MPSP Ministério Público
DO ESTADO DE SÃO PAULO
CENTRO DE APOIO OPERACIONAL CRIMINAL
Rua Riachuelo, 115 - 7º andar - sala 730 - São Paulo - CEP 01007-000 – tel. 3119-9922
caocrim@mp.sp.gov.br

NOVA LEI DE CRIMES CIBERNÉTICOS ENTRA EM VIGOR

Apelidada de “Lei Carolina Dieckmann”, a Lei nº 12.737, de 30 de novembro de 2012, entrou em pleno vigor no último dia 3 de abril de 2013, alterando o Código Penal para tipificar os *crimes cibernéticos propriamente ditos* (**invasão de dispositivo telemático e ataque de denegação de serviço telemático ou de informação**), ou seja, aqueles voltados contra dispositivos ou sistemas de informação e não os crimes *comuns* praticados por meio do computador. Colateralmente equiparou o cartão de crédito ou débito como documento particular passível de falsificação.

A lei é fruto de projeto apresentado pelo Deputado Federal Paulo Teixeira (PT-SP), cujo trâmite foi acelerado depois da invasão, subtração e exposição na internet de fotografias íntimas da referida atriz.

Cuidando-se de nova lei incriminadora, a Lei nº 12.737/2012 que, em seu art. 4º estabelece uma *vacatio legis* de 120 (cento e vinte) dias, não poderá retroagir para alcançar condutas pretéritas.

Assim, a nova lei incrimina as condutas de:

Invasão de dispositivo informático

- Invadir dispositivo informático alheio de qualquer espécie, conectados ou não em rede, desde que violado mecanismo de segurança (senha, *firewall* etc.), desde que a finalidade do criminoso seja obter, adulterar ou destruir dados ou informações.
- Instalar no dispositivo informático qualquer vulnerabilidade com o fim de obter uma vantagem ilícita (patrimonial ou não).

Rua Riachuelo, 115 - 7º andar - sala 730 - São Paulo - CEP 01007-000 – tel. 3119-9922
caocrim@mp.sp.gov.br

- Produzir, oferecer, distribuir, vender ou difundir dispositivo ou programa de computador com o intuito de permitir a invasão de dispositivo informático ou a instalação de vulnerabilidades.
- O objeto jurídico tutelado pela norma é a liberdade individual do usuário do dispositivo informático.
- As penas para esses delitos são de reclusão de 3 (três) meses a 1 (um) ano de detenção, e multa.
- As penas aumentam de 1/6 a 1/3 se a invasão resulta prejuízo econômico.
- O crime é qualificado, com penas que vão de 6 (seis) meses a 2 (dois) anos de reclusão e multa, caso a conduta não configure outro crime mais grave, quando a invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações definidas em lei como sigilosas. Se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos, a pena do crime qualificado será também aumentada de 1/3 a 2/3.
- As penas, conforme o caso (tipo simples ou qualificado) serão aumentadas de 1/3 até a metade, se o crime for praticado contra Presidente da República, Governadores e Prefeitos, Presidente do Supremo Tribunal Federal, da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal, ou dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.
- **Importante**: se a conduta for mais grave que a simples invasão com a finalidade de obtenção, adulteração ou destruição dos dados ou informações, ou a instalação de vulnerabilidades, como por exemplo, fraudes em *netbanking* (furto qualificado), estelionato ou extorsão,

Rua Riachuelo, 115 - 7º andar - sala 730 - São Paulo - CEP 01007-000 – tel. 3119-9922
caocrim@mp.sp.gov.br

interceptação de comunicação telemática, o crime de invasão de dispositivo informático será desconsiderado, porque constituirá somente um meio para o cometimento daquelas condutas.

- Para que o criminoso possa ser investigado pela Polícia e processado pelo Ministério Público, é preciso que a vítima autorize, oferecendo a representação. O Ministério Público pode processar diretamente o criminoso somente quando o crime é praticado contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos.

