

Criminalidade Global e insegurança Local

Um caso

Algumas questões

Maria José Morgado

Iniciou-se no passado mês de Abril o julgamento dum complexo caso de crime de associação criminosa para a prática de burlas de valores muito elevados através da prestação de serviços na Internet, segundo a Acusação deduzida pelo MP.

Não quero, nem posso, nem a minha intervenção pode ser interpretada nesse sentido, referir o caso em sede de apreciação das provas ou das culpas. Nada disso. Apenas, no que é possível de considerar externamente ao julgamento: numa análise criminológica, as características visíveis, dum realidade paradigmática de eventual criminalidade global e insegurança local. Diria mais- um caso extremo de insegurança local- a insegurança no interior do lar. PORQUÊ?

Uma operação policial de buscas e detenções, efectuada pela PJ, na sequência de centenas de queixas dos utilizadores das linhas telefónicas da Portugal Telecom veio revelar indícios fortes, da existência dum eventual fraude que terá rendido milhões aos seus autores, desencadeada com o auxílio dum programa informático. Esta operação foi de extrema importância e envergadura, uma vez que terá posto termo à possibilidade de continuação de causar prejuízos a utilizadores desprotegidos da Internet.

Descobriu-se então nesse dia, a existência de uma organização especial sediada em 2 andares com 400 m², num prédio do centro de Lisboa, que serviam de base de operações a uma empresa que acabaria Acusada da maior fraude de telefones até hoje praticada em Portugal. Foram apreendidos, por força dessa acção cerca de 200 mil contos de material informático, e detidos os principais responsáveis pela fraude- 1 holandês, 1 Espanhol, 1 Eslavo, e 1 Português.

As buscas realizadas foram decisivas para a prova pericial da existência do DIALER, um programa informático malicioso, cujo funcionamento permitia a transferência dissimulada, das ligações de quem acedia a determinados sitios da Internet, para chamadas de

valor acrescentado, fazendo disparar as contas de milhares de assinantes. A empresa dona do programa, utilizava sites eróticos como chamariz para os incautos, tendo-se constatado através das buscas na sede indicada, a existência de um estúdio, com vários “décors” onde eram emitidas imagens de sexo ao vivo, 24 H por dia.

Esta empresa esteve credenciada pelo ICP (Instituto de Telecomunicações de Portugal) até Outubro de 2001 (data em que lhe foi revogada a licença); tinha contrato com a PT, que lhe pagava antecipadamente a quase totalidade das chamadas, após dedução da comissão.

Foi a primeira vez que uma força policial, em Portugal, desmantelou uma empresa de telecomunicações ligada aos negócios eróticos, com ligações internacionais e de fins indiciariamente ilícitos, segundo os termos da Acusação agora em Julgamento.

Este caso, torna-se um importante quadro de reflexão sobre um novo campo de problemas no Direito Penal. Permitir-nos-à colocar a seguinte questão relacionada com o tema da nossa exposição- até que ponto o Direito Penal tradicional está preparado para fazer face aos novos riscos destas condutas? Porque falamos de condutas empreendidas através de meios sofisticados, com recurso às novas tecnologias de informação, que pela sua dimensão e agressividade colocam em risco bens colectivos e abstractos, como a paz social, a integridade das linhas telefónicas, mas que também atingem bens concretos e tradicionais como o património individual. E falamos de condutas, através das quais, neste ou noutros casos, o crime pode desenvolver-se silenciosamente, por caminhos que atravessam o mundo e acabam no interior das nossas casas.

1. SOBRE OS FACTOS E OS PRESSUPOSTOS DA PUNIÇÃO

Contra os arguidos/pessoas singulares enquanto sócios ou gerentes da de determinada empresa, foi deduzida Acusação pelo MP pelos crimes de **Burla informática, Associação Criminosa e Branqueamento de Capitais.**

Como surgiu esta Acusação, e em que consistiram estas condutas?

O caso teve origem em centenas de denúncias , a partir de Fevereiro de 2001, dando conta de uma eventual burla praticada através da Internet, e que de um momento para o outro assumiu proporções gigantescas.

O que acontecia? Os utilizadores acediam via modem à INTERNET através dum **ISP**. Durante o acesso à Internet e a determinados sites conotados com a empresa, no próprio computador do utente, produziam-se modificações no tipo de acesso e de taxação à Internet por valores de chamadas de valor acrescentado, que os utilizadores não reconheciam ter realizado. Estas modificações, desconhecidas dos utilizadores, só eram possíveis com a intervenção dum pequeno programa informático- o **DIALER**.

