Crimes informáticos

Comentários ao substitutivo do deputado Pellegrino

Vladimir Aras*

Em 26 de novembro de 2002, o deputado Nelson Pellegrino (PT/BA), relator da Comissão de Segurança Pública e Combate ao Crime Organizado, Violência e Narcotráfico da Câmara dos Deputados apresentou parecer pela aprovação do projeto de lei nº 84/99, e dos projetos nº 2.557/2000, 2.558/2000 e 3.796/2000, que tramitam em apenso. No mesmo ensejo, o relator na referida comissão apresentou substitutivo ao PL nº 84/99, para que as alterações preconizadas na legislação brasileira, em torno dos delitos informáticos, sejam introduzidas no próprio Código Penal, e não em lei extravagante, como pretende o deputado Luiz Piauhylino Filho, autor da proposta original.

No seu substitutivo, o deputado Nelson Pellegrino sugeriu a inserção de cinco novos tipos no Código Penal, dois deles categorizados como infrações penais de menor potencial ofensivo (artigos 154-A e 154-B) e, portanto, de competência dos Juizados Especiais Criminais, regulados pelas Leis nº 9.099/95 e 10.259/2001, especialmente pelo artigo 2º, parágrafo único, desta última. Seguem a regra geral o crime de difusão de vírus eletrônico, que será da competência do juízo comum, estadual ou federal, conforme o caso (artigo 109, da Constituição), o delito de pornografia infantil (artigo 218-A e §1º) e o crime de falsificação de telefone celular ou meio de acesso a sistema eletrônico.

O primeiro dos novos tipos é o de "acesso indevido a meio eletrônico" (artigo 154-A), punindo com pena de detenção de três meses a um ano, e multa. Trata-se do crime de hacking, que é de ação penal pública condicionada, salvo quando cometido contra a União, Estado, Município, empresa concessionária de serviços públicos ou sociedade de economia mista". Seria conveniente que se fizesse menção expressa às autarquias e fundações públicas, a fim de evitar controvérsias a respeito de tipicidade nestes casos. No §1º há uma conduta equiparada à do caput, no caso de favorecimento ao hacking. A competência para o processo e julgamento do crime será dos Juizados Especiais Criminais.

A "manipulação indevida de informação eletrônica" pode passar a ser prevista, como infração penal, no artigo 154-B do Código Penal, com penas de detenção de seis meses a um ano, e multa. Não se abordou a questão dos dados pessoais, principalmente os sensíveis, que merecem uma maior proteção. O delito também será de ação pública condicionada à representação. Convola-se em crime de ação pública incondicionada nas mesmas situações que o tipo do artigo 154-A. A competência também será dos Juizados Especiais. A redação é de certo modo confusa, podendo ser aperfeiçoada. No §1º, que padece do mesmo defeito, há uma conduta equiparada à do caput, como sendo a de "transportar" ilicitamente (melhor seria "transmitir" e "transferir") dado ou informação eletrônica para qualquer outro meio ou sistema.

O crime de inoculação de vírus de computador ("difusão de vírus eletrônico"), terceira inovação típica, está previsto no §3º do artigo 163, englobando todos as espécies de malicious codes (vírus, worms e cavalos-de-Tróia) e certos casos de denial of service. Este crime será em regra de ação penal pública incondicionada, mas dependerá de queixa-crime quando "o dado ou informação não tiver potencial de propagação ou alastramento". A pena será a do §1º, já existente para a modalidade qualificada do dano: seis meses a três anos de detenção, e multa. Será possível a suspensão condicional do processo penal, por proposta do Ministério Público (artigo 89, da Lei nº 9.099/95), mas o crime ficará sob a competência do juízo comum, pelo procedimento sumário, relativo aos delitos apenados com detenção.

