

Exmo. Senhor  
Presidente da Comissão de Assuntos  
Constitucionais, Direitos, Liberdades e  
Garantias  
Assembleia da República  
Palácio de São Bento  
1249 – 068 LISBOA

N/Ref. 02.02  
Proc. n.º 4780/2009  
Of. n.º 8428 07/07/2009

Assunto: Solicitação de Parecer sobre as Propostas de Lei n.ºs 289/X/4.ª (GOV).

Com referência ao assunto em epígrafe, fica. V. Exa. notificado para todo o conteúdo do Parecer desta CNPD n.º 37/2009, proferido em 06 de Julho p. p., cuja cópia se anexa.

Com os melhores cumprimentos.

A Secretária da CNPD,



(Isabel Cristina Cruz)

ASSEMBLEIA DA REPÚBLICA	
Divisão de Apoio às Comissões CACDLG	
N.º Único	319937
Entrega/Sendo n.º	631
Data:	07/07/2009

~~RC~~

Rua de São Bento, 148-3º • 1200-821 LISBOA  
Tel: 213 928 400 Fax: 213 976 832  
geral@cnpd.pt www.cnpd.pt

**21 393 00 39**

**LINHA PRIVACIDADE**  
Dias úteis das 10 às 13 h  
duvidas@cnpd.pt

Processo n° 4780/09

PARECER N° 37 /2009

### I. RELATÓRIO

A Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias, solicitou à CNPD, a emissão de parecer, relativamente à Proposta de Lei n° 289/X/4ª (GOV) a qual visa transpor para a ordem jurídica interna, a Decisão-Quadro n° 2005/222/JAI relativa a ataques contra sistemas de informação e adapta o Direito Interno à Convenção sobre Cibercrime do Conselho da Europa.

Dentre as competências da CNPD, elencadas no art° 23° da Lei n° 67/98 de 26 Out (doravante LPD), cabe a de emitir parecer sobre disposições legais relativas ao tratamento de dados pessoais, como se extrai da al.a) do n°1 do citado normativo legal.

Entende-se por dados pessoais “qualquer informação, de natureza e independentemente do respectivo suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável”, sendo que há tratamento dos mesmos, sempre que ocorra “qualquer operação ou conjunto de operações sobre dados pessoais, efectuadas com ou sem meios automatizados, tais como a recolha, o registo, a organização, a conservação...”.

Norteando ainda tais coordenadas, importa também salientar, o reconhecimento dos direitos à identidade pessoal, à imagem e à reserva da



COMISSÃO NACIONAL  
DE PROTECÇÃO DE DADOS

intimidade e, bem assim, as garantias efectivas contra a utilização abusiva ou contrária à dignidade humana, de informações relativas às pessoas, espelhados no artº 26º da Constituição da República Portuguesa.

Cumprе por fim salientar, a protecção à honra, reputação, reserva da vida privada, a qual só permite alguma ingerência, mediante mecanismo legal adequado e desde que constitua providência necessária, numa sociedade democrática, para a segurança nacional, pública, bem-estar económico do país, defesa da ordem e a prevenção de infracções penais – cfr. artsº 12º e 8º da Declaração Universal dos Direitos do Homem e Convenção Europeia dos Direitos do Homem, respectivamente.

Conclui-se que no caso em apreço, como se retira da leitura da proposta de diploma legal, estando abarcadas situações que envolvem pesquisa de dados informáticos, apreensão de dados informáticos, apreensão de correio electrónico, interceptação de comunicações, sendo que tais acções necessariamente visam também pessoas singulares, surge claro que se trata de caso de emissão de parecer, no que a tais aspectos directos concerne e, bem assim, do que indirectamente daí decorrer.

## II. APRECIACÃO

### *a) Geral*

Num primeiro momento colhe referir, como já se notou, surgir este projecto de proposta de Lei, na sequência da transposição para a ordem jurídica interna a Decisão-Quadro nº 2005/222/JAI relativa a ataques contra sistemas de informação e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa.

Do exame do complexo normativo em presença, desde logo da exposição de motivos surge cristalino que com o mesmo, se pretende condensar todo o quadro normativo respeitante à cibercriminalidade e não proceder à alteração de diversas fontes legislativas atinentes à matéria – Lei da Criminalidade Informática (Lei 109/91 de 17 de Agosto), Lei nº32/08 de 17 de Julho, Código Penal, Código de Processo Penal e Lei de Cooperação Judiciária Internacional (Lei 144/99 de 31 de Agosto).

