadora da pena; por ela se educa socialmente, se educa o grupo, o

povo como um todo, disseminando-se uma lição prévia, teórica, formalizada no texto do crime instituído, de que o crime – e, principalmente, o valor jurídico-social que ele resguarda e representa – constituirá atentado à harmonia social, com resposta sancionadora-educativa pelo Estado). A pena educará, também, o próprio infrator, na medida em que deve permitir, quando aplicada, sua ressocialização, educando-o para um reingresso social pacífico sem o ímpeto delitivo demonstrado.

Tudo isso, no entanto, não afastou, dos Estados, o poder – aliás, um poder-dever de intensa valia social-coletiva – de delimitação das condutas que, mesmo por exceção, mesmo como última "ratio", reclamem solução criminalizante.

O Estado não se demitiu, pela visão moderna do Direito Penal, de sua precípua missão institucional, que é a de realizar o bem comum.

A Constituição e as leis não suprimiram do Estado o poder de criminalizar condutas sociais-infracionais de grande relevo para o resguardo do interesse comunitário.

Não. Ao contrário, em respeito ao próprio Estado de Direito, é, muitas vezes, através de adequada delimitação criminal da conduta-tipo que se resguardará, ao conjunto dos cidadãos de bem, inocentes, mínima garantia da imunidade aos efeitos do crime. O crime, definido, formalizado, como tal, na lei (em países, como o nosso, que adotam o sistema positivo), é também um veículo, um meio, de realização do próprio Estado de Direito, na medida em que representa a seleção, garantista, da pré-definida conduta-social grave, para submete-la à repercussão sancionatória, ao tempo em que delimita, com ela, todo o campo que deverá ser a ela imune.

Dizendo de outra forma, as incertezas eventuais quanto à incriminação de novas condutas que mantenham limites confusos com os de crimes antigos, pré-definidos, arriscam incriminações (judiciais) injustas.

A analogia – com crimes antigos – não pode suprir, em matéria penal, a lacuna da lei penal antiga. Isto significa que, diante de ausência de lei expressa sobre determinada conduta nova, não se poderá impor a criminalização em juízo e, consequentemente, a pena.

É o princípio da reserva legal e da legalidade estrita em matéria penal – "nullum crimen, nulla poena, sine lege" (é nula a pena e o crime sem prévia lei que os defina) – que impedem que a analogia seja usada para suprimento de lacuna legal em desfavor do acusado.

Assim, sem lei expressa que regule novas atividades criminosas, nem se conseguirá, com analogia de suprimento, incriminação de condutas graves, nem se assegurará, ao inocente delas, segurança de livramento a acusações que busquem intepretações extensivas da norma antiga.

Isto é o que nos parece ocorrer com o crime eletrônico, cibernético, brasileiro.

Tamanhas as alternativas já empregadas, coletivamente, na atual perpetração do injusto eletrônico, que ele reclama, neste momento, típica e definida criminalização, com a qual seja este novo fato social estremado de outros tipos penais antigos (lembrando, aqui, que o Código Penal brasileiro, para que o exemplo se limite à menção da lei geral-penal do país, data de mais de 60 anos e não contempla meios de interpretação extensiva, tampouco analógica, de fatos eletrônicos que começaram a ser implementados no "Brasil pós-desestatização do Sistema Telebrás").

O atual Código Penal brasileiro não possui estruturação de crimes que possam abranger as imensas e inovadoras hipóteses do cybercrime (o "cracking", o "phishing scam", os atos de "gray hat", "black hat", o "pichamento digital", a espionagem eletrônica, as difusões de códigos eletrônicos maliciosos danosos e não-danosos, ou a fraude eletrônica).

A proporção episódica desses novos crimes, como se demonstrou, saiu, há muito, da esfera de ocorrências para as quais se pudesse cogitar de marcos ou sanções puramente regulatórios-inibitórios civis, reparatórios, éticos, ou administrativos.

Sem uma firme decisão do Estado brasileiro, já neste momento – de intenso crescimento da planta de prestadores e de usuários dos variados sistemas eletrônicos – no sentido de submeter a balizas seguras, garantidoras de ambiente minimamente saudável, a atividade eletrônica-cibernética, deixar-se-á a realidade densa-criminal eletrônica já posta em prática à própria sorte.

Somente a coercitividade estatal, o poder de império do Estado, que habilita a imposição da "sanctio iuris", da sanção penal típica e pré-definida, ou, a pena, poderá educar, prevenir, na generalidade, com um "piso" de efetividade, o conjunto da população usuária de sistemas eletrônicos, educação prévia que se direcionará à extensa juventude "orkutiana"

brasileira, à imensa maioria dos atuais usuários de rêdes internas e externas, à fatia crescente dos internautas e prestadores dos serviços brasileiros de Internet, à centena de milhões de usuários da telefonia móvel celular, e aos milhões de correntistas do sistema financeiro, consumidores dos serviços de saúde, dos serviços públicos estatais, como os da Justiça, dentre outros, a respeitarem regras mínimas do convívio eletrônico.

Não nos parece adequado aguardar marcos regulatórios, pré-instituição civil de regras – coisa nunca exigida, aliás, na incriminação de condutas eletrônicas no Brasil – para que o Estado atenda, sob a ótica do Direito Penal, à presente necessidade.

Em termos de política criminal, e em respeito à história do tratamento penal das telecomunicações brasileiras, repare-se que, há exatos dez anos, em 1997, a própria LGT-Lei Geral de Telecomunicações (Lei 9.472/97), em seu art. 183, lançou-se à criminalização direta de específicas condutas sem aguardo de qualquer

marco regulatório, civil, ético, ou administrativo, e o fez diante da também direta constatação da alta potencialidade ofensiva do ilícito de telecomunicações, coisa que o legislador de 1.962 – quando editada a Lei 4.117/62 (o antigo Código Brasileito de Telecomunicações[2]) – também

---

2

LEI Nº 4.117, DE 27 DE AGOSTO DE 1962.

