PROPOSTA DE LEI N.º 161/X

Exposição de Motivos

A protecção dos dados pessoais, da reserva da intimidade da vida privada, da correspondência e das telecomunicações assume uma relevância reconhecida no contexto da salvaguarda dos direitos fundamentais, tanto no plano interno dos Estados membros da União Europeia, como no plano comunitário.

Numa conjuntura em que as fronteiras entre o material e o virtual há muito se esbateram e em que as pessoas e as organizações actuam com uma agilidade crescente no domínio informático e das telecomunicações, também é reconhecido que as novas tecnologias consubstanciam uma ferramenta susceptível de ser utilizada para fins ilícitos contra a qual a comunidade e os Estados não podem deixar de se apetrechar.

A necessidade de dotar os Estados membros da União Europeia de instrumentos eficazes de combate à criminalidade e ao terrorismo levou as instâncias comunitárias a optar pela harmonização dos quadros jurídicos aplicáveis nesta matéria, através da criação da obrigação de conservação de certos dados referentes a comunicações, por parte dos fornecedores de serviços de comunicações electrónicas publicamente disponíveis ou de uma rede pública de comunicações, através da Directiva n.º 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de Maio de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações, que altera a Directiva n.º 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de Julho de 2002.

O principal objectivo desta directiva foi, pois, o de obrigar os fornecedores de serviços de comunicações electrónicas publicamente disponíveis ou de uma rede pública de comunicações a conservar um conjunto de dados definidos nessa directiva, por forma a que possam ser acedidos para fins de combate à criminalidade grave. Não está em causa a conservação dos dados relativos ao conteúdo das comunicações, mas antes os denominados «dados de tráfego e de localização», ou seja, dados necessários para, por exemplo, encontrar a fonte de uma comunicação, a data, hora e duração da mesma ou a localização do equipamento de comunicação móvel utilizado.

A presente proposta de lei visa a transposição da Directiva referida. Assim, os fornecedores de serviços de comunicações electrónicas publicamente disponíveis ou de uma rede pública de comunicações passam a estar obrigados a conservar certos dados de comunicação especificamente definidos, para que possam ser acedidos pelas autoridades competentes, exclusivamente para fins de investigação, detecção e repressão de crimes graves.

A presente proposta de lei reconhece a sensibilidade dos valores em presença e da conservação dos dados em causa. Por essa razão, são adoptadas especiais restrições, cautelas e medidas de segurança em sede de acesso e tratamento dos dados e de supervisão e fiscalização do cumprimento das obrigações aqui previstas.

Assim, em primeiro lugar, a conservação dos dados apenas poderá ter por finalidade a investigação, detecção e repressão criminal, estando expressamente vedada a utilização dos mesmos para outros fins.

Em segundo lugar, o acesso aos dados apenas pode ser solicitado pelo Ministério Público ou por certas autoridades de polícia criminal e depende sempre da decisão do juiz.

Em terceiro lugar, o acesso aos dados encontra ainda duas importantes limitações. Por um lado, apenas é admitido para a investigação, repressão ou detecção de crimes graves, ou seja, daqueles em que, nos termos da legislação processual penal, é possível a intercepção e a gravação do conteúdo das comunicações. Por outro lado, o acesso aos dados é limitado ao adequado, necessário e proporcional face ao caso concreto.

Em quarto lugar, os dados em causa não podem ser conservados eternamente. Estabelece-se que o período de conservação é de um ano, que corresponde a metade do período de conservação máximo permitido pela directiva que agora se transpõe.

Em quinto lugar, as pessoas que, no âmbito dos fornecedores de serviços de comunicações electrónicas publicamente disponíveis ou de uma rede pública de comunicações, devam desempenhar tarefas associadas ao cumprimento das obrigações previstas nesta proposta devem estar especialmente autorizadas e registadas junto da Comissão Nacional de Protecção de Dados (CNPD).

Em sexto lugar, adoptam-se regras exigentes em matéria de destruição dos dados conservados, assegurando-se que a sua utilização não excede os fins estritos de investigação, detecção e repressão de crimes graves para os quais foram conservados.

Finalmente, é cometida a uma entidade administrativa independente - a CNPD - a função de fiscalização do cumprimento da presente proposta de Lei. Assim, cabe nomeadamente a esta entidade elaborar um registo da extracção dos dados transmitidos e a aplicação de coimas pelo incumprimento das regras estabelecidas.
Foram ouvidos o Conselho Superior da Magistratura, o Conselho Superior do Ministério Público, a Ordem dos Advogados, a Comissão Nacional de Protecção de Dados e o Instituto de Comunicações de Portugal - Autoridade Nacional das Comunicações.

