Legislação

Lei n.º 109/2009, de 15 de Setembro

LEI DO CIBERCRIME (versão actualizada)

Contém as seguintes alterações:

- Lei n.º 79/2021, de 24/11

Ver versões do diploma:

- **2ª versão - a mais recente** (Lei n.º 79/2021, de 24/11)
- 1ª versão (Lei n.º 109/2009, de 15/09)

Procurar no presente diploma:
A expressão exacta Procurar

Ir para o art.:

Nº de artigos : 39

Ver índice sistemático do diploma Imprimir todo o diploma

SUMÁRIO

Aprova a Lei do Cibercrime, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação, e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa

---

Lei n.º 109/2009

de 15 de Setembro

Aprova a Lei do Cibercrime, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação, e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa.

A Assembleia da República decreta, nos termos da alínea c) do artigo 161.º da Constituição, o seguinte:

CAPÍTULO I
Objecto e definições

Artigo 1.º

Objecto

A presente lei estabelece as disposições penais materiais e processuais, bem como as disposições relativas à cooperação internacional em matéria penal, relativas ao domínio do cibercrime e da recolha de prova em suporte electrónico, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação, e adaptando o direito interno à Convenção sobre Cibercrime do Conselho da Europa.

Orientações do MP

1. Cfr. Despacho n.º 14115/2013 da PGR in D.R. n.º 213, Série II de 2013-11-04
Atribuição de competência ao DCIAP para iniciar, exercer e dirigir a acção penal relativamente a crimes sexuais praticados contra menores com recurso aos meios informáticos ou divulgados através destes, cuja notícia de crime seja adquirida através de comunicações provindas de outro Estado e organizações internacionais

Diversos

1. A Convenção sobre o Cibercrime do Conselho da Europa, foi aprovada por Resolução da Assembleia da República n.º 88/2009, in DR I Série de 15.09.2009. Sobre a Convenção, consulte a informação disponível no site do Gabinete de Documentação e Direito Comparado da PGR, AQUI

Jurisprudência

1. Ac. TRE de 25.10.2016 1 - No caso de investigação e repressão de infrações penais relativas a comunicações, dados de comunicações e sua conservação existe legislação especial que secundariza o Código de Processo Penal e torna quase irrelevantes as Leis nº 5/2004 e 41/2004 para efeitos processuais penais.2 - Tal legislação especial são as Leis nº 32/2008, de 17-07 (Lei relativa a conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações) e 109/2009, de 15-09 (Lei do Cibercrime), assim como a Convenção do Conselho da Europa sobre o Cibercrime de 23/11/2001 (Resolução da AR n.º 88/2009, de 15 de Setembro), também designada Convenção de Budapeste.3- Tratando-se de dados de comunicações conservadas ou preservadas já não é possível aplicar o disposto no artigo 189º do Código de Processo Penal - a extensão do regime das escutas telefónicas - aos casos em que são aplicáveis as Leis nº 32/2008 e 109/2009 e a Convenção de Budapeste. Isto é, para a prova de comunicações preservadas ou conservadas em sistemas informáticos existe um novo sistema processual penal, o previsto nos artigos 11º a 19º da Lei 109/2009, de 15-09, Lei do Cibercrime, coadjuvado pelos artigos 3º a 11º da Lei nº 32/2008, se for caso de dados previstos nesta última;4 - A Lei nº 32/2008 tem um regime processual privativo da matéria por si regulada, assente na existência de dados conservados nos termos do artigo 4.º, nº 1 pelos fornecedores de serviços.5 - O regime processual aplicável é o constante dessa lei, inclusivé o catálogo de crimes permissivo que ela criou, os crimes graves referidos no artigo artigo 3.º, nº 1. 6 - O conceito de «crime grave», abarcando a criminalidade violenta- artigo 2º, nº 1, al. g) do diploma -, abrange o crime de violência doméstica previsto no nº 1 do artigo 152º do Código Penal por via da previsão do artigo 1º, al. j) do C.P.P..7 - De onde resulta a aplicabilidade ao caso dos autos do regime processual previsto nos artigos 3º a 11º da Lei nº 32/2008. 8 - E, face ao nº 2 da Lei 32/2008, a transmissão dos dados as autoridades competentes - Ministério Público ou autoridade de polícia criminal competente - só pode ser ordenada ou autorizada por despacho fundamentado do juiz, nos termos do artigo 9.º do diploma, que regula a «transmissão dos dados» e que apresenta como pressuposto substancial que haja ?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. 9 - Esta transmissão ou processamento veio a ser regulada pela Portaria n.º 469/2009, de 06 de Maio - Condições Técnicas e de Segurança, Tratamento de Dados de Tráfego - que mantém hoje a redacção dada pela Portaria n.º 694/2010, de 16/08.

Artigo 2.º

Definições

Para efeitos da presente lei, considera-se:

a) «Sistema informático», qualquer dispositivo ou conjunto de dispositivos interligados ou associados, em que um ou mais de entre eles desenvolve, em execução de um programa, o tratamento automatizado de dados informáticos, bem como a rede que suporta a comunicação entre eles e o conjunto de dados informáticos armazenados, tratados, recuperados ou transmitidos por aquele ou aqueles dispositivos, tendo em vista o seu funcionamento, utilização, protecção e manutenção;

b) «Dados informáticos», qualquer representação de factos, informações ou conceitos sob uma forma susceptível de processamento num sistema informático, incluindo os programas aptos a fazerem um sistema informático executar uma função;

c) «Dados de tráfego», os dados informáticos relacionados com uma comunicação efectuada por meio de um sistema informático, gerados por este sistema como elemento de uma cadeia de comunicação, indicando a origem da comunicação, o destino, o trajecto, a hora, a data, o tamanho, a duração ou o tipo do serviço subjacente;

d) «Fornecedor de serviço», qualquer entidade, pública ou privada, que faculte aos utilizadores dos seus serviços a possibilidade de comunicar por meio de um sistema informático, bem como qualquer outra entidade que trate ou armazene dados informáticos em nome e por conta daquela entidade fornecedora de serviço ou dos respectivos utilizadores;

e) «Intercepção», o acto destinado a captar informações contidas num sistema informático, através de dispositivos electromagnéticos, acústicos, mecânicos ou outros;

f) «Topografia», uma série de imagens ligadas entre si, independentemente do modo como são fixadas ou codificadas, que representam a configuração tridimensional das camadas que compõem um produto semicondutor e na qual cada imagem reproduz o desenho, ou parte dele, de uma superfície do produto semicondutor, independentemente da fase do respectivo fabrico;

g) «Produto semicondutor», a forma final ou intermédia de qualquer produto, composto por um substrato que inclua uma camada de material semicondutor e constituído por uma ou várias camadas de matérias condutoras, isolantes ou semicondutoras, segundo uma disposição conforme a uma configuração tridimensional e destinada a cumprir, exclusivamente ou não, uma função electrónica.

Jurisprudência

1. Ac. TRC, de 04.02.2015 Em inquérito, o pedido ao operador de comunicações do registo de todas as comunicações recebidas (por exemplo SMS, MMs), num período temporal alargado, na medida em que permitem identificar, em tempo real ou ? posterior, os utilizadores, o relacionamento directo entre uns e outros através da rede, a localização, a frequência, a data, hora, e a duração da comunicação, devem participar das garantias a que está submetida a utilização do serviço, especialmente tudo quanto respeite ao sigilo das comunicações. Desde que os dados de base estejam em interligação com dados de tráfego ou dados de conteúdo, torna-se necessária a autorização do Juiz para a sua obtenção e junção aos autos.