CAPÍTULO VII
Das Infrações e Penalidades

Art. 52. A liberdade de radiodifusão não exclui a punição dos que praticarem abusos no seu exercício.

Art. 53. Constitui abuso, no exercício de liberdade da radiodifusão, o emprêgo dêsse meio de comunicação para a prática de crime ou contravenção previstos na legislação em vigor no País, inclusive: (Redação dada pelo Decreto-Lei nº 236, de 1968)

a) incitar a desobediência às leis ou decisões judiciárias; (Redação dada pelo Decreto-Lei nº 236, de 1968)

b) divulgar segredos de Estado ou assuntos que prejudiquem a defesa nacional; (Redação dada pelo Decreto-Lei nº 236, de 1968)

c) ultrajar a honra nacional; (Redação dada pelo Decreto-Lei nº 236, de 1968)

d) fazer propaganda de guerra ou de processos de subversão da ordem política e social; (Redação dada pelo Decreto-Lei nº 236, de 1968)

e) promover campanha discriminatória de classe, côr, raça ou religião; (Redação dada pelo Decreto-Lei nº 236, de 1968)

f) insuflar a rebeldia ou a indisciplina nas fôrças armadas ou nas organizações de segurança pública; (Redação dada pelo Decreto-Lei nº 236, de 1968)

g) comprometer as relações internacionais do País; (Redação dada pelo Decreto-Lei nº 236, de 1968)

h) ofender a moral familiar, pública, ou os bons costumes; (Redação dada pelo Decreto-Lei nº 236, de 1968)

i) caluniar, injuriar ou difamar os Poderes Legislativos, Executivo ou Judiciário ou os respectivos membros; (Redação dada pelo Decreto-Lei nº 236, de 1968)

j) veicular notícias falsas, com perigo para a ordem pública, econômica e social; (Redação dada pelo Decreto-Lei nº 236, de 1968)

l) colaborar na prática de rebeldia desordens ou manifestações proibidas. (Incluído pelo Decreto-Lei nº 236, de 1968)

Parágrafo único. Se a divulgação das notícias falsas houver resultado de êrro de informação e fôr objeto de desmentido imediato, a nenhuma penalidade ficará sujeita a concessionária ou permissionária. (Partes mantidas pelo Congresso Nacional)

.....

Art. 55. É inviolável a telecomunicação nos têrmos desta lei. (Partes mantidas pelo Congresso Nacional)

Art. 56. Pratica crime de violação de telecomunicação quem, transgredindo lei ou regulamento, exiba autógrafo ou qualquer documento do arquivo, divulgue ou comunique, informe ou capte, transmita a outrem ou utilize o conteúdo, resumo, significado, interpretação, indicação ou efeito de qualquer comunicação dirigida a terceiro.

§ 1º Pratica, também, crime de violação de telecomunicações quem ilegalmente receber, divulgar ou utilizar, telecomunicação interceptada.

§ 2º Sòmente os serviços fiscais das estações e postos oficiais poderão interceptar telecomunicação.

I - A recepção de telecomunicação dirigida por quem diretamente ou como cooperação esteja legalmente autorizado;

II - O conhecimento dado:

a) ao destinatário da telecomunicação ou a seu representante legal;

b) aos intervenientes necessários ao curso da telecomunicação;

c) ao comandante ou chefe, sob cujas ordens imediatas estiver servindo;

d) aos fiscais do Govêrno junto aos concessionários ou permissionários;

e) ao juiz competente, mediante requisição ou intimação dêste.

Parágrafo único. Não estão compreendidas nas proibições contidas nesta lei as radiocomunicações destinadas a ser livremente recebidas, as de amadores, as relativas a navios e aeronaves em perigo, ou as transmitidas nos casos de calamidade pública.

Art 57. Não constitui violação de telecomunicação:

I - A recepção de telecomunicação dirigida por quem diretamente ou como cooperação esteja legalmente autorizado;

II - O conhecimento dado:

a) ao destinatário da telecomunicação ou a seu representante legal;

b) aos intervenientes necessários ao curso da telecomunicação;

c) ao comandante ou chefe, sob cujas ordens imediatas estiver servindo;

d) aos fiscais do Govêrno junto aos concessionários ou permissionários;

e) ao juiz competente, mediante requisição ou intimação dêste.

Parágrafo único. Não estão compreendidas nas proibições contidas nesta lei as radiocomunicações destinadas a ser livremente recebidas, as de amadores, as relativas a navios e aeronaves em perigo, ou as transmitidas nos casos de calamidade pública.

Art. 58. Nos crimes de violação da telecomunicação, a que se referem esta Lei e o artigo 151 do Código Penal, caberão, ainda as seguintes penas: (Substituído pelo Decreto-lei nº 236, de 28.2.1967)

I - Para as concessionárias ou permissionárias as previstas no artigos 62 e 63, se culpados por ação ou omissão e independentemente da ação criminal.

II - Para as pessoas físicas:

a) 1 (um) a 2 (dois) anos de detenção ou perda de cargo ou emprego, apurada a responsabilidade em processo regular, iniciado com o afastamento imediato do acusado até decisão final;

b) para autoridade responsável por violação da telecomunicação, as penas previstas na legislação em vigor serão aplicadas em dobro;

c) serão suspensos ou cassados, na proporção da gravidade da infração, os certificados dos operadores profissionais e dos amadores responsáveis pelo crime de violação da telecomunicação.