O utente normal não notava, nem verificava qualquer alteração do tipo de acesso à Internet que efectuava, desconhecendo se estava a ser taxado a valores SVA¹.

Em que consistia o **DIALER**, enquanto estratagema fraudulento? É possível que serviços normais de Internet se possam transformar em incontroláveis e invisíveis instrumentos da prática de **crimes contra o património**? E não só, porque dada a sua enorme dimensão e facilidade de expansão, adquirem também a **natureza de crimes contra a paz pública**, provocando o conseqüente alarme social.

O **DIALER** actuava através do aliciamento do utentes que visitassem os sites www.loveball.com e www.sexoao.vivogratis.com.

Em ambos os sites aos utentes era indicada a opção de instalação de um programa informático denominado “Loveball.EXE”; a palavra GRÁTIS aparece como nome deste ficheiro, de modo a ser confundida com o programa “gratis EXE”. A instalação maliciosa deste pequeno programa informático obrigava a estabelecer uma ligação telefónica automática--- sem a intervenção da vontade do utilizador, sem o seu conhecimento, para dois números, qualquer um dos quais pertencente à operadora em causa,cuja taxação ascendia a 659\$00/minuto, 39.540\$00 H.

O **DIALER** , um software construído por programadores informáticos, com o fim específico de ser usado em Portugal tinha as seguintes características, segundo a investigação feita pela Unidade de combate ao crime Informático da DCICCEF /PJ:

- ordenar ao modem a execução de uma ligação dissimulada, automática para o número de SVA pertencente à Alcazar-Telecom;

¹ À data o baramento das chamadas aos SVA para serviços telefónicos audiotexto, não tinha efeito para chamadas via internet

- e provocar deste modo o acesso remoto a outro sistema informático em <http://pt.loveball.com>, mediante autenticação da password 003 e username 003; aqui a utilização é paga como sendo um serviço de audiotexto; e os utentes passam a ser membros dos sites sem o saberem, lavrando em erro sobre o custo que estavam a suportar pelo acesso à Internet.

- Entretanto, é de notar que os utentes passavam a ser membros dos sites pagos, em virtude de após o “download”, à entrada lhes ser atribuído logo uma “password” e um “username”. Porquê? Para não haver necessidade de recurso a cartão de crédito ou a transferência bancária, porque a Alcazar também era beneficiária dos lucros da empresa de SVA, cujas chamadas são comprovadas através das facturas da PT; a PT por sua vez, procede ao pagamento da percentagem devida às operadoras, imediatamente, descontada a sua comissão.

- Em suma, o DIALER é um programa que uma vez em funcionamento, transferia as ligações de quem acedia a determinados sítios em chamadas de valor acrescentado, o que fez disparar as contas telefónicas de milhares de assinantes. Aparentemente, mesmo depois de desligados os computadores, a chamada continuava a ser cobrada.

O **DIALER**, segundo a investigação da SICIT demonstrou, é assim um programa poderoso e altamente moldável, maleável consoante as necessidades; quando activado ,desliga a ligação normal, para a substituir por outra, após ter reconfigurado o computador pessoal dos queixosos. Mais, o acesso à Internet ,efectuado através do DIALER permite navegar por outros sites (alojados noutros servidores), aos utentes que por ali acedem, passam primeiro pela estrutura da rede informática fornecida pela fornecedora do serviço, sem se aperceberem dessa transição, com a taxação elevada que se menciona.

Ou seja, o Dialer será o autor dum estranho assalto. Mas se o Dialer tem que ser investigado e tem que ser julgado, e não corresponde a nenhuma identidade física singular e colectiva, então nós temo novos problemas no direito e no processo penal. E são problemas originados por uma criminalidade inovadora, sofisticada que parte de realidades novas: as novas tecnologias de informação, a globalização, os paraísos fiscais, como veremos.²

A execução do DIALER e as suas consequências:

2

A execução deste programa tinha como resultado e primeiro efeito desligar a ligação ao ISP escolhido pelo utente para acesso à NET, e em seguida, sem o conhecimento do utente, ordenar ao modem a marcação de determinado número de SVA personalizado (como foi comprovado pelo autos de exame directo e facturações detalhadas enviadas aos queixosos e utentes da PT). Tal mecanismo foi descoberto pelo estudo e análise do investigador da PJ que teve a seu cargo a investigação, e posteriormente confirmado através das buscas efectuadas em Dezembro de 2001 (documentos e software apreendidos na sede da Alcazar).

