O Mundo em Português Nº10
Julho 2000

Cibercrime: A Ameaça e Algumas Respostas

João Labescat

A expansão da Internet abriu o caminho para um novo tipo de crimes, para os quais as empresas e os Estados não estão ainda preparados. O G8, a União Europeia e os "gigantes" da alta tecnologia começam agora a trabalhar em instrumentos – policiais, legais, técnicos – para combater a ameaça do cibercrime.

Peritos de segurança informática dos países mais industrializados, reunidos no mês de Maio em Paris, lançaram um sério "aviso à navegação" apelando a uma resposta global no combate ao cibercrime e ao terrorismo informático.

Muito recentemente a Internet foi objecto de ataques diferenciados cuja natureza exige uma resposta global. Foi o caso do vírus destrutivo "ILOVEYOU", que poderá ter causado perto de uma dezena de milhões de dólares de prejuízos em todo o mundo e do assalto conjugado aos principais web sites da rede, Yahoo, eBay, Amazon.com, entre outros.

Já não se trata apenas da utilização pelo crime internacional da rede de computadores para a prática de actos ilícitos – como fazem com qualquer outro mecanismo tecnológico — mas, mais do que isso, procura-se afectar o comércio internacional, a actividade financeira e a acção de várias agências e departamentos governamentais.

Sem dúvida que o desenvolvimento da rede e das telecomunicações e a World Wide Web criaram novos portais para o fortalecimento da actividade económica mundial, onde começa a pesar significativamente a nova economia, ligada à alta tecnologia. Mas estes portais, dada a sua estrutura aberta, livre e global, deram à criminalidade organizada uma nova plataforma para as suas relações e para a sua actividade criminosa.

Na comunidade virtual nasceram novos tipos de crime directamente associados ao funcionamento da rede. Assalto a redes e a computadores para alterar ou aceder a dados, acesso a palavras-chave, espionagem electrónica industrial e política, usurpação de identidade de pessoas e de instituições, pirataria de software, destruição massiva de dados e quebra de confidencialidade do correio electrónico, "bombas" electrónicas que fazem "explodir" sistemas e que os deixam inacessíveis, vigilância dos passos electrónicos dos cidadãos ou das empresas, violação de cartões de crédito, fraude electrónica, constituem um catálogo impressionante de acções e métodos a necessitar de uma resposta.

A verdade é que os agentes do crime estão a mudar. Já não é apenas o jovem especialista "hacker" que, isolado no seu computador, consegue entrar em sistemas alegadamente seguros, compra online com um número de cartão de crédito roubado ou estabelece ligações telefónicas para todo o mundo sem pagar. São poderosos interesses organizados em várias partes do globo, com redes tentaculares diversificadas, que passaram a ter na rede uma ponte de transporte fundamental para os seus negócios ilícitos e a fazer dela mais uma fonte de lucros ilegais fabulosos. A nova economia tem também o seu lado obscuro e negro.

As empresas e os Estados não estavam (nem estão ainda) preparados para responder à natureza e aos meios utilizados pela nova criminalidade e pelo ciberterrorismo. A prevenção criminal era (e é) a excepção.

Escasseiam competências a nível das estruturas estaduais, as polícias estão ainda mal preparadas para combater o fenómeno, a formação específica é coisa rara, a ligação entre a indústria e as organizações de combate ao crime era ténue e pouco eficaz. Os números da debilidade são expressivos. A título de exemplo, estima-se que apenas 2% dos polícias americanos têm treino e formação na criminalidade informática.
Mas mais importante do que a debilidade das estruturas nacionais de ciberpolícia, era patente a inexistência de cooperação policial internacional, sabendo-se que este tipo de crimes envolve geralmente vários países em diversas zonas do globo. Os investigadores não estão devidamente treinados e não têm o conhecimento integral dos computadores e da rede, os mecanismos de fraude utilizados são cada vez mais complexos, envolvendo recursos que a maior parte dos Estados não possui e a cooperação policial é lenta se comparada com a rapidez e a sofisticação do crime cibernético.

Também o direito (nacional e internacional) é inadequado e não tem em consideração esta realidade e, mesmo nos casos em que existe previsão legal, a sua aplicação é difícil, lenta e pouco eficaz.

Os países mais industrializados e o mercado

Procurando responder a este desafio, o Grupo dos 8 países mais industrializados (G8), que reúne a Alemanha, os EUA, a Grã-Bretanha, o Japão, a França, o Canadá, a Itália e a Rússia, definiram em Dezembro de 1997 um conjunto de 10 princípios e um plano de acção de 10 pontos para o combate transnacional à acção criminosa organizada que utiliza as redes de comunicação, tendo criado um comité de peritos especializado no crime de alta tecnologia.

Entre as medidas preconizadas encontram-se as que respeitam à formação das polícias, à criação de standards tecnológicos que permitam prevenir e detectar a utilização abusiva da rede, a harmonização da análise forense electrónica, a assistência mútua em matéria de acesso e troca de provas nos casos em que estão envolvidos vários países, a permissão legal de acesso célere aos sistemas e aos dados por parte das polícias, o trabalho conjunto com a indústria de forma a preservar provas.
O Plano de Acção do G8 teve vários desenvolvimentos e, em 1999, estes países acordaram em criar serviços 24/7 (funcionam 24 horas por dia, os sete dias da semana), que permitem às autoridades nacionais pedir apoio permanente e encontrar formas de entreajuda que detectem eventuais crimes. Aos países do G8 juntaram-se nesta acção, a Suécia, a Finlândia, a Dinamarca e o Brasil.

