MINISTÉRIO PÚBLICO
PORTUGAL
EM DEFESA DA LEGALIDADE DEMOCRÁTICA
gabinete CIBERCRIME

NOTA PRÁTICA nº8/2016
18 de Fevereiro de 2016

Pedido de dados a operadores de comunicações

Pretende-se com esta nota prática, sumariamente, descrever as informações guardadas por operadores de comunicações (telefónicas e Internet), que podem vir a ser usadas em investigações criminais, bem como referenciar os fundamentos jurídicos que delimitam os pedidos dessas informações.

1. Dados em posse dos operadores

Em concretas investigações criminais, é cada vez mais frequente ser necessário obter informações de operadores de comunicações – sobretudo, referentes à identificação de quem efetuou uma determinada comunicação.

Os operadores de comunicações guardam informação:

- respeitante à identificação dos seus clientes (nome, morada, etc. - tradicionalmente conhecida como *dados de base*) e
- respeitante às comunicações efetuados por aqueles – os chamados *dados de tráfego*.

Os operadores não guardam – é proibido fazê-lo[1] –, o conteúdo das concretas comunicações. Obter o conteúdo de comunicações apenas é possível por via da interceção de comunicações, em *tempo real*, nos termos dos Artigos 187º e 188º do Código de Processo Penal e do Artigo 18º da Lei do Cibercrime.

2. Quadro legal

Estão simultaneamente em vigor três diplomas legais que regulam, em sede de processo penal, a obtenção de dados em posse de fornecedores de serviços de comunicações: o Código de Processo Penal (*maxime* o

[1] Por força do nº 2 do Artigo 1º da Lei nº 32/2008, de 17 de Julho, que estipula que "a conservação de dados que revelem o conteúdo das comunicações é proibida" e também do nº 2 do Artigo 4º da Lei nº 41/2004, de 18 de Agosto, que proíbe, foram do contexto processual penal, a *escuta*, *interceção* e *armazenamento de comunicações*. Esta proibição decorria já dos Artigos 32º, nº 8 e 34º, nº 4, da Constituição da República.

nº 2 do Artigo 189º), a Lei nº 32/2008, de 17 de Julho e, finalmente, a Lei do Cibercrime (Lei nº 109/2009, de 15 de Setembro). Porém, nem sempre as respetivas redações são facilmente conjugáveis. Daqui resulta, por um lado, insegurança jurídica na aplicação da lei ao caso concreto. Por outro lado, tratando-se de regras sobre obtenção de prova, estas incertezas criam dúvida sobre a validade dos elementos probatórios eventualmente obtidos.

O Artigo 189º do Código de Processo Penal (que foi introduzido pela alteração de 2007 - Lei nº 48/2007, de 29 de Agosto) regula a obtenção em inquérito, entre outros, "de registos da realização de conversações ou comunicações". Determina que esta diligência probatória siga o regime processual das interceções de comunicações telefónicas.

Por sua vez, a Lei nº 32/2008, regulamenta a chamada conservação de dados de tráfego. Cria a obrigação, para os operadores, de conservarem dados dos seus clientes (entre eles, os de tráfego), pelo prazo de um ano. Instituiu um específico e especialíssimo regime processual de acesso a esses dados que, além do mais, faz depender o acesso aos mesmos de "despacho fundamentado do juiz de instrução, se houver razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter no âmbito da investigação, deteção e repressão de crimes graves" (Artigo 9º, nº 1).

A conciliação destes três regimes não foi expressamente feita pelo legislador, exigindo assim esforço adicional do intérprete. Apenas ficou expressa a necessária convivência, com ambas em vigor, entre a Lei nº 32/2008 e a Lei do Cibercrime. Com efeito, no nº 2 do Artigo 11º da Lei do Cibercrime, determina-se que aquilo que nela se estipula *não prejudica* o regime da Lei nº 32/2008.

