COMISSÃO DE INFORMÁTICA JURÍDICA

RELATÓRIO SOBRE O PROJETO DE LEI SOBRE CRIMES COMETIDOS POR COMPUTADOR

INTRODUÇÃO

O Projeto de Lei que prevê crimes praticados por computador, atualmente remetido à Câmara dos Deputados, foi aprovado no Senado sob a forma de um Substitutivo, que ora se analisa.

Após sofrer diversas críticas, o projeto original restou nitidamente melhorado pelo texto Substitutivo aprovado no Senado. O texto, contudo, ainda contém falhas serão aqui analisadas.

CONSIDERAÇÕES GERAIS

O texto final aprovado pelo Senado simplificou e enxugou significativamente o projeto que ali tramitava, dele retirando dispositivos completamente despropositados, como era o caso da tão comentada - e criticada - "defesa digital", em que se autorizava, em circunstâncias abertas e por demais abrangentes, um verdadeiro **contra-ataque**, mais parecendo que o Estado, ao invés de cumprir sua tarefa de impor a lei e a ordem, estaria autorizando a volta da justiça de mão própria, em versão futurista.

Os tipos penais ali previstos também foram melhor redigidos, de modo que o projeto mais se aproximou da boa cultura jurídica nacional.

Entretanto, há questões centrais que ainda merecem reflexão. A lei penal se presta a tutelar determinados bens jurídicos, aqueles mais relevantes para a sociedade, tipificando condutas que atentem contra eles. Em alguns dos tipos penais previstos no texto atual do projeto ainda não parece claro qual é o bem jurídico protegido. Alguns dispositivos do texto, por sua excessiva abrangência, podem tornar crime fatos menos graves, o que

certamente não é o que a sociedade precisa, caminhando contrariamente ao princípio da intervenção mínima, que orienta a ciência penal.

Além disso, é importante lembrar também que a sanção que o Direito Penal impõe ao agente deve ser proporcionalmente mais grave quanto maior for a importância do bem jurídico atingido, ou quanto maior for o potencial ofensivo daquela conduta. Tipos penais demasiadamente genéricos tanto podem tornar criminosas condutas sem potencial ofensivo, que sequer mereceriam ser criminalizadas, como podem impor penas idênticas a fatos cuja gravidade seja também muitíssimo diferente.

Deste modo, merecem uma discussão mais profunda aqueles tipos penais do Projeto que tipificam condutas genericamente direcionadas a "dados", "redes de computador", "dispositivos informáticos" ou "dados informáticos". Isto porque queremos crer que o bem jurídico que é relevante para a sociedade e merece ser tutelado pelos chamados "crimes de informática" não é o computador em si, nem os bits nele armazenados, mas a utilidade que estes computadores desempenham, ou a importância dos seus dados.

Do modo como se encontra redigido o artigo 285-A, o mero acesso indevido aos computadores do sistema financeiro nacional, ou aos de setores críticos da administração pública (BACEN, Justiça ou Receita, por exemplo), ou que controlem sistemas sensíveis (tráfego aéreo, trens urbanos), está sujeito ao mesmo tratamento dado ao condômino que invadisse o *proxy* do seu próprio condomínio ou a rede entre dois computadores do vizinho, ou ao empregado que se desviasse de bloqueios internos para conseguir acessar a Internet de dentro do local de trabalho. Não se quer aqui, é claro, justificar nenhuma destas condutas, mas parece evidente que as primeiras se constituem em fatos muito mais graves. E duvidamos que mereça perseguição criminal pelo Estado, ou recolhimento à cadeia pública, muito menos sujeito à pena de reclusão prevista no Projeto, o condômino ou o empregado, nos exemplos dados acima; a administração condominial que lhe aplique as multas adequadas, o patrão que lhe imponha as sanções trabalhistas cabíveis, deixando-se o Direito Penal distante disso. Muitas condutas indesejadas, praticadas por computador, e que perigosamente podem ser

abrangidas nestes tipos penais, não são graves o bastante para que sejam criminalizadas, bem podendo ser tratadas e reprimidas nas esferas jurídicas não-penais.