Assim:
Nos termos da alínea *d)* do n.º 1 do artigo 197.º da Constituição, o Governo apresenta à Assembleia da República a seguinte proposta de lei:

Artigo 1.º

Objecto

1 – A presente lei regula a conservação e a transmissão dos dados de tráfego e de localização relativos a pessoas singulares e a pessoas colectivas, bem como dos dados conexos necessários para identificar o assinante ou o utilizador registado, para fins de investigação, detecção e repressão de crimes graves por parte das autoridades competentes, transpondo para a ordem jurídica interna a Directiva n.º 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de Março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Directiva n.º 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de Junho de 2002, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas.
2 – A conservação de dados que revelem o conteúdo das comunicações é proibida, sem prejuízo do disposto na Lei n.º 41/2004, de 18 de Agosto, e na legislação processual penal relativamente à intercepção e gravação de comunicações.

Artigo 2.º

Definições

1 – Para efeitos da presente lei, entende-se por:

a) «Dados», os dados de tráfego e os dados de localização, bem como os dados conexos necessários para identificar o assinante ou o utilizador;

b) «Serviço telefónico», qualquer dos seguintes serviços:

i) Os serviços de chamada, incluindo as chamadas vocais, o correio vocal, a teleconferência ou a transmissão de dados;

ii) Os serviços suplementares, incluindo o reencaminhamento e a transferência de chamadas; e

iii) Os serviços de mensagens e multimédia, incluindo os serviços de mensagens curtas (SMS), os serviços de mensagens melhoradas (EMS) e os serviços multimédia (MMS).

c) «Código de identificação do utilizador» («*user ID*»), um código único atribuído às pessoas, quando estas se tornam assinantes ou se inscrevem num serviço de acesso à *Internet*, ou num serviço de comunicação pela *Internet*;

d) «Identificador de célula» («*cell ID*»), a identificação da célula de origem e de destino de uma chamada telefónica numa rede móvel;

e) «Chamada telefónica falhada», uma comunicação em que a ligação telefónica foi estabelecida, mas que não obteve resposta, ou em que houve uma intervenção do gestor da rede;

f) «Autoridades competentes» as autoridades judiciárias e as autoridades de polícia criminal das seguintes entidades:

i) A Polícia Judiciária;

ii) A Guarda Nacional Republicana;

iii) A Polícia de Segurança Pública;

iv) A Polícia Judiciária Militar;

v) O Serviço de Estrangeiros e Fronteiras;

vi) A Polícia Marítima;

vii) A Inspecção-Geral do Ambiente e do Ordenamento do Território (IGAOT) e as entidades que, nos termos das normas aplicáveis, sejam competentes para a investigação, nas Regiões Autónomas, de crimes em matérias de incidência ambiental qualificados, nos termos da presente lei, como crimes graves;

viii) Os órgãos da administração tributária;

ix) Os órgãos da administração da segurança social.

g) «Crime grave», os crimes relativamente aos quais a legislação processual penal admita a intercepção e a gravação de conversações ou comunicações.

2 – Para efeitos da presente lei, são aplicáveis, sem prejuízo do disposto no número anterior, as definições constantes da Lei n.º 67/98, de 26 de Outubro, e da Lei n.º 41/2004, de 18 de Agosto.

Artigo 3.º

Finalidade do tratamento

1 – A conservação e a transmissão dos dados têm por finalidade exclusiva a investigação, detecção e repressão de crimes graves por parte das autoridades competentes.

2 – A transmissão dos dados às autoridades competentes só pode ser ordenada ou autorizada por despacho fundamentado do juiz, nos termos do artigo 9.º

3 – O titular dos dados não pode opor-se à respectiva conservação e transmissão.

Artigo 4.º

Categorias de dados a conservar

1 – Os fornecedores de serviços de comunicações electrónicas publicamente disponíveis ou de uma rede pública de comunicações devem conservar as seguintes categorias de dados:

a) Dados necessários para encontrar e identificar a fonte de uma comunicação;

b) Dados necessários para encontrar e identificar o destino de uma comunicação;

c) Dados necessários para identificar a data, a hora e a duração de uma comunicação;

d) Dados necessários para identificar o tipo de comunicação;

e) Dados necessários para identificar o equipamento de telecomunicações dos utilizadores, ou o que se considera ser o seu equipamento;

f) Dados necessários para identificar a localização do equipamento de comunicação móvel.