3. Dados de tráfego

Por aplicação das regras gerais da sucessão de leis no tempo, tem que concluir-se que o Artigo 189º do Código de Processo Penal foi parcelarmente revogado pela Lei do Cibercrime. Porém, apesar de ter sido substancialmente revogado, para o que agora está causa releva apenas que o trecho referente a *registos da realização de conversações ou comunicações*, incluído no nº 2 do Artigo 189º, se mantém em vigor. De facto, não foi nunca expressamente revogado. Por outro lado, o teor desta disposição não coincide com nenhuma outra, designadamente da Lei do Cibercrime, motivo pelo qual não operou a este específico propósito qualquer revogação tácita. Anote-se que também a Lei nº 32/2008 não produziu, neste aspeto em particular, qualquer revogação tácita, uma vez que, ao contrário do Código de Processo Penal, que é uma lei geral, esta lei de 2008 é especial – apenas se aplica à retenção de dados com a finalidade de investigação de uma gama muito reduzida de crimes.

Ou seja, a obtenção de dados de tráfego ou, no contexto telefónico, da chamada *faturação detalhada*, mantém-se regulada pelo Artigo 189º, nº 2 do Código de Processo Penal. É pois de acordo com este regime

que tem que processar-se a respetiva solicitação, à qual se aplica, por remissão, o regime de autorização das interceções telefónicas, previsto no Artigo 187º do Código de Processo Penal.

Anote-se que esta regulamentação legal não obsta a que, por exemplo no âmbito de uma pesquisa informática a um determinado telemóvel (ou outro dispositivo), se obtenha informação referente a chamadas efetuadas e recebidas. Os dados mencionados no Artigo 189º, nº 2 do Código de Processo Penal são os registos guardados pelos operadores de comunicações e não os registos guardados pelo próprio telemóvel. Assim é porque a tutela constitucional e legal do sigilo das telecomunicações incide apenas sobre a relação de confiança que se estabelece entre o operador e o cliente e não existe quando, de forma legítima, a investigação tem acesso ao aparelho do cliente – por exemplo, por via Artigo 15º da Lei do Cibercrime. Estes casos, em que, por via de acesso legítimo a um telemóvel ou outro dispositivo, se acede a "registos de comunicações", são disciplinados pelo Artigo 17º da Lei do Cibercrime.

4. Dados de identificação dos clientes

Já quanto ao tipo de informação a que a doutrina e a jurisprudência chamam tradicionalmente *dados de base*, está atualmente referida no Artigo 14º da Lei do Cibercrime. Ali se diz que a solicitação aos operadores de comunicações / fornecedores de serviço de "*dados relativos aos seus clientes ou assinantes, neles se incluindo qualquer informação diferente dos dados relativos ao tráfego ou ao conteúdo*" é da competência da autoridade judiciária - o Ministério Público, portanto, no decurso do inquérito.

Neste conjunto de dados está porém incluída informação sobre o concreto endereço de IP utilizado numa determinada comunicação, já identificada na investigação. Ou seja, é igualmente da competência do Ministério Público solicitar aos operadores que indiquem a identidade do seu cliente que, num determinado contexto temporal (dia e hora) utilizou um determinado endereço IP. O mesmo raciocínio é aplicável à situação em que a investigação tem necessidade de saber qual o concreto endereço IP utilizado por um determinado cliente de um operador[2]. Assim, apesar de este tipo de informação ser tecnicamente agrupado na informação referente a tráfego, o regime jurídico da sua obtenção é o mesmo dos chamados *dados de base* (modernamente referidos como *dados relativos aos clientes*) – Artigo 14º, nº 4, alínea b) da Lei do Cibercrime.

Anote-se que os dados aqui em causa terão que ser "*dados informáticos ou sob qualquer outra forma, detida pelo fornecedor de serviços*". Quer isto dizer, por um lado, que esta medida processual não se confunde com a preservação de dados nem com a revelação expedita de dados preservados – a preservação é proactiva e visa a conservação de dados que de outra forma não seriam conservados. Por outro lado, aquela fórmula legal quer dizer que o operador apenas está obrigado a fornecer aqueles dados que efetivamente detenha – e que detenha, naturalmente, dentro dos parâmetros legais.

[2] Sobre este particular aspeto foram emitidas as Notas Práticas 1 e 2, para as quais se remete.