Por isso, melhor seria tratar diferentemente essas situações em que se queira punir o mero acesso indevido, sem outros desdobramentos, em tipos penais distintos, até para ser possível identificar em cada uma destas normas qual é o **bem jurídico** que se quer tutelar. E aplicar penas proporcionais. Afinal, o mero acesso, quando indevido, só se constitui fato potencialmente perigoso à sociedade conforme se trate de um sistema informático sensível e socialmente relevante.

Assim, nestes casos em que se pretende punir o *mero acesso* a sistemas computadorizados, não parece apropriado falar-se em *crimes contra a segurança de sistemas informatizados*, como se o bem jurídico a proteger fosse o *computador* em si, qualquer computador. Melhor seria termos, destacadamente, figuras típicas de acesso indevido a *determinadas redes*, espalhadas entre os crimes contra o sistema financeiro nacional, crimes de concorrência desleal, crimes contra a administração pública, crimes contra a proteção dos sigilos, crimes contra a privacidade individual, crimes contra as comunicações e transportes e assim por diante, onde quer que tenhamos computadores usados para gestão de *bens jurídicos relevantes*, cujo acesso indevido constitua algum perigo e, por isso, mereça ser criminalizado. Isso porque, insista-se, o bem jurídico que precisa de proteção é a relevante função desempenhada ou dado armazenado em determinados sistemas, e não o sistema em si.

De certo modo, as propostas de alteração do Código Penal Militar soam mais adequadas, dentro desta ótica acima esboçada, do que aquelas que atingem o Código Penal: afinal, no CPM é possível definir com mais clareza o bem jurídico atingido, eis que os crimes ali tipificados estão necessariamente relacionados com sistemas e instalações militares.

O Substitutivo final já trouxe um esforço considerável na melhoria do texto, ao aproximar as condutas inicialmente

previstas no projeto original aos tipos penais já existentes na legislação em vigor.

Não é demais lembrar, porém, que vários tipos penais já em vigor, ao não distinguir *o modo* como o agente atinge o seu intento, abrangem condutas que atingem aquela finalidade com ou sem o uso do computador. Tipos penais assim mostram-se mais adequados; até porque, se violado o mesmo bem jurídico, não se vê razão alguma para tratar o crime de modo diverso pelo mero fato de ter sido praticado com ou sem o uso dos meios informatizados.

Textos suprimidos no Substitutivo

O parecer apresentado em abril de 2007 pelo Senador Azeredo iniciava-se com a inclusão do artigo 141-A que previa o aumento de pena de dois terços caso o crime fosse praticado por intermédio de redes de computadores, dispositivo de comunicação ou sistema informatizado. Ocorre que o artigo 141 em vigência, no seu inciso III, prevê o aumento de um terço no caso de o crime ser cometido *"na presença de várias pessoas, ou por meio que facilite a divulgação da calúnia, da difamação ou da injúria"*. Dessa forma era inconsistente o tratamento dado, uma vez que estabelecia maior gravidade para crimes praticados por meio de redes de computadores do que pela televisão. Esta disposição foi excluída do substitutivo apresentado à Câmara dos Deputados.

Diversos dispositivos que criavam formas delituosas qualificadas, com aumento de pena, pelo fato do crime ser cometido por meio de computadores, também foram corretamente retiradas do texto aprovado no Senado.

Oportuna também foi a retirada do texto que acrescentava mais uma hipótese de prisão preventiva, no artigo 313 do Código de Processo Penal, pelo mero fato do crime ter sido cometido *contra* redes de computadores (como se estas redes fossem as vítimas...). A prisão preventiva recolhe pessoas em favor de quem milita presunção de inocência constitucionalmente assegurada, de modo que deve ser tratada com mais

responsabilidade tanto por parte do legislador, como por parte do aplicador da norma penal. Elogiável, portanto, a supressão.

COMENTÁRIOS AOS ARTIGOS DO PROJETO

Alterações no Código Penal

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

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

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

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

Obtenção, transferência ou fornecimento não autorizado de dado ou informação

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

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

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

Ação Penal

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

O substitutivo apresentado na Câmara dos Deputados se inicia com a criação do Capítulo IV no Código Penal, no qual estão os artigos 285-A, 285-B e 285-C. Os artigos 285-A e 285-B correspondem aos artigos 154-A e 154-B do relatório apresentado pelo Sen. Eduardo Azeredo em abril de 2007.