2. Ac. TRL de 22-04-2013: - A obtenção de um concreto endereço IP que esteve na origem da uma determinada comunicação efetuada é da competência do Ministério Público - e não do juiz.

3. Ac. TRC de 03-10-2012: - O endereço IP é um dado de tráfego, sendo a sua obtenção dependente de autorização do JIC - no despacho recorrido, de JIC, a posição assumida no despacho recorrido era a oposta.

4. Ac. TRL de 18-01-2011: - A identificação completa, morada e endereço de correio eletrónico do titular de determinado blog, bem como o IP de criação desse blog e o IP onde foi efetuado determinado post, constituem dados de base.

CAPÍTULO II
Disposições penais materiais

Artigo 3.º

Falsidade informática

1 - Quem, com intenção de provocar engano nas relações jurídicas, introduzir, modificar, apagar ou suprimir dados informáticos ou por qualquer outra forma interferir num tratamento informático de dados, produzindo dados ou documentos não genuínos, com a intenção de que estes sejam considerados ou utilizados para finalidades juridicamente relevantes como se o fossem, é punido com pena de prisão até 5 anos ou multa de 120 a 600 dias.

2 - Quando as ações descritas no número anterior incidirem sobre os dados registados, incorporados ou respeitantes a qualquer dispositivo que permita o acesso a sistema de comunicações ou a serviço de acesso condicionado, a pena é de 1 a 5 anos de prisão.

3 - Quem, atuando com intenção de causar prejuízo a outrem ou de obter um benefício ilegítimo, para si ou para terceiro, usar documento produzido a partir de dados informáticos que foram objeto dos atos referidos no n.º 1 ou dispositivo no qual se encontrem registados, incorporados ou ao qual respeitem os dados objeto dos atos referidos no número anterior, é punido com as penas previstas num e noutro número, respetivamente.

4 - Quem produzir, adquirir, importar, distribuir, vender ou detiver qualquer dispositivo, programa ou outros dados informáticos destinados à prática das ações previstas no n.º 2, é punido com pena de prisão de 1 a 5 anos.

5 - Se os factos referidos nos números anteriores forem praticados por funcionário no exercício das suas funções, a pena é de prisão de 2 a 5 anos.

Contém as alterações dos seguintes diplomas:
- Lei n.º 79/2021, de 24/11

Consultar versões anteriores deste artigo:
-1ª versão: Lei n.º 109/2009, de 15/09

Jurisprudência

1. Ac. TRP de 24-04-2013 , sumário retirado da CJ, 2013, T2, pág.223: I. Comete o crime de falsidade informática aquele que cria informaticamente contas, nas quais produz dados de perfil não genuínos de outra pessoa, através da ultilização dos seus dados pessoais que, simulando ser a própria, introduz no sistema informático, para criar, via internet, um sítio pr´oprio da plataforma da rede social facebook, imagem psicológica, carácter, personalidade e identidade daquela pessoa, que não correspondem`á realidade, com intenção de serem considerados genuínos; e, através daquelas contas, fingindo ser tal pessoa, divulgar conteúdos íntimos da sua vida pessoal, provocando dessa forma engano, com intenção de que fossem tomadas por verdeiras e reais, aquelas contas, dessa forma causando prejuízo á honra e imagem de tal pessoa, como era seu desiderato.
II. Neste crime, o prejuízo não tem de ser patrimonial, pois o bem jurídico que nele se protege não é o património, mas a confidencialidade, integridade e disponibilidade de sistemas informáticos, das redes e dados informáticos.

2. Ac. TRE de 19-05-2015 : 1. O tipo objetivo do crime de falsidade informática previsto no nº 1 do artigo 3º da Lei nº 109/2009, de 15 de setembro, é integrado, no plano objetivo, pela introdução, modificação, apagamento ou supressão de dados informáticos ou por qualquer outra forma de interferência num tratamento informático de dados, de que resulte a produção de dados ou documentos não genuínos, consumando-se o crime apenas com a produção deste resultado.
2. Do ponto de vista subjetivo, o tipo legal supõe o dolo, sob qualquer das formas previstas no artigo 14º do Código Penal, exigindo, enquanto elemento

subjetivo especial do tipo, a intenção de provocar engano nas relações jurídicas, bem como, relativamente á produção de dados ou documentos não genuínos, a particular intenção do agente de que tais dados ou documentos sejam considerados ou utilizados para finalidades juridicamente relevantes como se fossem genuínos.
3. O crime de falsidade informática previsto no artigo 3º da Lei nº 109/2009 visa proteger a segurança das relações jurídicas enquanto interesse público essencial que ao próprio Estado de Direito compete assegurar e não a confidencialidade, integridade e disponibilidade de sistemas informaiticos, de redes e de dados informaìticos.
4. A utilização do nome ou de parte do nome de outrem no nome de utilizador e/ou endereço eletrónico, por parte de quem criou conta de correio eletrónico, traduz, no plano objetivo, a produção de dados ou documentos não genuínos, mediante a introdução de dados informáticos, e é idóneo a fazer crer que foi a pessoa a quem respeita o nome ou parte de nome quem efetivamente criou e utilizou a conta de correio eletrónico em causa.

3. Ac. TRP de 26-05-2015 : I. No crime de Falsidade informática, quer na redação do art. 4.º n.º 1, da Lei da Criminalidade Informática, em vigor aquando dos factos, quer na atual formulação do art. 3.º n.º 1, da Lei do Cibercrime (Lei n.º 109/2009, de 15 de setembro), os dados informáticos têm de ser alterados com o propósito de desvirtuar a demonstração dos factos que com aqueles dados podem ser comprovados.
II. Comete tal crime a arguida que fez introduzir no sistema informático do hospital episódios de cirurgias realizadas em regime de ambulatório como se tivessem sido levadas a cabo em regime de internamento, quando tal não correspondia á realidade.
III. A relação jurídica que em virtude do comportamento da arguida foi introduzida no sistema informático não corresponde á verdade, sendo certo que os dados assim vertidos no sistema informático produzem os mesmos efeitos de um documento falsificado, pondo em causa o seu valor probatório e consequentemente a segurança nas relações jurídicas.

4. Ac. Trib. da Relação do Porto, de 24 de abril de 2013:- O bem jurídico tutelado pelo crime de falsidade informática (Artigo 3º, nºs 1 e 3 da Lei do Cibercrime),não é o património, mas antes a integridade dos sistemas de informação, através do qual se pretendeimpedir os atos praticados contra a confidencialidade, integridade e disponibilidade de sistemasinformáticos, de redes e dados informáticos, bem como a utilização fraudulenta desses sistemas, redes edados.

5. Ac. Trib. da Relação de Lisboa, de 30 de junho de 2011:- O bem jurídico protegido pelo crime de contrafação de moeda é a intangibilidade do sistema monetário,incluindo a segurança e credibilidade do tráfego monetário; o bem jurídico protegido pelo crime defalsificação informática é a integridade dos sistemas de informação. Se a ação consiste em duplicar eutilizar cartões bancários, com acesso a dados que neles se encontravam, produzindo com estes dadosdocumentos não genuínos para os utilizar no levantamento de dinheiro ou pagamento de bens, ocorrem,em concurso efetivo, aqueles dois crimes.

6. Ac. TRP de 30-04-2008: - Se a burla se realizou mediante a introdução de dados incorretos/falsos no sistema informático da Segurança Social, existe concurso efetivo de burla e falsidade informática.