5. Prazo de conservação dos dados

A conclusão que acaba de retirar-se requer, de quem solicita os dados, que conheça as condições e termos nos quais os operadores detêm os dados. Quanto à informação de tráfego (nela se incluindo, como se disse, os respeitantes à identificação do seu cliente que, em dadas circunstâncias temporais, usou um determinado IP), de forma simplificada, pode dizer-se que os operadores guardam os dados de acordo com dois diferentes regimes legais:

- o regime geral, previsto na Lei do Cibercrime, na Lei nº 41/2004 e no Artigo 189º, nº 2 do Código de Processo Penal e
- o regime especial, previsto na Lei nº 32/2008.

6. Regime especial da Lei nº 32/2008

A Lei 32/2008 prevê a obrigação de os operadores de comunicações conservarem dados de tráfego (entre outros) pelo período de um ano. Porém, estipula de forma expressa (Artigo 1º, nº 1), que tal conservação de dados é efetuada "para fins de investigação, deteção e repressão de crimes graves". Esta norma estabelece, de forma taxativa, corroborada pelo nº 1 do Artigo 3º da mesma Lei, que "a conservação e a transmissão dos dados têm por finalidade exclusiva a investigação, deteção e repressão de crimes graves". Por outro lado, o mesmo diploma fixa, no Artigo 2º, nº1, alínea g), que são crimes graves os "crimes de terrorismo, criminalidade violenta, criminalidade altamente organizada[3], sequestro, rapto e tomada de reféns, crimes contra a identidade cultural e integridade pessoal, contra a segurança do Estado, falsificação de moeda ou títulos equiparados a moeda e crimes abrangidos por convenção sobre segurança da navegação aérea ou marítima".

Portanto, em suma, além de vários outros requisitos, apenas podem solicitar-se estes dados, retidos ao abrigo da Lei 32/2008, se estiver em investigação um dos tipos de crime acima referenciados. Tal solicitação deve ser feita por ordem judicial, nos termos do Artigo 3º, nº 2 e do Artigo 9º da Lei nº 32/2008.

7. Regime geral

Fora do contexto da Lei nº 32/2008, não existe qualquer outro prazo específico para guarda de dados de tráfego. Porém, no seu conjunto, o quadro normativo permite aos operadores que conservem tais dados por

[3] Considera-se serem "criminalidade violenta" as condutas que dolosamente se dirigirem contra a vida, a integridade física, a liberdade pessoal, a liberdade e autodeterminação sexual ou a autoridade pública e forem puníveis com pena de prisão de máximo igual ou superior a 5 anos (Artigo 1º, alínea j) do Código de Processo Penal); por outro lado, considera-se serem "criminalidade altamente organizada" as condutas que integrarem crimes de associação criminosa, tráfico de pessoas, tráfico de armas, tráfico de estupefacientes ou de substâncias psicotrópicas, corrupção, tráfico de influência, participação económica em negócio ou branqueamento (Artigo 1º, alínea m) do Código de Processo Penal). Estas definições, consagradas no Código de Processo Penal, na prática, alargam consideravelmente o âmbito de aplicação da Lei nº 32/2008.

seis meses. Ou seja, não se estando no âmbito de investigações de crimes referidos na Lei nº 32/2008, é pois de seis meses o prazo durante o qual os operadores podem dispor desses dados e, reflexamente, é esse o prazo durante o qual dispõem dos mesmos para os fornecer às autoridades de investigação criminal. A motivação jurídica desta conclusão é que a segue.

7.1.

O Artigo 4º, nº 2, da Lei nº 41/2004 estipula a proibição genérica de guarda de dados de tráfego, salvaguardando apenas as exceções determinadas pela própria lei. Esta proibição é corroborada pelo Artigo 6º, nº 1, da mesma Lei, que estipula que, "sem prejuízo do disposto nos números seguintes, os dados de tráfego relativos aos assinantes e utilizadores tratados e armazenados pelas empresas que oferecem redes e ou serviços de comunicações eletrónicas devem ser eliminados ou tornados anónimos quando deixem de ser necessários para efeitos da transmissão da comunicação". Ou seja, o quadro legal vigente determina, como princípio geral, a obrigação de eliminação de dados de tráfego logo que a comunicação terminar. Sublinhe-se que esta disposição não está em conflito com a Lei nº 32/2008, que é posterior e, de forma clara, introduziu exceções adicionais a esta proibição.

