

SOL

15-01-2010

Periodicidade: Semanal

Classe: Informação Geral

Âmbito: Nacional

Tiragem: 67140

Temática: Justiça

Dimensão: 235

Imagem: N/Cor

Página (s): 26/27



## (In)segurança e a nova 'lei

**T**EM-SE verificado um acréscimo das notícias sobre a (in)segurança de Sistemas Informáticos (SI). Os *hackers*, para além das empresas privadas, têm também na mira os organismos oficiais do Estado, utilizando diversas ferramentas de *malware* como Worms, Trojans, Rootkits e uma infinidade de vírus.

As entidades alvo destas intrusões normalmente não as divulgam, pela publicidade negativa que causam na opinião

**João Gonçalves de Assunção**  
Advogado

pública e porque levam a um incremento das tentativas de intrusão por outros *hackers*.

**E**STES actos nem sempre tiveram consequências a nível penal. A obsoleta lei 109/91 previa que o acesso ilegítimo a um SI era apenas punível se o *hacker* tivesse intenção de alcançar, para si ou

para outrem, um benefício ou vantagem ilegítimos.

Com a entrada em vigor da nova 'lei do cibercrime' (lei 109/2009), o mero acesso, ou tentativa de acesso a um SI, passou a ser criminalmente punível, incluindo também quem produzir, colocar à disposição de terceiros ou introduzir meios destinados a aceder a um SI. Atente-se que a lei explicita «...**quem ilegítimamente...**», exceptuando, obviamente, a criação deste tipo

## do cibercrime'

de programas para fins militares, de investigação ou outros, desde que a finalidade seja lícita.

**E**STE tipo de actuação pode cumular-se com outros crimes, como a interceptação da transmissões de dados ou a sabotagem informática, no caso de se entravar, impedir, interromper ou perturbar gravemente o funcionamento de um SI. E a pena, neste últi-

mo caso, poderá atingir 10 anos de prisão.

Entre as inovações introduzidas pela nova 'lei do cibercrime' destacam-se os diversos meios processuais para identificar os agentes destes crimes e obter as provas necessárias para os incriminar - permitindo-se, nomeadamente, que as entidades judiciárias ordenem a pesquisa, preservação e apreensão de documentos e e-mails, bem como a inter-

cepção de comunicações, à semelhança do que sucede com as escutas telefónicas. Em alguns casos excepcionais, permite-se mesmo que os órgãos de polícia criminal actuem sem prévia autorização de uma autoridade judiciária.

Existem, também, empresas nacionais privadas altamente especializadas no sector da informática forense que, verificadas certas condições, colaboram no senti-

do de recolher, examinar e relatar provas de crimes informáticos.

**P**IOR cenário revelam as conclusões do relatório *Tracking GhostNet* elaborado pela Universidade de Toronto e o relatório *A GhostNet em Portugal* da Trusted Technologies, que constata a infiltração de uma rede de espionagem electrónica - baseada na China - em diversos organismos

públicos do Estado português, entre os quais o Ministério da Justiça.

Neste tipo de casos, a lei portuguesa é obviamente inaplicável. Não existindo tratados internacionais com a China nesta matéria, como sucede, por exemplo, com a Convenção Europeia sobre o Cibercrime, resta o recurso à via diplomática para perseguir e punir os *hackers* localizados naquele país.