Segue-se assim uma opção que vem sendo utilizada no domínio do Direito Penal, na ordem jurídica portuguesa, tratar em diploma próprio e específico, matérias de reconhecida especialidade e estrutura peculiar, como já são exemplos, entre outros, a criminalidade relacionada com o tráfico de estupefacientes, a criminalidade fiscal, a lei do cheque, a criminalidade económico-financeira, a prevenção e repressão de branqueamento.

Parece inquestionável que a realidade dos nossos dias e necessariamente o Direito Penal, se debate com problemas oriundos da utilização cada vez mais massificada da informática e das tecnologias das telecomunicações que suscitam e desencadeiam, um intenso tráfico de informação/dados, surgindo as novas tecnologias não só como novas formas de comunicação quase imediata, mas também como novas ferramentas para a prática de “velhos crimes”, como bem salienta HELENA MONIZ in “As Telecomunicações e o Direito na Sociedade de Informação”, “Internet e Globalização – Problemas Jurídico-Penais”, Instituto Jurídico da Comunicação 1999, pg 367.

Cumpre ainda salientar que sendo esta matéria de sensibilidade reconhecida e importância primordial, a Convenção que serve de “mote” a esta proposta

de lei, foi trabalhada pelo Conselho da Europa desde 1997, socorrendo-se tal entidade de duas Recomendações suas – Recomendação R(89) 9 sobre a criminalidade relacionada com o computador e a Recomendação R(95) 13 sobre os problemas do processo penal ligados à tecnologia da informação.

Adite-se ainda que sobre esta matéria o Grupo de Trabalho do artº29º - Grupo de Trabalho de Protecção de dados Pessoais emitiu o Parecer 4/01 em 22 de Março de 2001, relativo ao Projecto de Convenção do Conselho da Europa sobre Cibercriminalidade.

Cabe ainda citar o Parecer 13/01 de 26 de Junho de 2001, emitido por esta CNPD, relativo ao Projecto de Convenção do Conselho da Europa sobre Cibercrime e bem assim o Parecer 2798/09 de 14 de Abril de 2009, igualmente proferido por esta Comissão, referente à Proposta de Lei apresentada pelo Governo.

Nota a ter em atenção será também a Recomendação de 4 de Março de 2008, do Grupo de Trabalho das Telecomunicações – “International Working Group on Data Protection in Telecommunications” - , a propósito da implementação e aplicação da Convenção do Conselho da Europa nº 185 relativa ao Cibercrime.

Por último, há que focar a atenção na Decisão-Quadro do Conselho Europeu de 27 de Novembro de 2008, relativa à protecção de dados pessoais no âmbito da cooperação policial e judiciária, em matéria penal, mormente ao seu artº13º respeitante à transferência de dados para Estados Terceiros.

Aqui fixam-se princípios a seguir que importa chamar à colação na análise ora em presença.



COMISSÃO NACIONAL  
DE PROTECÇÃO DE DADOS

Determina-se que a transferência para Estados Terceiros – dados pessoais – ou para instâncias internacionais, operará desde que:

- tal seja necessário para fins de prevenção e perseguição de infracções penais ou para a execução de sanções penais;
- a autoridade destinatária seja a competente;
- o Estado Membro onde os dados foram colhidos tenha dado o seu acordo à transferência;
- O Estado Terceiro garanta um nível de protecção adequada em matéria de dados pessoais.

Estipula-se ainda que a não verificação destas exigências só poderá ocorrer quando estiver em causa a prevenção de um perigo sério e imediato relativo à segurança pública de um Estado Membro ou de um Estado Terceiro ou nas situações previstas no nº3 do artº 13º da Decisão-Quadro referida.

Estes vectores enformadores deverão ser atendidos, crê-se, no projecto de diploma que se apresenta.

Debruçando agora o olhar pelo complexo em presença, ressalta com evidência que o mesmo dedica o Capítulo I à definição de conceitos, o Capítulo II relativo ao chamado Direito Penal Material onde se define um elenco de comportamentos integradores de diversos tipos criminais, o Capítulo III versando sobre aspectos processuais – Direito Processual Penal - o Capítulo IV orientado para as regras de cooperação internacional e por último o Capítulo V sobre disposições finais transitórias, onde se integra um dispositivo genérico relativo à protecção de dados pessoais.

### *b)Particular*

Tentar-se-á abordar cada comando legal, em particular, mormente aqueles que podem suscitar pontos de controvérsia:

**Artigo 1º** - Refere o objecto da presente Lei, nada havendo a salientar;

**Artigo 2º**- Definindo conceitos, seguiu a linha já consagrada na Convenção, usando e terminologia “dados informáticos”, não se fazendo uma inclusão clara e inequívoca da protecção de dados pessoais, não se optando por consagrar uma definição de dados pessoais neste domínio.