7. Ac. TRP, de 14.09.2016 Entre os crimes de burla informática (art.º 221.º CP) e o crime de falsidade informática (artº 3º da Lei 109/2009 de 15/9 Lei do Cibercrime) existe concurso real de infrações.

Artigo 3.º-A

Contrafação de cartões ou outros dispositivos de pagamento

Quem, com intenção de provocar engano nas relações jurídicas, contrafizer cartão de pagamento ou qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou meio de pagamento, nomeadamente introduzindo, modificando, apagando, suprimindo ou interferindo, por qualquer outro modo, num tratamento informático de dados registados, incorporados, ou respeitantes a estes cartões ou dispositivos, é punido com pena de prisão de 3 a 12 anos.

Aditado pelo seguinte diploma: Lei n.º 79/2021, de 24 de Novembro

Artigo 3.º-B

Uso de cartões ou outros dispositivos de pagamento contrafeitos

1 - Quem, atuando com intenção de causar prejuízo a outrem ou de obter um benefício ilegítimo, para si ou para terceiro, usar cartão de pagamento contrafeito, ou qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou meio de pagamento contrafeito, é punido com pena de prisão de 1 a 5 anos.
2 - As ações descritas no número anterior são punidas com pena de prisão de 2 a 8 anos se o prejuízo ou o benefício for de valor consideravelmente elevado.
3 - As ações descritas no n.º 1 são punidas com pena de prisão de 3 a 12 anos se o agente as praticar de concerto com o agente dos factos descritos no artigo 3.º-A.

Aditado pelo seguinte diploma: Lei n.º 79/2021, de 24 de Novembro

Artigo 3.º-C

Aquisição de cartões ou outros dispositivos de pagamento contrafeitos

Quem, atuando com intenção de causar prejuízo a outrem ou de obter um benefício ilegítimo, adquirir, detiver, exportar, importar, transportar, distribuir, vender ou por qualquer outra forma transmitir ou disponibilizar cartão de pagamento contrafeito ou qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou meio de pagamento contrafeito, é punido com pena de prisão de 1 a 5 anos.

Aditado pelo seguinte diploma: Lei n.º 79/2021, de 24 de Novembro

Artigo 3.º-D

Atos preparatórios da contrafacção

Quem produzir, adquirir, importar, distribuir, vender ou detiver qualquer cartão, dispositivo, programa ou outros dados informáticos, ou quaisquer outros instrumentos, informáticos ou não, destinados à prática das ações descritas no artigo 3.º-A, é punido com pena de prisão de 1 a 5 anos.

Aditado pelo seguinte diploma: Lei n.º 79/2021, de 24 de Novembro

Artigo 3.º-E

Aquisição de cartões ou outros dispositivos de pagamento obtidos mediante crime informático

Quem, atuando com intenção de causar prejuízo a outrem ou de obter um benefício ilegítimo, adquirir, detiver, exportar, importar, transportar, distribuir, vender ou por qualquer outra forma transmitir ou disponibilizar:
a) Dados registados, incorporados ou respeitantes a cartão de pagamento ou a qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou meio de pagamento, que hajam sido obtidos mediante facto ilícito típico previsto nos artigos 4.º, 5.º, 6.º e 7.º;
b) Cartão de pagamento ou qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou meio de pagamento, que haja sido obtido mediante facto ilícito típico previsto nos artigos 4.º, 5.º, 6.º e 7.º;
é punido com pena de prisão de 1 a 5 anos.

Aditado pelo seguinte diploma: Lei n.º 79/2021, de 24 de Novembro

Artigo 3.º-F
Agravação

Se os factos referidos nos artigos 3.º-A a 3.º-E forem praticados por funcionário no exercício das suas funções, o limite mínimo da pena de prisão aplicável é:
a) De 2 anos, tratando-se dos factos previstos no n.º 1 do artigo 3.º-B, no n.º 1 do artigo 3.º-C, no artigo 3.º-D e no artigo 3.º-E;
b) Agravado em um terço, nos restantes casos.

Aditado pelo seguinte diploma: Lei n.º 79/2021, de 24 de Novembro

Artigo 3.º-G
Moeda virtual

Para efeitos da presente lei, considera-se também sistema ou meio de pagamento aquele que tenha por objeto moeda virtual.

Aditado pelo seguinte diploma: Lei n.º 79/2021, de 24 de Novembro

Artigo 4.º
Dano relativo a programas ou outros dados informáticos

1 - Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, apagar, alterar, destruir, no todo ou em parte, danificar, suprimir ou tornar não utilizáveis ou não acessíveis programas ou outros dados informáticos alheios ou por qualquer forma lhes afectar a capacidade de uso, é punido com pena de prisão até 3 anos ou pena de multa.
2 - A tentativa é punível.
3 - Incorre na mesma pena do n.º 1 quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos destinados a produzir as acções não autorizadas descritas nesse número.
4 - Se o dano causado for de valor elevado, a pena é de prisão até 5 anos ou de multa até 600 dias.
5 - Se o dano causado for de valor consideravelmente elevado, a pena é de prisão de 1 a 10 anos.
6 - Nos casos previstos nos n.os 1, 2 e 4 o procedimento penal depende de queixa.

Artigo 5.º
Sabotagem informática

1 - Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, entravar, impedir, interromper ou perturbar gravemente o funcionamento de um sistema informático, através da introdução, transmissão, deterioração, danificação, alteração, apagamento, impedimento do acesso ou supressão de programas ou outros dados informáticos ou de qualquer outra forma de interferência em sistema informático, é punido com pena de prisão até 5 anos ou com pena de multa até 600 dias.
2 - Na mesma pena incorre quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos destinados a produzir as acções não autorizadas descritas no número anterior.
3 - Nos casos previstos no número anterior, a tentativa não é punível.
4 - A pena é de prisão de 1 a 5 anos se o dano emergente da perturbação for de valor elevado.
5 - A pena é de prisão de 1 a 10 anos se:
a) O dano emergente da perturbação for de valor consideravelmente elevado;
b) A perturbação causada atingir de forma grave ou duradoura um sistema informático que apoie uma actividade destinada a assegurar funções sociais críticas, nomeadamente as cadeias de abastecimento, a saúde, a segurança e o bem-estar económico das pessoas, ou o funcionamento regular dos serviços públicos.

Artigo 6.º
Acesso ilegítimo

1 - Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, de qualquer modo aceder a um sistema informático, é punido com pena de prisão até 1 ano ou com pena de multa até 120 dias.
2 - Na mesma pena incorre quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas, um conjunto executável de instruções, um código ou outros dados informáticos destinados a produzir as ações não autorizadas descritas no número anterior.
3 - A pena é de prisão até 2 anos ou multa até 240 dias se as ações descritas no número anterior se destinarem ao acesso para obtenção de dados registados, incorporados ou respeitantes a cartão de pagamento ou a qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou meio de pagamento.
4 - A pena é de prisão até 3 anos ou multa se:
a) O acesso for conseguido através de violação de regras de segurança; ou
b) Através do acesso, o agente obtiver dados registados, incorporados ou respeitantes a cartão de pagamento ou a qualquer outro dispositivo, corpóreo ou

incorpóreo, que permita o acesso a sistema ou meio de pagamento.
5 - A pena é de prisão de 1 a 5 anos quando:
a) Através do acesso, o agente tiver tomado conhecimento de segredo comercial ou industrial ou de dados confidenciais, protegidos por lei; ou
b) O benefício ou vantagem patrimonial obtidos forem de valor consideravelmente elevado.
6 - A tentativa é punível, salvo nos casos previstos nos n.os 2 e 3.
7 - Nos casos previstos nos n.os 1, 4 e 6 o procedimento penal depende de queixa.