Art. 59. As penas por infração desta lei são: (Substituído pelo Decreto-lei nº 236, de 28.2.1967)

a) multa, até o valor .....NCR$ 10.000,00; (Incluído pelo Decreto-lei nº 236, de 28.2.1967)

b) suspensão, até trinta (30) dias; (Incluído pelo Decreto-lei nº 236, de 28.2.1967)

c) cassação; (Incluído pelo Decreto-lei nº 236, de 28.2.1967)

d) detenção; (Incluído pelo Decreto-lei nº 236, de 28.2.1967)

§ 1º Nas infrações em que, o juízo do CONTEL, não se justificar a aplicação de pena, o infrator será advertido, considerando-se a advertência como agravante na aplicação de penas por inobservância do mesmo ou de outro preceito desta Lei. (Incluído pelo Decreto-lei nº 236, de 28.2.1967)

§ 2º A pena de multa poderá ser aplicada isolada ou conjuntamente, com outras sanções especiais estatuídas nesta Lei. (Incluído pelo Decreto-lei nº 236, de 28.2.1967)

§ 3º O valor das multas será atualizado de 3 em 3 anos, de acordo com os níveis de correção monetária. (Incluído pelo Decreto-lei nº 236, de 28.2.1967)

Art. 60. A aplicação das penas desta Lei compete: (Substituído pelo Decreto-lei nº 236, de 28.2.1967)

a) ao CONTEL: multa e suspensão, em qualquer caso; cassação, quando se tratar de permissão; (Incluído pelo Decreto-lei nº 236, de 28.2.1967)

b) ao Presidente da República: cassação, mediante representação do CONTEL em parecer fundamentado. (Incluído pelo Decreto-lei nº 236, de 28.2.1967)

Art. 61. A pena será imposta de acordo com a infração cometida, considerados os seguintes fatores: (Substituído pelo Decreto-lei nº 236, de 28.2.1967)

a) gravidade da falta;

b) antecedentes da entidade faltosa;

c) reincidência específica.

implementara com amplitude e a Lei Geral das Telecomunicações, em pleno Estado de Direito democrático, resolveu referendar em seu art. 215[3].

Aliás, os crimes definidos pela LGT penalizam, com pena privativa de liberdade, de dois a quatro anos, aumentada da metade se houver dano a terceiro, o desenvolvimento clandestino de atividades de telecomunicação. Não houve surpresa ou questionamentos na época da tramitação congressual da LGT e a questão atual,

---

Art. 62. A pena de multa poderá ser aplicada por infração de qualquer dispositivo legal ou quando a concessionária ou permissionária não houver cumprido, dentro do prazo estipulado, exigência que tenha sido feita pelo CONTEL. (Substituído pelo Decreto-lei nº 236, de 28.2.1967)

Art. 63. A pena de suspensão poderá ser aplicada nos seguintes casos: (Substituído pelo Decreto-lei nº 236, de 28.2.1967)

a) infração dos artigos 38, alíneas a, b, c, e, g e h; 53, 57, 71 e seus parágrafos;

b) infração à liberdade de manifestação do pensamento e de informação (Lei nº 5.250 de 9 de fevereiro de 1967);

c) quando a concessionária ou permissionária não houver cumprido, dentro do prazo estipulaçao, exigência que lhe tenha sido feita pelo .....CONTEL;

d) quando seja criada situação de perigo de vida;

e) utilização de equipamentos diversos dos aprovados ou instalações fora das especificações técnicas constantes da portaria que as tenha aprovado;

f) execução de serviço para o qual não está autorizado. (Incluído pelo Decreto-lei nº 236, de 28.2.1967)

Parágrafo único. No caso das letras d, e e f deste artigo poderá ser determinada a interrupção do serviço pelo agente fiscalizador, "ad-referedum" do CONTEL.

.....

Art. 70. Constitui crime punível com a pena de detenção de 1 (um) a 2 (dois) anos, aumentada da metade se houver dano a terceiro, a instalação ou utilização de telecomunicações, sem observância do disposto nesta Lei e nos regulamentos. (Substituído pelo Decreto-lei nº 236, de 28.2.1967)

Parágrafo único. Precedendo ao processo penal, para os efeitos referidos neste artigo, será liminarmente procedida a busca e apreensão da estação ou aparelho ilegal.

Art. 72. A autoridade que impedir ou embaraçar a liberdade da radiodifusão ou da televisão fora dos casos autorizados em lei, incidirá no que couber, na sanção do artigo 322 do Código Penal. (Substituído pelo Decreto-lei nº 236, de 28.2.1967)

[3] Art. 215. Ficam revogados:

I - a Lei n° 4.117, de 27 de agosto de 1962, salvo quanto a matéria penal não tratada nesta Lei e quanto aos preceitos relativos à radiodifusão;

quando passada uma década do fenômeno da desestatização do Sistema Telebrás, se apresenta muito mais grave e mais extensa, pois, ao invés de termos, no Brasil, meros circuitos de telecomunicações, há serviços densos, extensos, de comunicação eletrônica (por dados e voz), trafegando por rêdes corporativas, públicas e privadas, de grande relevância.

Confira-se o art. 183 da Lei 9472/97:

" Lei 9472/97:
Capítulo II
Das Sanções Penais
Art. 183. Desenvolver clandestinamente atividades de telecomunicação:
Pena - detenção de dois a quatro anos, aumentada da metade se houver dano a terceiro, e multa de R$ 10.000,00 (dez mil reais).
Parágrafo único. Incorre na mesma pena quem, direta ou indiretamente, concorrer para o crime.
Art. 184. São efeitos da condenação penal transitada em julgado:
I - tornar certa a obrigação de indenizar o dano causado pelo crime;
II - a perda, em favor da Agência, ressalvado o direito do lesado ou de terceiros de boa-fé, dos bens empregados na atividade clandestina, sem prejuízo de sua apreensão cautelar.
Parágrafo único. Considera-se clandestina a atividade desenvolvida sem a competente concessão, permissão ou autorização de serviço, de uso de radiofreqüência e de exploração de satélite.
Art. 185. O crime definido nesta Lei é de ação penal pública, incondicionada, cabendo ao Ministério Público promovê-la."

Nossa posição é, portanto, a de que a criminalização dos ilícitos cibernéticos se impõe, constituindo exigência social de envergadura no momento.

Vamos, com esta premissa, ao derradeiro ponto.