A redação dada ao artigo 154-A parecia dúbia porque determinava que haveria crime se o acesso ocorresse sem a autorização do titular quando esta fosse devida. No entanto seria objeto de muita discussão o estabelecimento de quando a autorização seria devida. Seria devida quando existissem medidas de segurança para se acessar determinadas informações? Ou quando se violasse disposições contratuais como "Termos de Uso" de um sítio de Internet?

Nesse sentido parece-nos que o substitutivo aprovado no Senado apresentou uma sensível melhora em sua redação, prevendo que o crime ocorrerá quando o acesso se der mediante "violação de segurança". Tal determinação, inclusive, se coaduna com o texto da Convenção de Cibercrimes que prevê que *"A Party may require that the offence be committed by infringing security measures"*[1].

Ainda assim, o texto atual peca por sua excessiva generalidade, como já foi objeto de comentários gerais deste Relatório.

Já o artigo 154-B do relatório anteriormente apresentado previa o crime para caso de obtenção, manutenção, transporte ou fornecimento não autorizado de informação eletrônica ou digital ou similar. A redação dada pelo relatório penalizava apenas a obtenção da informação, mas

1 Tradução livre do texto: Uma Parte poderá requerer que a ofensa seja cometida pela infração de medidas de segurança.

se omitia sobre "*damaging, deletion, deterioration, alteration or suppression of computer data"*[1] que estão previstos na Convenção de Cibercrimes e que parecem ser tipos igualmente relevantes. Este ponto foi parcialmente corrigido no presente substitutivo com a inclusão no artigo 163 do Código Penal do tipo de destruição de dado eletrônico.

Quanto à questão da alteração não autorizada de dado eletrônico resta a dúvida se a mesma poderia estar prevista no artigo 298 do Código Penal, cuja redação dada pelo substitutivo apresentado à Câmara dos Deputados prevê o crime de *"alterar dado eletrônico ou documento particular verdadeiro"*. Diz-se dúvida porque o crime de falsificação implica na intenção de alterar os fatos representados no documento ou dado, sendo certo que a alteração do dado eletrônico pode ocorrer sem que haja essa intenção, mas com a intenção de dificultar o acesso a determinadas informações contidas no documento. Assim, a fim de evitar a configuração do crime previsto no art. 163 o indivíduo poderia apenas alterar o dado eletrônico de forma a tornar praticamente impossível a obtenção das informações nele representadas sem destruí-lo ou apagá-lo.

Há ainda que se ressaltar que houve melhora na redação do art. 285-B com a supressão do tipo de portar dado obtido indevidamente, uma vez que não parecia haver lógica em punir quem está portando as informações se nem se sabe como essa pessoa obteve as mesmas. A punição penal deve recair sobre quem invadiu e obteve para si as informações, até porque esta prova é muito mais objetiva e facilmente feita.

Por outro lado, causa certa estranheza o agravamento da pena prevista no parágrafo único deste artigo. Compreende-se que se queira punir de modo mais severo quem transfere para outrem os dados obtidos indevidamente, pois a violação à privacidade ou aos sigilos se mostra mais danosa com a divulgação; entretanto, se tal crime deve ser tratado como mais grave, igual pena merece quem, mesmo sendo o guardião dos dados, os transfere indevidamente. Isto é, o bem jurídico protegido pela tipificação da conduta de *transferir* dados, do *caput,* é o mesmo que se quer proteger pelo citado parágrafo e deveriam ter a mesma pena. Não há diferença, quanto ao

1 Tradução livre do texto: causar dano, apagar, deteriorar, alterar ou suprimir dado de computador.

bem jurídico a proteger, se os dados são indevidamente divulgados por quem tenha a guarda deles, ou se por quem os obteve de forma ilícita; tal pena, por sua vez, haveria de ser maior, em ambos os casos, do que a prevista para a conduta de meramente obter os dados para si.

Uma crítica que merece ser feita é que o crime deste artigo supõe falta de autorização "do legítimo titular da rede de computadores"; a falta de autorização do titular dos dados ou informações foi desprezada, em prejuízo da proteção à privacidade deste. Além disso, a rede ou sistema informático pode ser mera hospedeira de dados alheios (um *data center*, por exemplo), caso em que a vítima do delito seria o titular desses dados, e não o titular da rede em si.