Contém as alterações dos seguintes diplomas:
- Lei n.º 79/2021, de 24/11

Consultar versões anteriores deste artigo:
-1ª versão: Lei n.º 109/2009, de 15/09

Jurisprudência

1. Ac. Trib. Relação de Coimbra, de 17 de fevereiro de 2016: - Comete o crime de acesso ilegítimo (Artigo 6º, nºs 1 e 4, al a, da Lei nº 109/2009), o inspetor tributário que, por motivos estritamente pessoais, acede ao sistema informático da Autoridade Tributária, consultando declarações de IRS de outrem. O tipo subjetivo daquele ilícito penal não exige qualquer intenção específica (como seja o prejuízo ou a obtenção de benefício ilegítimo), ficando preenchido com o dolo genérico de intenção de aceder a sistema).

2. Ac. Trib. Relação do Porto, de 8 de janeiro de 2014: - O crime de acesso ilegítimo, previsto no Artigo 6º da Lei do Cibercrime (Lei nº 109/2009) incrimina exatamente a mesma factualidade que era incriminada pelo crime correspondente (Artigo 7º da Lei nº 109/91). Todavia, na lei nova, não se exige qualquer intenção específica (por exemplo, a de causar prejuízo ou a de obter qualquer benefício ilegítimo), apenas se exigindo dolo genérico. O bem jurídico protegido é a segurança dos sistemas informáticos.

3. Ac. Trib. Relação de Coimbra, de 15 de outubro de 2008: O bem jurídico protegido do crime de acesso ilegítimo é a segurança do sistema informático ? a proteção ao designado domicílio informático algo de semelhante ? introdução em casa alheia.

Artigo 7.º
Intercepção ilegítima

1 - Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, e através de meios técnicos, interceptar transmissões de dados informáticos que se processam no interior de um sistema informático, a ele destinadas ou dele provenientes, é punido com pena de prisão até 3 anos ou com pena de multa.
2 - A tentativa é punível.
3 - Incorre na mesma pena prevista no n.º 1 quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos destinados a produzir as acções não autorizadas descritas no mesmo número.

Artigo 8.º
Reprodução ilegítima de programa protegido

1 - Quem ilegitimamente reproduzir, divulgar ou comunicar ao público um programa informático protegido por lei é punido com pena de prisão até 3 anos ou com pena de multa.
2 - Na mesma pena incorre quem ilegitimamente reproduzir topografia de um produto semicondutor ou a explorar comercialmente ou importar, para estes fins, uma topografia ou um produto semicondutor fabricado a partir dessa topografia.
3 - A tentativa é punível.

Jurisprudência

1. Ac. TRL de 08-09-2015: - De acordo com o Decreto-Lei nº 252/04, que criou o direito de autor sobre programas de computador, a autorização de utilização do programa não implica a transmissão dos direitos atribuídos ao autor do programa de computador - designadamente os direitos de reprodução, transformação e colocação em circulação.

2. Ac. TRC de 30-10-2013: - O tipo de crime de reprodução ilegítima de programa protegido não exige que, cumulativamente, haja reprodução, divulgação e comunicação ao público, bastando-se, por exemplo, com a instalação não autorizada de um programa informático protegido.

3. Ac. TRC de 30-10-2013: - A instalação de um único programa informático licenciado em vários computadores de uma empresa traduz-se numa reprodução de programa não autorizada. O tipo de crime de reprodução de programa protegido não exige intenção de lucro.

Artigo 9.º
Responsabilidade penal das pessoas colectivas e entidades equiparadas

As pessoas colectivas e entidades equiparadas são penalmente responsáveis pelos crimes previstos na presente lei nos termos e limites do regime de responsabilização previsto no Código Penal.

Artigo 10.º
Perda de bens

1 - O tribunal pode decretar a perda a favor do Estado dos objectos, materiais, equipamentos ou dispositivos que tiverem servido para a prática dos crimes previstos na presente lei e pertencerem a pessoa que tenha sido condenada pela sua prática.
2 - À avaliação, utilização, alienação e indemnização de bens apreendidos pelos órgãos de polícia criminal que sejam susceptíveis de vir a ser declarados perdidos a favor do Estado é aplicável o disposto no Decreto-Lei n.º 11/2007, de 19 de Janeiro.

CAPÍTULO III
Disposições processuais

Artigo 11.º
Âmbito de aplicação das disposições processuais

1 - Com excepção do disposto nos artigos 18.º e 19.º, 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 n.º 32/2008, de 17 de Julho.