Igualmente os membros da "Aliança Internet", que reúne algumas da maiores empresas de telecomunicações e de informática (America Online, IBM, Microsoft, Deutsche Telecom, Prodigy, Bell Atlantic),reconhecendo embora as dificuldades que existem na aplicação dos mecanismos legais existentes e o seu posicionamento estratégico no mercado, consideram que a cooperação da indústria com as polícias e as agências e departamentos do governo deve ter apenas um carácter voluntário.

A posição da União Europeia

O Conselho Europeu de Amsterdão de Junho de 1997 aprovou um plano de acção do grupo de alto nível contra a criminalidade organizada, do qual constam propostas de reforço da luta contra o crime de alta tecnologia e tendo adoptado

mais tarde, em Dezembro de 1998, um documento estratégico denominado "Aspectos da estratégia da União contra o crime de alta tecnologia". Não sendo particularmente inovadores quanto ao conteúdo, não deixam de conter importantes linhas de acção para os Estados.

A evolução recente na União Europeia mostra a relevância destas matérias que passaram a constar, de forma permanente, das agendas dos Conselhos de Ministros da Justiça e da Administração Interna.

O Tratado de Amsterdão (TA) constituiu um passo extremamente importante na estratégia da União. Os mecanismos consagrados no Tratado relativos à cooperação policial e judicial (artigos 30º e 31º do TA) e à harmonização legislativa vão permitir a actuação concreta num novo ambiente comum facilitador de acções conjugadas.

A criação da Europol – enquanto serviço europeu de polícia – e a sua habilitação para apoiar e incentivar a coordenação e execução de acções específicas de investigação, incluindo actividades operacionais de equipas conjuntas (em que participam funcionários da Europol pondo ao dispor recursos comuns quanto à criminalizada organizada) é um sinal claro que também na União a situação tende a inverter-se. Resta saber até onde irão estas medidas e qual será a eficácia das acções. Mas por um lado se teria que começar e a verdade é que temos hoje um quadro mais favorável e dinâmico para o combate ao crime informático. A iniciativa conjunta, desenvolvida com a cooperação de várias polícias, de combate à pornografia infantil, incluindo a que circula na rede, foi um bom exemplo do tipo de acções concertadas que têm êxito prático e que são de importância vital para o estabelecimento da confiança dos cidadãos nas instituições europeias.

A União, que tem acompanhado os trabalhos do Conselho da Europa neste domínio aprovou, em 27 de Maio de 1999, uma posição comum relativa ao projecto de Convenção (do Conselho da Europa) em matéria de cibercrime.
A União sublinha alguns dos aspectos estratégicos que aquela Convenção deve consagrar:
• a introdução de disposições que facilitem as investigações e o exercício da acção penal relativamente às infracções relacionadas com os sistemas e dados informáticos;
• o completar do direito penal substantivo de forma a abranger os crimes no domínio da confidencialidade, integridade, fraude e falsificação informática, bem como a pornografia infantil;
• o princípio da cooperação internacional, incluindo o auxílio judiciário mútuo;
• a criação de pontos de contacto nacionais que funcionam em permanência (aqui recuperando a iniciativa do G8 dos 24/7, gabinetes que funcionam 24 horas por dia, os 7 dias da semana);
• a introdução de disposições legais que permitam às partes contratantes uma busca rápida dos dados armazenados no seu próprio território, aquando de investigação de crimes graves e mesmo buscas transfronteiriças em casos particularmente graves e em situações de emergência.

Estas linhas estratégicas vieram a ter desenvolvimento muito recente, designadamente na decisão do Conselho de 29 de Maio relativa à pornografia infantil. Entre algumas das medidas salienta-se a informação à Europol dos casos de suspeita de pornografia infantil, a sua eliminação da Internet e a cooperação com o sector industrial. Particularmente importante é o desenvolvimento da ideia de manutenção de um diálogo construtivo com o sector industrial, a colaboração na troca de experiências e o incentivo à produção de filtros e outros meios técnicos destinados a impedir e a detectar a divulgação de material de pornografia infantil.

A Proposta do Conselho da Europa

O grupo de peritos do Conselho da Europa pôs em debate público em finais de Abril deste ano um Projecto de Convenção sobre Cibercrime. No caso de vir a ser adoptada, a Convenção será o primeiro Tratado internacional nesta matéria.

Pretende-se definir grandes princípios, facilitar a investigação e consolidar a cooperação internacional. Prevê-se uma versão consolidada do texto da Convenção em Dezembro de 2000, de forma a poder ser aberta à adopção pelos Estados durante o ano 2001.

O debate a travar em redor desta Convenção corre o risco de ser limitado. Esta matéria é demasiado importante. Os cidadãos e as suas associações devem participar activamente e contribuir para as soluções a adoptar que podem não ser, nalguns aspectos, pacíficas. É o caso da conservação de provas sem limite, da intercepção das telecomunicações, dos perigos para a privacidade e para o exercício da liberdade de opinião e expressão. A vulnerabilidade da rede e as formas de combate ao crime não podem, nem devem pôr em causa direitos, liberdades e garantias. A pessoa tem que manter o seu espaço de liberdade. O contributo dos cibernautas jovens é crucial no futuro próximo. As medidas de combate ao cibercrime não podem esquecer a formação (desde a escola) e a informação. Só de forma articulada é possível combater eficazmente o cibercrime. Os próximos anos dirão dos êxitos, dos limites e dos fracassos das medidas...