PROJECTO DE LEI Nº 240/X

APROVA O REGIME DE OBTENÇÃO DA PROVA DIGITAL ELECTRÓNICA

Exposição de motivos

O eficaz combate ao crime e, em particular, ao crime organizado e transnacional, que de forma mais séria e profunda coloca em causa a segurança das pessoas e do seu património, exige meios de investigação adequados.

Ora, a Internet é hoje e cada vez mais um poderoso meio de comunicação, utilizado para a prática de crimes tão diversos e graves como o tráfico de armas e de droga, o terrorismo, o branqueamento de capitais e a exploração sexual de crianças.

Os próprios sistemas informáticos são também amiúde objecto de acções criminosas que visam quebrar a confidencialidade dos dados contidos nos mesmos, a fim de através da manipulação de tais sistemas e daqueles dados se causarem danos a empresas e particulares, interferindo, por exemplo, com o sistema bancário.

Torna-se necessário, portanto, dotar as autoridades de novos métodos de investigação, desde que enquadrados pelo acervo constitucional e legal dos direitos à reserva da vida privada, ao sigilo das comunicações e à protecção de dados pessoais, revelando-se, assim, essenciais as ideias de proporcionalidade e de ponderação relativa dos interesses em presença.

Por outro lado, a inexistência da obrigatoriedade das operadoras de comunicações de manterem e conservarem os dados que permitam a recolha de informação quanto à origem, percurso, destino e duração, entre outros dados (dados de tráfego), tem constituído uma dificuldade inultrapassável para a recolha da ora denominada prova digital.

Há, assim, que garantir que a informação relevante para a investigação seja preservada pelos operadores de telecomunicações e, simultaneamente, que as autoridades a eles acedam em tempo útil.

Deste modo, no presente projecto de lei são, antes de mais, apresentadas as definições dos dados aos quais é permitido o acesso: dados de localização, de tráfego, de base e de conteúdo.

O acesso aos dados de localização e de tráfego, bem como aos dados de base que não estejam sujeitos ao regime de confidencialidade, depende apenas de pedido da autoridade de polícia criminal ou da autoridade judiciária, o qual não está sujeito a quaisquer formalidades.

Já o acesso aos dados de base que impliquem a adopção de um regime de confidencialidade só é possível se for autorizado pela autoridade judiciária, em despacho fundamentado.

Com efeito, a partir do momento em que os dados aos quais se pretende ter acesso são pessoais e o respectivo titular os considerou reservados tem de ser a autoridade judiciária a ponderar, face aos interesses envolvidos, se se justifica que no caso em apreço seja dada prevalência à investigação criminal em curso.

Finalmente, no que concerne aos dados de conteúdo, só é possível aceder aos mesmos nas mesmas condições em que é possível efectuar escutas telefónicas, nos termos previstos no Código de Processo Penal.

Trata-se, na verdade, da situação em que a invasão da reserva da vida privada e do sigilo das comunicações é mais contundente, porquanto o que está em causa é precisamente o conhecimento do teor das comunicações dos sujeitos, pelo que se impõe nestes casos um maior rigor.

Prevê-se igualmente a possibilidade de acesso por parte da autoridade de polícia criminal aos dados de localização, de tráfego e de base, em sede de acções de prevenção permitidas face à criminalidade grave ou organizada, com todas as garantias que nos termos da lei estão consagradas para estas acções.

Por outro lado, o combate ao crime, e sobretudo às formas graves de criminalidade, tem necessariamente de contar com a colaboração dos operadores e fornecedores de serviços, que estão particularmente bem posicionados para auxiliarem as autoridades na realização da justiça, considerando-se que o ónus imposto a estas entidades não é desproporcional face à necessidade e características da prevenção e repressão criminais de hoje e estando, aliás, os próprios operadores naturalmente interessados em que os seus serviços não funcionem como verdadeiros «*instrumentos do crime*».

Por fim, importa ainda estabelecer, em relação aos operadores em geral, um dever de colaboração que faça com que, sempre que estes detectem, no âmbito da sua actividade,

condutas que possam indiciar a existência dos mencionados crimes, o comuniquem às autoridades competentes para efeitos de investigação criminal.
Adoptou-se, nesta matéria, uma terminologia consensual e recentemente consagrada na Convenção sobre o Cibercrime, do Conselho da Europa, aberta à assinatura dos Estados a 23 de Novembro de 2001, em Budapeste.