O artigo 285-C prevê que os tipos previstos neste capítulo serão processados apenas mediante representação, salvo no caso de o crime ser cometido contra *"a União, Estado, Município, empresa concessionária de serviços públicos, agências, fundações, autarquias, empresas públicas ou sociedade de economia mista e subsidiárias"*, o que parece uma opção válida do legislador.

Vale frisar, ainda, que o relatório apresentado pelo Senador Azeredo incluía no artigo 154-C as definições de dispositivo de comunicação, sistema informatizado, redes de computadores e defesa digital. Essas definições, no entanto, no presente substitutivo foram deslocadas para a parte final da lei, e serão comentadas mais a frente.

> ***Divulgação ou utilização indevida de informações e dados pessoais***
>
> *Art. 154-A. Divulgar, utilizar, comercializar ou disponibilizar dados e informações pessoais contidas em sistema informatizado com finalidade distinta da que motivou seu registro, salvo nos casos previstos em lei ou mediante expressa anuência da pessoa a que se referem, ou de seu representante legal:*
>
> *Pena – detenção, de 1 (um) a 2 (dois) anos, e multa.*

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

O artigo 3º do substitutivo apresentado na Câmara prevê a criação do artigo 154-A, o qual cria o tipo penal para a divulgação ou utilização indevida de dados pessoais. Este artigo não tem correlato na Convenção de Cibercrimes, mas se insere no sistema de proteção de dados pessoais adotado pela União Européia. O texto do caput é um pouco limitado, especialmente quanto à definição de "dado pessoal". Não se mostra conveniente tratar do tema desta forma. Se o desejo é ter uma legislação específica de proteção de dados pessoais, o mais adequado seria um ordenamento próprio que definisse melhor dados pessoais, processamento de dados, responsável pelo processamento de dados, etc.

O regime de proteção de dados pessoais ainda é muito pouco explorado em nosso ordenamento jurídico, até mesmo em nível doutrinário, razão pela qual a inserção do dispositivo prevendo a criminalização desta conduta traria uma enorme insegurança jurídica.

Note-se, por exemplo, que definir o que seria a finalidade pela qual se deu o registro dos dados pessoais implicaria em uma grande controvérsia, para a qual entendemos que nosso ordenamento jurídico não fornece elementos suficientemente claros para solucionar.

Dessa forma, parece mais prudente que antes de se criar um tipo penal que se mostra desconexo com o resto do ordenamento jurídico, que se desenvolva no âmbito civil um sistema melhor articulado de proteção de dados pessoais para que somente então se criminalize atos que violem essa política.

Dano

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

..... (NR)

Inserção ou difusão de código malicioso

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

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

Inserção ou difusão de código malicioso seguido de dano

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

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

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

O artigo 4º do substitutivo apresentado na Câmara dos Deputados apresenta primeiramente uma alteração ao caput do artigo 163 do Código Penal, incluindo a expressão "dado eletrônico", o que parece adequado, ressalvadas as observações feitas mais adiante quanto à necessidade de harmonização da terminologia utilizada no substitutivo. Com essa inclusão a criação do artigo 183-A que previa a equiparação para os fins do Código Penal entre coisa e dado eletrônico, a qual estava prevista no relatório apresentado pelo Sen. Azeredo, foi excluída.

Além disso, cria o tipo penal de distribuição de código malicioso no artigo 163-A com a agravante de distribuição seguida de dano. Há que se notar que a redação do artigo 163-A dada no substitutivo foi melhorada em relação à que estava no relatório apresentado pelo Sen. Azeredo, uma vez que foi excluído o tipo de "criar" código malicioso. A

alteração parece adequada, uma vez que profissionais de segurança muitas vezes precisam criar esse tipo de código para testar a segurança de sistemas.

Não obstante as melhoras trazida no texto Substitutivo, o Projeto continua com penas anacrônicas. Se destruir dados, simplesmente, implica na pena de *"detenção, de um a seis meses, ou multa"* prevista no artigo 163, soa despropositado que a mesma destruição de dados seja apenada com sanção tão mais severa, a de *"reclusão, de 2 (dois) a 4 (quatro) anos, e multa",* pelo só fato de ter sido provocada por código malicioso. O bem jurídico a proteger é o mesmo; o crime parece ser o mesmo. É estranho à ciência penal punir diferentemente um crime em função exclusiva dos meios de execução.