- <u>Terceiro</u> –

BREVE ANÁLISE DOS DISPOSITIVOS SUGERIDOS PELO SUBSTITUTIVO EM DISCUSSÃO

O primeiro grande ponto deste tópico, ou aquele que nos preocupa nesse momento, é o que se relaciona com a linguagem normativa proposta.

Na medida em que decidida a criminalização, a linguagem definidora do tipo penal se mostra de grande relevância, sobretudo no Brasil, em que a interpretação da norma penal deve observar rigoroso limite de legalidade – que comanda o princípio de que a dúvida prestigiará sempre a inocência (“in dubio pro reo”).

Entretanto, paralelamente a este aspecto, deve-se salientar que a tendência moderna-mundial, de regramento dos tipos tecnológicos, caminha para antagônico sentido,

que é o da delimitação "aberta" dos elementos, ou, das circunstâncias elementares que os caracterizem, pois, em razão da inovação tecnológica, não se pode perder a essência da definição legal frente às evolutivas alterações estruturais que o tempo permite.

Em matéria penal, então, a questão se avoluma, pois, na medida em que se pode inovar o meio com maior velocidade, corre-se o risco, no enfeixamento gramatical de hipóteses normativas cujo alvo seja a tecnologia da informação, de se transformar a norma incriminadora em instrumento inócuo de aplicação, por rápida desatualização.

Como conciliar, então, no bojo da (antiga) lei penal brasileira, e dentro do escopo constitucional de observância da legalidade estrita, a correta definição, que será sempre gramatical, dos novos crimes informáticos ?

Dosagem da linguagem, sua adequação teleológica ao caráter (universal) das rêdes telecomunicativas – o que constituirá

missão de atividade empregável "a posteriori" e não "a priori" do processo legislativo, pois ligada ao próprio trabalho interpretativo (jurisdicional e jurisprudencial, e não congressual). Além disso, uma certa inspiração dosada por medidas externas ao âmbito nacional – o exemplo maior nos parece ser a Convenção Européia de Cybercrimes, atualmente firmada, na Europa, por mais de 40 países – sintetizam, digamos, o "estado da arte" que poderá ser adotado na missão de disciplinar, criminalmente, o cybercrime.

Neste ponto, parece-nos que o substitutivo apresentado aos três Projetos em análise atende ao propósito.

Vejamos um-a-um os tipos novos por ele editados (nossas notas estão feitas em caixas de texto laterais a cada um):

" Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), o Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), a Lei nº 9.296, de 24 de julho de 1996, o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código do Processo Penal), a Lei nº 10.446, de 8 de maio de 2002, e a Lei nº 8.078, de 11 de setembro de 1990 (Código do Consumidor), para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, de rede de computadores, ou que sejam praticadas contra dispositivos de

comunicação ou sistemas informatizados e similares, e dá outras providências.

O CONGRESSO NACIONAL decreta:

Art.1º Esta Lei altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), o Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), a Lei nº 9.296, de 24 de julho de 1996, Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código do Processo Penal), a Lei nº 10.446, de 8 de maio de 2002, e a Lei nº 8.078, de 11 de setembro de 1990 (Código do Consumidor), para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, de rede de computadores, ou que sejam praticadas contra dispositivos de comunicação ou sistemas informatizados e similares, e dá outras providências.

Art. 2º O Capítulo V do Título I da Parte Especial do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) fica acrescido do seguinte 141-A:

Aumento razoável dos crimes contra a honra, de grde. Incidência no meio eletrônico atual

"**Art. 141-A.** As penas neste Capítulo aumentam-se de dois terços caso os crimes sejam cometidos por intermédio de rede de computadores, dispositivo de comunicação ou sistema informatizado."

Art. 3º O Título I da Parte Especial do Código Penal fica acrescido do Capítulo VI-A, assim redigido:

"Capítulo VI-A

DOS CRIMES CONTRA A VIOLAÇÃO DE REDE DE COMPUTADORES, DISPOSITIVO DE COMUNICAÇÃO OU SISTEMA INFORMATIZADO

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

O bem jurídico é a proteção ao sigilo de dados sensíveis. Está bem alocado pois resguarda ao legítimo titular a garantia à guarda de dados sob sigilo. Bem alocado em crimes contra a pessoa. Crime de mera conduta. Se exaure com ela. A conduta é reprimida. É ela que ameaça, que obriga ao grande custo operacional

Art. 154-A. Acessar rede de computadores, dispositivo de comunicação ou sistema informatizado, sem autorização do legítimo titular, quando exigida:

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

§ 1º Nas mesmas penas incorre quem, permite, facilita ou fornece a terceiro meio não autorizado de acesso a rede de computadores, 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 nome falso ou da utilização de identidade de terceiros para a prática de acesso.

§ 4º Não há crime quando o agente acessa a título de defesa digital, excetuado o desvio de finalidade ou o excesso.

Conduta menos grave – o bem jurídico é o de resguardo do sigilo de dados, sendo que, nesta hipótese, não houve o ato de acesso – que é o mais grave, pois acessar é invadir um ambiente eletrônico vedado. Aqui a obtenção não tem a conduta anterior, de acesso. A pena máxima comporta conversão em restritiva de direitos

Obtenção, manutenção, transporte ou fornecimento não autorizado de informação eletrônica ou digital ou similar

Art. 154-B. Obter dado ou informação disponível em rede de computadores, dispositivo de comunicação ou sistema informatizado, sem autorização do legítimo titular, quando exigida:

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

§ 1º Nas mesmas penas incorre quem mantém consigo, transporta ou fornece dado ou informação obtida nas mesmas circunstâncias do "caput", ou desses se utiliza alem do prazo definido e autorizado.

§ 2º Se o dado ou informação obtida desautorizadamente é fornecida a terceiros pela rede de computadores, dispositivo de comunicação ou sistema informatizado, ou em qualquer outro meio de divulgação em massa, a pena é aumentada de um terço.

§ 3º 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.