Sobre a empresa utilizadora , no caso que à nossa reflexão importa: resultou indiciado que esta empresa licenciada como prestadora de serviços de Audiotexto, estava a criar um erro ou engano nos utentes da Internet, a fim de incrementar tráfego de telecomunicações e o consequente enriquecimento ilegítimo em quantias avultadas, com a concepção e aplicação do programa indicado.

Quanto aos factos: temos a organização duma empresa ,licenciada no mercado de audiotexto, cuja suposta finalidade se dirigia à prática de fraudes através do meio Internet--- ou seja, com a utilização de um programa informático malicioso, a empresa obtinha em seu proveito indevido, e com o prejuízo de milhares de queixosos, lucros fabulosos.

O erro ou engano é produzido num meio imaterial, por pessoas que agem através da Internet, sem nenhum contacto pessoal com as vítimas, e que no entanto “entram na casa de cada um “, originando consequências e insegurança porventura superiores às dos assaltos de rua, ou de uma burla tradicional. Uma vez que a Internet aumenta o grau de exposição e de passividade das vítimas. Note-se que a vítima só tem consciência do “ataque” muito mais tarde- quando recebe a conta do telefone, ou seja quando tudo está consumado. O que representa um grau de danosidade novo, associado à volatilidade das condutas danosas, praticadas a uma escala internacional.

Vejamos que neste caso, o iter criminis não é representado pela intervenção directa duma pessoa junto doutra, a quem se provoca um estado de erro, mas sim por o autor do crime produzir o dano mediante a interferência dum sistema informático. O que comporta novos problemas de incriminação, quanto ao bem jurídico protegido, e novos problemas de recolha da prova.

Quanto ao bem jurídico protegido, considerando ainda a previsão do art. 221 n.º 2 do CP³, a burla nas telecomunicações integra um crime de dano, cuja consumação depende não só da efectiva ocorrência de um prejuízo patrimonial como também do dano para a integridade do serviço de telecomunicações. Ou seja, trata-se da protecção dum bem jurídico criminal misto: o património individual, e o património abstracto, colectivo, das telecomunicações, enquanto meio de comunicação.

Esta conjugação de tutela de bens abstractos de interesse social e de bens patrimoniais de interesse individual, consiste porventura no traço mais inquietante dum direito penal do futuro.

2. O CARACTER INTERNACIONAL E NACIONAL DOS CRIMES

A ORIGEM DA EMPRESA

A empresa referida teve origem numa outra, a empresa-mãe, sediada num paraíso fiscal, Gibraltar; o sócio gerente de ambas é o mesmo, tem nacionalidade Holandesa, é arguido no processo. Desenvolveu actividade no México, e preparava-se para desenvolver porventura o mesmo tipo de actividade na Republica Checa, França, Inglaterra e Alemanha, uma vez que foi encontrado um contrato para fornecimento de infra-estruturas de redes para prestação de serviços de comunicações de dados, nesses países. Segundo indícios recolhidos durante o inquérito, preparava-se para usar um DIALER Internacional.

O DIALER foi encomendado pelo dono desta empresa, a um programador russo informático. Já vimos como era possível, a concepção de um programa que tivesse a capacidade de terminar a ligação que o utilizador tinha no momento do acesso à internet, efectuando outra ligação para um outro número de telefone- de valor acrescentado, sem conhecimento ou participação do cibernauta (com o que se consuma o assalto).

O programador russo contratado, arguido também nos autos, que afirmava desconhecer, até às primeiras reclamações, que a ligação era feita para um número de valor acrescentado, afirma-se no entanto como, o **primeiro programador a nível mundial** a conseguir que um DIALER terminasse a ligação de acesso à internet, substituindo-a por outra;

³ na alteração introduzida pela Reforma de 1998- Lei 65/98, de 2 de Setembro, que acrescentou ao art. 221 o seu

trata-se de um conceito totalmente **inovador** na altura, por não se conhecer até à data, nenhum outro programa com essa capacidade.

Também a descoberta do investigador policial é inovadora, e tem servido de case study às congéneres policiais - porque, através dessa descoberta, foi possível recolher prova da existência da Burla, dos seus mecanismos e dos seus autores. Sem essa descoberta dir-se-ia estarmos perante um banal caso de incumprimento contratual face às regras administrativas de licenciamento dos serviços de audiotexto, e até de não pagamento das contas telefónicas por parte dos clientes da Portugal Telecom, afinal verdadeiros lesados de toda esta trama, e que apareciam inicialmente como os “maus da fita”.

