PROJECTO DE LEI N.º 367/X

REGIME JURÍDICO DA OBTENÇÃO DE PROVA DIGITAL ELECTRÓNICA NA INTERNET

Exposição de motivos

1 — A utilização massiva e generalizada dos sistemas informáticos, potenciada pelo crescente aumento das capacidades de armazenamento e processamento dos computadores, pela fusão do processo de informação com as novas tecnologias de comunicação e pela fácil transmissão, em segundos ou minutos, dos dados criados, processados ou armazenados, não só permitiu a mutação das práticas tradicionais do crime, como também originou novos tipos de criminalidade (os chamados crimes virtuais puros e crimes virtuais mistos).

Seja da manipulação fraudulenta de dados com intuito lucrativo que estejamos a falar, seja da utilização indevida de informação contida em arquivos ou suportes informáticos alheios, designadamente a falsidade informática e acesso ilegítimo, seja de qualquer outra utilização possível das tecnologias de informação e comunicação como instrumento de trabalho ilícito e fonte inesgotável de mecanismos que facilitam as actividades criminosas, não é difícil chegar à conclusão que ainda há um longo caminho a percorrer, no sentido de se dotar a investigação criminal das condições necessárias a um combate profícuo a esta criminalidade que se dotou de novos meios.

Torna-se necessário, portanto, dotar as autoridades de novos métodos de investigação, proporcionando-lhes o acesso a informação relevante dentro dos parâmetros impostos pelo direito à reserva da intimidade da vida privada e familiar e pelo sigilo das telecomunicações.

2 — A Internet constitui, de facto um instrumento privilegiado de redes internacionais organizadas para a prática de crimes como o comércio de armas, o tráfico de droga, o terrorismo e o branqueamento de capitais, mas, também, de difusão de conteúdos que atingem outro tipo de valores, associados à subsistência e à liberdade da própria humanidade, como são os casos do incitamento ao ódio e à violência racial ou religiosa ou de exploração sexual de crianças e adolescentes.

Cada vez mais a Internet vem servindo de palco, meio e fonte de inspiração de desvios comportamentais especialmente danosos, como, por exemplo, a pedofilia, e, simultaneamente, de realização de um variado número de negócios relacionados com esses actos, tudo a coberto da ocultação da identidade dos diversos intervenientes.

É, pois, crucial o acesso urgente, por parte das autoridades, à informação necessária e suficiente para a investigação criminal, proporcionando-lhes a forma de acederem, em tempo útil, à informação disponível nas operadoras de comunicações que permita a identificação dos autores e o registo dos actos ilícitos praticados através dos meios informáticos e de comunicações.

3 — 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.

Está em causa o tratamento de dados pessoais com vista à respectiva protecção, bem como a protecção da privacidade no sector das comunicações electrónicas. Mas o que importa não esquecer é que a reserva da intimidade da vida privada e familiar e o sigilo das comunicações não são os únicos valores que, nestes domínios, importa ao Estado de direito salvaguardar: a par deles, e porque contendem com os seus padrões éticos e com a liberdade e autodeterminação dos seres humanos, avultam outros tão ou mais importantes e que podem igualmente ser postergados pelo uso indevido das telecomunicações e pela falta de prevenção do uso ilícito dos meios electrónicos, tarefa da qual as operadoras devem partilhar por natureza e necessidade.

4 — 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.

Daí que se estabeleça a obrigação para os operadores de comunicações (ISP, GSM, Rede Fixa, SVA e outros) da manutenção e conservação dos registos durante um ano, período que se considerou adequado ao desenvolvimento da reacção da justiça, em caso de ilícito. Esta obrigação abrange não só os dados de tráfego, como também os chamados dados de base, estes igualmente por motivos de cooperação internacional.

De igual modo, parece útil acautelar junto dos operadores a salvaguarda de determinadas comunicações, mediante solicitação das autoridades de polícia criminal, sem prejuízo da intervenção posterior da autoridade judiciária.

Adoptou-se, nesta matéria, 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.

Deste modo, a recolha de prova para efeitos de investigação criminal será feita:

— Pelas autoridades de polícia criminal (com o alcance previsto pela alínea d) do artigo 1.º do Código de Processo Penal) no que concerne à informação a colher junto das operadoras relativamente a dados de tráfego;
— Pelas autoridades de polícia criminal e (ou) pelas autoridades judiciárias competentes, e consoante o respectivo acesso seja ou não público, quanto à dos dados de base; e
— Com a aplicação do regime previsto nos artigos 188.º e 189.º do Código do Processo Penal, em relação aos dados de conteúdo.