Relação meramente exemplificativa, não-taxativa. Necessidade mínima de tipo penal que assegure-preveja a hipótese de inovação tecnológica, sem vácuo para a incriminação

Dispositivo de comunicação, sistema informatizado, rede de computadores e defesa digital

Art. 154-C. Para os efeitos penais considera-se:

I – dispositivo de comunicação: o computador, o telefone celular, o processador de dados, os instrumentos de armazenamento de dados eletrônicos ou digitais ou similares, os instrumentos de captura de dados, os receptores e os conversores de sinais de rádio ou televisão digital ou qualquer outro meio capaz de processar, armazenar, capturar

ou transmitir dados utilizando-se de tecnologias magnéticas, óticas ou qualquer outra tecnologia eletrônica ou digital ou similar;

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

III – rede de computadores: os instrumentos físicos e lógicos através dos quais é possível trocar dados e informações, compartilhar recursos, entre máquinas, representada pelo conjunto de computadores, dispositivos de comunicação e sistemas informatizados, que obedecem de comum acordo a um conjunto de regras, parâmetros, códigos, formatos e outras informações agrupadas em protocolos, em nível topológico local, regional, nacional ou mundial;

IV – defesa digital: manipulação de código malicioso por agente técnico ou profissional habilitado, em proveito próprio ou de seu preponente, e sem risco para terceiros, de forma tecnicamente documentada e com preservação da cadeia de custódia no curso dos procedimentos correlatos, a título de teste de vulnerabilidade, de resposta a ataque, de frustração de invasão ou burla, de proteção do sistema, de interceptação defensiva, de tentativa de identificação do agressor, de exercício de forense computacional e de práticas gerais de segurança da informação;

Bem jurídico ainda é o sigilo de dados sensíveis. Aqui é a divulgação, sem acesso e sem obtenção interna. É o intermediário dos dados, que está hoje intermediando o negócio do crime eletrônico e precisa ser contido. A pena é baixa e permite, delito de pequeno potencial ofensivo (pode ser convertida em reparaçção de danos ou restritiva de direitos).

V - código malicioso: o conjunto de instruções e tabelas de informações ou programa de computador ou qualquer outro sistema capaz de executar uma seqüência de operações que resultem em ação de dano ou de obtenção indevida de informações contra terceiro, de maneira dissimulada ou oculta, transparecendo tratar-se de ação de curso normal.

Divulgação ou utilização indevida de informações contidas em banco de dados

Art. 154-D Divulgar, utilizar, comercializar ou disponibilizar informações contidas em banco de dados com finalidade distinta da que motivou o registro das mesmas, incluindo-se informações privadas referentes, direta ou indiretamente, a dados

econômicos de pessoas naturais ou jurídicas, ou a dados de pessoas naturais 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 nos casos previstos em lei ou mediante expressa anuência da pessoa a que se referem, ou de seu representante legal.

Pena – detenção, de um a dois anos, e multa.

§ 1º A pena é aumentada de sexta parte, se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime.

§ 2º Se o crime ocorre em rede de computadores, dispositivo de comunicação ou sistema informatizado, ou em qualquer outro meio de divulgação em massa, a pena é aumentada de um terço.“

Art. 4º O § 4º do art. 155 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), passa a vigorar acrescido do seguinte inciso V:

“**Art. 155.**

.....

.....

§ 4º

.....

.....

V - mediante uso de rede de computadores, dispositivo de comunicação ou sistema informatizado ou similar, ou contra rede de computadores, dispositivos de comunicação ou sistemas informatizados e similares”.

..... (NR) ”

Forma qualificada do furto – crime mais grave contra o patrimônio. Justifica-se por causa das inúmeras tentativas de obtenção de valores com uso de redes de computadores (fraudes bancárias, etc.). É o tipo mais grave – furto qualificado (2 a 8 anos de reclusão). Regime inicial semi-aberto.

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

“**Dano por difusão de código malicioso eletrônico ou digital ou similar**

O bem jurídico tutelado é a imunidade a vírus de computador, de alta incidência. Pena baixa inclusive, por crimes simples, com possib. de suspensão condicional do processo e imposição de restritiva de direitos (art. 44 da Lei 9099/95)

Art. 163-A. Criar, inserir ou difundir código malicioso em dispositivo de comunicação, rede de computadores, ou sistema informatizado.

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

Dolo específico. "Animus necandi". Forma grave. Não é apenas o pixador digital. Quer destruir com vírus. É o black hat. O pior delinqüente. O crime dá conversão por restritiva de direitos.

Dano qualificado por difusão de código malicioso eletrônico ou digital ou similar

§ 1º Se o crime é cometido com finalidade de destruição, inutilização, deterioração, alteração, dificultação do funcionamento, ou funcionamento desautorizado pelo titular, de dispositivo de comunicação, de rede de computadores, ou de sistema informatizado:

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

Crime preterdoloso. Agravação pela obtenção (involuntária-culposa) do resultado mais grave – o dano do sistema eletrônico. É a única forma de educar socialmente contra a disseminação de vírus, prevendo que sua disseminação danosa, mesmo involuntária, causará pena.A pena pode ser iniciada, se fixada no máximo, em regime semi-aberto, com trabalho extra-muros.

Difusão de código malicioso eletrônico ou digital ou similar seguido de dano

§ 2º Se do crime resulta destruição, inutilização, deterioração, alteração, dificultação do funcionamento, ou funcionamento desautorizado pelo titular, de dispositivo de comunicação, de rede de computadores, ou de sistema informatizado, e as circunstâncias demonstram que o agente não quis o resultado, nem assumiu o risco de produzi-lo:

Pena – reclusão, de 3 (dois) a 5 (cinco) anos, e multa.

§ 3º A pena é aumentada de sexta parte, se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime.

§ 4º Não há crime quando a ação do agente é a título de defesa digital, excetuado o desvio de finalidade ou o excesso."

