Previsão de cibercrimes em projeto do Senado carece de precisão técnica

O Direito Penal vem sofrendo profundas transformações a partir da globalização e do advento das novas tecnologias. A disciplina se encontra em franca expansão e é discutida sua legitimidade para disciplinar interesses originários das *sociedades de risco*. A tensão dialética estabelecida pela flexibilização das regras tradicionais do Direito Penal é marca notável do desenvolvimento dogmático contemporâneo, e a proposta do novo Código Penal parece optar por relativizar tais postulados.

Ao fim de 2013, foi entregue ao presidente do Senado o relatório final do PLS 236/12, a ser analisado pela Comissão de Constituição, Justiça e Cidadania (CCJ). Entre as mais variadas temáticas contempladas na iniciativa de reforma do Código está a da hostilidade digital. Além de reproduzir o sumário conceitual da Convenção de Budapeste (2001), o projeto traz, em título exclusivo, um rol de "crimes cibernéticos", atribuindo tipicidade a uma série de condutas vinculadas ao uso de sistemas informatizados, para as quais comina, sem exceção, pena privativa de liberdade. Características também intersectas aos delitos minutados, a titularidade da ação penal será sempre do Ministério Público, condicionada, porém, à representação do ofendido em casos específicos, e que será maior o desvalor da conduta dirigida contra a Administração Pública.

No artigo 208 são introduzidos conceitos básicos para a compreensão dos tipos penais, já sinalizando a dificuldade de delimitação do tema e uma clara opção por um Direito Penal mais aberto e flexível.

Apesar de fugir ao direito positivo na definição de institutos jurídicos, a proposta vai bem ao conceituar *sistema informatizado*, *dados informatizados*, *provedor de serviços* e *dados de tráfego* para atender o princípio da legalidade. Por outro lado, no mesmo princípio reside a crítica: por trás dele está o inafastável postulado da segurança jurídica, cujo conteúdo se revela na paz e estabilidade social. Todo comando proibitivo deve ser claro para não gerar dúvidas, já que a lei é dirigida ao cidadão, prestando-se a modelar comportamentos. Deve, pois, lhe garantir a segurança de estar agindo em conformidade com a ordem jurídica e, na hipótese de sua violação, a ciência da sanção correspondente.

A falta de intimidade da doutrina com o teor informático revela justamente o maior desafio do tema: sua alta tecnicidade. O conteúdo da nova tecnologia não é de fluida compreensão para leigos e juristas, demandando conhecimento específico de disciplinas complementares, abalando o princípio da legalidade. São conceitos que não caberiam ao texto legal, mas à doutrina — sobretudo pelo desenvolvimento ininterrupto da tecnologia.

Adiante, o artigo 209 do projeto tipifica o *acesso indevido*, cuja ação penal se procede mediante representação da vítima. Os parágrafos primeiro e segundo aventam circunstâncias qualificadoras: ocorrência de prejuízo econômico; divulgação, comercialização ou transmissão dos dados, arquivos, senhas ou informações porventura obtidos; ocorrência de controle remoto do dispositivo comprometido; cometimento da infração contra a Administração Pública.

A ação descrita afronta o princípio da confidencialidade, que, oriundo do campo da Segurança da

Informação, garante o acesso à informação somente por pessoal autorizado. No Código Penal em vigor, praticamente a mesma conduta é prevista no artigo 154-A. Uma das principais diferenças é a troca do núcleo verbal *invadir* por *acessar*. Além disso, é suprimida a necessidade do dolo com especial fim de agir, amplificando seu raio de incriminação já que, hoje, para configuração do delito, é exigida a intenção de *obter, adulterar ou destruir dados* ou, ainda, de *instalar vulnerabilidades para obter vantagem indevida*.

O Artigo 210 apresenta a *sabotagem informática,* consistente em causar *entrave, impedimento, interrupção ou perturbação grave, ainda que parcial,* na funcionalidade de sistema ou comunicação de dados informatizados sem permissão legal ou autorização do titular. Os princípios da informação aqui atacados são o da disponibilidade (diz respeito à eficácia do sistema) e o da integridade (garante a idoneidade da informação).

O delito proposto remete à conduta do atual artigo 266, parágrafo 1º, CP (*Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública*). É curioso que o legislador tenha alocado a sabotagem em artigo diverso daquele que tratou do acesso indevido; porém, nem toda atividade maliciosa é mecanicamente coordenada por um *insider,* não sendo necessário acessar remotamente um sistema para afetá-lo ou danificá-lo — dada a existência de programas maliciosos (*malwares*) de ação automática.

No artigo 211 do projeto se trata a ocorrência de dano a dados informatizados, discriminada em *destruir, danificar, deteriorar, inutilizar, apagar, modificar, suprimir ou, de qualquer outra forma,* neles *interferir*. A conduta estampada também afronta o princípio da integridade da informação, comprometendo sua veridicidade. Sua leitura permite identificar a ação do atual artigo 313-A, CP (*Inserção de dados falsos em sistema de informações*), embora não seja crime próprio quanto aos sujeitos ativo e passivo. De igual maneira, são também abarcadas pelo artigo 211 as condutas do vigente 313-B, CP (*Modificação ou alteração não autorizada de sistema de informações*) e do 266, parágrafo 1º, CP, já comentado.

