CISION

ID: 27076664

VidaEconómica

09-10-2009

Tiragem: 22400
País: Portugal
Period.: Semanal
Âmbito: Economia, Negócios e.

Pág: 36
Cores: Preto e Branco
Área: 28,18 x 28,84 cm²
Corte: 1 de 1

Segurança informática

CÉLIA CORREIA FRANÇA
Jurista da CTOC

No mundo de hoje é cada vez mais comum os negócios jurídicos concretizarem-se pela Internet, a consulta do extracto bancário online é prática corrente, pagar contas, fazer transferências bancárias, carregar o telemóvel, etc. As novas tecnologias permitem uma comodidade nunca antes vista, mas é preciso cautela no manuseamento da informação que se fornece.

Se a Internet veio acelerar muitos negócios, também abriu caminho a muitas burlas. Compete a cada usuário estar atento e prevenir-se porque existem informações básicas que pode e deve sempre obter. Por exemplo, na compra de um veículo automóvel pela Internet, assegure-se que o registo está efectivamente no nome do vendedor.

Outra prática comum é que muitas informações são concedidas de uma forma ingénua em redes sociais a pessoas estranhas que apenas se aproximam com intenção de burlar. Por isso é preciso estar atento e não prestar dados confidenciais de contas bancárias, que possam levar terceiros a ter acesso às mesmas contas.

Muitas vezes as pessoas usam, de forma negligente, a sua data de nascimento como password. É recomendável o uso de letras e números na medida em que esta técnica irá dificultar o acesso a um eventual burlão.

Está a tornar-se frequente os sites de relacionamento serem usados para fins comerciais e de verdadeiros negócios, sendo colocados links a circular entre os usuários e as comunidades existentes. A globalização potencia a multiplicação destes sites. A questão que se coloca é: quem fiscaliza esses negócios que proliferam como cogumelos?

A lei que regula estas questões diz respeito ao foro do direito internacional privado, em que terão de se estabelecer as devidas conexões entre os diversos intermediários que fazem parte do negócio assim como ter em conta o lugar onde é feito o mesmo. O objectivo é saber qual a lei aplicável ao caso concreto, para se aferir qual a autoridade que tem competência para aceitar determinada queixa.

Em Portugal existe um departamento especializado na Polícia Judiciária sobre esta matéria que fornece alguma informação que visa contribuir para o aumento de uma cultura de segurança informática.

De entre esses crimes, a SICIT (departamento responsável dentro da Polícia Judiciária) detém competência nacional para investigação da chamada criminalidade informática, a qual compreende a generalidade das infracções penais previstas e punidas pela Lei 109/91, de 17 de Agosto, designadamente: fraude informática, dano relativo a dados ou programas informáticos, sabotagem informática, acesso ilegítimo, intercepção ilegítima, reprodução ilegítima de programa protegido e de topografia, bem como as infracções penais previstas e punidas pela Lei 67/98, de 26 de Outubro, designadamente: não cumprimento de obrigações relativas a protecção de dados, acesso indevido, viciação ou destruição de dados pessoais, desobediência qualificada, violação do dever de sigilo.

Há vários tipos de crimes informáticos que a seguir elencamos:

"BBS's" – Significa a figura de prática irregular ou crime de quem afixa ou disponibiliza, no todo ou em parte, dados relativos a explosivos, números de cartões de crédito, descrição de formas de cometimento de crimes, software protegido por copyright, mesmo que este esteja comprimido por outros programas ou mesmo que seja disponibilizado por partes ou incompleto.

"Sniffing" – O crime de intercepção ilegítima pune com pena de prisão até três anos quem, seja de que forma for, interceptar a transmissão de informação.

"Hacking" - Termo geralmente empregue para se fazer referência à intrusão em sistemas informáticos. As actividades de "hacking" ou de "cracking" (acesso ilegítimo com intuito de destruição de dados), são, à face da Lei portuguesa, crime de acesso ilegítimo, e por isso punido com pena de prisão até um ano, agravado até três anos ou multa se o acesso for conseguido através de violação de regras de segurança.

Se com o acesso ilegítimo se tiver tomado conhecimento de segredo comercial ou industrial ou de dados confidenciais, protegidos por lei, ou obtiver benefício ou vantagem patrimonial de valor consideravelmente elevado, a pena será a de prisão de um a cinco anos. Cabem nestas punições a utilização sem autorização prévia de "default accounts" e de passwords que lhes não pertençam, como, por exemplo, usar as contas de acesso de terceiros para aceder à Internet. A pena é agravada até cinco anos se o valor da vantagem obtida for elevado ou se tomarem conhecimento de dados confidenciais protegidos por lei ou de segredos industriais ou comerciais. A simples tentativa de acesso ilegítimo é punível.