Art. 6º O Capitulo VI do Título II do Código Penal passa a vigorar com o seguinte artigo:

Estelionato digital. Crime contra o patrimônio. O bem jurídico tutelado é o patrimônio do "homus medius", simples, que não está afeito, habilitado à lida com sistemas eletrônicos e está sujeito, por isso, à engenharia social. Pena comporta suspensão condicional do processo, com imposição de restrição de direitos.

"Difusão de código malicioso

Art. 171-A. Difundir, por qualquer meio, programa, conjunto de instruções ou sistema informatizado com o propósito de levar a erro ou, por qualquer forma indevida, induzir alguém a fornecer, espontaneamente e por qualquer meio, dados ou informações que facilitem ou permitam o acesso indevido ou sem autorização, à rede de computadores, dispositivo de comunicação ou a sistema informatizado, ou a obtenção de qualquer vantagem ilícita:

Pena – reclusão, de um a três anos.

§ 1º A pena é aumentada de sexta parte, se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática de difusão de código malicioso.

§ 2º Não há crime quando a difusão ocorrer a título de defesa digital, excetuado o desvio de finalidade ou o excesso."

Art. 7º O Código Penal passa a vigorar acrescido do seguinte art. 183-A:

O dispositivo é importante para vincular, dentro da reserva legal-penal, o dado eletrônico ao sentido semântico de coisa

"**Art. 183-A.** Para efeitos penais, equiparam-se à coisa o dado, informação ou unidade de informação em meio eletrônico ou digital ou similar, a base de dados armazenada, o dispositivo de comunicação, a rede de computadores, o sistema informatizado, a senha ou similar ou qualquer instrumento que proporcione acesso a eles."

Art. 8º Os arts. 265 e 266 do Código Penal passam a vigorar com as seguintes redações:

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

O dispositivo nada faz senão acrescentar serviço de informação e de telecomunicação ao escopo de tutela do bem jurídico (a proteção dos meios de comunicação). É uma atualização, no particular, do CP

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

..... (NR)"

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

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

.....
..... (NR)”

Art. 9º 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 ou digital ou similar portátil de captura, processamento, armazenamento e transmissão de informações.

Parágrafo único. Equipara-se a documento particular o cartão de crédito ou débito ou qualquer outro dispositivo portátil capaz de capturar, processar, armazenar ou transmitir dados, utilizando-se de tecnologias magnéticas, óticas ou qualquer outra tecnologia eletrônica ou digital ou similar.(NR)”

Equipara o cartão de crédito ou dispositivo eletrõnico de captação de dados débito para efeito de falsificação (não há inovação em si; há extensão do crime ao documento eletrônico)

Art. 10. O Código Penal passa a vigorar acrescido do seguinte art. 298-A:

“**Falsificação de telefone celular ou meio de acesso a rede de computadores, dispositivo de comunicação ou sistema informatizado**

Art. 298-A. Criar ou copiar, indevidamente, ou falsificar código, seqüência alfanumérica, cartão inteligente, transmissor ou receptor de rádio freqüência ou telefonia celular, ou qualquer instrumento que permita o acesso a rede de computadores, dispositivo de comunicação ou sistema informatizado:

Pena – reclusão, de um a cinco anos, e multa.”

Falsificação de códigos alfanuméricos – sobretudo agora que teremos a portabilidade legal no país – é o meio de se resguardar o bem jurídico representado pelo número alfanumérico e pelos dados de conexão telefônica e de conexão computacional (resguarda e protege contra clonagem e resguarda a prática de VoIP). A pena permite suspensão condicional do processo, com imposição de restrição de direitos.

Art. 11. O § 6º do art. 240 do Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), passa a vigorar acrescido do seguinte inciso V:

“**Art. 240.**
.....
.....

.....
.....

Furto qualificado

§ 6º
.....
.....
.....
.....
V - mediante uso de rede de computadores, dispositivo de comunicação ou sistema informatizado ou similar, ou contra rede de computadores, dispositivos de comunicação ou sistema.

.....
.....(NR) ”

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

“**Dano por difusão de código malicioso eletrônico ou digital ou similar**

Art. 262-A. Criar, inserir ou difundir código malicioso em dispositivo de comunicação, rede de computadores, ou sistema informatizado.

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

Dano qualificado por difusão de código malicioso eletrônico ou digital ou similar

§ 1º Se o crime é cometido com finalidade de destruição, inutilização, deterioração, alteração, dificultação do funcionamento, ou funcionamento desautorizado pelo titular, de dispositivo de comunicação, de rede de computadores, ou de sistema informatizado:

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

Difusão de código malicioso eletrônico ou digital ou similar seguido de dano

§ 2º Se do crime resulta destruição, inutilização, deterioração, alteração, dificultação do funcionamento, ou funcionamento desautorizado pelo titular, de dispositivo de comunicação, de rede de computadores, ou de sistema informatizado, e as circunstâncias demonstram que o agente não quis o resultado, nem assumiu o risco de produzi-lo:

Pena – reclusão, de 3 (dois) a 5 (cinco) anos, e multa. “

§ 3º A pena é aumentada de sexta parte, se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime.

§ 4º Não há crime quando a ação do agente é a título de defesa digital, excetuado o desvio de finalidade ou o excesso.”

Art. 13. 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**

DOS CRIMES CONTRA A VIOLAÇÃO DE REDE DE COMPUTADORES, DISPOSITIVO DE COMUNICAÇÃO OU SISTEMA INFORMATIZADO

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

Art. 339-A. Acessar rede de computadores, dispositivo de comunicação ou sistema informatizado, sem autorização do legítimo titular, quando exigida:

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

§ 1º Nas mesmas penas incorre quem, permite, facilita ou fornece a terceiro meio não autorizado de acesso a rede de computadores, dispositivo de comunicação ou sistema informatizado.

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

§ 3º Não há crime quando o agente acessa a título de defesa digital, excetuado o desvio de finalidade ou o excesso.