7.2.

É o mesmo Artigo 6º da Lei nº 41/2004 que, nos números 2 e 3, introduz exceções a esta proibição do nº 1, estipulando que os dados de tráfego *necessários à faturação dos assinantes e ao pagamento de interligações* podem ser guardados e tratados até ao final do *período durante o qual a fatura pode ser legalmente contestada ou o pagamento reclamado*.

Este diploma não fixa este *período legal*, durante o qual o pagamento pode ser reclamado. Porém, a Lei nº 23/96, de 26 de Julho, diploma legal que define regras respeitantes à prestação de serviços públicos essenciais, já fixava no seu Artigo 10º, nº 1, que "o direito ao recebimento do preço do serviço prestado prescreve no prazo de seis meses após a sua prestação". Esta orientação é corroborada pelo nº 4 do mesmo Artigo 10º, que fixa igualmente em 6 meses o prazo para eventual propositura da ação pelo prestador de serviços. Recorde-se que o regime deste diploma é aplicável aos serviços de comunicações eletrónicas, por força do respetivo Artigo 1º, nº 2, alínea d).

Em suma, estando em causa a prestação de serviços de comunicações eletrónicas, o prazo que o fornecedor de serviço tem para reclamar o respetivo preço é de seis meses. Uma vez decorridos esses seis meses, tem efetiva aplicação a obrigação de eliminação dos dados de tráfego, fixada pelo Artigo 6º, nº 1 da Lei nº 41/2004. É também apenas nessa altura que se torna efetiva a proibição genérica de guarda de dados de tráfego, consagrada no Artigo 4º, nº 2, da mesma lei.

7.3.

Ou seja, por força da lei, depois de decorridos seis meses sobre uma determinada comunicação, os dados de tráfego por ela gerados têm que ser eliminados. Por essa razão, tais dados já não podem ser legalmente detidos pelos fornecedores de serviços.

Entre os dados que a autoridade judiciária está legitimada a solicitar, com fundamento no Artigo 14º, nº 4 da Lei do Cibercrime estão, como se disse, os dados de identificação e localização dos seus clientes – os tradicionalmente chamados *dados de base*. Quanto a estes, a lei não impõe qualquer prazo de guarda ou eliminação.

Esta norma legal, do Artigo 14º, nº 4 da Lei do Cibercrime, é também aquela que fundamenta a obtenção, em inquérito, do endereço de IP utilizado por um determinado cliente de um operador, desde que relacionado com uma concreta investigação. Porém, sendo o endereço de IP agrupado na categoria técnica de informação de tráfego, os operadores apenas o pode conservar por seis meses. Por isso, a autoridade judiciária apenas está legitimada a solicitar os dados referentes a comunicações que tenham ocorrido nos seis meses anteriores ao pedido que é efetuado, uma vez que apenas esses dados podem ser legitimamente detidos pelo fornecedor de serviços.

8. Possibilidade de preservação dos dados

Importa ainda sublinhar que a lei prevê a possibilidade de preservar dados que estejam em risco de "deixar de estar disponíveis" (Artigo 12º, nº 1, da Lei do Cibercrime). Assim, se numa investigação em concreto se aperceber que determinados dados, incluindo dados de tráfego, estiverem em *risco de deixar de estar disponíveis*, é possível ordenar a "quem tenha disponibilidade ou controlo desses dados, designadamente a fornecedor de serviço, que preserve os dados em causa".

Esta possibilidade legal, que é expedita, é particularmente útil quando a investigação se apercebe de que o prazo de conservação de dados está próximo do seu termo. Pode mesmo ser desencadeada por iniciativa de órgão de polícia criminal, "quando haja urgência ou perigo na demora" (Artigo 12º, nº 2 da Lei do Cibercrime).