2 – Para os efeitos do disposto na alínea *a)* do número anterior, os dados necessários para encontrar e identificar a fonte de uma comunicação são os seguintes:

a) No que diz respeito às comunicações telefónicas nas redes fixa e móvel:

i) O número de telefone de origem;

ii) O nome e endereço do assinante ou do utilizador registado.

b) No que diz respeito ao acesso à *Internet*, ao correio electrónico através da *Internet* e às comunicações telefónicas através da *Internet*:

i) Os códigos de identificação atribuídos ao utilizador;

ii) O código de identificação do utilizador e o número de telefone atribuídos a qualquer comunicação que entre na rede telefónica pública;

iii) O nome e o endereço do assinante ou do utilizador registado, a quem o endereço do protocolo IP, o código de identificação de utilizador, ou o número de telefone estavam atribuídos no momento da comunicação.

3 – Para os efeitos do disposto na alínea *b)* do n.º 1, os dados necessários para encontrar e identificar o destino de uma comunicação são os seguintes:

a) No que diz respeito às comunicações telefónicas nas redes fixa e móvel:

i) Os números marcados e, em casos que envolvam serviços suplementares, como o reencaminhamento ou a transferência de chamadas, o número ou números para onde a chamada foi reencaminhada;

ii) O nome e o endereço do assinante, ou do utilizador registado.

b) No que diz respeito ao correio electrónico através da *Internet* e às comunicações telefónicas através da *Internet*:

i) O código de identificação do utilizador ou o número de telefone do destinatário pretendido, ou de uma comunicação telefónica através da *Internet*;

ii) Os nomes e os endereços dos subscritores, ou dos utilizadores registados, e o código de identificação de utilizador do destinatário pretendido da comunicação.

4 – Para os efeitos do disposto na alínea *c)* do n.º 1, os dados necessários para identificar a data, a hora e a duração de uma comunicação são os seguintes:

a) No que diz respeito às comunicações telefónicas nas redes fixa e móvel, a data e a hora do início e do fim da comunicação;

b) No que diz respeito ao acesso à *Internet*, ao correio electrónico através da *Internet* e às comunicações telefónicas através da *Internet*:

i) A data e a hora do início (*log-in*) e do fim (*log-off*) da ligação ao serviço de acesso à *Internet* com base em determinado fuso horário, juntamente com o endereço do protocolo IP, dinâmico ou estático, atribuído pelo fornecedor do serviço de acesso à *Internet* a uma comunicação, bem como o código de identificação de utilizador do subscritor ou do utilizador registado;

ii) A data e a hora do início e do fim da ligação ao serviço de correio electrónico através da *Internet* ou de comunicações através da *Internet*, com base em determinado fuso horário.

5 – Para os efeitos do disposto na alínea *d)* do n.º 1, os dados necessários para identificar o tipo de comunicação são os seguintes:

a) No que diz respeito às comunicações telefónicas nas redes fixa e móvel, o serviço telefónico utilizado;

b) No que diz respeito ao correio electrónico através da *Internet* e às comunicações telefónicas através da *Internet*, o serviço de *Internet* utilizado.

6 – Para os efeitos do disposto na alínea *e)* do n.º 1, os dados necessários para identificar o equipamento de telecomunicações dos utilizadores, ou o que se considera ser o seu equipamento são os seguintes:

a) No que diz respeito às comunicações telefónicas na rede fixa, os números de telefone de origem e de destino;

b) No que diz respeito às comunicações telefónicas na rede móvel:

i) Os números de telefone de origem e de destino;

ii) A Identidade Internacional de Assinante Móvel (*International Mobile Subscriber Identity*, ou IMSI) de quem telefona;

iii) A Identidade Internacional do Equipamento Móvel (*International Mobile Equipment Identity*, ou IMEI) de quem telefona;

iv) A IMSI do destinatário do telefonema;

v) A IMEI do destinatário do telefonema;

vi) No caso dos serviços pré-pagos de carácter anónimo, a data e a hora da activação inicial do serviço e o identificador da célula a partir da qual o serviço foi activado.

c) No que diz respeito ao acesso à *Internet*, ao correio electrónico através da *Internet* e às comunicações telefónicas através da *Internet*:

i) O número de telefone que solicita o acesso por linha telefónica;

ii) A linha de assinante digital (*digital subscriber line*, ou DSL), ou qualquer outro identificador terminal do autor da comunicação.