Obtenção, manutenção, transporte ou fornecimento não autorizado de informação eletrônica ou digital ou similar

Art. 339-B. Obter dado ou informação disponível em rede de computadores, dispositivo de comunicação ou sistema informatizado, sem autorização do legítimo titular, quando exigida:

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

§ 1º Nas mesmas penas incorre quem mantém consigo, transporta ou fornece dado ou informação obtida nas mesmas circunstâncias do “caput”, ou desses se utiliza alem do prazo definido e autorizado.

§ 2º Se o dado ou informação obtida desautorizadamente é fornecida a terceiros pela rede de computadores, dispositivo de comunicação ou sistema informatizado, ou em qualquer outro meio de divulgação em massa, a pena é aumentada de um terço.

Dispositivo de comunicação, sistema informatizado, rede de computadores e defesa digital

Art. 339-C. Para os efeitos penais considera-se:

I – dispositivo de comunicação: o computador, o telefone celular, o processador de dados, os instrumentos de armazenamento de dados eletrônicos ou digitais ou similares, os instrumentos de captura de dados, os receptores e os conversores de sinais de rádio ou televisão digital ou qualquer outro meio capaz de processar, armazenar, capturar ou transmitir dados utilizando-se de tecnologias magnéticas, óticas ou qualquer outra tecnologia eletrônica ou digital ou similar;

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

III – rede de computadores: os instrumentos físicos e lógicos através dos quais é possível trocar dados e informações, compartilhar recursos, entre máquinas, representada pelo conjunto de computadores, dispositivos de comunicação e sistemas informatizados, que obedecem de comum acordo a um conjunto de regras, parâmetros, códigos, formatos e outras informações agrupadas em protocolos, em nível topológico local, regional, nacional ou mundial;

IV – defesa digital: manipulação de código malicioso por agente técnico ou profissional habilitado, em proveito próprio ou de seu preponente, e sem risco para terceiros, de forma tecnicamente documentada e com preservação da cadeia de custódia no curso dos procedimentos correlatos, a título de teste de vulnerabilidade, de resposta a

ataque, de frustração de invasão ou burla, de proteção do sistema, de interceptação defensiva, de tentativa de identificação do agressor, de exercício de forense computacional e de práticas gerais de segurança da informação;

V - código malicioso: o conjunto de instruções e tabelas de informações ou programa de computador ou qualquer outro sistema capaz de executar uma seqüência de operações que resultem em ação de dano ou de obtenção indevida de informações contra terceiro, de maneira dissimulada ou oculta, transparecendo tratar-se de ação de curso normal.

Divulgação ou utilização indevida de informações contidas em banco de dados

Art. 339-D Divulgar, utilizar, comercializar ou disponibilizar informações contidas em banco de dados com finalidade distinta da que motivou o registro das mesmas, incluindo-se informações privadas referentes, direta ou indiretamente, a dados econômicos de pessoas naturais ou jurídicas, ou a dados de pessoas naturais 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 nos casos previstos em lei ou mediante expressa anuência da pessoa a que se referem, ou de seu representante legal.

Pena – detenção, de um a dois anos, e multa.

§ 1º A pena é aumentada de sexta parte, se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime.

§ 2º Se o crime ocorre em rede de computadores, dispositivo de comunicação ou sistema informatizado, ou em qualquer outro meio de divulgação em massa, a pena é aumentada de um terço.“

Art. 14. O 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 Capítulo VIII-A, assim redigido:

“**Capítulo VIII-A**

DISPOSIÇÕES GERAIS

Art. 267-A. Para efeitos penais, equiparam-se à coisa o dado, informação ou unidade de informação em meio eletrônico ou digital ou similar, a base de dados armazenada, o dispositivo de comunicação, a rede de computadores, o sistema informatizado, a senha ou similar ou qualquer instrumento que proporcione acesso a eles.”

Art. 15. 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 de código malicioso**

Art. 281-A. Difundir, por qualquer meio, programa, conjunto de instruções ou sistema informatizado com o propósito de levar a erro ou, por qualquer forma indevida, induzir alguém a fornecer, espontaneamente e por qualquer meio, dados ou informações que facilitem ou permitam o acesso indevido ou sem autorização, à rede de computadores, dispositivo de comunicação ou a sistema informatizado, ou a obtenção de qualquer vantagem ilícita:

Pena – reclusão, de um a três anos.

§ 1º A pena é aumentada de sexta parte, se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática de difusão de código malicioso.

§ 2º Não há crime quando a difusão ocorre a título de defesa digital, excetuado o desvio de finalidade ou o excesso.”

Art. 16. 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:

O dispositivo permite a interceptação telefônica em crimes apenados com detenção, quando se tratar de telefonia por IP (computadores) – VoIP. Neste caso, mesmo com detenção, poderá haver a interceptação por ordem judicial

"**Art. 2º** .....

.....

§ 2º O disposto no inciso III do *caput* não se aplica quando se tratar de interceptação do fluxo de comunicações em rede de computadores, dispositivo de comunicação ou sistema informatizado." (NR)

Art. 17. O art. 313 do Decreto-Lei nº 3.689, de 3 de outubro de 1941, Código do Processo Penal (CPP), passa a vigorar acrescido do seguinte inciso IV:

"**Art. 313.** .....

.....

Rigor grande – da prisão preventiva – mas dentro do critério da prevenção geral educativa, no sentido de que, apesar de penas (quase todas) conversíveis em restritiva de direitos e suspensão condicional do processo, o ataque eletrônico pode determinar prisão preventiva.

IV – punidos com detenção, se tiverem sido praticados contra rede de computadores, dispositivo de comunicação ou sistema informatizado, ou se tiverem sido praticados mediante uso de rede de computadores, dispositivo de comunicação ou sistema informatizado, nos termos da lei penal.(NR)"

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

Art. 19. O art. 1º da Lei nº 10.446, de 8 de maio de 2002 passa a vigorar com a seguinte redação:

Insere os delitos cibernéticos-eletrônicos na competência de atuação da Polícia Federal, quando tiverem repercussão interesetadual ou internacional, o que logiciza o fato de que o crime eletrônico se desapega de critérios espaciais-convencionais e por isso reclama providências policiais de investigação mais amplas

"**Art. 1º** .....