Anote-se que os dados em causa podem ser preservados por um período máximo de três meses, o qual pode ser renovado por períodos não superiores a três meses, desde que se verifiquem os respetivos requisitos de admissibilidade, até ao limite máximo de um ano (Artigo 12º, nº 3, alínea c) e nº 5 da Lei do Cibercrime).

9. Tabela de sumário

Sumariam-se de seguida os diferentes tipos de dados que é possível solicitar aos operadores. Refere-se o universo de inquéritos (com referência ao tipo de crime em investigação) em que é legítimo solicitar os dados.

Acrescenta-se o prazo durante o qual os dados estão disponíveis, a partir da data da comunicação. Indica-se ainda a autoridade processual competente para solicitar os dados, bem como o respetivo fundamento legal.

Tipo de dados	***Âmbito***	***Prazo***	***Competência***	***Fundamento Legal***
Identificação do cliente	Todos os crimes	Sem prazo	Ministério Público	Artigo 14, nº 4, b) da Lei do Cibercrime
Endereço IP	Todos os crimes	6 meses	Ministério Público	Artigo 14, nº 4, b) da Lei do Cibercrime
Tráfego	Crimes do catálogo do Artigo 187º do CPP	6 meses	Juiz de Instrução	Artigos 187º e 189º, nº 2 do CPP
Tráfego	Crimes do catálogo da Lei nº 32/2008	1 ano	Juiz de Instrução	Artigos 3º, 6 e 9º da Lei nº 32/2008
Conteúdo da comunicação (apenas por interceção em tempo real)	Crimes dos catálogos dos Artigo 187º do CPP e do Artigo 18º da Lei do Cibercrime	(apenas possível para comunicações futuras)	Juiz de Instrução	Artigos 187º e 188º, nº 2 do CPP e Artigo 18º da Lei do Cibercrime

Anexo – Legislação

Código de Processo Penal

Artigo 187º
Admissibilidade

1 - A intercepção e a gravação de conversações ou comunicações telefónicas só podem ser autorizadas durante o inquérito, se houver razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter, por despacho fundamentado do juiz de instrução e mediante requerimento do Ministério Público, quanto a crimes:

a) Puníveis com pena de prisão superior, no seu máximo, a 3 anos;
b) Relativos ao tráfico de estupefacientes;
c) De detenção de arma proibida e de tráfico de armas;
d) De contrabando;
e) De injúria, de ameaça, de coacção, de devassa da vida privada e perturbação da paz e do sossego, quando cometidos através de telefone;
f) De ameaça com prática de crime ou de abuso e simulação de sinais de perigo; ou
g) De evasão, quando o arguido haja sido condenado por algum dos crimes previstos nas alíneas anteriores.

2 - A autorização a que alude o número anterior pode ser solicitada ao juiz dos lugares onde eventualmente se puder efectivar a conversação ou comunicação telefónica ou da sede da entidade competente para a investigação criminal, tratando-se dos seguintes crimes:

a) Terrorismo, criminalidade violenta ou altamente organizada;
b) Sequestro, rapto e tomada de reféns;
c) Contra a identidade cultural e integridade pessoal, previstos no título iii do livro ii do Código Penal e previstos na Lei Penal Relativa às Violações do Direito Internacional Humanitário;
d) Contra a segurança do Estado previstos no capítulo i do título v do livro ii do Código Penal;
e) Falsificação de moeda ou títulos equiparados a moeda prevista nos artigos 262º, 264º, na parte em que remete para o artigo 262º, e 267º, na parte em que remete para os artigos 262º e 264º, do Código Penal;
f) Abrangidos por convenção sobre segurança da navegação aérea ou marítima.

3 - Nos casos previstos no número anterior, a autorização é levada, no prazo máximo de setenta e duas horas, ao conhecimento do juiz do processo, a quem cabe praticar os actos jurisdicionais subsequentes.

4 - A intercepção e a gravação previstas nos números anteriores só podem ser autorizadas, independentemente da titularidade do meio de comunicação utilizado, contra:

a) Suspeito ou arguido;
b) 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) Vítima de crime, mediante o respectivo consentimento, efectivo ou presumido.

5 - É proibida a intercepção e a gravação de conversações ou comunicações entre o arguido e o seu defensor, salvo se o juiz tiver fundadas razões para crer que elas constituem objecto ou elemento de crime.