Jurisprudência

1. Ac. TRE de 20-01-2015 : 1. O regime processual das comunicações telefónicas previsto nos artigos 187º a 190º do Código de Processo Penal deixou de ser aplicável por extensão ás «telecomunicações electrónicas», «crimes informáticos» e «recolha de prova electrónica (informática)» desde a entrada em vigor da Lei 109/2009, de 15-09 (Lei do Cibercrime) como regime regra. 2. Esse mesmo regime processual das comunicações telefónicas deixara de ser aplicável á recolha de prova por «localização celular conservada» - uma forma de «recolha de prova electrónica - desde a entrada em vigor da Lei 32/2008, de 17-07. 3. Para a prova electrónica preservada ou conservada em sistemas informáticos existe um novo sistema processual penal, o previsto nos artigos 11º a 19º da Lei 109/2009, de 15-09, Lei do Cibercrime, coadjuvado pela Lei nº 32/2008, neste caso se estivermos face á prova por «localização celular conservada». 4. Nessa Lei do Cibercrime coexistem dois regimes processuais: o regime dos artigos 11º a 17º e o regime dos artigos 18º e 19º do mesmo diploma. O regime processual dos artigos 11º a 17º surge como o regime processual «geral» do cibercrime e da prova electrónica. Isto porquanto existe um segundo catálogo na Lei n. 109/2009, o do artigo 18º, n. 1 do mesmo diploma a que corresponde um segundo regime processual de autorização e regulação probatória. Só a este segundo regime - o dos artigos 18º e 19º - são aplicáveis por remissão expressa os artigos 187º, 188º e 190º do C.P.P. e sob condição de não contrariarem e Lei 109/2009. 5. As normas contidas nos artigos 12º a 17º da supramencionada Lei contêm um completo regime processual penal para os crimes que, nos termos das alíneas do n. 1 do artigo 11º, estão (a) previstos na lei nº 109/2009, (b) são ou foram cometidos por meio de um sistema informático ou (c) em relação aos quais seja necessário proceder á recolha de prova em suporte electrónico. 6. A diferenciação de regimes assenta na circunstância de os dados preservados nos termos dos artigos 12º a 17º se referirem á pesquisa e recolha, para prova, de dados já produzidos mas preservados, armazenados, enquanto o artigo 18º do diploma se refere á intercepção de comunicações electrónicas, em tempo real, de dados de tráfego e de conteúdo associados a comunicações específicas transmitidas através de um sistema informático. 7. Assim, o Capítulo III da Lei 109/2009, relativo ás disposições processuais, deve ser encarado como um «escondido Capítulo V («Da prova electrónica»), do Título III («Meios de obtenção de prova») do Livro III («Da prova») do Código de Processo Penal» (Dá Mesquita). 8. Tratando-se de obter prova por «localização celular conservada», isto é, a obtenção dos dados previstos no artigo 4º, n. 1 da Lei 32/2008, de 17-07, o regime processual aplicável assume especialidade nos artigos 3º e 9º desta lei. 9. Em suma, numa interpretação conjugada das Leis 32/2008, 109/2009 e da Convenção de Budapeste sobre o Cibercrime do Conselho da Europa (aprovada pela Resolução da Assembleia da República nº 88/2009, publicada no DR de 15-09-2009), devem ter-se em consideração os seguintes catálogos de crimes quanto a dados preservados ou conservados: - o catálogo de crimes do n. 1 do artigo 11º da Lei 109/2009 como pressuposto de aplicação do regime processual contido nos artigos 11º a 17º dessa Lei; - o catálogo de crimes do n. 1 do artigo 18º da Lei 109/2009 como pressuposto de aplicação do regime processual contido nesse artigo 18º e no 19º dessa Lei aos crimes previstos na al. a) do artigo 18º; - o catálogo de crimes do n. 1 do artigo 187º do Código de Processo Penal, por remissão expressa da Lei 109/2009, como pressuposto de aplicação do regime processual contido nesse artigo 18º e no 19º dessa Lei para os crimes previstos na al. b) do artigo 18º; - o catálogo de crimes («crimes graves») do artigo 3º da Lei nº 32/2008 quanto a especiais «dados conservados» (localização celular), como requisito de aplicação dos artigos 3º e 9º da Lei nº 32/2008. 10. O artigo 189º do Código de Processo Penal nunca é aplicável a crimes informáticos, seja qual for o catálogo aplicável. 11. O objecto de ambas as leis - de 2008 e 2009 - é parcialmente coincidente. Ambas se referem e regulam «dados conservados» (Lei nº 32/2008) e «dados preservados» (Lei nº 109/2009) ou seja, depositados, armazenados, arquivados, guardados. A Lei de 2009 assume um carácter geral no seu âmbito de aplicação, não distinguindo dados arquivados pela sua natureza, o que abrange todos eles, portanto (á excepção do correio electrónico, especificamente previsto no seu artigo 17º). 12. O regime processual da Lei nº 32/2008 constitui relativamente aos dados «conservados» que prevê no seu artigo 4º, um regime especial relativamente ao capítulo processual penal geral que consta dos artigos 11º a 19º da Lei nº 109/2009. 13. Consequentemente devemos concluir que o regime processual da Lei 32/2008, designadamente o artigo 3º, nº 1 e 2 e o artigo 9º: - mostra-se revogado e substituído pelo regime processual contido na Lei nº 109/2009 para todos os dados que não estejam especificamente previstos no artigo 4º, n. 1 da Lei nº 32/2008 ou seja, dados conservados em geral; - revela-se vigente para todos os dados que estejam especificamente previstos no artigo 4º, n. 1 da Lei nº 32/2008, isto é, para os dados conservados relativos á localização celular. Só para este último caso ganha relevo o conceito de «crime grave». 14. Antes da entrada em vigor das Leis 32/2008 e 109/2009 podia afirmar-se que havia duas formas úteis «processualmente úteis» de usar a localização celular. Uma delas a medida cautelar de polícia prevista no artigo 252º-A do C.P.P. e a outra o meio de obtenção de prova previsto no artigo 189º, n. 2 do mesmo código, que se mantém em vigor para a localização celular em tempo real. 15. Agora co-existem três realidades distintas através do acrescento da obtenção de dados de localização celular «conservados» por via da Lei nº 32/2008.16. Os requisitos do número 3 do artigo 9º da Lei 32/2008 mostram-se de verificação alternativa. O conceito de «suspeito» dele constante exige «determinabilidade» e não «determinação». 17. A previsão do artigo 252º-A do Código de Processo Penal é claramente uma previsão de carácter excepcional para situações de carácter excepcional.

2. Ac. TRG de 15-04-2012: - A transcrição de mensagens SMS do telemóvel de um queixoso que espontaneamente as fornece, pode valer como prova, apesar de não ter sido ordenada pelo juiz. Só será necessária a intervenção do JIC quando quem fornece aquelas mensagens não puder dispor delas.

3. Ac. TRP de 12-09-2012: - A jurisprudência tem equiparado as mensagens SMS ? s cartas de correio, distinguindo se ainda estão fechadas ou se foram já abertas pelo destinatário. Porém, a Lei do Cibercrime alterou esta abordagem: a leitura de mensagens guardadas num cartão de telemóvel por um agente policial sem autorização do seu dono ou do JIC é prova proibida, em nada relevando que as mesmas tivessem sido ou não abertas e lidas pelo destinatário pois que a lei não distingue entre essas duas situações.

4. Ac. TRL de 19-06-2014 : I. estando apenas em causa a obtenção da identificação de um utilizador de um endereço IP ou o número de IP usado por um determinado indivíduo, em circunstâncias temporais determinadas, a competência para a respectiva obtenção é do M°P° II. a identificação de um determinado endereço de IP conjugada com a identidade de quem o utilizou num dado dia e hora não revela informação sobre o percurso da comunicação nem sobre outro eventual tráfego comunicacional da pessoa em causa III. os direitos constitucionais dos arguidos não são absolutos, face aos direitos dos restantes cidadãos, mormente das vítimas em processo penal, e as entidades públicas, ao enquadrar o uso dos diversos meios de prova têm de considerar os direitos dos vários intervenientes processuais

5. Ac. TRE de 25.10.2016 1 - No caso de investigação e repressão de infrações penais relativas a comunicações, dados de comunicações e sua conservação existe legislação especial que secundariza o Código de Processo Penal e torna quase irrelevantes as Leis nº 5/2004 e 41/2004 para efeitos processuais penais.2 - Tal legislação especial são as Leis nº 32/2008, de 17-07 (Lei relativa a conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações) e 109/2009, de 15-09 (Lei do Cibercrime), assim como a Convenção do Conselho da Europa sobre o Cibercrime de 23/11/2001 (Resolução da AR n.º 88/2009, de 15 de Setembro), também designada Convenção de Budapeste.3- Tratando-se de dados de comunicações conservadas ou preservadas já não é possível aplicar o disposto no artigo 189º do Código de Processo Penal - a extensão do regime das escutas telefónicas - aos casos em que são aplicáveis as Leis nº 32/2008 e 109/2009 e a Convenção de Budapeste. Isto é, para a prova de comunicações preservadas ou conservadas em sistemas informáticos existe um novo sistema processual penal, o previsto nos artigos 11º a 19º da Lei 109/2009, de 15-09, Lei do Cibercrime, coadjuvado pelos artigos 3º a 11º da Lei nº 32/2008, se for caso de dados previstos nesta última;4 - A Lei nº 32/2008 tem um regime processual privativo da matéria por si regulada, assente na existência de dados conservados nos termos do artigo 4.º, nº 1 pelos fornecedores de serviços.5 - O regime processual aplicável é o constante dessa lei, inclusivé o catálogo de crimes permissivo que ela criou, os crimes graves referidos no artigo artigo 3.º, nº 1. 6 - O conceito de «crime grave», abarcando a criminalidade violenta- artigo 2º, nº 1, al. g) do diploma -, abrange o crime de violência doméstica previsto no nº 1 do artigo 152º do Código Penal por via da previsão do artigo 1º, al. j) do C.P.P..7 - De onde resulta a aplicabilidade ao caso dos autos do regime processual previsto nos artigos 3º a 11º da Lei nº 32/2008. 8 - E, face ao nº 2 da Lei 32/2008, a transmissão dos dados as autoridades competentes - Ministério Público ou autoridade de polícia criminal competente - só pode ser ordenada ou autorizada por despacho fundamentado do juiz, nos termos do artigo 9.º do diploma, que regula a «transmissão dos dados» e que apresenta como pressuposto substancial que haja ?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. 9 - Esta transmissão ou processamento veio a ser regulada pela Portaria n.º 469/2009, de 06 de Maio - Condições Técnicas e de Segurança, Tratamento de Dados de Tráfego - que mantém hoje a redacção dada pela Portaria n.º 694/2010, de 16/08.