.....

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

Art. 20. O art. 9º da Lei nº 8.078, de 11 de setembro de 1990 passa a vigorar com a seguinte redação:

"Art. 9º .....

.....

Parágrafo único. O disposto neste artigo se aplica à segurança digital do consumidor, mediante a informação da necessidade do uso de senhas ou similar para a proteção do uso do produto ou serviço e para a proteção dos dados trafegados, quando se tratar de dispositivo de comunicação, sistema informatizado ou provimento de acesso a rede de computadores ou provimento de serviço por meio dela.(NR)"

Obrigação não-criminal dos provedores (administrativa), de guarda de dados, que só poderão ser entregues a autoridades públicas e por ordem judicial. O sigilo de comunicações já funciona desta forma, tendo as empresas de telecomunicações igual dever

Art. 21. O responsável por liberar o acesso a uma rede de computadores ou prestar serviços mediante seu uso é obrigado a:

I – manter em ambiente controlado e de segurança os dados de conexões realizadas por seus equipamentos, aptos à identificação do usuário e dos endereços eletrônicos de origem, da data, do horário de início e término e referência GMT, das conexões, pelo prazo de três anos, para prover os elementos probatórios essenciais de identificação da autoria das conexões na rede de computadores;

II – tornar disponíveis à autoridade competente, por expressa autorização judicial, os dados e informações mencionados no inciso I no curso de auditoria técnica a que forem submetidos;

III – fornecer, por expressa autorização judicial, no curso de investigação, os dados de conexões realizadas e os dados de identificação de usuário;

IV – preservar imediatamente, após a solicitação

expressa da autoridade judicial, no curso de investigação, os dados de conexões realizadas, os dados de identificação de usuário e o conteúdo das comunicações realizadas daquela investigação, cuidando da sua absoluta confidencialidade e inviolabilidade;

A norma não inova, pois obriga ao atendimento de um dever, que é o de não ocultar prática criminosa no meio eletrônico. Pois ocultar é praticar crime de favorecimento pessoal ou real (art. 348/349 do CP). Ver art. 22 a seguir

V – informar, de maneira sigilosa, à autoridade policial competente, denúncia da qual tenha tomado conhecimento e que contenha indícios de conduta delituosa na rede de computadores sob sua responsabilidade;

VI – informar ao seu usuário que o uso da rede sob sua responsabilidade obedece às leis brasileiras e que toda comunicação ali realizada será de exclusiva responsabilidade do usuário, perante as leis brasileiras;

VII – alertar aos seus usuários, em campanhas periódicas, quanto ao uso criminoso de rede de computadores, dispositivo de comunicação e sistema informatizado;

VIII – divulgar aos seus usuários, em local destacado, as boas práticas de segurança no uso de rede de computadores, dispositivo de comunicação e sistema informatizado.

§ 1º Os dados de conexões realizadas em rede de computadores, aptos à identificação do usuário, as condições de segurança de sua guarda, a auditoria à qual serão submetidos, a autoridade competente responsável pela auditoria e o texto a ser informado aos usuários de rede de computadores serão definidos nos termos de regulamento.

§ 2º Os dados e procedimentos de que cuida o inciso I deste artigo deverão estar aptos a atender ao disposto nos incisos II , III e IV no prazo de cento e oitenta dias, a partir da promulgação desta Lei.

§ 3º O responsável citado no *caput* deste artigo que não cumprir o disposto no § 2º, independentemente do ressarcimento por perdas e danos ao lesado, estará sujeito ao pagamento de multa variável de R$ 2.000,00 (dois mil reais) a R$ 100.000,00 (cem mil reais) a cada verificação ou

solicitação, aplicada em dobro em caso de reincidência, que será imposta mediante procedimento administrativo, pela autoridade judicial desatendida, considerando-se a natureza, a gravidade e o prejuízo resultante da infração.

§ 4º Os recursos financeiros resultantes do recolhimento das multas estabelecidas neste artigo serão destinados ao Fundo Nacional de Segurança Pública, de que trata a Lei nº 10.201, de 14 de fevereiro de 2001.

Art. 22. Não constitui violação do dever de sigilo a comunicação, às autoridades competentes, de prática de ilícitos penais, abrangendo o fornecimento de informações de acesso, hospedagem e dados de identificação de usuário, quando constatada qualquer conduta criminosa.

Art. 23. Esta Lei entrará em vigor sessenta dias após a data de sua publicação.

Disso se tem, além da adequação da criminalização, o seguinte:

1 – Afora as propostas de instituição do crime de furto qualificado e de crime preterdoloso de dano, todos os demais tipos penais criados pelo Substitutivo contêm penalidades (penas privativas da liberdade) que se sujeitam ora a conversão direta a indenização ou penas restritivas de direito (na forma do art. 61 e 75 da Lei 9.099/95) ora a suspensão condicional do processo (na forma do art. 89 da mesma Lei 9.099/95), ora, ainda, a conversão pura em penas

restritivas de direitos (na forma do art. 33 c/c art. 44 do Código Penal brasileiro);

2 – Não se proclama, portanto, exacerbação penalisadora, pelo que se vê preservação de proporcionalidade na resposta penal cominada a cada infração nova proposta.

CONCLUSÃO

Por todo o exposto, somos de opinião de que o Substitutivo apresentado aos três Projetos de Lei recomenda aprovação, pela adequação com a gravidade dos fatos tratados e pelo respeito que promove à finalidade preventiva-geral dos ilícitos proclamados, sendo que a penalisação proposta evidencia submissão a princípios e balizas aceitáveis de proporcionalidade e razoabilidade.

Opinamos pela aprovação do Substitutivo no âmbito desta Comissão.

Fernando Neto Botelho