Os dois textos criariam até mesmo situações curiosas. Alguém que destruísse fisicamente um computador a marretadas, acarretando também a perda dos dados nele armazenados, estaria sujeito a penas de até 6 meses de detenção; mas quem destruísse *apenas* os dados, utilizando-se de "código malicioso", sujeitar-se-ia a penas de 2 a 4 anos de reclusão.

Mais destoante, então, se mostra a pena prevista no *caput* do artigo 163-A: se o dano puro e simples provoca penas de um a seis meses de detenção, a difusão do código malicioso, sem causar dano algum, como previsto no *caput*, não pode apenar alguém a um a três anos de reclusão.

"Art. 171.

.....

.....

§ 2º Nas mesmas penas incorre quem:

.....

Estelionato Eletrônico

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

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

O artigo 6º cria o inciso VII do §2º do artigo 171, criando o tipo de Estelionato Eletrônico. Este tipo estava previsto no artigo 171-A, do relatório apresentado pelo Sen. Azeredo, e sofreu substancial alteração em sua redação. A nova redação é mais objetiva, determinando que incorre na mesma pena do crime de estelionato quem difunde código malicioso com o intuito de facilitar ou permitir acesso indevido a rede de computadores, dispositivo de comunicação ou sistema informatizado.

Este tipo em princípio parece ser desnecessário, uma vez que o tipo previsto no artigo 163-A já englobaria esta atividade.

Além disso, o tipo penal descrito neste inciso VII destoa do estelionato, que supõe a obtenção de uma vantagem indevida pelo agente. Esta conduta teria sido melhor colocada no texto como uma segunda forma qualificada do crime de **difusão de código malicioso**, como mais um parágrafo ao artigo 163-A, eis que é disso que o inciso em comento realmente trata. Se o código causar dano, temos a incidência do crime qualificado previsto no primeiro parágrafo; então, parece lógico completar aquele artigo com mais esta forma qualificada, que se verifica quando o código malicioso abre portas de entrada no sistema informático infectado. Resta, porém, atribuir pena proporcional a este delito qualificado. O dano provocado por código malicioso deve receber pena mais grave do que o mero risco que o código malicioso provoca. Se, mediante abertura de portas, o agente provoca destruição de dados, pratica o crime de dano; se com a abertura do sistema propiciada pelo código malicioso o agente consegue obter vantagem indevida, comete o crime de estelionato.

Quanto ao tipo penal de estelionato, este deve permanecer intocado. A conduta descrita no artigo 171 é e sempre foi suficiente para penalizar as fraudes cometidas por computador, eis que não está presa ao *meio* utilizado pelo agente. Obter vantagem indevida mediante fraude é crime, seja mediante os velhos contos do bilhete premiado, seja mediante qualquer ardil eletrônico. A forma de execução do crime, nos termos da redação vigente, é indiferente, pois o que interessa é o resultado da conduta.

> ***Atentado contra a segurança de serviço de utilidade pública***
>
> *Art. 265. Atentar contra a segurança ou o funcionamento de serviço de água, luz, força, calor, informação ou telecomunicação, ou qualquer outro de utilidade pública:*
>
> ..... *(NR)*
>
> ***Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático, dispositivo de comunicação, rede de computadores ou sistema informatizado***
>
> *Art. 266. Interromper ou perturbar serviço telegráfico, radiotelegráfico, telefônico, telemático, informático, de dispositivo de comunicação, de rede de computadores, de sistema informatizado ou de telecomunicação, assim como impedir ou dificultar-lhe o restabelecimento:*
>
> ..... *(NR)*

O artigo 7º do substitutivo apresentado à Câmara dos Deputados altera a redação dos artigos 265 (atentado contra serviço de utilidade pública) e 266 (Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático, dispositivo de comunicação, rede de computadores ou sistema informatizado).

Ocorre que as alterações na forma como propostas causam certas inconsistências que devem ser abordadas.

Note-se que a redação vigente do artigo 265 prevê a proteção de serviços de utilidade pública, e dá a esses maior importância que os serviços previstos no artigo 266 que podem ou não ser de utilidade pública.

Assim, enquanto a pena do crime previsto no artigo 265 é de reclusão de um a cinco anos e multa, a pena do crime do artigo 266 é de detenção de um a três anos e multa.

Além disso, enquanto o crime do artigo 265 se configura mediante o mero atentado, o do artigo 266 apenas com a efetiva interrupção e perturbação.