"Phreaking" - Para além de se aplicarem os mesmos princípios relativos às actividades de "blueboxing", a utilização de redes de comunicações com base na manipulação de centrais telefónicas acedidas sem autorização para o efeito constitui o crime de acesso ilegítimo.

"Blackboxing e "blueboxing" - Todas as formas de perturbação de telecomunicações, quer por injecção de frequências nas linhas telefónicas quer por ligar a estas dispositivos electrónicos cujo efeito, de entre outros, sejam o impedimento total ou a diminuição da taxação devida à operadora de telecomunicações, constitui o crime de burla nas comunicações, punido pelo artigo 221, n.º 2, do Código Penal até 3 anos de prisão.

"NUI's" e "VUI's" - A utilização indevida dos chamados NUI's e VUI's para acesso a redes x.25, constituem crime de acesso ilegítimo, punido pela Lei da Criminalidade Informática.

"Cracking" - A descompilação de programas é prevista e punida pelo artigo 7.º do Decreto-Lei nº 252/94 de 20 de Outubro (Protecção Jurídica dos Programas de Computador) e pelo artigo 9.º da Lei da Criminalidade Informática (Lei nº 109/91 de 17 de Agosto). Esta legislação abrange os programas residentes em memória, (TSR's), que permitem a utilização de software utilitário e de jogos violando assim os direitos de autor.

"Carding" - Todas as formas de manipulação de dados ou de elementos de identificação quer na face quer contidos em bandas magnéticas de cartões de crédito, de débito ou de telecomunicações, bem como a implantação de dados ou de elementos de identificação noutros suportes técnicos, constituem um crime de falsificação, punido com pena de prisão até 3 anos. A utilização em "mail orders" de elementos de identificação ou de dados bancários de terceiros constitui um crime de burla, punido com a pena de prisão até 3 anos e é agravada se o montante em causa for elevado ou se mantiverem essa conduta mais que uma vez. O abuso da possibilidade conferida pela posse de cartão de crédito ou de garantia, mesmo que só pela forma tentada, é punível com pena de prisão até 3 anos, podendo ser agravada até 5 anos ou de 2 a 8 anos, caso o valor seja elevado ou consideravelmente elevado.

"Spam" - Termo empregue para referir a emissão simultânea de uma mensagem de e-mail para vários utilizadores ao mesmo tempo tem, regra geral, as seguintes características:

1. não é solicitado pelo receptor;
2. a identificação do remetente é falsa;
3. é usada a máquina servidora de correio electrónico de uma vítima, seja de um ISP ou de uma entidade pública ou privada. Em Portugal é este terceiro ponto que confere a tipificação criminosa a quem envia o "spam", uma vez que, quem naqueles termos usar um servidor de e-mail de terceiro pode ser acusado da prática do crime de acesso ilegítimo. Pode ainda coexistir o crime de falsificação se a identificação de endereço falsificada referida no ponto "2." for a de alguém em concreto. Se o intuito do "spam" é interferir no normal funcionamento de um sistema informático, poderá ser considerado crime de sabotagem informática, punido com pena de prisão de cinco anos, ou com pena de multa.

Abuso sexual de crianças – O art. 172.º do Código Penal pune com prisão até três anos quem exibir, ceder a qualquer título ou por qualquer meio, fotografias, filmes ou gravações pornográficas de menores de 14 anos. Este artigo abrange a posse, a mera troca e a afixação de imagens desta natureza nos "IRC's" e nos Newsgroups. A venda destas imagens constitui uma agravante da pena de prisão de seis meses a cinco anos.

Uso e reprodução ilegítima de software - A cópia e a distribuição a terceiros de programas informáticos protegidos por lei - vulgo "copyright" - são proibidos e punidos por lei até três anos de prisão.

A tentativa de cópia ou de distribuição é também punível. São abrangidos por esta norma a distribuição total ou parcial de programas informáticos, mesmo que comprimidos por outros programas, em newsgroups, "IRC's", sites da internet, ftp's, etc. O uso ilegítimo de programas de computador é punido pelo Código de Direitos de Autor e Direitos Conexos, com prisão até três anos e multa.

Estar alerta relativamente a este vasto naipe de questões é fundamental para a boa condução dos negócios na web.