6. Ac. TRP de 05.04.2017 I ? O Facebook é uma rede social que funciona através da internet, operando no âmbito de um sistema informático pelo que a recolha de prova está sujeita ? Lei do Cibercrime - DL 109/2009 de 15/9.II ? Constitui prova legal a cópia de informação que alguém publicita no seu mural do Facebook sem restrição de acesso.III ? Só esta sujeita ? disciplina do art.º 16º 1 e 3 da Lei do Cibercrime a apreensão da informação original inserta na plataforma, esteja ou não disponível.

7. Ac. TRP de 13.09.2017 Facebook. Conta. Fotografias. Prova. A prova da titularidade da conta do Facebook e o conteúdo na mesma divulgado não obedece a qualquer principio de prova legal de natureza digital, a obter através da pesquisa de dados informáticos e sua apreensão, mas apenas submetido ao principio da livre apreciação da prova.

Artigo 12.º

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 253.º 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.

Jurisprudência

1. Ac. TRE de 20-01-2015 : 1. O regime processual das comunicações telefónicas previsto nos artigos 187º a 190º do Código de Processo Penal deixou de ser aplicável por extensão ás «telecomunicações electrónicas», «crimes informáticos» e «recolha de prova electrónica (informática)» desde a entrada em vigor da Lei 109/2009, de 15-09 (Lei do Cibercrime) como regime regra. 2. Esse mesmo regime processual das comunicações telefónicas deixara de ser aplicável á recolha de prova por «localização celular conservada» - uma forma de «recolha de prova electrónica - desde a entrada em vigor da Lei 32/2008, de 17-07. 3. Para a prova electrónica preservada ou conservada em sistemas informáticos existe um novo sistema processual penal, o previsto nos artigos 11º a 19º da Lei 109/2009, de 15-09, Lei do Cibercrime, coadjuvado pela Lei nº 32/2008, neste caso se estivermos face á prova por «localização celular conservada». 4. Nessa Lei do Cibercrime coexistem dois regimes processuais: o regime dos artigos 11º a 17º e o regime dos artigos 18º e 19º do mesmo diploma. O regime processual dos artigos 11º a 17º surge como o regime processual «geral» do cibercrime e da prova electrónica. Isto porquanto existe um segundo catálogo na Lei n. 109/2009, o do artigo 18º, n. 1 do mesmo diploma a que corresponde um segundo regime processual de autorização e regulação probatória. Só a este segundo regime - o dos artigos 18º e 19º - são aplicáveis por remissão expressa os artigos 187º, 188º e 190º do C.P.P. e sob condição de não contrariarem e Lei 109/2009. 5. As normas contidas nos artigos 12º a 17º da supramencionada Lei contêm um completo regime processual penal para os crimes que, nos termos das alíneas do n. 1 do artigo 11º, estão (a) previstos na lei nº 109/2009, (b) são ou foram cometidos por meio de um sistema informático ou (c) em relação aos quais seja necessário proceder á recolha de prova em suporte electrónico. 6. A diferenciação de regimes assenta na circunstância de os dados preservados nos termos dos artigos 12º a 17º se referirem á pesquisa e recolha, para prova, de dados já produzidos mas preservados, armazenados, enquanto o artigo 18º do diploma se refere á intercepção de comunicações electrónicas, em tempo real, de dados de tráfego e de conteúdo associados a comunicações específicas transmitidas através de um sistema informático. 7. Assim, o Capítulo III da Lei 109/2009, relativo ás disposições processuais, deve ser encarado como um «escondido Capítulo V («Da prova electrónica»), do Título III («Meios de obtenção de prova») do Livro III («Da prova») do Código de Processo Penal» (Dá Mesquita). 8. Tratando-se de obter prova por «localização celular conservada», isto é, a obtenção dos dados previstos no artigo 4º, n. 1 da Lei 32/2008, de 17-07, o regime processual aplicável assume especialidade nos artigos 3º e 9º desta lei. 9. Em suma, numa interpretação conjugada das Leis 32/2008, 109/2009 e da Convenção de Budapeste sobre o Cibercrime do Conselho da Europa (aprovada pela Resolução da Assembleia da República nº 88/2009, publicada no DR de 15-09-2009), devem ter-se em consideração os seguintes catálogos de crimes quanto a dados preservados ou conservados: - o catálogo de crimes do n. 1 do artigo 11º da Lei 109/2009 como pressuposto de aplicação do regime processual contido nos artigos 11º a 17º dessa Lei; - o catálogo de crimes do n. 1 do artigo 18º da Lei 109/2009 como pressuposto de aplicação do regime processual contido nesse artigo 18º e no 19º dessa Lei aos crimes previstos na al. a) do artigo 18º; - o catálogo de crimes do n. 1 do artigo 187º do Código de Processo Penal, por remissão expressa da Lei 109/2009, como pressuposto de aplicação do regime processual contido nesse artigo 18º e no 19º dessa Lei para os crimes previstos na al. b) do artigo 18º; - o catálogo de crimes («crimes graves») do artigo 3º da Lei nº 32/2008 quanto a especiais «dados conservados» (localização celular), como requisito de aplicação dos artigos 3º e 9º da Lei nº 32/2008. 10. O artigo 189º do Código de Processo Penal nunca é aplicável a crimes informáticos, seja qual for o catálogo aplicável. 11. O objecto de ambas as leis - de 2008 e 2009 - é parcialmente coincidente. Ambas se referem e regulam «dados conservados» (Lei nº 32/2008) e «dados preservados» (Lei nº 109/2009) ou seja, depositados, armazenados, arquivados, guardados. A Lei de 2009 assume um carácter geral no seu âmbito de aplicação, não distinguindo dados arquivados pela sua natureza, o que abrange todos eles, portanto (á excepção do correio electrónico, especificamente previsto no seu artigo 17º). 12. O regime processual da Lei nº 32/2008 constitui relativamente aos dados «conservados» que prevê no seu artigo 4º, um regime especial relativamente ao capítulo processual penal geral que consta dos artigos 11º a 19º da Lei nº 109/2009. 13. Consequentemente devemos concluir que o regime processual da Lei 32/2008, designadamente o artigo 3º, nº 1 e 2 e o artigo 9º: - mostra-se revogado e substituído pelo regime processual contido na Lei nº 109/2009 para todos os dados que não estejam especificamente previstos no artigo 4º, n. 1 da Lei nº 32/2008 ou seja, dados conservados em geral; - revela-se vigente para todos os dados que estejam especificamente previstos no artigo 4º, n. 1 da Lei nº 32/2008, isto é, para os dados conservados relativos á localização celular. Só para este último caso ganha relevo o conceito de «crime grave». 14. Antes da entrada em vigor das Leis 32/2008 e 109/2009 podia afirmar-se que havia duas formas úteis «processualmente úteis» de usar a localização celular. Uma delas a medida cautelar de polícia prevista no artigo 252º-A do C.P.P. e a outra o meio de obtenção de prova previsto no artigo 189º, n. 2 do mesmo código, que se mantém em vigor para a localização celular em tempo real. 15. Agora co-existem três realidades distintas através do acrescento da obtenção de dados de localização celular «conservados» por via da Lei nº 32/2008.16. Os requisitos do número 3 do artigo 9º da Lei 32/2008 mostram-se de verificação alternativa. O conceito de «suspeito» dele constante exige «determinabilidade» e não «determinação». 17. A previsão do artigo 252º-A do Código de Processo Penal é claramente uma previsão de carácter excepcional para situações de carácter excepcional.