Interrupção de Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação ou utilidade pública (ataque de denegação de serviço – DOS/DDOS).

- O artigo 266 do Código Penal pune a conduta de interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento, estabelecendo penas que variam de 1 (um) a 3 (três) anos de reclusão e multa, que são aplicadas em dobro em caso de calamidade pública.
- A Lei nº 12.327 alterou a denominação do crime do art. 266 do Código Penal, acrescentando que a interrupção de serviço telemático ou de informação de utilidade pública, bem como impedir ou dificultar-lhe o restabelecimento também é crime.
- Essa interrupção ou impedimento pode ser realizada de várias formas (crime de forma livre), por exemplo, a destruição física de uma determinada rede. Mas também pode ser feita mediante um ataque virtual, o qual também está contemplado pela alteração legislativa.
- Portanto, hoje, no Brasil, é crime a conduta denominada **ataque de denegação de serviço (DOS/DDOS)**. O DOS (*denial of service*) não constitui geralmente uma invasão de sistema alvo, mas uma sobrecarga

de acessos que fazem com que o fluxo de dados da rede seja interrompido. É chamado de ataque de denegação de serviço difundido ou DDOS (*distributed denial of service*) quando o criminoso infunde por meio de seu computador (mestre) vulnerabilidades ou programas maliciosos em vários computadores (zumbis), fazendo com que contra a vontade ou mesmo sem que os usuários afetados percebam, acessem simultaneamente ou sequencialmente o serviço que pretende ser travado.

Equiparação do cartão de crédito e débito com documento particular

- A nova Lei também equiparou o cartão de crédito ou débito com o documento particular, transformando-os em objetos materiais do crime de falsidade documental.
- Para a configuração do crime basta que exista a inserção de dados impregnados na tarja magnética (parte juridicamente relevante do documento), que permite o acesso a sistemas bancários ou de crédito pertencentes a determinado correntista, não emitidos pela instituição correspondente.
- Todavia, somente a conduta de falsificar no todo ou em parte o cartão será considerada crime, o que não ocorre com a simples posse de um cartão clonado por quem não foi responsável pela falsificação.
- Se utilizado o cartão e alcançado o dano patrimonial, em regra, tratar-se-á de crime de furto qualificado pela fraude e a falsidade será absorvida.

Como visto, a Lei nº 12.737/2012, embora represente certo avanço ao tipificar crimes cibernéticos propriamente ditos, contém inúmeras deficiências e

Rua Riachuelo, 115 - 7º andar - sala 730 - São Paulo - CEP 01007-000 – tel. 3119-9922
caocrim@mp.sp.gov.br

confrontos com o sistema penal e processual penal vigente, o que deve merecer a atenção dos aplicadores.

Os crimes cibernéticos propriamente ditos são a porta de entrada para outras condutas criminosas, facilitando a utilização do computador como instrumento para cometer delitos.

O legislador não contemplou a invasão de sistemas, como os de *clouding computing*, optando por restringir o objeto material àquilo que denominou dispositivo informático, sem, contudo, defini-lo. Atividades de comercialização de *cracking codes* e de engenharia reversa de *software* também não foram objeto da norma.

Além das imperfeições na redação dos tipos, as penas cominadas na nova lei são ínfimas se considerada a potencial gravidade das condutas incriminadas, bastando dizer que um ataque de denegação de serviço pode colocar em risco vidas de uma população inteira.

Implicam, por outro lado, a competência do Juizado Especial Criminal, cujo procedimento sumaríssimo é incompatível com a complexidade da investigação e da produção da prova de crimes de alta tecnologia (perícia no dispositivo informático afetado, por exemplo).

Numa síntese, os tipos e penas da Lei nº 12.737/2012 não conseguem dar as respostas esperadas pela Sociedade para desestimular aqueles que abusam das facilidades tecnológicas.

Centro de Apoio Operacional Criminal

Para acessar a Lei nº 12.737/2012 clique aqui