Dessa forma, ao se incluir na redação do artigo 265 os termos "informação ou telecomunicação" e na do artigo 266 os termos "informático, de dispositivo de comunicação, de rede de computadores, de sistema informatizado ou de telecomunicação" cria-se uma situação que uma tentativa de interromper um serviço de telecomunicação (artigo 265) seria punida com pena mais grave do que uma efetiva interrupção desse serviço (artigo 266).

Portanto parece mais adequado não alterar a redação do artigo 265, alterando-se apenas a redação do artigo 266 de forma a penalizar a interrupção do serviço de telecomunicação.

Há que se limitar a inclusão dos bens protegidos no artigo 266, sob pena de se criminalizar condutas que não deveriam ser tuteladas penalmente. Note-se que se mantida a redação na forma apresentada o ato de se desligar um computador poderia caracterizar o crime do artigo 266.

Falsificação de dado eletrônico ou documento público

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

..... (NR)

Falsificação de dado eletrônico ou documento particular

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

..... (NR)

O artigo 8º do substitutivo prevê a alteração dos tipos de falsificação de documento público e particular (arts. 297 e 298 do Código Penal). Essa alteração parece ter a intenção de viabilizar eventual adesão do Brasil à Convenção de Cibercrimes, que prevê a necessidade de os países signatários adotem medidas para vedar falsificações relacionadas a computadores ("computer related forgery"[1]).

Alterações no Código Penal Militar

Art. 251.

.....

§ 1º Nas mesmas penas incorre quem:

.....

Estelionato Eletrônico

VI - Difunde, por qualquer meio, código malicioso com o intuito de facilitar ou permitir o acesso indevido a rede de

1 Tradução livre do texto: "falsificação relacionada a computador"

computadores, dispositivo de comunicação ou a sistema informatizado, em prejuízo da administração militar.

.....

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

Reitera-se, aqui, o comentário feito sobre equivalente proposta de alteração do Código Penal. Melhor seria incluir este tipo penal como forma qualificada do crime que o Projeto inclui no artigo 262-A, do Código Penal Militar.

Dano Simples

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

..... *(NR)*

Dano em material ou aparelhamento de guerra ou dado eletrônico

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

..... *(NR)*

Inserção ou difusão de código malicioso

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

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

Inserção ou difusão de código malicioso seguido de dano

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

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

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

Neste ponto fazemos referência aos comentários ao artigo 4 do substitutivo. A equalização das penas previstas nos tipos se faz necessária também nestes artigos.

Note-se que o tipo previsto no artigo 262 prevê reclusão de até seis meses, enquanto aquele previsto no 262-A, §1º prevê pena de 2 a 4 anos de reclusão e multa.

CAPÍTULO VIII - DOS CRIMES CONTRA A SEGURANÇA DOS SISTEMAS INFORMATIZADOS

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

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

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

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

Obtenção, transferência ou fornecimento não autorizado de dado ou informação

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

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

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

Divulgação ou utilização indevida de informações e dados pessoais

Art. 339-C. Divulgar, utilizar, comercializar ou disponibilizar dados e informações pessoais contidas em sistema informatizado sob administração militar com finalidade distinta da que motivou seu registro, salvo nos

casos previstos em lei ou mediante expressa anuência da pessoa a que se referem, ou de seu representante legal:

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

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

Temos aqui a repetição de tipos penais também incluídos, pelo Projeto, no Código Penal. Como já foi objeto de crítica, na parte inicial deste relatório, ao menos aqui as alterações propostas pelo Projeto encontram uma melhor definição quanto ao bem jurídico protegido, que são, agora, os sistemas informáticos e dados mantidos pelas Forças Armadas, e não todo e qualquer dado ou sistema.

Falsificação de documento

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

..... *(NR)*

Reiteramos os comentários supra, sobre as alterações propostas nos tipos penais de falsificação contidos no Código Penal (arts. 297 e 298).

CAPÍTULO I - DA TRAIÇÃO

Favor ao inimigo

Art. 356.

.....

.....

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

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

..... *(NR)*

Incluiu-se aqui, nestes tipos penais já existentes no CPM, a expressão *"dado eletrônico"*, o que parece adequado; afinal, os dados militares são tão relevantes para estas Forças, ou para a segurança nacional, quanto os demais bens relacionados nestes incisos. Reitere-se, mais uma vez, que aqui o Projeto não se refere genericamente a um dado qualquer, simplesmente mantido em meio eletrônico, mas a informações militares.