2. Ac. TRL de 22-04-2013: - A obtenção de um concreto endereço IP que esteve na origem da uma determinada comunicação efetuada é da competência do Ministério Público - e não do juiz.

3. Ac. TRL de 11 de abril de 2023:
I - Da leitura do artigo 155.º do Código de Processo Penal decorre que a presença de consultor técnico na perícia não é imperiosa [1- Ordenada a perícia, o Ministério Público, o arguido, o assistente e as partes civis podem designar para assistir a realização da mesma, se isso ainda for possível, um consultor técnico da sua confiança.[...], não tem que anteceder a realização da perícia [3 - Se o consultor técnico for designado após a realização da perícia, pode, salvo no caso previsto na alínea a) do n.º 5 do artigo anterior, tomar conhecimento do relatório] e não pode constituir motivo para atrasar as démarches do processo [4- A designação de consultor técnico e o desempenho da sua função não podem atrasar a realização da perícia e o andamento normal do processo].
II - A emissão da DEI encontra-se rodeada de diversas cautelas, pressupõe a verificação de diversas condições e é suscetível de recurso, pelo que, inexistindo qualquer elemento nos autos ou qualquer notícia de que tenha sido emitida em desobediência aos respetivos preceitos legais que a regulamentam ou que sobre essa decisão tenha incidido qualquer recurso, não há qualquer razão que impeça o tribunal de fazer uso dos elementos de prova transmitidos ao processo, pelas autoridades francesas, através da DEI.
III - Nos casos em que os pedidos se reportam a dados já preservados, já obtidos e já armazenados por autoridades estrangeiras, em que se pretende a sua transmissão para um processo penal nacional, regem exclusivamente os artigos 12.º a 17.º da Lei do Cibercrime [Lei n.º 109/2009 de 15/09] e não o artigo 187.º do Código de Processo Penal.

Artigo 13.º

Revelação expedita de dados de tráfego

Tendo em vista assegurar a preservação dos dados de tráfego relativos a uma determinada comunicação, independentemente do número de fornecedores de serviço que nela participaram, o fornecedor de serviço a quem essa preservação tenha sido ordenada nos termos do artigo anterior indica à autoridade

judiciária ou ao órgão de polícia criminal, logo que o souber, outros fornecedores de serviço através dos quais aquela comunicação tenha sido efectuada, tendo em vista permitir identificar todos os fornecedores de serviço e a via através da qual aquela comunicação foi efectuada.

Jurisprudência

1. Ac. TRE de 20-01-2015 :

1. O regime processual das comunicações telefónicas previsto nos artigos 187º a 190º do Código de Processo Penal deixou de ser aplicável por extensão ás «telecomunicações electrónicas», «crimes informáticos» e «recolha de prova electrónica (informática)» desde a entrada em vigor da Lei 109/2009, de 15-09 (Lei do Cibercrime) como regime regra.
2. Esse mesmo regime processual das comunicações telefónicas deixara de ser aplicável á recolha de prova por «localização celular conservada» - uma forma de «recolha de prova electrónica - desde a entrada em vigor da Lei 32/2008, de 17-07.
3. Para a prova electrónica preservada ou conservada em sistemas informáticos existe um novo sistema processual penal, o previsto nos artigos 11º a 19º da Lei 109/2009, de 15-09, Lei do Cibercrime, coadjuvado pela Lei nº 32/2008, neste caso se estivermos face á prova por «localização celular conservada».
4. Nessa Lei do Cibercrime coexistem dois regimes processuais: o regime dos artigos 11º a 17º e o regime dos artigos 18º e 19º do mesmo diploma. O regime processual dos artigos 11º a 17º surge como o regime processual «geral» do cibercrime e da prova electrónica. Isto porquanto existe um segundo catálogo na Lei n. 109/2009, o do artigo 18º, n. 1 do mesmo diploma a que corresponde um segundo regime processual de autorização e regulação probatória. Só a este segundo regime - o dos artigos 18º e 19º - são aplicáveis por remissão expressa os artigos 187º, 188º e 190º do C.P.P. e sob condição de não contrariarem e Lei 109/2009.
5. As normas contidas nos artigos 12º a 17º da supramencionada Lei contêm um completo regime processual penal para os crimes que, nos termos das alíneas do n. 1 do artigo 11º, estão (a) previstos na lei nº 109/2009, (b) são ou foram cometidos por meio de um sistema informático ou (c) em relação aos quais seja necessário proceder á recolha de prova em suporte electrónico.
6. A diferenciação de regimes assenta na circunstância de os dados preservados nos termos dos artigos 12º a 17º se referirem á pesquisa e recolha, para prova, de dados já produzidos mas preservados, armazenados, enquanto o artigo 18º do diploma se refere á intercepção de comunicações electrónicas, em tempo real, de dados de tráfego e de conteúdo associados a comunicações específicas transmitidas através de um sistema informático.
7. Assim, o Capítulo III da Lei 109/2009, relativo ás disposições processuais, deve ser encarado como um «escondido Capítulo V («Da prova electrónica»), do Título III («Meios de obtenção de prova») do Livro III («Da prova») do Código de Processo Penal» (Dá Mesquita).
8. Tratando-se de obter prova por «localização celular conservada», isto é, a obtenção dos dados previstos no artigo 4º, n. 1 da Lei 32/2008, de 17-07, o regime processual aplicável assume especialidade nos artigos 3º e 9º desta lei.
9. Em suma, numa interpretação conjugada das Leis 32/2008, 109/2009 e da Convenção de Budapeste sobre o Cibercrime do Conselho da Europa (aprovada pela Resolução da Assembleia da República nº 88/2009, publicada no DR de 15-09-2009), devem ter-se em consideração os seguintes catálogos de crimes quanto a dados preservados ou conservados:
- o catálogo de crimes do n. 1 do artigo 11º da Lei 109/2009 como pressuposto de aplicação do regime processual contido nos artigos 11º a 17º dessa Lei;
- o catálogo de crimes do n. 1 do artigo 18º da Lei 109/2009 como pressuposto de aplicação do regime processual contido nesse artigo 18º e no 19º dessa Lei aos crimes previstos na al. a) do artigo 18º;
- o catálogo de crimes do n. 1 do artigo 187º do Código de Processo Penal, por remissão expressa da Lei 109/2009, como pressuposto de aplicação do regime processual contido nesse artigo 18º e no 19º dessa Lei para os crimes previstos na al. b) do artigo 18º;
- o catálogo de crimes («crimes graves») do artigo 3º da Lei nº 32/2008 quanto a especiais «dados conservados» (localização celular), como requisito de aplicação dos artigos 3º e 9º da Lei nº 32/2008.
10. O artigo 189º do Código de Processo Penal nunca é aplicável a crimes informáticos, seja qual for o catálogo aplicável.
11. O objecto de ambas as leis - de 2008 e 2009 - é parcialmente coincidente. Ambas se referem e regulam «dados conservados» (Lei nº 32/2008) e «dados preservados» (Lei nº 109/2009) ou seja, depositados, armazenados, arquivados, guardados. A Lei de 2009 assume um carácter geral no seu âmbito de aplicação, não distinguindo dados arquivados pela sua natureza, o que abrange todos eles, portanto (á excepção do correio electrónico, especificamente previsto no seu artigo 17º).
12. O regime processual da Lei nº 32/2008 constitui relativamente aos dados «conservados» que prevê no seu artigo 4º, um regime especial relativamente ao capítulo processual penal geral que consta dos artigos 11º a 19º da Lei nº 109/2009.
13. Consequentemente devemos concluir que o regime processual da Lei 32/2008, designadamente o artigo 3º, nº 1 e 2 e o artigo 9º: - mostra-se revogado e substituído pelo regime processual contido na Lei nº 109/2009 para todos os dados que não estejam especificamente previstos no artigo 4º, n. 1 da Lei nº 32/2008 ou seja, dados conservados em geral; - revela-se vigente para todos os dados que estejam especificamente previstos no artigo 4º, n. 1 da Lei nº 32/2008, isto é, para os dados conservados relativos á localização celular. Só para este último caso ganha relevo o conceito de «crime grave».
14. Antes da entrada em vigor das Leis 32/2008 e 109/2009 podia afirmar-se que havia duas formas úteis «processualmente úteis» de usar a localização celular. Uma delas a medida cautelar de polícia prevista no artigo 252º-A do C.P.P. e a outra o meio de obtenção de prova previsto no artigo 189º, n. 2 do mesmo código, que se mantém em vigor para a localização celular em tempo real.
15. Agora co-existem três realidades distintas através do acrescento da obtenção de dados de localização celular «conservados» por via da Lei nº 32/2008.
16. Os requisitos do número 3 do artigo 9º da Lei 32/2008 mostram-se de verificação alternativa. O conceito de «suspeito» dele constante exige «determinabilidade» e não «determinação».
17. A previsão do artigo 252º-A do Código de Processo Penal é claramente uma previsão de carácter excepcional para situações de carácter excepcional.