Este aspecto foi alertado no Parecer desta CNPD acima referido, continuando assim a inexistir, pensa-se, uma cobertura directa relativa a condutas lesivas dos dados pessoais, prevendo-se de forma clara para aquelas, tipos de infracções penais.

Nesta esteira, todos os comportamentos que se enunciam como tipificadores dos diversos ilícitos recorrem à noção de “dados informáticos”, inexistindo normativo no quadro ora apresentado, apelando aos dados pessoais o que parece demonstrar um claro retrocesso ao caminho já traçado com a Convenção 108 do Conselho da Europa e seu Protocolo Adicional, Directiva 95/94/CE e com a Lei 67/98 de 26 de Outubro;

**Artigos 3º a 9º** - Definem os vários ilícitos e respectivas punições, assentando, como se expendeu na noção de dados informáticos, nada se consignando que expressamente refira a expressão dados pessoais como já se fez notar supra;

**Artigo 10º** - Vem estender a responsabilidade penal, na esteira de outras situações já existentes na ordem jurídica portuguesa, às pessoas colectivas ou equiparadas, socorrendo-se do regime ínsito no CPenal;

**Artigo 12º** - O nº2 deste preceito parece estender as regras processuais ora fixadas, em relação a crimes que não os aqui previstos e especialmente

regulados, o que pode suscitar “confronto” de regimes, mormente com o disposto no CPPenal e, por essa via, beliscar com direitos fundamentais, como é o da inviolabilidade do domicílio e da correspondência – artº 34º da CRP;

**Artigo 13º** - Nenhuma questão a suscitar em termos de Protecção de dados Pessoais;

**Artigo 14º** - Referindo-se à Preservação Expedita de Dados, consagra a possibilidade de tal ser ordenado pelo órgão de polícia criminal – ainda que em situações muito específicas e concretas -, o que parece excessivo já que tudo se passa no decurso de um processo de natureza criminal, cuja direcção compete à autoridade judiciária (MºPº, Juiz de Instrução ou Juiz de Julgamento, dependendo das fases), não se descortinando a necessidade de estender tal competência aos órgãos de polícia, sendo que, tal poderá violar regras constitucionalmente consagradas e fixadas no domínio do Código de Processo Penal e, bem assim, poderá contender com as regras de protecção de dados pessoais.

Na verdade a fórmula usada no nº 2 – “A preservação pode também ser ordenada pelo órgão de polícia criminal mediante autorização da autoridade judiciária...”, é ambígua e pouco segura. Se houve autorização da autoridade judiciária, tal decorreu de uma decisão desta e, conseqüentemente é esta que ordena e não o órgão de polícia criminal.

Acresce que o nº5 do mesmo preceito, se socorre da mesma fórmula para a ordem da renovação da medida, o que igualmente pode conduzir a ambigüidades em matéria de reconhecida sensibilidade.

Nesta medida entende-se que em termos de protecção adequada de direitos fundamentais e, concomitantemente de protecção de dados pessoais, se



COMISSÃO NACIONAL  
DE PROTECÇÃO DE DADOS

deverá seguir a linha do sistema processual penal vigente, mantendo-se uma linha uniforme nestas matérias, deixando à autoridade judiciária competente o poder de decidir e ordenar.

**Artigo 15º** - Pretendendo regular a revelação expedita dos dados de tráfego, igualmente estende a possibilidade de tal operar directamente ao órgão de polícia criminal, valendo aqui as razões acima adiantadas;

**Artigo 16º** - Nada a mencionar, a não ser que o legislador aqui consagra a possibilidade de injunção com base apenas em ordem da autoridade judiciária, tornando assim menos entendível a solução preconizada nos dispositivos anteriores, para além de que se nota mais evidente, alguma desarmonia no sistema a implementar;

**Artigo 17º** - Face ao regime de rigor aqui fixado, renova-se o que se referiu anteriormente, ou seja, as soluções diversas adiantadas neste complexo, quanto à entidade competente para autorizar e ordenar determinados actos de recolha de prova. Aqui usa-se um mecanismo muito semelhante ao vigente no CPPenal, cabendo à autoridade judiciária autorizar e/ou ordenar a pesquisa de dados informáticos, abrindo-se tal possibilidade aos órgãos de polícia criminal, apenas em casos devidamente definidos e limitados.