Propugna-se igualmente a utilização dos mesmos meios de obtenção de prova quanto aos chamados crimes comuns cometidos com recurso a meios informáticos, dada a salvaguarda de apreciação judicial individualizada.

5 — 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.

Nestes termos, os Deputados abaixo assinados apresentam o seguinte projecto de lei:

Artigo 1.º

(Definições)

Para os efeitos da presente lei, considera-se:

a) 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, o tamanho, a duração ou o tipo do serviço subjacente;

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

c) Dados de conteúdo: os dados relativos ao conteúdo da comunicação ou de uma mensagem.

Artigo 2.º

(Do acesso aos dados de tráfego)

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, sempre que estes lhes sejam por elas solicitados, no prazo máximo de cinco dias.

Artigo 3.º

(Do acesso aos dados de base)

1 — O disposto no artigo anterior é aplicável aos 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.

3 — No caso de dados de base sujeitos a esse regime, o pedido para o seu fornecimento incumbe a autoridade judiciária titular da direcção do processo, em despacho fundamentado, sem prejuízo da delegação genérica de 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 29 de Novembro.

Artigo 4.º

(Da recusa injustificada de acesso aos dados de tráfego e de base)

A recusa injustificada de fornecimento dos dados solicitados nos termos dos artigos anteriores faz incorrer os operadores em crime de desobediência qualificada.

Artigo 5.º

(Do acesso aos dados de conteúdo)

Ao acesso aos dados de conteúdo é aplicável, independentemente da natureza e da gravidade da infracção, o preceituado nos artigos 188.º e 189.º do Código de Processo Penal.

Artigo 6.º

(Da obrigação de preservação de dados)

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

2 — Sem prejuízo do disposto no artigo 5.º, e até à intervenção judicial, impende sobre os operadores de comunicações o dever de preservação de uma comunicação, mediante solicitação concreta da autoridade de polícia criminal.
3 — O incumprimento dos deveres previstos nos n.os 1 e 2 constitui contra-ordenação punível com coima de 2 500 a 25 000 euros, no caso de pessoas singulares, e de 5 000 a 50 000 euros, no caso de pessoas colectivas.
4 — No caso de reincidência, a coima é elevada ao dobro nos seus limites mínimo e máximo.

Artigo 7.º

(Dos fornecedores de serviços de acesso às redes de comunicações)

1 — Os fornecedores de serviços de acesso às redes de comunicações, designadamente todas as que facultem aos utilizadores dos seus serviços a possibilidade de comunicar por meio de uma tecnologia de informação e comunicação, bem como qualquer outra entidade, pública ou privada, que processe ou armazene informação, devem identificar os respectivos utilizadores, através de documento legal de identificação, bem como registar o terminal e período de tempo utilizado.
2 — É aplicável o disposto nos n.os 1 a 4 do artigo anterior.

Artigo 8.º

(Dever especial de colaboração)

1 — Sempre que, no decurso da sua actividade, os operadores de comunicações constatem, através da utilização dos seus serviços, condutas que sejam passíveis de integrar a prática, com carácter de habitualidade, dos crimes previstos nos artigos 172.º, n.º 3, alíneas a) a d), e n.º 4, 173,º, n.º 2, e 240.º do Código Penal são obrigados a comunicá-las às autoridades de polícia criminal ou às autoridades judiciárias, no prazo máximo de cinco dias.
2 — O dever de colaboração previsto no número anterior implica a obrigação de preservação de toda a informação adequada à identificação dos factos e dos seus autores.
3 — À prestação das informações previstas neste diploma é aplicável o disposto nos artigos 10.º, n.º 4, e 13.º do Decreto-Lei n.º 313/93, de 15 de Setembro.

4 — É aplicável o disposto nos n.os 3 e 4 do artigo 6.º.

Artigo 9.º

(Negligência e tentativa)

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

Artigo 10.º

(Sanções acessórias)

Às contra-ordenações previstas nos artigos anteriores são aplicáveis, em função da sua gravidade e da culpa do agente, as sanções acessórias do artigo 21.º, alíneas b) c) f) e g), do Decreto-Lei n.º 433/82, de 27 de Outubro, sem prejuízo do disposto nos nºs 2 e 3 do mesmo artigo.

Artigo 11.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% revertem para o Estado e 30% para a ANC.

Artigo 12.º

Entrada em vigor

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

Palácio de S. Bento, 7 de Março de 2007

Os Deputados,