

IMPACTOS DA TECNOLOGIA DIGITAL NO DIREITO PENAL

Erick Nilson Souto (*)

CRIMES DE INFORMÁTICA

Conceito – Pelo caráter dogmático do Direito Penal, o conceito de crime por si só é essencialmente jurídico. Neste aspecto, os “crimes de informática” são os realizados com o suporte físico de computadores e/ou equipamentos eletronicamente processados. Pode ser definido pelo bem jurídico protegido ou pelo meio utilizado para sua consumação, entendido como toda ação típica, antijurídica culpável contra, ou pela utilização de equipamentos de processamento eletrônico de dados ou sua transmissão.

Atendendo-se ao princípio penal básico "*nullum crimen nulla poena sine lege*", ainda pode-se ter como “crime eletrônico”, “digital”, “de informática”, os delitos descritos em lei específica que tratam sobre meios eletrônicos digitais ou bens jurídicos digitais. É a utilização de sistemas e equipamentos de informática para atentar contra um bem ou interesse juridicamente protegido, qualquer que seja este bem jurídico, de ordem econômica, referente à liberdade individual, à privacidade, à honra, ao patrimônio público ou privado, etc... .

Há que se lembrar sempre que, diante da gravidade do bem jurídico que se procura restringir pela atuação penal do Estado, a liberdade, em última instância, o sujeito ativo do delito informático só é passível de punição se a lei especificar exatamente a matéria de suas proibições, os fatos que são proibidos sob ameaça de sanção penal, ou seja, o que é considerado crime com o uso de computadores ou equipamentos eletrônicos, ou contra eles, quer seja nos considerados **crimes de informática puros**, como atos de vandalismos contra a integridade física do sistema, acesso desautorizado ou indevido a dados e sistemas computacionais, ou nos **crimes de informática mistos**, em que o sistema de informática é ferramenta imprescindível à sua consumação, apesar do bem juridicamente protegido ser diverso de bem eletrônico, de informática, computacional.

Sumarizando, o criminoso virtual, **o sujeito ativo nos crimes de informática**, é aquele que utiliza meios eletrônicos para consecução da atividade ilícita, desde que esta seja plenamente tipificada, *mutatis mutandis*, **sujeito passivo no caso de crime digital, é o detentor de direitos violados através de meios digitais, eletrônicos.**

DA INTERCEPTAÇÃO TELEMÁTICA

É notória a existência do programa “Carnívoro” do FBI, que alguns maus profissionais de provedores (motivados por detetives ou competidores de empresas rivais) espionam seus clientes e certas empresas “monitorando” (ilegalmente) todas as atividades pela Internet. Estas práticas condenáveis são o exercício negro do conhecimento digital em benefício de interesses escusos. Em vários casos o tráfego de informações pode ser interceptado por computadores que compartilham a mesma LAN (rede local de computadores) ou a mesma rede sem fio. Interceptação de dados é um perigo eminente que empresas e usuários finais devem se preocupar.

Como pode ser feita a interceptação de dados? A Internet é construída em um sistema hierárquico, como na figura anexa, temos, de uma forma simplificada que como os usuários finais são conectados ao Provedor, através de cabos ou modems, que são conectados à provedores muito maiores, que são ligados entre si, a inúmeras possibilidades de interceptação são feitas ligando, física ou logicamente, outros computadores ou aparelhos eletrônicos no ponto onde se pretende bisbilhotar.

Existente ainda ligados à Internet, computadores especiais para encontrar o caminho para o envio dos pacotes de dados através da rede, são os roteadores, que examinam cada pacote que passa através dela e transferem estes para o próximo roteador até que a informação encontre seu destino. Por causa destes equipamentos é que o caminho entre o computador originário e o final é chamado rota. Quanto maior é essa rota, maior a possibilidade de interceptação de informações, sendo que facilmente pode-se fazer nova rota, duplicando o caminho da informação, para se remeter informações a mais de um destinatário, no caso, a outro destinatário não autorizado. (Alguns exemplos na figura anexa)

SEGURANÇA ELETRÔNICA COMO PREVENÇÃO AO CRIME VIRTUAL

Várias são as maneiras para se impedir a interceptação telemática, todas válidas e, infelizmente, passíveis de quebra, como arquivos protegidos por senhas, programas de firewall's, programas de criptografia, link de rede dedicado, etc..., mas sempre tendo em mente que quanto mais acesso se tem à Internet, mais vulnerável se está, porque a possibilidade de acesso é uma via de mão dupla, para se conectar à rede, tem-se que abrir portas e permitir protocolos computacionais que muitas vezes são o convite para a entrada de pessoas não autorizadas no sistema do usuário da Internet.

No site do aluno do CENSI ou no endereço <http://www.nbso.nic.br/docs/cartilha/> é possível se obter uma cartilha com dicas de segurança na Internet.

APLICABILIDADE DA LEGISLAÇÃO PENAL VIGENTE

Quanto à prevenção legal aos crimes de informática, a muito se vem buscando suas tipificações, como na Lei 9.296/96, que trata da interceptação telemática, ou interceptação de dados, mas por mais que se tente tipificar todas as situações possíveis, a verdade é que a tecnologia de informática avança muito mais rápido, criando situações não acobertadas pela legislação penal, de caráter de legalidade rígido, o que tem gerado decisões judiciais por analogia, APLICAÇÃO ANALÓGICA IMPOSSÍVEL, sob pena de condenação de inocentes.

(*) Erick Nilson Souto é Advogado em Belo Horizonte/MG, Bacharel em Ciências da Computação e Direito pela PUCMINAS e Professor de Direito Digital no Centro de Ensino Superior de Itabira/MG