Definições contidas no Projeto de Lei

Art. 16. Para os efeitos penais considera-se, dentre outros:

I – dispositivo de comunicação: qualquer meio capaz de processar, armazenar, capturar ou transmitir dados utilizando-se de tecnologias magnéticas, óticas ou qualquer outra tecnologia;

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

III – rede de computadores: o conjunto de computadores, dispositivos de comunicação e sistemas informatizados, que

obedecem a um conjunto de regras, parâmetros, códigos, formatos e outras informações agrupadas em protocolos, em nível topológico local, regional, nacional ou mundial através dos quais é possível trocar dados e informações;

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

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

VI – dados de tráfego: todos os dados informáticos relacionados com sua comunicação efetuada por meio de uma rede de computadores, sistema informatizado ou dispositivo de comunicação, gerados por eles como elemento de uma cadeia de comunicação, indicando origem da comunicação, o destino, o trajeto, a hora, a data, o tamanho, a duração ou o tipo do serviço subjacente.

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

O artigo 16 cria definições que deverão ser utilizadas para efeitos penais.

Primeiramente há que se tecer uma crítica quanto à inclusão de definições na legislação, que vai contra a tradição de nosso ordenamento jurídico, e que, via de regra, quando contrariada, traz resultados pouco proveitosos.

A tentativa de incluir estas definições no texto legal parece ser decorrente de influência do ordenamento jurídico norte-americano

que tem por tradição incluir definições extremamente detalhadas em sua legislação.

Essa prática, porém, como mencionado acima, não não se alinha com o nosso ordenamento jurídico, e as definições como colocadas mostram-se confusas e com pouco ou nenhum rigor metodológico.

Assim, parece mais adequado relegar à doutrina e à jurisprudência a tarefa de definir os termos contidos na lei, suprimindo as definições previstas neste artigo.

Não obstante, vale no presente relatório fazer críticas pontuais às definições apresentadas, muito embora, como já mencionado, seja o nosso entendimento que todas as definições deveriam ser simplesmente suprimidas.

Quanto às definições propriamente ditas, note-se que as dos incisos I a III desse artigo não possuem qualquer rigor metodológico, mas parecem ter por objetivo incluir todo e qualquer dispositivo de processamento de dados (computador, celulares, PDAs, etc.), bem como a(s) rede(s) que os integra(m). A falta de rigor metodológico, porém, causa a imprestabilidade das definições, uma vez que a excessiva abrangência descaracteriza o objetivo de uma definição legal, que é o de estipular limites, o que se mostra ainda mais grave por se tratar de norma de natureza penal.

Ademais, a distinção entre dispositivo de comunicação e sistema informatizado parece confusa, não ficando claro se distingue-se *hardware* de *software* ou se está a diferenciar computador de dispositivos móveis (i.e. telefone celular).Assim, fosse para a lei definir, entendemos que seria mais adequada a unificação do conceito de sistema informatizado e dispositivo de comunicação sob um único termo que o sintetize, como o “dispositivo de processamento de dados”.

Mas o grande problema aqui, insista-se nisso mais uma vez, porque é esta a grande falha do Projeto, continua sendo a falta de precisão do bem jurídico a ser protegido pelas normas penais nele propostas.

Estamos observando, com o progresso da eletrônica, que todo e qualquer aparelho eletro-eletrônico logo será provido de um sistema de processamento e comunicação, o que poderá incluir geladeiras, fornos de microondas, abajures ou torradeiras no espectro de proteção da norma penal contida no projeto de lei em comento. E isso evidentemente não faz sentido, sob a ótica do Direito Penal.

O inciso IV, por sua vez, contém a definição de código malicioso como aquele desenvolvido para executar ações danosas ou obter dados ou informações de forma indevida. Parece, no entanto, que falta à definição o elemento da falta de conhecimento do dono do dispositivo/sistema sobre a atuação do código malicioso..