Assim sendo, menos se entende a solução encontrada nas previsões dos artsº 14º e 15º;

**Artigo 18º** - Nada a referir, sendo certo que a apreensão aqui abarcada surge na sequência de uma Pesquisa anteriormente ordenada, pelo que o que a entidade policial apreender está acobertado por um despacho prévio da autoridade judiciária competente.

Por outro lado, quando estão em causa “dados pessoais ou íntimos” susceptíveis de beliscar a privacidade do respectivo titular ou de terceiro,

eles são de imediato apresentados ao juiz, o que parece salvaguardar as regras vigentes e as exigências de protecção de dados pessoais;

**Artigo 19º** - Refere-se à apreensão de correio electrónico e registos de comunicação de natureza semelhante, sendo que tudo ocorre na sequência de uma pesquisa electrónica previamente ordenada e mediante autorização ou ordem do juiz, remetendo-se para as regras respeitantes à apreensão de correspondência, expressas no CPPenal, pelo que se crê estarem salvaguardadas as exigências relativas à protecção de dados pessoais;

**Artigo 20º** - Consagra o regime da interceptação de comunicações, o qual se mostra conforme ao exigido no CPPenal, nada havendo a salientar;

**Artigo 21º** - Nada a referir, em matéria de protecção de dados pessoais;

**Artigo 22º** - Preceito no Capítulo relativo à Cooperação Internacional abre desde logo a possibilidade de se aplicar o regime deste diploma em matéria de Cooperação Policial.

Por outro lado, permite a utilização dos mecanismos aqui previstos para investigações e recolha de prova, relativas a infracções penais que não sejam as em causa neste diploma.

Cumpre desde já mencionar que em matéria de protecção de dados pessoais, tal pode suscitar questões em termos de garantias do seu respeito. Este normativo cria a possibilidade de envio de dados pessoais para Estados terceiros, o que reclama se avalie em cada situação concreta da adequação do nível de protecção que cada um pode conferir.

No que tange à matéria policial – que como acima se mencionou este dispositivo abre a possibilidade de aplicação - há que atentar na Recomendação nº R(87) 15, adoptada pelo Comité dos Ministros e Estados



COMISSÃO NACIONAL  
DE PROTECÇÃO DE DADOS

Membros, em 17/Setembro/1987, e que visou regulamentar a utilização dos dados de carácter pessoal no sector da polícia.

Acresce que o envio de dados pessoais para Estados terceiros, no âmbito penal, à luz da Lei 67/98 de 26 de Outubro, só pode acontecer quando aqueles Estados garantam um nível de Protecção adequado – o que também reclama a Decisão-Quadro de 27 de Novembro de 2008 acima enunciada -, sendo que nada se consignando neste complexo que tal salvaguarde, deixando-se abertura para aplicação deste regime em diversos quadros criminais, poderá permitir-se uma “transmissão massiva” e “indiscriminada” de informação, enfraquecendo os direitos dos respectivos titulares e, conseqüentemente beliscando os direitos, liberdades e garantias. Tal torna-se tanto mais evidente, quando se atenta no artº 24º do Projecto em exame, quando se consagram como motivos de recusa de transferência de dados, apenas e só em situações que tal possa lesar a ordem pública, a soberania, a segurança, infracção de natureza política ou conexas e outros interesses da República Portuguesa.

Face ao exposto, resulta que se estiverem envolvidos Estados terceiros que não garantam um nível de protecção adequada, tal não constitui motivo de recusa, o que deveria configurar;

**Artigo 23º** - Fica por saber da leitura do preceito, o que está abrangido na expressão “prestação de assistência imediata” o que também pode desencadear a prática de actos envolvendo a transmissão de dados pessoais, direitos, liberdades e garantias fundamentais, nas circunstâncias já salientadas, sendo certo que o responsável por tal é um órgão de polícia criminal e não uma autoridade judiciária.



COMISSÃO NACIONAL  
DE PROTECÇÃO DE DADOS

Diga-se ainda que se remete a regulamentação do regime a observar nos contactos, para protocolos de cooperação entre entidades policiais, o que de novo reclama cautelas a ter em matéria de níveis de protecção de dados pessoais;

**Artigo 24º** - No seu nº1, faz-se uma remissão genérica para o artº 12º, entendendo-se que para uma melhor leitura e clareza, dado o nº2 deste último preceito, fosse preferível uma literalidade elencando claramente as situações em que se admite a preservação e revelação em termos de cooperação internacional.