Com a introdução de §2º ao artigo 163 do Código Penal (crime de dano), serão equipados ao conceito de "coisa" tanto "o dado, a informação ou a base de dados presente em meio eletrônico ou sistema informatizado" quanto a "senha ou qualquer meio de identificação que permita o acesso a meio eletrônico ou sistema informatizado" (art. 163, §2º, I e II). Com isso, poderão se encerrar as discussões a respeito da natureza jurídica dos dados informáticos.

No capítulo do Código Penal atinente aos crimes contra os costumes, o substitutivo propõe a inserção do artigo 218-A, para tipificar o delito de "pornografia infantil" (quarta inovação), punindo com penas de um a quatro anos de reclusão, e multa, quem "fotografar, publicar ou divulgar, por qualquer meio, cena de sexo explícito ou pornográfica envolvendo criança ou adolescente". A redação do dispositivo é semelhante à do artigo 241 do Estatuto da Criança e do Adolescente, que será revogado (artigo 10 do projeto), mas avança por introduzir a este tipo de conduta múltipla a ação de "divulgar" pornografia infantil, bem como por tornar indiferente o meio da prática criminosa, com a expressão "por qualquer meio", ausente do ECA. A sanção permanece a mesma, não se alterando também a natureza pública incondicionada da ação penal. Todavia, o §1º do novo artigo proposto prevê uma forma qualificada, que determina o aumento da pena de metade até dois terços, "se o crime é cometido por meio de rede de computadores ou outro meio de alta propagação".

O crime de pornografia infantil (artigo 218-A do CP) será de competência do juízo comum, podendo haver, como hoje (artigo 241 do ECA), proposta de suspensão condicional do processo em relação à figura do caput. A forma qualificada, aquela cometida pela Internet ou por meio equivalente, não admitirá o instituto do artigo 89 da Lei nº 9.099/95, pois a pena mínima, abstratamente cominada ao tipo (artigo 218-A, c/c o §1º), superará o limite de um ano, estabelecido para a obtenção do sursis processual. Entendemos que a gravidade do problema da pornografia infantil on-line autoriza essa solução mais rigorosa.

O quinto novo tipo preconizado no substitutivo do deputado Nelson Pellegrino é o de "falsificação de telefone celular ou meio de acesso a sistema eletrônico" (artigo 298-A), colocado no capítulo atinente à falsidade documental (crimes contra a fé pública), com penas de um a cinco anos de reclusão, e multa. Aqui as condutas consideradas são o phreaking e comportamentos ilícitos correlatos, inclusive delitos de uso de mídias eletrônicas. A competência será do juízo comum, com possibilidade de sursis processual.

Dois outros tipos penais mereceram proposta de nova redação, para adequação às necessidades de combate à cibercriminalidade. Ambos são e continuarão a ser (caso aprovado o substitutivo) de competência do juízo comum e sujeitos a suspensão condicional do processo. Com efeito, o artigo 265 do Código Penal, de "atentado contra a segurança de serviço de utilidade pública", com penas de um a cinco anos de reclusão e multa, é alterado simplesmente para inserir no caput, como objeto material da conduta, os serviços de

telecomunicação. A modificação é despicienda, pois entre os serviços de utilidade pública já estão os de telecomunicação.

No tocante ao artigo 266 do Estatuto Repressivo, a alteração é mais apropriada, embora proponha-se tão-somente a inclusão do mesmo objeto material, "serviço de telecomunicação", ao rol ali existente. Cremos que este dispositivo pode ensejar conflito com a última conduta da parte final do artigo 163, §3º, sugerido pelo substitutivo, em relação aos ataques da espécie denial of service, quando atinjam sistemas informáticos de prestadores de serviços de telecomunicação. Entretanto, o conflito é apenas aparente, bastando, para a sua solução, o emprego do princípio da especialidade. A pena cominada é de um a três anos de reclusão, e multa, não havendo, neste passo, qualquer alteração.