O artigo 212 do código pendente de aprovação, trazendo a figura da *fraude informática,* convoca reflexões mais pormenorizadas. Em seus termos, o crime ocorre se o agente obtém, *para si ou para outrem, em prejuízo alheio, vantagem ilícita, mediante a introdução, alteração ou supressão de dados informatizados, ou interferência indevida, por qualquer outra forma, no funcionamento de sistema informatizado,* aumentando-se a pena se é utilizado nome falso ou identidade de terceiros para tanto.

É prudente refletir sobre a opção do legislador por criar mais uma figura típica (e sitiá-la nesse capítulo) para uma conduta que pode ser subsumida por outros tipos já previstos: a fraude e o furto mediante fraude.

De plano, é imperioso recordarmos que o núcleo da intervenção penal nas relações sociais é a proteção de bens jurídicos — que continuam a ser o ponto de partida para qualquer incriminação e devem, para tanto, ser clara e precisamente identificados.

A fraude é caracterizada pela indução ou mantença da vítima em erro — ou seja, uma falsa percepção da realidade — com o fito de obter, para si ou para outrem, a vantagem ilícita que resultará no prejuízo

alheio. O bem jurídico comum a todos os tipos de fraude é *o patrimônio alheio em qualquer de seus integrantes* — ou seja, direitos, bens móveis, imóveis etc. (MUÑOZ CONDE, 2002, p. 410). É o que ocorre quando, arrastada ao erro, a vítima efetua compras de produtos inexistentes ou efetua, espontaneamente, depósitos via internet em contas diversas daquelas nas quais imagina fazê-lo. Já no furto mediante fraude, a quantia é subtraída da vítima mediante emprego de embuste ou mecanismo ardil criado pelo agente. É o que ocorre, por exemplo, nas fraudes bancárias operadas por meio de *phishing.*

Trata-se de um método de indução comportamental em que a vítima, recebendo e-mails falsos, é induzida a clicar em botões para receber supostos prêmios ou preencher formulários. Ao clicar nesses ícones, é feito o download de um arquivo executável e a máquina é infectada. Em alguns casos, o atacante utiliza páginas simuladas e redirecionamento de URLs para desviar o usuário para sites maliciosos, onde são coletadas informações sensíveis. São práticas que em muito comprometem a segurança no *e-commerce.*

Ora, deve-se recordar a função sistemática do bem jurídico-penal, traduzida em formar um parâmetro de catalogação topográfica dos tipos na parte especial do Código. Desse modo, parece mais afortunado dispensar a criação de mais um artigo e inserir a *fraude informática* no capítulo que trata especificamente do estelionato e demais modalidades de fraude, bem como fazê-lo quanto ao dispositivo reprovador do furto mediante fraude, que poderia, por exemplo, ter seu comando normativo adaptado para melhor incluir a versão informática do crime.

O projeto tipifica, no artigo 213, a *obtenção indevida de credenciais de acesso* – conduta que também viola o princípio da autenticidade. As credenciais de acesso são concebidas como instrumentos que identificam indivíduos no mundo virtual (o mesmo papel que têm os documentos pessoais no universo físico). Exemplos dessas credenciais são as senhas e os registros de autenticação biométrica – tais como a geometria de dedos, impressões digitais e o reconhecimento de voz e de íris.

Uma das investidas mais comuns visando credenciais é o emprego de *keyloggers*, um tipo específico de spyware capaz de capturar as teclas digitadas; em geral é atrelado a uma ação (evidentemente, não intencional) do próprio usuário, como o acesso a um site malicioso. Outro método para esses fins é o *sniffing* – usado para interceptar dados trafegados em conexões inseguras.

Outra observação sobre o artigo 213 é a possibilidade de uso de credenciais sem prévia apropriação indevida: é o caso do profissional que opera diretamente bancos de dados, tendo a posse legítima de grande quantidade delas. Note-se que, como apresentado, o artigo não menciona o *uso* indevido de credenciais, mas somente a sua *apropriação* indevida. Por outro lado, o agente que utiliza credenciais de acesso de outrem em virtude de tê-las sob sua guarda incorreria, *a priori*, no crime de acesso indevido e no já previsto crime de *falsa identidade* (307, CP). A lógica no ciberespaço não deixa de ser a mesma: o indivíduo que se passa por outro atribui a si uma falsa identidade. Novamente, deve-se repensar a necessidade de criação de mais um tipo penal.