Admite-se a possibilidade de a Polícia Judiciária “ordenar” a preservação dos dados na sequência de solicitação de autoridade estrangeira, sendo que aqui tal surge acobertado por prévia autorização da autoridade judiciária, ou fundamentada em urgência ou perigo na demora, situação em que, posteriormente há sempre “fiscalização” por parte do Ministério Público.

Nesta segunda hipótese, crê-se que, em termos de harmonização do diploma em sindicância com as regras vigentes no domínio do CPPenal, dever-se-ia consagrar uma solução semelhante à constante no artº18º, onde claramente se prevê o acto de validação por parte da autoridade judiciária competente, abrangendo assim as situações em que, a competência cabe ao juiz e não ao Ministério Público,

Por outro lado esta possibilidade de intervenção por parte da Policia Judiciária, parece ser contrariada com a literalidade do nº8 do mesmo dispositivo, quando expressamente se consagra que a “autoridade judiciária competente” para decidir do pedido de auxílio, determina a preservação dos dados...”.



COMISSÃO NACIONAL  
DE PROTECÇÃO DE DADOS

Anote-se ainda que na al.b) no nº9 e no nº10 do preceito em avaliação, se prevê a intervenção de uma “autoridade nacional”, ficando por saber que autoridade é essa, quais as suas atribuições, o que cria dificuldades em termos de ponderação do respeito pelas regras de protecção de dados, mormente em matérias tão sensíveis como as aqui em presença;

**Artigo 25º** - Como acima já se enunciou, entende-se que seria de consagrar como motivo de recusa, para além das situações previstas e perante a possibilidade deste regime se estender a Estados terceiros, a da recusa alicerçada na salvaguarda dos dados pessoais, sempre que não ofereça o Estado requisitante, garantias adequadas de protecção;

**Artigo 26º** - Vale aqui o que se apontou em relação à remissão para o artº 12º constante do nº1 do artº 24º;

**Artigo 27º** - Regula-se o acesso das autoridades estrangeiras, sem necessidade de pedido prévio às autoridades portuguesas, prevendo-se a possibilidade de tal ocorrer em relação a dados publicamente disponíveis e àqueles em que tenha havido consentimento do titular.

Continua a suscitar questões o acesso por parte de autoridades de países em que não haja as garantias adequadas de protecção de dados.

Por seu turno, no que tange ao acesso com base no consentimento, fica por saber, quem obtém o consentimento, como foi obtido, respeita ou não o mesmo as exigências plasmadas no artº3º al.h) da Lei 67/98 de 26 de Outubro, há ou não garantias de confidencialidade e segurança;

**Artigos 28º a 31º** - Nada a referir;

**Artigo 32º** - Faz apelo à aplicação, no que respeita ao tratamento de dados pessoais, à Lei 67/98 de 26 de Outubro, remetendo no entanto para o Capítulo VI do Diploma em apreço, sendo que se deve tratar de lapso pois,

o texto apenas apresenta 5 capítulos, o que não permite avaliar a que adaptações pretende o legislador referir-se.

### III.CONCLUSÕES

- 1. A matéria vertida na proposta em análise, por conter dispositivos legais susceptíveis de interferir com dados da natureza pessoal e sensível, cabe no âmbito das competências desta CNPD;**
- 2. O Diploma em apreço deverá compaginar o seu quadro normativo, mormente no que tange à transferência para Estados terceiros, às regras relativas à protecção de dados pessoais, insertas na Lei 67/98 de 26 de Outubro, à Convenção 108 do Conselho da Europa de 28 de Janeiro de 1981 e seu Protocolo Adicional e ainda, à Recomendação nº R(87) 15, adoptada pelo Comité dos Ministros e Estados Membros, em 17 de Setembro de 1987, à Decisão-Quadro do Conselho Europeu de 27 de Novembro de 2008 e, bem assim à Recomendação do Grupo de Trabalho das Telecomunicações - “International Working Group on Data Protection in Telecommunications “ - de 4 de Março de 2008;**
- 3. Apontam-se como ajustes a efectuar, todos os aspectos referidos nos vários pontos do capítulo II b) Particular e, no mesmo, salientados.**

É este o Parecer da CNPD



COMISSÃO NACIONAL  
DE PROTECÇÃO DE DADOS

Lisboa, 08 de Julho de 2009.

Carlos de Campos Lobo (relator), Ana Roque, Helena Delgado

António, Luís Barroso, Luís Paiva de Andrade, Vasco Almeida

Rep.  (Dr. Luís Barroso, vogal que presidiu à sessão)  
Luís Lingnau da Silveira (Presidente)