UM PANORAMA SOBRE OS PROJETOS DE LEI SOBRE CRIMES DIGITAIS

Coriolano Almeida Camargo

Advogado CEO da banca Almeida Camargo Advogados. Presidente da Comissão de Direito Eletrônico e Crimes de Alta Tecnologia da OAB/SP é Mestre em Direito na Sociedade da Informação e certificado internacional em Direito Digital pela *Caldwell Community College and Technical Institute*. Professor em programas de pós-graduação no Mackenzie, USP, EPD e FIA e outras.

Marcelo Crespo

Advogado da banca David Rechulski, Advogados. É especialista em crimes digitais, possuindo certificação internacional em Segurança Digital pela Universidade de Salamanca. É Doutor em Direito Penal pela USP, membro das Comissões de Direito Criminal e de Direito Eletrônico Crimes de Alta Tecnologia da OAB/SP e professor em cursos de pós-graduação.

Na tarde de ontem a Câmara dos Deputados aprovou o texto de dois projetos de leis – PL 84/99 e PL 2793/11 – que ficaram conhecidos, respectivamente, por “Lei Azeredo” e “Lei Carolina Dieckmann”, em alusões ao relator do projeto 84/99, Eduardo Azeredo, e à atriz global, que em maio teve divulgadas em que aparecia nua. Desta forma, assunto que já há algum tempo tomou as notícias do cotidiano, os crimes digitais poderão finalmente contar com leis específicas que alteram o Código Penal. Isto é, a menos que a Presidente exerça a prerrogativa do veto.

Com isto, ao que parece, não subsistirá a ideia de que a internet era uma verdadeira "terra de ninguém" pela ausência de tipos penais específicos para os crimes digitais. A ideia de que a falta de legislação específica não permitia a persecução penal era parcialmente equivocada porque muitos dos crimes praticados no âmbito da internet já eram previstos em nosso ordenamento e podiam ser alvo de processo. São os casos do estelionato e de fraudes em geral, de crimes contra o consumidor, de crimes contra a honra e, ainda, daqueles relacionados à pornografia infantil.

Condutas como a criação e disseminação de vírus computacional, a de ataques de negação de serviço (DoS) e, ainda, o chamado *hacking* (acesso não autorizado a sistemas) não poderiam ser punidas porque não tipificadas. Sendo os projetos de leis sancionados pela Presidente, este cenário poderá mudar. Veja-se.

Relativamente à **"Lei Dieckmann"**, foram criados os artigos 154-A e 154-B, sendo que o primeiro recebeu o *nomen juris* de "Invasão de dispositivo informático" e o segundo trata da ação penal, que será, em regra, pública condicionada à representação, exceto quanto a conduta for praticada em desfavor da administração pública.

Quanto à conduta incriminada no art. 154-A, ter-se-á "invasão" quando alguém "Devassar dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo, instalar vulnerabilidades ou obter vantagem ilícita". Neste caso a pena cominada é de detenção de 03 meses a 01 ano e multa.

Mas não é só. O §1º incrimina, ainda, a conduta de "quem produz, oferece, distribui, vende ou difunde programa de computador com o intuito de permitir a prática da conduta definida no *caput*". Já o §2º traz causa de aumento de pena (de um sexto a um terço) se das condutas decorrer prejuízo econômico e o §3º prevê que as penas sejam de reclusão de 06 meses a 02 anos e multa, caso haja a "obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais e industriais, informações sigilosas assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido". Por sua vez, o §4º traz mais uma causa de aumento de penal (de um a dois terços) se houver "divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos, se o fato não constitui crime mais grave". Encerrando as disposições do art. 154-A, o §5º prevê que as penas sejam aumentadas de um terço até a metade caso as condutas praticadas sejam dirigidas a autoridades (Presidente da República, do Supremo Tribunal Federal, Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal e dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federa)

Em suma, o art. 154-A pretendeu atender as diretivas internacionais sobre crimes digitais, procurando tipificar as condutas de "hacking" ou "invasão" ("Devassar dispositivo informático"...), de criação e disseminação de vírus computacional ("produz,

oferece, distribui, vende ou difunde programa computacional com o intuito de permitir a conduta prevista no caput") e, ainda, de obtenção e disseminação ilegal de dados ("Se da invasão resultar a obtenção de conteúdo"...). Lamenta-se que para a redação do art. 154-A tenha-se esquecido que a lei 9.504/97 já continha alguns dispositivos relativos ao "hacking" e criação de vírus computacional (art. 72, incisos I e II) e que, talvez fosse o caso de uniformizar a tipificação de condutas semelhantes, evidentemente distintas, no entanto, em face do caráter eleitoral das normas contidas na lei de 1997.

Ainda quanto à **"Lei Dieckmann"**, pretendeu-se alterar o Código Penal para que incriminasse a interferência em sistemas, geralmente ultimadas pelos ataques "Denial of servisse" (DoS) ou, no vernáculo, denegação de serviço. Por tal razão se acrescentou um parágrafo ao art. 266, que trata da "Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública". Assim, incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento. Ocorre que com a tipificação proposta pela inserção do §1º não foram abarcadas as condutas que venham a atingir os serviços de telecomunicação ou informação particulares, que podem ser bastante deletérias.

Por fim, a **"Lei Dieckmann"** previu uma alteração nos crimes de falso, precisamente no art. 298 (falsificação de documento particular). Assim, criou-se o parágrafo único, que equipara a documento particular o cartão de crédito ou débito. Neste particular, o legislador tornou crime a clonagem de cartão de crédito ou débito, independentemente que sejam utilizados para efetivar compras. Tal inovação, todavia, não se mostrará de grande utilidade. Isso porque os cartões falsificados se prestam, na sua imensa maioria, que sirvam de instrumento para a aquisição de bens e produtos. Ocorre que a falsificação seguida da compra configura crime de estelionato, segundo o entendimento do Superior Tribunal de Justiça (Súmula 17. Quando o falso se exaure no estelionato, sem mais potencialidade lesiva, e por este absorvido).

No que tange à "Lei Azeredo", projeto que já foi chamado até mesmo de "AI-5 digital" por conta dos pontos polêmicos que continha – especialmente pela guarda dos logs – , acabou esvaziado após acordo celebrado na Câmara. Até ontem à noite o texto final não se encontrava disponível no site da Câmara, mas saber-se que a grande maioria dos seus artigos foi rejeitada, como ocorreu com os artigos 2º, 3º, 4º, 5º, 6º, 7º, 8º,10,

11,12, 13, 14,16, 17, 20, 21 e 22. Permaneceram apenas quatro artigos, aprovados em maio deste ano na Comissão de Ciência e Tecnologia, Comunicação e Informática. Assim, o texto aprovado determina que os órgãos da polícia judiciária deverão criar delegacias especializadas no combate a crimes digitais. Além disso, tipificou a divulgação de dado eletrônico em tempo de guerra que favoreça o inimigo, prejudique operações militares ou comprometa a eficiência militar do País (penas variando entre 20 anos de reclusão e à morte). Por fim, foi introduzido dispositivo para obrigar que mensagens com conteúdo racista sejam retiradas do ar imediatamente.

Concluindo, é possível reconhecer que a legislação a ser sancionada pode representar um avanço na tentativa de reprimir a prática de crimes digitais, mas isso não significa que todas as práticas serão punidas. Afinal, não basta a tipificação, sendo necessário investimento nas polícias (equipamentos e pessoal e especialização no atendimento), aderência a tratados e acordos de cooperação internacional, além da educação digital.