CRIMINALIDADE INFORMÁTICA

por ***Carlos Miguel Filipe Branco***

Sumário. A criminalidade informática é algo de novo para as autoridades judiciais de todo o planeta. Toda a legislação existente até ao momento não contemplava este tipo de crimes, e devido ao seu surgimento extremamente rápido foi necessário fazer uma adaptação também extremamente rápida. Será que já estamos mesmo preparados para combater este tipo de crimes?

Palavras chave. Comunicação, encriptação, internet.

1. Introdução

Com o aparecimento das novas tecnologias surgiram também alguns problemas legais associados. A rápida evolução destas novas tecnologias levou à existência de "vazios legais" e à difícil definição de crime informático. A década passada ficou marcada pelo boom das telecomunicações e pelo surgimento de um ciberespaço global frequentado por mais e mais pessoas dos quatro cantos do mundo, tornam-se necessárias análises e reflexões sobre as potencialidades das novas tecnologias ao nosso dispor. Mas convém não esquecer também os riscos que toda esta evolução nos traz.

A falta de Maios por parte das autoridades e a dificuldade de detecção deste tipo de crimes faz com que a sua detecção seja extremamente complicada.

Mas afinal o que é um crime informático? Quais os mecanismos de combate a este tipo de crime? E como obter os meios de prova?

2. Criminalidade informática

Para a maior parte das pessoas o crime informático parece uma prática muito distante e algo muito obscuro que não sabem definir muito bem. A justiça tem tentado definir de forma objectiva este tipo de crime, uns dizem que é a "realização de uma acção que, reunindo as características que delimitam o conceito de crime, seja levada a cabo utilizando um meio informático, seja hardware ou software". Outros dizem apenas que se trata de "qualquer acto ilegal onde o conhecimento de tecnologia da Informática é essencial para a sua execução, investigação e acusação".

Estas duas definições mostram a dificuldade de um consenso na definição de crime informático.

Outra grande dificuldade encontrada pelas autoridades é a inexistência de fronteiras, ou seja, com a grande divulgação da Internet a criminalidade informática é um crime sem fronteiras. Assim é necessário encontrar soluções de cooperação internacional. Neste tipo de crime podemos ter o criminoso a milhares de quilómetros de distância num país distante a atacar a página web da nossa empresa.

Esta internacionalização dos crimes informáticos é um grande problema para o sistema judicial, dado que existe um forte senso de territorialidade nas legislações penais nacionais.

Até aos nosso dias a justiça tem tentado acompanhar a evolução tecnológica e com o aparecimentos de novos conceitos que fazem agora parte do nosso dia-a-dia podemos dizer que a justiça tem andado a reboque desta enorme explosão tecnológica.

Para evitar os ataques maliciosos, as empresas têm recorrido a várias formas de encriptação dos dados. Começam a surgir nos dias de hoje tecnologias de encriptação capazes de num formato eficiente proporcionar troca de mensagens segura na Internet. A aplicação destas técnicas de encriptação nas comunicações pode evitar que técnicas como o sniffing (perscrutar todos os pacotes de uma ciomunicação, normalmente em busca de palavras-chave e de números de cartões de crédito) forneçam informações privilegiadas ao pirata informático e, deste modo tornar mais seguras as transacções efectuadas, com grandes benefícios em áreas como o comércio electrónico. No reverso da medalha está o uso de técnicas de encriptação por parte dos próprios criminosos. Estes poderão assim beneficiar de privacidade no levar a cabo das suas acções e desse modo tornar ineficazes as investigações criminais.

O futuro neste assunto joga-se assim em dois campos distintos: por um lado no rever das situações de excepção à legislação de sigilo nas telecomunicações e por outro no tomar de uma decisão acerca da limitação ou não no uso de técnicas de encriptação. O processo desenrola-se na área legislativa, na análise dos direitos do cidadão, uma vez que no campo tecnológico já todas as opções são correntemente possíveis.

Quando se fala de criminalidade informática é necessário falar nos principais interveniente, os *Hackers* ou piratas informáticos. Existe uma camada

de "cybercriminosos" que, pela sua longa e activa permanência no meio, merecem um destaque especial neste ensaio. De facto, estes "criminosos" existiam mesmo antes de a Internet se popularizar da forma como fez nos últimos anos, estabelecendo as suas actividades em BBSs locais, redes X.25, loops, etc...
Apesar do termo hacker ter sido usado desde os anos 50 para descrever programadores "free-lancer" e de tecnologia de ponta, essa conotação tem caído em desuso, dando lugar a uma outra que tem sido popularizada pelos media: *hacker* é aquele que obtém acesso não autorizado a um sistema informático.
Apesar deste tipo de criminoso provocar graves danos nos sistemas informáticos de grandes empresas, podendo em alguns casos poder levar à falência (devido à forte dependência das novas tecnologias). Só recentemente é que estes criminosos foram encarados como tal.
No nosso pais ainda não é significativo o número de casos detectados. Sendo que quando se fala de criminalidade informática a maior parte das pessoas pensa que apenas se trata da vulgar cópia de software.

Devido à nossa grande dependência das novas tecnologias temos cada vez mais que garantir a integridade dos dados e proteger os equipamentos contra intrusões. Isto deve ser feito para aumentar o grau de confiança neste tipo de sistemas. E quando todas as medidas de prevenção não funcionam a justiça deve estar preparada para lidar com este tipo de criminosos.

3. Conclusões

Pretendeu-se que este trabalho viesse clarificar a ideia errada que muitas pessoas têm de criminalidade informática e tentar esclarecer o contexto do seu aparecimento e quais os seus intervenientes e motivações. A criminalidade informática existe e a justiça deve criar todos os méis para a combater. Um crescimento deste tipo de crime pode levar a uma total perda de confiança nos sistemas informáticos existentes e isso pode ter consequências gravíssimas numa sociedade totalmente “técno-dependente”

Referências

1. Ministério da Justiça, http://www.min-jus.

2. Pagina com dicas para hackers
http://www.hackershomepage.com/

3. Novas medidas do governo dos estado unidos para combater os hackers,
http://www.computerweekly.com/articles/article.asp?liArticleID=131748&liFlavourID=1&sp=1