O parecer propôs também definições legais para "meio eletrônico" e "sistema informatizado" (melhor seria "sistema informático"). Entende-se por meio eletrônico, "o computador, o processador de dados, o disquete, o CD-Rom ou qualquer outro meio capaz de armazenar ou transmitir dados magnética, óptica ou eletronicamente". A definição merece crítica por não respeitar, às inteiras, o princípio da neutralidade tecnológica. Já o "sistema informatizado" é "a rede de computadores, a base de dados, o programa de computador ou qualquer outro sistema capaz de armazenar ou transmitir dados eletronicamente".

Por sua vez, pelo projeto, o artigo 298 do Código Penal, que cuida do crime de falsificação de documento particular, passará a ter um parágrafo único, para equiparar a documento particular o cartão de crédito ou de débito. Com isso, surge uma modalidade especial do crime tradicional de falsidade documental, com penas de um a cinco anos de reclusão, e multa, idêntica à do caput. A competência permanecerá no juízo comum, com possibilidade de sursis processual.

Infelizmente, a única alteração proposta pelo substitutivo em relação às leis processuais penais é a que introduz um novo parágrafo ao artigo 2º da Lei nº 9.296/96, que cuida da interceptação de comunicações telefônicas e telemáticas. Outras alterações necessárias, especialmente no Código de Processo Penal, foram deixadas de lado. O §1º do artigo 2º da Lei Federal nº 9.296, de 1996 passará a prever que o disposto no inciso III do caput não se aplicará "quando se tratar de interceptação do fluxo de comunicações em sistema de informática ou telemática".

A alteração é essencial para a investigação de crimes de informática, tendo em vista que o referido inciso III veda a interceptação para os crimes apenados com detenção. Ou seja, hoje só admite a escuta telefônica ou telemática quando o fato investigado é tipificado como infração sujeita a pena de reclusão (artigo 2º, inciso III, da Lei nº 9.296/96). Se aprovado o projeto, a vedação persistirá apenas em relação às comunicações telefônicas, ao passo que em qualquer crime informático (próprio ou impróprio), apenado com reclusão ou detenção, será possível a interceptação.

Quanto ao artigo 11 do substitutivo, que determina vigência imediata das novas disposições, pensamos que é conveniente estabelecer um prazo de vacatio legis razoável, a fim de permitir a adequação dos operadores ao novo sistema. Noventa dias seria um período adequado. Neste aspecto, não se podem olvidar as recomendações do artigo 8º da Lei Complementar Federal nº 95/98: "A vigência da lei será indicada de forma expressa e de modo a contemplar prazo razoável para que dela se tenha amplo conhecimento, reservada a cláusula 'entra em vigor na data de sua publicação' para as leis de pequena repercussão".

Concluindo esta breve análise, não se pode deixar de lamentar a perda de oportunidade para uma regulamentação mais abrangente da cibercriminalidade, enfocando não só o direito material, mas também o direito processual. Como quer que seja, o projeto do deputado Luiz Piauhylino Filho, com os substitutivos dos deputados Leo Alcântara e Nelson Pellegrino, é uma das iniciativas de melhor qualidade em curso no Congresso Nacional. Espera-se que o projeto (ou outro que o venha substituir) seja acolhido em breve no plenário da Câmara dos Deputados e pelas comissões que o analisarão no Senado. Espera-se também que possam ser acrescidas inovações, corrigidos os pequenos equívocos existentes e supridas as omissões, a fim de que o ordenamento jurídico nacional venha a fazer frente à ameaça cibernética. A melhor maneira de fazê-lo é, sem dúvida, aproveitando o paradigma da Convenção contra a Cibercriminalidade do Conselho da Europa - CoE (www.coe.int) . Com efeito, a chamada Convenção de Budapeste, de 2001, encarta um modelo cibercriminal completo, englobando tipos penais, medidas processuais e mecanismos de cooperação internacional muito específicos. Neste particular, a legislação portuguesa, em especial a Lei nº 109/91 (Lei de Criminalidade Informática) e a Lei nº 67/98 (Lei de Proteção a Dados Pessoais) , também podem servir de inspiração ao legislador brasileiro.

Retirado de: Revista Consultor Jurídico, 27 de novembro de 2002.