Os conteúdos de cariz erótico/sexual eram garantidos entre outras modalidades pela arregimentação de mulheres oriundas dos países de Leste, que prestavam esses serviços em condições de exploração ilegal, nas instalações da própria empresa.

Não fosse a intervenção policial a tendência era para a expansão internacional deste tipo de “serviços”. Segundo os investigadores, e com base em determinados documentos, são bem patentes os propósitos específicos deste tipo de “empresas”: as motivações de enriquecimento através do “DIALER”, enquanto modus operandi totalmente inovador, tendo por base o desenvolvimento duma actividade empresarial.

3. A INVESTIGAÇÃO

A propósito desta nova criminalidade, não só do caso concreto como de toda a criminalidade praticada através da Internet e das telecomunicações importa enunciar um dos problemas novos, fundamentais:

- a conciliação entre os interesses da protecção da privacidade das telecomunicações e da recolha da prova em tempo-real. O conflito entre a privacidade e a eficácia do processo penal.
- Para melhor compreendermos o problema basta dizer que os meios de prova, nestes casos, dependem de um conjunto de **prova** digital a produzir imediatamente, da qual depende a

prova da existência dos crimes e a identificação dos seus autores. A Prova digital é constituída pelos dados de conteúdo, dados de tráfego e dados de base.

O quadro legal actual , em Portugal, não se adequa às necessidades de combate a esta criminalidade, uma vez que não consagra as excepções necessárias para a protecção da segurança do Estado e para a prevenção, investigação ou repressão de crimes. A Lei 67/98 de 26 de Outubro, e Lei da protecção de dados Pessoais face à Informática- Lei 10/91 protegem a segurança e o tratamento de dados, o sigilo profissional, mas não prevêm as derrogações necessárias por razões de perseguição criminal.⁴

Segundo a Convenção do CiberCrime “ Cada Parte deverá adoptar as medidas do foro legislativo necessárias no sentido de permitir às autoridades competentes exigir, ou de forma semelhante obter a preservação expedita dos dados de tráfego, armazenados por meio de um sistema informático, em especial nos casos em que existam motivos para crer que tais dados sejam particularmente vulneráveis a perdas ou modificações”.

Com o quadro legal vigente as operadoras de telecomunicações são mesmo obrigadas à destruição dos dados de tráfego⁵, após 24H, o que se traduz numa volatilidade da prova incompatível com o direito de punir, de consagração constitucional.

4. O ENRIQUECIMENTO INDEVIDO E O BRANQUEAMENTO DO PRODUTO DO CRIME (CONCLUSÕES/ exame da contabilidade):

Este tipo de criminalidade, que se destina a produzir, e produz lucros milionários, salvaguarda os seus proventos através de engenharias financeiras com apoio nos paraísos fiscais: ou seja, o produto do crime é transferidos para empresas sediadas em paraísos fiscais, a título de custos ou outros expedientes.

⁴ Estão pendentes duas propostas legislativas, na AR, sobre a obrigatoriedade para as empresas de telecomunicações, de preservação dos dados de tráfego, e sobre as condições de acesso pelas autoridades de policia criminal.

⁵ Dados de tráfego, segundo a definição da Convenção do Cibercrime: “ Significa qualquer dado informatizado, relacionado com uma comunicação efectuada por meio de um sistema informático, gerado pelo sistema informático e que faz parte integrante da cadeia de comunicação, através da qual se indicam os aspectos da comunicação, tais como a sua origem, destino, caminho, hora, data, volume de informação, a duração, ou o tipo de serviço subjacente à mesma”

A investigação das transferências bancárias , o seguimento do caminho do dinheiro enquanto meio de atingir a verdade material , no processo crime, coloca-nos problemas novos muito complexos. De forma muito simples, o principal problema é este:

- É que, enquanto o crime não tem fronteiras a justiça é ainda excessivamente territorial, local. O que pode transformar-se, nestes casos, num factor de impunidade (se não houver cooperação judicial estreita, rápida, eficaz).

- A investigação destes crimes súbitamente, tem que ser feita também nas Bahamas, México, Gibraltar, etc.

5. OS OFENDIDOS E APREVENÇÃO GERAL

Os ofendidos nestes casos, em geral são cidadãos incautos, às centenas, espalhados por todo o país. Apenas detectaram a fraude, como afirmámos, no momento da recepção das contas telefónicas. Em muitos dos casos as consultas tinham sido efectuadas por menores, atraídos pelos conteúdos eróticos, sem conhecimento dos pais- o que levanta problemas vários, nomeadamente dum educação para o conhecimento destas realidades; dum nova cultura de segurança.

