Despacho:

PARECER

Ref.ª: Anteprojecto de Lei [*s/n*]
Ofício n.º 1198, de 01.04.2009, Gabinete do Ministro da Justiça

Assunto: Parecer sobre o Anteprojecto de Proposta de Lei do Cibercrime, que transpõe paraa ordem jurídica interna a Decisão-Quadro n.º 2005/222/JAI relativa a ataques contra sistemas de informação e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa.

Excelentíssimo Senhor Vice-Presidente do Conselho Superior da Magistratura
Excelência,

1. Objecto

Por Sua Excelência, o Ministro da Justiça, foi determinada a remessa ao Conselho Superior da Magistratura do texto de Anteprojecto da Proposta de Lei do Cibercrime, que transpõe para a ordem jurídica interna a Decisão-Quadro n.º 2005/222/JAI relativa a ataques contra sistemas de informação e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa., solicitando que sobre a mesma seja emitido parecer.

Por Sua Excelência, o Juiz Conselheiro Vice-Presidente do Conselho Superior da Magistratura, foi determinado que sobre esta matéria seja emitido parecer pelo Gabinete de Apoio ao Vice-Presidente e aos membros do Conselho Superior da Magistratura.

Rua Mouzinho da Silveira, n.º 10
1269 – 273 Lisboa Portugal
Telefone 213 220 020
Fax 213 474 918
http://www.csm.org.pt
E-mail: csm@csm.mj.pt

2. Âmbito

2.1. O presente anteprojecto de proposta de lei visa transpor para a ordem jurídica interna a Decisão-Quadro n.º 2005/222/JAI relativa a ataques contra sistemas de informação e adaptar o direito interno à Convenção sobre Cibercrime do Conselho da Europa.

2.2. A Convenção sobre Cibercrime, assinada em Budapeste, data de Novembro de 2001 e surgiu como o primeiro instrumento internacional sobre este tipo de criminalidade. O documento visa a harmonização das legislações nacionais dos Estados na área do cibercrime, bem como facilitar a cooperação internacional e as investigações de natureza criminal. A Convenção define crimes contra a confidencialidade, integridade e disponibilidade dos sistemas de computadores, crimes referentes aos conteúdos e crimes informáticos. Inclui também medidas processuais, de investigação e cooperação internacional adaptadas às infracções ao crime cometida no ciberespaço ou por meio de computadores.

2.3. Já a Decisão-Quadro *supra* referenciada, visa o reforço da cooperação entre as autoridades judiciárias e outras autoridades competentes, nomeadamente as autoridades policiais e outros serviços especializados responsáveis pela aplicação da lei nos Estados-Membros, mediante uma aproximação das suas disposições de direito penal em matéria dos ataques contra os sistemas de informação.

2.4. O legislador nacional adopta a metodologia de transposição praticamente literal dos textos originais da Decisão-Quadro, razão por que, na sua generalidade, não contém soluções que mereçam especiais considerações por parte do Conselho Superior da Magistratura, na medida em que este não deve, em cumprimento do princípio da separação dos poderes, interferir em matéria de opções político-legislativas, mas apenas observar aquilo que tenha influência sobre o regular funcionamento das instâncias judiciais nacional e do exercício da função jurisdicional.

2.5. Nesta conformidade, este parecer limitar-se-á a efectivar as observações e propostas que se consideram pertinentes a evitar interpretações dúbias sobre a forma da sua aplicação ou da extensão em que execução seja idónea a efectivar-se.

★

Rua Mouzinho da Silveira, n.º 10
1269 – 273 Lisboa Portugal
Telefone 213 220 020
Fax 213 474 918
http://www.csm.org.pt
E-mail: csm@csm.mj.pt

3. Apreciação

3.1. Crimes já previstos na Lei da Criminalidade Informática

O anteprojecto alarga o âmbito de crimes já tipificados na Lei da Criminalidade Informática (LCI) — Lei n.º 109/91, de 17 de Agosto. Assim sucede com os seguintes crimes:

— Crime de falsidade informática (art.º 2.º do anteprojecto *vs* art.º 4.º da LCI);

— Crime de dano relativo a programas ou outros danos informáticos (art.º 3.º do anteprojecto *vs.* art.º 5.º da LCI);

— Crime de sabotagem informática (art.º 4.º do anteprojecto *vs*. art.º 6.º da LCI);

— Crime de acesso ilegítimo (art.º 5.º do anteprojecto *vs* art.º 7.º da LCI);

— Crime de intercepção ilegítima (art.º 6.º do anteprojecto *vs*. art.º 8.º da LCI);

— Crime de reprodução ilegítima de programa protegido (art.º 7.º do anteprojecto *vs* art.º 9.º da LCI).