O inciso V do artigo contém a definição de "dados informáticos". A definição em si parece adequada. No entanto, enquanto neste artigo se faz menção a "dado informático", as redações propostas aos artigos 163, 297 e 298 fazem menção a "dado eletrônico" e o artigo 17 do próprio substitutivo utiliza unicamente a palavra "dado". Dessa forma, vê-se que o próprio projeto não se harmoniza consigo mesmo, no que diz respeito às definições terminológicas nele propostas.

Nesse caso a expressão "dado informático" parece ser mais adequada porque é mais neutra tecnologicamente, uma vez que "eletrônico" refere-se a elétrons, enquanto informático se foca no conteúdo do dado.

O inciso VI apresenta a definição de dados de tráfego. A definição parece em princípio adequada, mas poderia ser minimamente melhorada para que ficasse mais clara. Assim, caso não se atenda à sugestão de supressão total das definições,sugerimos a seguinte redação: "todos os dados informáticos relacionados com uma comunicação efetuada por meio de uma rede de computadoresou dispositivo de processamento de dados, gerados por como elementos de uma cadeia de comunicação, de forma a possibilitar a determinação da origem, do destino, do trajeto, a hora, a data, o tamanho e a duração da comunicação ou o tipo do serviço subjacente".

Suprimiu-se das definições, e de diversos outros dispositivos do texto, o conceito de "defesa digital". Vale destacar que o conceito de "defesa digital" havia sido criada diante de experiências em outros países (Alemanha por exemplo) nos quais a criminalização de atos como acesso não autorizado ou difusão de código malicioso expôs peritos em segurança ao risco de serem punidos criminalmente por sua atividade (o que obviamente não é desejável). Ocorre que o item claramente passava dos limites, permitindo, entre outras coisas, "interceptação defensiva" e "tentativa de identificação do agressor".

O artigo 17 prevê como bens protegidos para efeitos penais *"o dado, o dispositivo de comunicação, a rede de computadores, o sistema informatizado"*. Esta disposição parece redundante diante das alterações ao CP já previstas nos artigos anteriores.

Trata-se, também, de norma desnecessária. O bem jurídico protegido é o que decorre implicitamente da proibição contida nos tipos penais. Em nenhum outro texto legal se encontra disposição semelhante, dizendo que vida, patrimônio, etc. sejam "bens protegidos para efeitos penais".

De outro lado, é controvertida a afirmação de que os bens protegidos sejam *"o dado, o dispositivo de comunicação, a rede de computadores, o sistema informatizado"*. Não interessa à sociedade dar proteção penal a **quaisquer** dados, dispositivos, redes ou sistemas informáticos, o que já foi objeto de crítica nos comentários gerais acima expostos.

Alterações em outras leis:

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

.....

§ 3º.....

.....

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

..... (NR)

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

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

..... (NR)

A alteração prevista no art. 20 não parece ser necessária, uma vez que a adequação do Estatuto da Criança e do Adolescente já é objeto de projeto de lei próprio (o projeto de lei nº 250/08 do Senado o qual já foi aprovado por esta casa).

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

Art. 1º

.....

.....

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

..... *(NR)*

Referida lei trata da repressão uniforme a alguns delitos, atribuindo competência da Polícia Federal para sua invetigação e repressão. Com a generalização que se faz de dado ou sistema informático, esta norma também se mostra exagerada. Melhor seria definir a atuação da PF em situações melhor especificadas, quando os dados ou sistemas em questão sejam ainda mais relevantes.

Informações necessárias à investigação

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

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

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

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

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

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

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

Outro ponto que merece ser criticado é o prazo pelo qual os provedores de acesso estão obrigados a manter os dados de tráfego, que é demasiadamente extenso, valendo lembrar que a manutenção de dados por tanto tempo implica em grave risco contra a privacidade, além de impor enormes gastos aos provedores de acesso.

Ademais, aqui também existe falta de homogeneidade nos termos usados, não se fazendo menção a dados de tráfego (mencionado entre as definições previstas no artigo 16) mas se incluindo de forma expressa quais dados devem ser mantidos.

Parece mais adequado fazer referência apenas a dados de tráfego deixando a tarefa de definir e limitar o significado desta expressão para a doutrina e jurisprudência.

São Paulo, 27 de novembro de 2008

Augusto Tavares Rosa Marcacini
Presidente da Comissão de Informática Jurídica
OAB-SP 95.689

João Fábio Azevedo e Azeredo
Membro da Comissão de Informática Jurídica
OAB-SP 182.454