Há a necessidade de uma abordagem multidisciplinar destes problemas, fazendo intervir um conjunto de actores tais como os professores, os pais, os fornecedores de conteúdos, por forma a proteger os jovens da Internet, nomeadamente dos conteúdos lesivos.

A nível da prevenção geral ,como modo de agir sobre a generalidade das pessoas, existem iniciativas como a “Rede Europeia de Prevenção da Criminalidade” (Decisão do conselho de 28.05.01). Uma prevenção eficaz deve apelar ao empenho de toda a sociedade civil neste âmbito, no desenvolvimento de parcerias entre autoridades públicas nacionais, regionais e internacionais, organizações não governamentais, sector privado e cidadãos.

CONCLUSÃO : criminalidade global e insegurança local.

Este pareceu-nos um dos mais importantes exemplos de como através de novas modalidades de actuação, com origem em criminalidade desenvolvida à escala mundial, cada um de nós pode ser atingido, não na rua, não no trabalho, mas no sossego e na intimidade mais profunda do seu lar.

Esta nova criminalidade, caracterizada pelo recurso sofisticado, organizado às novas tecnologias de informação, pela volatilidade, agressividade e rapidez de actuação, mostra-nos um novo campo de problemas num Direito Penal tradicional orientado para a exclusiva protecção de bens jurídicos individuais e concretos.

O fim principal do direito Penal é a protecção de bens jurídicos, subjacente ao conceito de crime e à sua previsão; bens jurídicos principais como a vida, a liberdade, a integridade física, a auto determinação sexual, a honra, o património, a realização da justiça e certos valores da vida em sociedade . Só que estes casos, têm o condão de nos demonstrar a mutabilidade do conceito de bem jurídico, uma vez que não se trata apenas de proteger o património mas valores da vida em comum e da paz social.

Esta problemática resulta destas formas especiais do crime e da necessidade daí decorrente de uma incriminação cada vez mais ampla e menos vinculada, e de uma tutela de bens jurídicos cada vez mais inapreensíveis.

Tal realidade conduzirá porventura a uma nova noção de culpa jurídico penal, sempre dentro dos limites dum Estado de Direito. É que estamos perante modalidades de condutas criminosas, que pelos instrumentos utilizados e pela dimensão internacional nos levam a colocar a questão da necessidade dum direito penal preventivo, capaz duma intervenção mais eficaz, sem nunca beliscar as garantias essenciais do processo criminal democrático.

“A um contexto similar pertence a discussão em torno do “Direito Penal do Risco”, que foi suscitada pelo livro do sociólogo Beck sobre “sociedade de risco” (“Risikogesellschaft”, 1986) e que foi tratada monograficamente pela primeira vez na obra de Prittwitz sobre “direito Penal e Risco” (“Strafrecht und Risiko”, 1993). Nela se trata da questão de até que ponto o direito Penal está em condições de fazer frente com a sua tradicional ferramenta liberal ajustada ao estado de Direito, à qual também pertence sobretudo o conceito de bem jurídico, aos modernos riscos da vida (como os de tipo atómico, químico, ecológico ou de técnica genética). Muitos respondem negativamente a esta questão e aludem à necessidade de desactivar as causas sociais originadoras de tais riscos. Pois bem, como tal só é possível sempre de modo limitado, o certo é que não se poderá renunciar nunca à intervenção do direito penal neste campo. Mas também , ao lutar contra o risco através do direito penal há que preservar a refrência ao bem

*jurídico e aos restantes princípios de imputação próprios do Estado de Direito; e onde tal não seja possível, deve abster-se de intervir o direito penal. "Só há espaço para a intervenção do direito Penal ali onde as decisões sobre o risco pode imputar-se subjectivamente de modo justo"*⁶

Aqui chegados, parece-nos possível enunciar alguns dos grandes desafios do direito e processo penal do século XXI:

- o reforço dum direito e processo penal de intervenção com salvaguarda do princípio da culpa jurídico penal;
- o reforço dum direito penal do risco, capaz de maior eficácia na protecção dos interesses individuais e colectivos com salvaguarda das garantias do processo penal democrático;
- Um direito Penal capaz de fazer face aos riscos da vida moderna e das novas formas de criminalidade organizada global sem perder a sua face humana e justa.
- Um direito penal dum mundo tornado pequeno demais pela Internet, e grande demais pelos paraísos fiscais.

Maria José Morgado

⁶ Claus Roxin, in "Derecho Penal", parte general, T.I pag. ,Ed. Civitas