O diploma tem coerência sistemática porque no seu art.º 32.º declara revogada a LCI.

3.2. Definição de intercepção

3.2.1. Apesar da citada coerência sistemática, no artigo 1.º do anteprojecto (referente às *definições* para os efeitos da lei), não se faz expressa referência à definição de *intercepção*. Ora, no art.º 2.º, al. *f)* da actual LCI é considerado intercepção o "acto destinado a captar informações contidas num sistema automatizado de dados, através de dispositivos electromagnéticos, acústicos, mecânicos ou outros".

Esta definição é muito relevante para a integração de condutas no âmbito da previsão do respectivo crime (*cfr*. art.º 6.º do texto do anteprojecto) que, sem uma definição precisa é susceptível de interpretações dúbias, atento o *princípio da tipicidade* que vigora no direito penal.

3.2.2. Estão neste âmbito, as seguintes acções:

- *Sniffing* (este, mais pacífico, por se enquadrar totalmente na intercepção)
- *Varredura de portas* (utilização de programas que procuram na internet os computadores que tenham portas activas, abertas e/ou com componentes ou periféricos compartilhados em rede, isto é, que podem ser acedidos por terceiros);
- *Ataques DoS — Denial of Service,* mediante a utilização de computador que gere múltiplas mensagens aparentemente normais, como no caso dos pacotes UDP — User Datagram Protocol. Esses pacotes dão a impressão de que se originam no

Rua Mouzinho da Silveira, n.º 10
1269 – 273 Lisboa Portugal
Telefone 213 220 020
Fax 213 474 918
http://www.csm.org.pt
E-mail: csm@csm.mj.pt

mesmo servidor que os está a receber. Ao tentar responder a esse fluxo constante de dados defeituosos, o servidor que está a ser vitimado, torna-se incapaz de aceitar outras conexões, o que faz com que qualquer envio de mensagem implique um retorno nulo.

- *Ping O'Death,* que consiste em enviar-se um pacote IP com tamanho maior que o máximo permitido (65535 bytes), para o computador que se deseja atacar. O pacote é enviado na forma de fragmentos (a razão é que nenhum tipo de rede permite o tráfego de pacotes deste tamanho) e quando a máquina destino tenta montar estes fragmentos, inúmeras situações podem ocorrer: a maioria dos sistemas bloqueiam, alguns reinicializam, outras abortam e mostram mensagens de erro irrecuperável.

3.2.3. Deste modo, e face à sua relevância conceptual em sede de integração de acções na previsão do crime de intercepção ilegítima, *sugere-se* que seja aditada uma alínea ao artigo 1.º com a definição de intercepção, designadamente com a redacção constante da al. *f)* do art.º 2.º da LCI.

3.3. Crime de acesso ilegítimo

3.3.1. No art.º 5.º do anteprojecto, relativamente ao crime de acesso ilegítimo, reproduz-se *grosso modo* o teor do actual art.º 6.º da LCI, apenas se acrescentando que o benefício ou vantagem ilegítimo seja *"de natureza patrimonial ou não patrimonial"*.

3.3.2. Crê-se que este aditamento relaciona-se com o teor do art.º 2.º da Convenção sobre o Cibercrime, que estabelece quanto ao crime de acesso ilegítimo que «Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, no seu direito interno, o acesso intencional e ilegítimo à totalidade ou a parte de um sistema informático. As Partes podem exigir que a infracção seja cometida com a violação de medidas de segurança, com a intenção de obter dados informáticos ou outra intenção ilegítima, ou que seja relacionada com um sistema informático conectado a outro sistema informático».

3.3.3. Ora, esta é uma noção completamente diversa da que consta da Lei da Criminalidade Informática Portuguesa, designadamente *deixa de ser essencial a obtenção de uma vantagem patrimonial*, passando o núcleo da protecção a ser o *acesso intencional e ilegítimo à totalidade ou a parte de um sistema informático* [1].

[1] Para ROGÉRIO BRAVO, *O Crime de acesso ilegítimo na Lei da Criminalidade Informática e na Ciberconvenção,* Direito na Rede n.º 1 [on-line], Ordem dos Advogados, Lisboa, 2004, *in* www.oa.pt/direitonarede/detalhe.asp?

Rua Mouzinho da Silveira, n.º 10
1269 – 273 Lisboa Portugal
Telefone 213 220 020
Fax 213 474 918
http://www.csm.org.pt
E-mail: csm@csm.mj.pt

Esta diferença pode ser essencial na integração de condutas ilícitas, designadamente de *crackers*, se devem ser consideradas como sabotagem informática (mais grave) ou como simples acesso ilegítimo [2].