Assim, nos termos constitucionais e regimentais aplicáveis, os Deputados abaixo assinados, do Grupo Parlamentar do Partido Social Democrata, apresentam o seguinte projecto de lei:

Artigo 1.º
Objecto

O presente diploma aprova o regime de obtenção da prova digital electrónica.

Artigo 2.º
Definições

Para os efeitos da presente lei, considera-se:

a) «*Dados de localização*», quaisquer dados tratados numa rede de comunicações electrónicas que indiquem a posição geográfica do equipamento terminal de um utilizador de um serviço de comunicações electrónicas publicamente disponível;

b) «*Dados de tráfego*», os dados informáticos ou técnicos relacionados com uma comunicação efectuada por meio de tecnologias de informação e comunicação, por si gerados, indicando, designadamente, a origem da comunicação, o destino, os trajectos, a hora, a data, a extensão, a duração ou o tipo do serviço subjacente;

c) «*Dados de base*», os dados pessoais relativos à conexão com a rede de comunicações, designadamente número, identidade e morada de assinante, bem como a listagem de movimentos de comunicações, que constituem elementos necessários ao estabelecimento de uma base para a comunicação;

d) «*Dados de conteúdo*», os dados relativos ao conteúdo da comunicação ou de uma mensagem.

Artigo 3.º

Acesso aos dados de localização e de tráfego

1 — Para efeitos de prevenção e investigação criminal, os operadores de comunicações devem facultar às autoridades de polícia criminal ou às autoridades judiciárias os dados de tráfego e os dados de localização, sempre que estes lhes sejam por elas solicitados.

2 — O pedido não está sujeito a formalidades especiais e deve ser satisfeito no prazo máximo de cinco dias.

3 — O acesso aos dados referidos neste artigo para efeitos de prevenção criminal só é possível relativamente aos seguintes crimes:

- **a)** Os crimes previstos no n.º 1 do artigo 1.º da Lei n.º 36/94, de 29 de Setembro, alterada pelas Leis n.º 90/99, de 10 de Julho, n.º 101/2001, de 25 de Agosto, e n.º 5/2002, de 11 de Janeiro, que estabelece medidas de combate à corrupção e criminalidade económica e financeira, e nos n.ºs 2 e 3 do artigo 368.º- A do Código Penal, aditado pela Lei n.º 11/2004, de 27 de Março, que estabelece o regime de prevenção do branqueamento de vantagens de proveniência ilícita;
- **b)** Crimes contra a paz e a humanidade;
- **c)** Escravidão, sequestro, rapto ou tomada de refém;
- **d)** Organizações terroristas e terrorismo;
- **e)** Crimes contra a segurança do Estado, com excepção dos crimes eleitorais;
- **f)** Captura ou atentado à segurança de transporte por ar, água, caminho-de-ferro ou rodovia a que corresponda, em abstracto, pena igual ou superior a oito anos de prisão;
- **g)** Abuso sexual de crianças.

4 — As acções de prevenção realizadas no âmbito do número anterior regem-se pelo disposto na Lei n.º 36/94, de 29 de Setembro.

Artigo 4.º

Acesso aos dados de base

1 — Salvo quanto à listagem de movimentos de comunicação, o disposto no artigo anterior é aplicável aos demais dados de base, sempre que estes não estejam sujeitos ao regime de confidencialidade.

2 — Entende-se que se encontram sujeitos ao regime da confidencialidade os dados relativamente aos quais o utilizador tenha expressamente manifestado o desejo de não

serem publicitados, nos termos dos artigos 6.º e 13.º da Lei n.º 41/2004, de 18 de Agosto.

3 — Nos casos de listagem de movimentos de comunicação, bem como naqueles em que vigore o regime de confidencialidade relativamente aos demais dados de base, o pedido para o seu fornecimento incumbe à autoridade judiciária titular da direcção do processo, em despacho fundamentado.

4 — No despacho referido no número anterior pode a autoridade judiciária delegar as competências de investigação criminal nos órgãos de polícia criminal, nos termos do Código de Processo Penal e do Decreto-Lei n.º 275-A/2000, de 9 de Novembro, que aprova a Lei Orgânica da Polícia Judiciária, alterado pela Lei n.º 103/2001, de 25 de Agosto, e pelos Decreto-Lei n.ºs 323/2001, de 17 de Dezembro, 304/2002, de 13 de Dezembro, 43/2003, de 13 de Março, e 235/2005, de 12 de Dezembro.