6 - A intercepção e a gravação de conversações ou comunicações são autorizadas pelo prazo máximo de três meses, renovável por períodos sujeitos ao mesmo limite, desde que se verifiquem os respectivos requisitos de admissibilidade.

7 - Sem prejuízo do disposto no artigo 248º, a gravação de conversações ou comunicações só pode ser utilizada em outro processo, em curso ou a instaurar, se tiver resultado de intercepção de meio de comunicação utilizado por pessoa referida no n.º 4 e na medida em que for indispensável à prova de crime previsto no nº 1.

8 - Nos casos previstos no número anterior, os suportes técnicos das conversações ou comunicações e os despachos que fundamentaram as respectivas intercepções são juntos, mediante despacho do juiz, ao processo em que devam ser usados como meio de prova, sendo extraídas, se necessário, cópias para o efeito.

Artigo 189º
Extensão

1 - O disposto nos artigos 187º e 188º é correspondentemente aplicável às conversações ou comunicações transmitidas por qualquer meio técnico diferente do telefone, designadamente correio electrónico ou outras formas de transmissão de dados por via telemática, mesmo que se encontrem guardadas em suporte digital, e à intercepção das comunicações entre presentes.

2 - A obtenção e junção aos autos de dados sobre a localização celular ou de registos da realização de conversações ou comunicações só podem ser ordenadas ou autorizadas, em qualquer fase do processo, por despacho do juiz, quanto a crimes previstos no nº 1 do artigo 187º e em relação às pessoas referidas no nº 4 do mesmo artigo.

Lei nº 23/96, de 26 de Julho
Lei dos Serviços Públicos

Artigo 1º
Objecto e âmbito

1 - A presente lei consagra regras a que deve obedecer a prestação de serviços públicos essenciais em ordem à protecção do utente.
2 - São os seguintes os serviços públicos abrangidos:
…
d) Serviço de comunicações electrónicas;
…

Artigo 10º
Prescrição e caducidade

1 - O direito ao recebimento do preço do serviço prestado prescreve no prazo de seis meses após a sua prestação.
2 - Se, por qualquer motivo, incluindo o erro do prestador do serviço, tiver sido paga importância inferior à que corresponde ao consumo efectuado, o direito do prestador ao recebimento da diferença caduca dentro de seis meses após aquele pagamento.
3 - A exigência de pagamento por serviços prestados é comunicada ao utente, por escrito, com uma antecedência mínima de 10 dias úteis relativamente à data-limite fixada para efectuar o pagamento.
4 - O prazo para a propositura da acção ou da injunção pelo prestador de serviços é de seis meses, contados após a prestação do serviço ou do pagamento inicial, consoante os casos.
5 - O disposto no presente artigo não se aplica ao fornecimento de energia eléctrica em alta tensão.

Lei nº 41/2004, de 18 de Agosto
Lei da Proteção de Dados Pessoais e Privacidade nas Telecomunicações

Artigo 4º
Inviolabilidade das comunicações eletrónicas

1 - As empresas que oferecem redes e ou serviços de comunicações eletrónicas devem garantir a inviolabilidade das comunicações e respetivos dados de tráfego realizadas através de redes públicas de comunicações e de serviços de comunicações eletrónicas acessíveis ao público.
2 - É proibida a escuta, a instalação de dispositivos de escuta, o armazenamento ou outros meios de interceção ou vigilância de comunicações e dos respetivos dados de tráfego por terceiros sem o consentimento prévio e expresso dos utilizadores, com exceção dos casos previstos na lei.
3 - O disposto no presente artigo não impede as gravações legalmente autorizadas de comunicações e dos respetivos dados de tráfego, quando realizadas no âmbito de práticas comerciais lícitas, para o efeito de prova de uma transação comercial nem de qualquer outra comunicação feita no âmbito de uma relação contratual, desde que o titular dos dados tenha sido disso informado e dado o seu consentimento.
4 - São autorizadas as gravações de comunicações de e para serviços públicos destinados a prover situações de emergência de qualquer natureza.