3.3.4. Ou seja, parece-nos que a inserção da menção «*de natureza patrimonial ou não patrimonial*", além de ser susceptível de conduzir a complexas interpretações sobre em que consiste a natureza *não patrimonial*, vai no sentido oposto ao da Convenção do Cibercrime, que em no rigor formal e conceptual exigiria que fosse retirada da previsão legal o requisito da intenção de alcançar benefício ou vantagem ilegítima, na medida em que o núcleo da protecção deve ser **apenas** o *acesso intencional e ilegítimo à totalidade ou a parte de um sistema informático*.

---

idc=11741&scid=17730&idr=11760&ida=17734, "desde há muito que o computador deixou de ser um mero ordenador. Um computador, seja de secretária ou de bolso, constitui hoje um terminal de comunicações complexo, que permite deter, exibir, processar e difundir informação, mormente sob as formas de som e de imagem, em que o papel escrito aparece como uma forma marginal de representação dessa informação. Este terminal de comunicações é hoje um apetrecho tecnológico que tanto equipa um gabinete como um domicílio, por isso mesmo comportando inexoravelmente uma dimensão pessoal daqueles que o utilizam e que acabam, invariavelmente, por nele deixarem informação de carácter pessoal, comercial, de qualquer dos modos restrita, no sentido de não destinada a ser partilhada. Parece-nos portanto ser grande a propriedade e a clarividência dos juristas portugueses já o tinham percebido, quer aquando da transposição da Recomendação R(89)9 para a nossa LCI, referindo-se, directa ou indirectamente, uns ao "domicílio informático", outros ao conceito de "segurança do sistema informático. (…) A este panorama, o texto da Convenção vem agora impor uma de duas vias: um mínimo, que é o da punição do acesso ilegítimo a sistemas ou a redes informáticas, seja a todo ou a parte do sistema ou da rede - passou a ser punido o mero acesso, com ou sem uma intenção, de obtenção do que quer que seja".

[2] Cfr. Acórdão de 19.06.1997, da 9.ª Vara Criminal de Lisboa, 3.ª Secção, Processo 1/97, *in* MANUEL LOPES ROCHA, *Direito da Informática nos Tribunais Portugueses (1990-1998),* Centro Atlântico, V.N.Famalicão, 1999, pp. 17-26. Tratou-se do caso de um estudante português, que foi condenado pela prática de um crime, p. e p. pelo art.º 6.º, n.º 1 da Lei 109/97, mas ao qual era imputada também a prática de crimes previstos nos art.^{os} 7.º, n.^{os} 1, 2 e 3, al.*a)* da mesma lei. Enquanto aluno do Instituto Superior, com acesso a uma determinada parte no sistema informática, o mesmo serviu-se de um programa disponível na Internet e, após a obtenção das passwords dos administradores do sistema, entrou em diversas áreas de outros utilizadores, substituindo comando do sistema operativo, enviando mensagens simuladas, criando ainda criando directórios, ficheiros e contas de utilizadores inexistentes. Ficou provado que o estudante actuou na ânsia de conseguir algo que não lhe era facilmente acessível e de desafiar as proibições através dos seus conhecimentos informáticos pelo prazer de ultrapassar barreiras e por rivalidade com outro estudante. Não ficou provado que o mesmo tenha tido qualquer benefício, mas apenas que provocou prejuízos. Por isso, o Tribunal entendeu que tal conduta se subsumia apenas na previsão do art.º 6.º (sabotagem informática) e não no art.º 7.º. Escreveu-se nesse acórdão o seguinte (para o que aqui releva):

> "Não se apurou, igualmente, que o arguido tivesse violado quaisquer regras de segurança ou segredo legalmente protegido. Porém, entende-se que incorreu tão só na prática de um crime de sabotagem informática, por se considerar existir entre as aludidas normas referidas uma situação
> de concurso aparente. Com efeito, cumpre fazer referência, desde logo, ao conceito de sistema informático, entendendo este como conjunto de um ou mais computadores, equipamento periférico e suporte lógico que assegura o processamento de dados. No que respeita ao tipo p. e p. pelo aludido artigo 7.º da Lei nº 109/91, de 17/ 08, o bem jurídico protegido pelo mesmo é a segurança do sistema informático. Para que tal tipo se verifique é necessário que o agente, não estando autorizado, aceda, de qualquer modo, a um sistema ou rede informáticos. No que respeita aos elementos subjectivos do tipo, terá o agente de actuar com a específica intenção de alcançar para si ou para terceiro benefícios ou vantagens ilegítimas. No que se refere ao crime previsto no artigo 6º da dita Lei, o bem jurídico protegido pelo mesmo é o interesse do proprietário ou do utente de um sistema informático em que o mesmo funcione bem. Para que o mesmo se verifique é necessário que o agente: introduza, altere, apague ou suprima dados ou programas informáticos num sistema informático ou de telecomunicações de dados à distância. No que toca ao elemento subjectivo do tipo, deverá o agente actuar com a intenção de entravar ou perturbar o funcionamento do sistema de comunicações (dolo específico). Trata-se, portanto, de um crime de dano. O arguido praticou todas as suas descritas condutas, para além do mais, em obediência à resolução de aceder a áreas do CIIST a que não estava autorizado e de perturbar o normal funcionamento do aludido sistema, o que conseguiu, tendo causado os referidos prejuízos no mesmo. Porém, a prática do segundo dos ditos ilícitos envolve necessariamente a prática do primeiro, representando como que um mais em relação àquele, pelo que se considera que o consome-relação de consunção. E assim sendo, incorreu o arguido na prática de um crime p. e p. pelo artigo 6.º, n.º 1 da Lei n.º 109/91, de 17/08.