Artigo 5.º

Recusa de acesso aos dados de localização, de tráfego e de base

A recusa de fornecimento dos dados solicitados nos termos dos artigos anteriores faz incorrer os operadores em crime de desobediência, nos termos previstos na legislação penal.

Artigo 6.º

Acesso aos dados de conteúdo

Ao acesso a dados de conteúdo é aplicável, com as necessárias adaptações, o disposto nos artigos 187.º a 189.º do Código de Processo Penal.

Artigo 7.º

Obrigação de conservação de dados

1 — Os operadores de comunicação são obrigados a conservar, pelo período de um ano, a informação relativa aos dados de localização, de tráfego e de base.

2 — O incumprimento do dever previsto no número anterior constitui contra-ordenação punível com coima de € 2 500 a € 25 000, no caso de pessoas singulares, e de € 5 000 a € 50 000, no caso de pessoas colectivas.

3 — No caso de reincidência, a coima é elevada ao dobro nos seus limites mínimo e máximo.

Artigo 8.º

Fornecedores de serviços de acesso às redes de comunicações

1 — Os fornecedores de serviços de acesso às redes de comunicações, designadamente a todas as que facultem aos utilizadores dos seus serviços a possibilidade de comunicar por meio de tecnologia de informação e comunicação, bem como qualquer outra entidade, pública ou privada, que trate informação, estão sujeitos à obrigação de conservação de dados prevista no artigo anterior.

2 — As entidades a que se refere o número anterior devem identificar os respectivos utilizadores, através de documento legal de identificação, bem como registar o terminal e período de tempo utilizado.

Artigo 9.º

Dever especial de colaboração

1 — Sempre que, no decurso da sua actividade, os operadores de comunicações constatem a prática, através dos seus serviços, dos crimes previstos no n.º 3 do artigo 3.º, são obrigados a comunicá-la às autoridades de polícia criminal ou às autoridades judiciárias.

2 — O dever de colaboração previsto no número anterior implica a obrigação de preservação de toda a informação necessária à identificação dos factos e dos seus autores.

3 — É correspondentemente aplicável ao previsto nos n.os 1 e 2 o disposto nos n.os 2 e 3 do artigo 7.º.

Artigo 10.º

Obrigação de sigilo

1 — Os operadores e os fornecedores de comunicações, bem como os membros dos respectivos órgãos, as pessoas que nelas exerçam funções de direcção, gerência ou chefia, os seus empregados, os mandatários e outras pessoas que lhes prestem serviço a

título permanente ou ocasional não podem revelar ao cliente ou a terceiros a comunicação de informações nos termos dos artigos anteriores, nem que se encontra em curso uma investigação criminal.

2 — As informações prestadas de boa fé não constituem violação de qualquer dever de segredo, nem implicam, para quem as preste, responsabilidade de qualquer tipo.

Artigo 11.º

Negligência e tentativa

São puníveis a negligência e a tentativa na prática das contra-ordenações previstas no presente diploma.

Artigo 12.º

Sanções acessórias

1 — Às contra-ordenações previstas nos artigos anteriores são aplicáveis, em função da sua gravidade e da culpa do agente, as sanções acessórias previstas nas alíneas b), c), f) e g) do n.º 1 do artigo 21.º do Decreto-Lei n.º 433/82, de 27 de Outubro, que institui o regime do ilícito de mera ordenação social, alterado pelos Decretos-Lei n.º 356/89, de 17 de Outubro, n.º 244/95, de 14 de Setembro, n.º 323/2001, de 17 de Dezembro, e pela Lei n.º 109/2001, de 24 de Dezembro, aplicando-se igualmente o disposto no n.º 2 do mesmo artigo.

2 — Pode ser dada publicidade adequada à aplicação de sanção acessória prevista no número anterior.

Artigo 13.º

Processamento e aplicação das coimas e sanções acessórias

1 — A aplicação das coimas e sanções acessórias previstas na presente lei compete ao ICP - Autoridade Nacional de Comunicações (ICP-ANACOM).

2 — A instauração e instrução do processo de contra-ordenação é da competência da mesma autoridade.

3 — Do montante das coimas aplicadas, 70% reverte para o Estado e 30% para o ICP-ANACOM.

Artigo 14.º

Entrada em vigor

A presente lei entra em vigor trinta dias após a sua publicação.

Palácio de S. Bento, de Março de 2006

Os Deputados do PSD,