Artigo 6º
Dados de tráfego

1 - Sem prejuízo do disposto nos números seguintes, os dados de tráfego relativos aos assinantes e utilizadores tratados e armazenados pelas empresas que oferecem redes e ou serviços de comunicações eletrónicas devem ser eliminados ou tornados anónimos quando deixem de ser necessários para efeitos da transmissão da comunicação.
2 - É permitido o tratamento de dados de tráfego necessários à faturação dos assinantes e ao pagamento de interligações, designadamente:
a) Número ou identificação, endereço e tipo de posto do assinante;
b) Número total de unidades a cobrar para o período de contagem, bem como o tipo, hora de início e duração das chamadas efetuadas ou o volume de dados transmitidos;
c) Data da chamada ou serviço e número chamado;
d) Outras informações relativas a pagamentos, tais como pagamentos adiantados, pagamentos a prestações, cortes de ligação e avisos.
3 - O tratamento referido no número anterior apenas é lícito até final do período durante o qual a fatura pode ser legalmente contestada ou o pagamento reclamado.
4 - As empresas que oferecem serviços de comunicações eletrónicas só podem tratar os dados referidos no nº 1 se o assinante ou utilizador a quem os dados digam respeito tiver dado o seu consentimento prévio e expresso, que pode ser retirado a qualquer momento, e apenas na medida do necessário e pelo tempo necessário à comercialização de serviços de comunicações eletrónicas ou à prestação de serviços de valor acrescentado.
5 - Nos casos previstos no nº 2 e, antes de ser obtido o consentimento dos assinantes ou utilizadores, nos casos previstos no n.º 4, as empresas que oferecem serviços de comunicações eletrónicas devem fornecer-lhes informações exatas e completas sobre o tipo de dados que são tratados, os fins e a duração desse tratamento, bem como sobre a sua eventual disponibilização a terceiros para efeitos da prestação de serviços de valor acrescentado.
6 - O tratamento dos dados de tráfego deve ser limitado aos trabalhadores e colaboradores das empresas que oferecem redes e ou serviços de comunicações eletrónicas acessíveis ao público encarregados da faturação ou da gestão do tráfego, das informações a clientes, da deteção de fraudes, da comercialização dos serviços de comunicações eletrónicas acessíveis ao público, ou da prestação de serviços de valor acrescentado, restringindo-se ao necessário para efeitos das referidas atividades.

7 - O disposto nos números anteriores não prejudica o direito de os tribunais e as demais autoridades competentes obterem informações relativas aos dados de tráfego, nos termos da legislação aplicável, com vista à resolução de litígios, em especial daqueles relativos a interligações ou à faturação.

Lei nº 32/2008, de 17 de Julho
Lei da Conservação de Dados Gerados ou Tratados no Contexto de Oferta de Serviços de Comunicações Eletrónicas

Artigo 1º
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 nº 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de Março, 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 nº 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de Junho, 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 nº 41/2004, de 18 de Agosto, e na legislação processual penal relativamente à intercepção e gravação de comunicações.

Artigo 2º
Definições

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

…

g) «Crime grave», crimes de terrorismo, criminalidade violenta, criminalidade altamente organizada, sequestro, rapto e tomada de reféns, crimes contra a identidade cultural e integridade pessoal, contra a segurança do Estado, falsificação de moeda ou títulos equiparados a moeda e crimes abrangidos por convenção sobre segurança da navegação aérea ou marítima.

…

Artigo 3º
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 9º.

3 - Os ficheiros destinados à conservação de dados no âmbito da presente lei têm que, obrigatoriamente, estar separados de quaisquer outros ficheiros para outros fins.

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

Artigo 9º
Transmissão dos dados

1 - A transmissão dos dados referentes às categorias previstas no artigo 4º só pode ser autorizada, por despacho fundamentado do juiz de instrução, se houver razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter no âmbito da 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 e à protecção do segredo profissional, nos termos legalmente previstos.

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 252º-A do Código de Processo Penal.