Rua Mouzinho da Silveira, n.º 10 Telefone 213 220 020 http://www.csm.org.pt
1269 – 273 Lisboa Portugal Fax 213 474 918 E-mail: csm@csm.mj.pt

3.3.5. Por outro lado, convém considerar que na Convenção sobre o cibercrime, ao contrário do que sucede com a legislação nacional e do que consta no n.º 4 do art.º 5.º do anteprojecto em apreciação, *não está prevista a punibilidade da tentativa*.

3.4. Penas acessórias

A actual Lei da Criminalidade Informática (Lei n.º 109/91, de 17 de Agosto) estabelece no seu capítulo III (artigos 11.º e ss.) várias *penas acessórias* que podem ser aplicadas aos crimes previstos nesse diploma.

No presente anteprojecto apenas se faz referência à perda de bens (art.º 10.º), cujo regime já resulta do regime geral previsto no Código Penal.

O elenco das penas acessórias previstas na actual LCI, a saber, caução de boa conduta, interdição temporária do exercício de certas actividades ou profissões, encerramento temporário do estabelecimento, encerramento definitivo do estabelecimento e publicidade da decisão condenatória mantêm significativa relevância em crimes desta natureza e a sua manutenção não contrariaria qualquer disposição da Convenção sobre o cibercrime, nem a Decisão-Quadro n.º 2005/222/JAI — antes, pelo contrário, reclama sanções específicas designadamente para as pessoas colectivas (*cfr.* art.º 9.º da Decisão-Quadro [3]), razão por que se *sugere* que esse elenco se mantenha na proposta de lei do Cibercrime, com as especificidades relativamente às pessoas colectivas nos termos do art.º 9.º da Decisão-Quadro.

3.5. Restante conteúdo do Projecto de Proposta de Lei

A redacção proposta para os restantes normativos corresponde, na sua generalidade, à transposição com grande proximidade literal das normas constantes da Decisão-Quadro e da Convenção sobre o Cibercrime.

Na medida em que tal redacção não implica qualquer influência sobre o regular funcionamento das instâncias judiciais nacional e do exercício da função jurisdicional nos termos constitucionalmente previstos, antes resume-se a matéria com natureza de política legislativa, é nosso parecer que o Conselho Superior da Magistratura deve abster-se de sobre a mesma efectivar qualquer outra observação.

[3] Texto do art.º 9.º da Decisão-Quadro:

Artigo 9.º
Sanções aplicáveis às pessoas colectivas

1. Cada Estado-Membro deve tomar as medidas necessárias para assegurar que uma pessoa colectiva considerada responsável nos termos do n.o 1 do artigo 8.o seja passível de sanções efectivas, proporcionadas e dissuasivas, incluindo multas ou coimas e eventualmente outras sanções, designadamente:
a) Exclusão do benefício de vantagens ou auxílios públicos;
b) Interdição temporária ou permanente de exercer actividade comercial;
c) Colocação sob vigilância judicial;
d) Dissolução por via judicial.
2. Cada Estado-Membro deve tomar as medidas necessárias para assegurar que uma pessoa colectiva considerada responsável nos termos do n.o 2 do artigo 8.o seja passível de sanções ou medidas efectivas, proporcionadas e dissuasivas.

Rua Mouzinho da Silveira, n.º 10
1269 – 273 Lisboa Portugal
Telefone 213 220 020
Fax 213 474 918
http://www.csm.org.pt
E-mail: csm@csm.mj.pt

★

Submete-se o presente parecer ao melhor e douto entendimento de Vossa Excelência.

★

Lisboa, 09 de Abril de 2009.

Joel Timóteo Ramos Pereira

Adjunto do Gabinete de Apoio ao Vice-Presidente e aos Membros do CSM.

Rua Mouzinho da Silveira, n.º 10
1269 – 273 Lisboa Portugal
Telefone 213 220 020
Fax 213 474 918
http://www.csm.org.pt
E-mail: csm@csm.mj.pt