7 – Para os efeitos do disposto na alínea *f)* do n.º 1, os dados necessários para identificar a localização do equipamento de comunicação móvel são os seguintes:

a) O identificador da célula no início da comunicação;

b) Os dados que identifiquem a situação geográfica das células, tomando como referência os respectivos identificadores de célula durante o período em que se procede à conservação de dados.

Artigo 5.º

Âmbito da obrigação de conservação dos dados

1 – Os dados telefónicos e da *Internet* relativos a chamadas telefónicas falhadas devem ser conservados quando sejam gerados ou tratados e armazenados pelas entidades referidas no n.º 1 do artigo 4.º, no contexto da oferta de serviços de comunicação.

2 – Os dados relativos a chamadas não estabelecidas não são conservados.

Artigo 6.º

Período de conservação

As entidades referidas no n.º 1 do artigo 4.º devem conservar os dados previstos no mesmo artigo pelo período de um ano a contar da data da conclusão da comunicação.

Artigo 7.º

Protecção e segurança dos dados

1 – As entidades referidas no n.º 1 do artigo 4.º devem:

a) Conservar os dados referentes às categorias previstas no artigo 4.º por forma a que possam ser transmitidos imediatamente, mediante despacho fundamentado do juiz, às autoridades competentes;

b) Garantir que os dados conservados sejam da mesma qualidade e estejam sujeitos à mesma protecção e segurança que os dados na rede;

c) Tomar as medidas técnicas e organizativas adequadas à protecção dos dados previstos no artigo 4.º contra a destruição acidental ou ilícita, a perda ou a alteração acidental e o armazenamento, tratamento, acesso ou divulgação não autorizado ou ilícito;

d) Tomar as medidas técnicas e organizativas adequadas para garantir que apenas pessoas especialmente autorizadas tenham acesso aos dados referentes às categorias previstas no artigo 4.º;

e) Destruir os dados no final do período de conservação, excepto os dados que tenham sido facultados e preservados;

f) Destruir os dados que tenham sido facultados e preservados, quando tal lhe seja determinado pelo juiz.

2 – Os dados referentes às categorias previstas no artigo 4.º devem permanecer bloqueados desde o início da sua conservação, só sendo alvo de desbloqueio para efeitos de transmissão, nos termos da presente lei, às autoridades competentes.

3 – São fixadas, em portaria conjunta dos membros do Governo responsáveis pelas áreas da administração interna, da justiça e das comunicações, as condições técnicas relativas à protecção e segurança dos dados.

4 – O disposto nos números anteriores não prejudica a observação dos princípios nem o cumprimento das regras relativos à qualidade e à salvaguarda da confidencialidade e da segurança dos dados, previstos na Lei n.º 67/98, de 26 de Outubro, e na Lei n.º 41/2004, de 18 de Agosto.

5 – A autoridade pública competente para o controlo da aplicação do disposto no presente artigo é a Comissão Nacional de Protecção de Dados (CNPD).

Artigo 8.º

Registo de pessoas especialmente autorizadas

1 – A CNPD deve manter um registo electrónico permanentemente actualizado das pessoas especialmente autorizadas a aceder aos dados, nos termos da alínea *d)* do n.º 1 do artigo anterior.

2 – Para os efeitos previstos no número anterior, os fornecedores de serviços de comunicações electrónicas ou de uma rede pública de comunicações devem remeter à CNPD, por via exclusivamente electrónica, os dados necessários à identificação das pessoas especialmente autorizadas a aceder aos dados.

Artigo 9.º

Transmissão dos dados

1 – A transmissão dos dados referentes às categorias previstas no artigo 4.º só pode ser autorizada, por despacho fundamentado do juiz, quanto tal se mostre necessário à investigação, detecção e repressão de crimes graves.

2 – A autorização prevista no número anterior só pode ser requerida pelo Ministério Público ou pela autoridade de polícia criminal competente.

3 – Só pode ser autorizada a transmissão de dados relativos:

a) Ao suspeito ou arguido;

b) A pessoa que sirva de intermediário, relativamente à qual haja fundadas razões para crer que recebe ou transmite mensagens destinadas ou provenientes de suspeito ou arguido; ou

c) A vítima de crime, mediante o respectivo consentimento, efectivo ou presumido.

4 – A decisão judicial de transmitir os dados deve respeitar os princípios da adequação, necessidade e proporcionalidade, designadamente no que se refere à definição das categorias de dados a transmitir e das autoridades competentes com acesso aos dados.