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

Lei do Cibercrime - Lei nº 109/2009 de 15 de Setembro

Artigo 11º
Âmbito de aplicação das disposições processuais

1 - Com excepção do disposto nos artigos 18º e 19º, as disposições processuais previstas no presente capítulo aplicam-se a processos relativos a crimes:

a) Previstos na presente lei;

b) Cometidos por meio de um sistema informático; ou

c) Em relação aos quais seja necessário proceder à recolha de prova em suporte electrónico.

2 - As disposições processuais previstas no presente capítulo não prejudicam o regime da Lei nº 32/2008, de 17 de Julho.

Artigo 12º
Preservação expedita de dados

1 - Se no decurso do processo for necessário à produção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos armazenados num sistema informático, incluindo dados de tráfego, em relação aos quais haja receio de que possam perder -se, alterar -se ou deixar de estar disponíveis, a autoridade judiciária competente ordena a quem tenha disponibilidade ou controlo desses dados, designadamente a fornecedor de serviço, que preserve os dados em causa.

2 - A preservação pode também ser ordenada pelo órgão de polícia criminal mediante autorização da autoridade judiciária competente ou quando haja urgência ou perigo na demora, devendo aquele, neste último caso, dar notícia imediata do facto à autoridade judiciária e transmitir -lhe o relatório previsto no artigo 253º do Código de Processo Penal.

3 - A ordem de preservação discrimina, sob pena de nulidade:

a) A natureza dos dados;

b) A sua origem e destino, se forem conhecidos; e

c) O período de tempo pelo qual deverão ser preservados,

até um máximo de três meses.

4 - Em cumprimento de ordem de preservação que lhe seja dirigida, quem tenha disponibilidade ou controlo sobre esses dados, designadamente o fornecedor de serviço, preserva de imediato os dados em causa, protegendo e conservando a sua integridade pelo tempo fixado, de modo a permitir à autoridade judiciária competente a sua obtenção, e fica obrigado a assegurar a confidencialidade da aplicação da medida processual.

5 - A autoridade judiciária competente pode ordenar a renovação da medida por períodos sujeitos ao limite previsto na alínea c) do n.º 3, desde que se verifiquem os respectivos requisitos de admissibilidade, até ao limite máximo de um ano.

Artigo 14º
Injunção para apresentação ou concessão do acesso a dados

1 - Se no decurso do processo se tornar necessário à produção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos e determinados, armazenados num determinado sistema informático, a autoridade judiciária competente ordena a quem tenha disponibilidade ou controlo desses dados que os comunique ao processo ou que permita o acesso aos mesmos, sob pena de punição por desobediência.

2 - A ordem referida no número anterior identifica os dados em causa.

3 - Em cumprimento da ordem descrita nos nºs 1 e 2, quem tenha disponibilidade ou controlo desses dados comunica esses dados à autoridade judiciária competente ou permite, sob pena de punição por desobediência, o acesso ao sistema informático onde os mesmos estão armazenados.

4 - O disposto no presente artigo é aplicável a fornecedores de serviço, a quem pode ser ordenado que comuniquem ao processo dados relativos aos seus clientes ou assinantes, neles se incluindo qualquer informação diferente dos dados relativos ao tráfego ou ao conteúdo, contida sob a forma de dados informáticos ou sob qualquer outra forma, detida pelo fornecedor de serviços, e que permita determinar:

a) O tipo de serviço de comunicação utilizado, as medidas técnicas tomadas a esse respeito e o período de serviço;

b) A identidade, a morada postal ou geográfica e o número de telefone do assinante, e qualquer outro número de acesso, os dados respeitantes à facturação e ao pagamento, disponíveis com base num contrato ou acordo de serviços; ou

c) Qualquer outra informação sobre a localização do equipamento de comunicação, disponível com base num contrato ou acordo de serviços.

5 - A injunção prevista no presente artigo não pode ser dirigida a suspeito ou arguido nesse processo.

6 - Não pode igualmente fazer -se uso da injunção prevista neste artigo quanto a sistemas informáticos utilizados para o exercício da advocacia, das actividades médica e bancária e da profissão de jornalista.

7 - O regime de segredo profissional ou de funcionário e de segredo de Estado previsto no artigo 182º do Código de Processo Penal é aplicável com as necessárias adaptações.