O último delito rascunhado no novo *codex* insculpe o *artefato malicioso* (artigo 214). O pretendido foi dar resposta penal à figura do desenvolvedor, pelo que se criou um tipo plurinuclear, elencando variados verbos para preenchê-lo:*produzir, adquirir, obter, vender, manter, possuir ou por qualquer forma distribuir, sem autorização, artefatos maliciosos destinados à prática de crimes previstos neste Título.*

Porém, a Comissão não atentou para a existência de spams.

Spams são e-mails não solicitados, em geral, enviados em massa, podendo ser remetidos via redes sociais, programas de conversação instantânea e via telefonia móvel — hoje imbuída na Internet — contendo programas que, instalados,permitem que, sem a ciência do usuário, sejam enviados outros spams para novos destinatários.

Outra hipótese que independe da vontade e do conhecimento do usuário é a atividade de malwares da espécie *downloaders*, que baixam programas automaticamente. É importante que a redação do novo tipo penal atente para essas questões para não presumir que uma infecção computacional ocorra, necessariamente, com dolo do usuário remetente – na maioria dos casos, também vítima.

Por fim, o projeto traz, no parágrafo único do artigo 214, quatro excludentes de ilicitude:

Excludente de ilicitude

Parágrafo único. Não são puníveis as condutas descritas no caput quando realizadas para fins de:

I – investigação por agentes públicos no exercício de suas funções;

II – pesquisa acadêmica;

III – testes e verificações autorizadas de vulnerabilidades de sistemas; ou

IV – desenvolvimento, manutenção e investigação visando o aperfeiçoamento de sistemas de segurança.

É imperiosa a indagação: cuida-se de uma dirimente da ilicitude ou de um afastamento da punibilidade?

A ilicitude corresponde à contrariedade ao direito positivo; a consequência jurídica de sua exclusão é a atipicidade. Ao contrário dela, a punibilidade não integra o conceito analítico de crime (fato *típico, ilícito e culpável*), sendo a possibilidade jurídica de o Estado sancionar o agente violador da norma proibitiva. O fato de uma conduta não ser punida não a libera de ser criminosa, merecendo reformulação tal dispositivo para desatar a questão.

Visando isentar da incriminação do artigo 214 os analistas de segurança da informação, a Comissão teve o cuidado de inseri-los em um dos incisos do parágrafo único. Contudo, profissionais que desenvolvem análise de segurança e solução para incidentes não se aventuram em inspetorias independentes. Auditores de vulnerabilidades e peritos em análise forense computacional são certificados por seus centros de treinamento, e, não raro, credenciados em organismos internacionais; atuam sob autorização das empresas inspecionadas estando, pois, acobertados pelo *consentimento do ofendido*, conhecida excludente supralegal da ilicitude e que, por assim sê-la, afasta o ilícito penal.

Por outro lado, merece cautela o inciso I do mesmo parágrafo único, que elimina o caráter ilegal do *caput* se a ação é cometida para fins de *investigação por agentes públicos no exercício de suas funções.* Embora não expressa no dispositivo, qualquer interceptação comunicacional só está autorizada mediante ordem judicial, conforme o inciso XII do artigo 5º da Constituição e a Lei 9.296/96. Em nenhuma

hipótese, portanto, bastará o exercício regular de direito para afastar a ilicitude de uma interceptação desprovida de um provimento do Judiciário.

A expansão tecnológica hoje impõe ao legislador a hercúlea tarefa de normatizar ocorrências sob aprimoramento ininterrupto. É urgente um combate efetivo a situações cada vez mais nocivas, mas é igualmente relevante que as iniciativas legais tocantes ao assunto tenham precisão técnica, de modo que não se esvazie a identidade de *ultima ratio* do Direito Penal, nem que se aumente o catálogo incriminador sem real necessidade.

A primeira reflexão deve circular o bem jurídico que, efetivamente, se pretende tutelar. De antemão, não parece exagerada a afirmação de que apontar como crime informático (ou cibernético, conforme variações na doutrina) qualquer conduta que guarde relação com computadores é tão leviano quanto considerar como um delito de natureza econômico-financeira qualquer conduta que guarde relação com o dinheiro.

———

CONDE, Muñoz, Francisco. Derecho Penal – Parte Especial. 14 ed. Valencia: Tirant to Blanch, 2002.

HEFENDEHL, ROLAND. Linhas Gerais de uma Teoria do Bem Jurídico. In: O Bem Jurídico como Limitação do Poder Estatal de Incriminar? Coord. Luís Greco; Fernanda Lara Tórtima. pp. 57-75 Rio de Janeiro: Lumen Juris, 2011.

PRADO, Luiz Régis. Bem Jurídico-Penal e Constituição. São Paulo: Revista dos Tribunais, 2011.

SILVA SÁNCHEZ, Jesús-María. A expansão do direito penal: aspectos da política criminal nas sociedades pós-industriais. Tradução Luiz Otavio de Oliveira Rocha – São Paulo: Editora Revista dos Tribunais, 2002

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Cartilha de Segurança na Internet. Disponível em: <http://cartilha.cert.br/>. Acesso em: 21.02.2014.

Date Created
05/03/2014