5 – O disposto nos números anteriores não prejudica a obtenção de dados sobre a localização celular necessários para afastar perigo para a vida ou de ofensa à integridade física grave, nos termos do artigo 252.º-A do Código de Processo Penal.

6 – As entidades referidas no n.º 1 do artigo 4.º devem elaborar registos da extracção dos dados transmitidos às autoridades competentes e enviá-los à CNPD.

Artigo 10.º

Condições técnicas da transmissão dos dados

A transmissão dos dados referentes às categorias previstas no artigo 4.º processa-se mediante comunicação electrónica, nos termos das condições técnicas e de segurança fixadas em portaria conjunta dos membros do Governo responsáveis pelas áreas da administração interna, da justiça e das comunicações.

Artigo 11.º

Destruição dos dados

1 – O juiz determina, oficiosamente ou a requerimento de qualquer interessado, a destruição dos dados na posse das autoridades competentes, bem como dos dados facultados e preservados pelas entidades referidas no n.º 1 do artigo 4.º, logo que os mesmos deixem de ser estritamente necessários para o fim a que se destinam.

2 – Considera-se que os dados deixam de ser estritamente necessários para o fim a que se destinam logo que ocorra uma das seguintes circunstâncias:

a) Arquivamento definitivo do processo penal;

b) Absolvição, transitada em julgado;

c) Condenação, transitada em julgado;

d) Prescrição do procedimento penal;

e) Amnistia.

Artigo 12.º

Contra-ordenações

1 – Sem prejuízo da responsabilidade criminal a que haja lugar nos termos da lei, constitui contra-ordenação:

a) A não conservação das categorias dos dados previstas no artigo 4.º;

b) O incumprimento do prazo de conservação previsto no artigo 6.º;

c) A não transmissão dos dados às autoridades competentes, quando autorizada nos termos do disposto no artigo 9.º;

d) O incumprimento de qualquer das regras relativas à protecção e à segurança dos dados previstas no artigo 7.º;

e) O não bloqueio dos dados, nos termos previstos no n.º 2 do artigo 7.º;

f) O acesso aos dados por pessoa não especialmente autorizada nos termos do n.º 1 do artigo 8.º;

g) O não envio dos dados necessários à identificação das pessoas especialmente autorizadas, nos termos do n.º 2 do artigo 8.º

2 – As contra-ordenações previstas no número anterior são puníveis com coimas de € 1500 a € 25 000 ou de € 5000 a € 5 000 000 consoante o agente seja uma pessoa singular ou colectiva.

3 – A tentativa e a negligência são puníveis.

Artigo 13.º

Processos de contra-ordenação e aplicação das coimas

1 – Compete à CNPD a instrução dos processos de contra-ordenação e a respectiva aplicação de coimas relativas às condutas previstas no artigo anterior.

2 – O montante das importâncias cobradas, em resultado da aplicação das coimas é distribuído da seguinte forma:

a) 60% para o Estado;

b) 40% para a CNPD.

Artigo 14.º

Aplicabilidade dos regimes sancionatórios previstos na Lei n.º 67/98, de 26 de Outubro, e na Lei n.º 41/2004, de 18 de Agosto

O disposto nos artigos 12.º e 13.º não prejudica a aplicação do disposto no Capítulo VI da Lei n.º 67/98, de 26 de Outubro, e no Capítulo III da Lei n.º 41/2004, de 18 de Agosto.

Artigo 15.º

Estatísticas para informação anual à Comissão das Comunidades Europeias

1 – A CNPD transmite anualmente à Comissão das Comunidades Europeias as estatísticas sobre a conservação dos dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de uma rede pública de comunicações.

2 – Tendo em vista o cumprimento do disposto no número anterior, as entidades referidas no n.º 1 do artigo 4.º devem, até 1 de Março de cada ano, remeter à CNPD as seguintes informações, relativas ao ano civil anterior:

a) O número de casos em que foram transmitidas informações às autoridades nacionais competentes;

b) O período de tempo decorrido entre a data a partir da qual os dados foram conservados e a data em que as autoridades competentes solicitaram a sua transmissão; e

c) O número de casos em que as solicitações das autoridades não puderam ser satisfeitas.

3 – As informações previstas no número anterior não podem conter quaisquer dados pessoais.

Artigo 16.º

Entrada em vigor

A presente lei entra em vigor no dia seguinte ao da sua publicação.

Vista e aprovada em Conselho de Ministros de 6 de Setembro de 2007

O Primeiro-Ministro

O Ministro da Presidência

O Ministro dos Assuntos Parlamentares