2. Ac. TRL de 22-04-2013: - A obtenção de um concreto endereço IP que esteve na origem da uma determinada comunicação efetuada é da competência do Ministério Público - e não do juiz.

Artigo 14.º

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 n.os 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 182.º do Código de Processo Penal é aplicável com as necessárias adaptações.

Jurisprudência

1. Ac. TRL de 19-06-2014 : I. estando apenas em causa a obtenção da identificação de um utilizador de um endereço IP ou o número de IP usado por um determinado indivíduo, em circunstâncias temporais determinadas, a competência para a respectiva obtenção é do M°P° II. a identificação de um

determinado endereço de IP conjugada com a identidade de quem o utilizou num dado dia e hora não revela informação sobre o percurso da comunicação nem sobre outro eventual tráfego comunicacional da pessoa em causa III. os direitos constitucionais dos arguidos não são absolutos, face aos direitos dos restantes cidadãos, mormente das vítimas em processo penal, e as entidades públicas, ao enquadrar o uso dos diversos meios de prova têm de considerar os direitos dos vários intervenientes processuais

2. Ac. TRE de 20-01-2015 : 1. O regime processual das comunicações telefónicas previsto nos artigos 187º a 190º do Código de Processo Penal deixou de ser aplicável por extensão ás «telecomunicações electrónicas», «crimes informáticos» e «recolha de prova electrónica (informática)» desde a entrada em vigor da Lei 109/2009, de 15-09 (Lei do Cibercrime) como regime regra. 2. Esse mesmo regime processual das comunicações telefónicas deixara de ser aplicável á recolha de prova por «localização celular conservada» - uma forma de «recolha de prova electrónica - desde a entrada em vigor da Lei 32/2008, de 17-07. 3. Para a prova electrónica preservada ou conservada em sistemas informáticos existe um novo sistema processual penal, o previsto nos artigos 11º a 19º da Lei 109/2009, de 15-09, Lei do Cibercrime, coadjuvado pela Lei nº 32/2008, neste caso se estivermos face á prova por «localização celular conservada». 4. Nessa Lei do Cibercrime coexistem dois regimes processuais: o regime dos artigos 11º a 17º e o regime dos artigos 18º e 19º do mesmo diploma. O regime processual dos artigos 11º a 17º surge como o regime processual «geral» do cibercrime e da prova electrónica. Isto porquanto existe um segundo catálogo na Lei n. 109/2009, o do artigo 18º, n. 1 do mesmo diploma a que corresponde um segundo regime processual de autorização e regulação probatória. Só a este segundo regime - o dos artigos 18º e 19º - são aplicáveis por remissão expressa os artigos 187º, 188º e 190º do C.P.P. e sob condição de não contrariarem e Lei 109/2009. 5. As normas contidas nos artigos 12º a 17º da supramencionada Lei contêm um completo regime processual penal para os crimes que, nos termos das alíneas do n. 1 do artigo 11º, estão (a) previstos na lei nº 109/2009, (b) são ou foram cometidos por meio de um sistema informático ou (c) em relação aos quais seja necessário proceder á recolha de prova em suporte electrónico. 6. A diferenciação de regimes assenta na circunstância de os dados preservados nos termos dos artigos 12º a 17º se referirem á pesquisa e recolha, para prova, de dados já produzidos mas preservados, armazenados, enquanto o artigo 18º do diploma se refere á intercepção de comunicações electrónicas, em tempo real, de dados de tráfego e de conteúdo associados a comunicações específicas transmitidas através de um sistema informático. 7. Assim, o Capítulo III da Lei 109/2009, relativo ás disposições processuais, deve ser encarado como um «escondido Capítulo V («Da prova electrónica»), do Título III («Meios de obtenção de prova») do Livro III («Da prova») do Código de Processo Penal» (Dá Mesquita). 8. Tratando-se de obter prova por «localização celular conservada», isto é, a obtenção dos dados previstos no artigo 4º, n. 1 da Lei 32/2008, de 17-07, o regime processual aplicável assume especialidade nos artigos 3º e 9º desta lei. 9. Em suma, numa interpretação conjugada das Leis 32/2008, 109/2009 e da Convenção de Budapeste sobre o Cibercrime do Conselho da Europa (aprovada pela Resolução da Assembleia da República nº 88/2009, publicada no DR de 15-09-2009), devem ter-se em consideração os seguintes catálogos de crimes quanto a dados preservados ou conservados: - o catálogo de crimes do n. 1 do artigo 11º da Lei 109/2009 como pressuposto de aplicação do regime processual contido nos artigos 11º a 17º dessa Lei; - o catálogo de crimes do n. 1 do artigo 18º da Lei 109/2009 como pressuposto de aplicação do regime processual contido nesse artigo 18º e no 19º dessa Lei aos crimes previstos na al. a) do artigo 18º; - o catálogo de crimes do n. 1 do artigo 187º do Código de Processo Penal, por remissão expressa da Lei 109/2009, como pressuposto de aplicação do regime processual contido nesse artigo 18º e no 19º dessa Lei para os crimes previstos na al. b) do artigo 18º; - o catálogo de crimes («crimes graves») do artigo 3º da Lei nº 32/2008 quanto a especiais «dados conservados» (localização celular), como requisito de aplicação dos artigos 3º e 9º da Lei nº 32/2008. 10. O artigo 189º do Código de Processo Penal nunca é aplicável a crimes informáticos, seja qual for o catálogo aplicável. 11. O objecto de ambas as leis - de 2008 e 2009 - é parcialmente coincidente. Ambas se referem e regulam «dados conservados» (Lei nº 32/2008) e «dados preservados» (Lei nº 109/2009) ou seja, depositados, armazenados, arquivados, guardados. A Lei de 2009 assume um carácter geral no seu âmbito de aplicação, não distinguindo dados arquivados pela sua natureza, o que abrange todos eles, portanto (á excepção do correio electrónico, especificamente previsto no seu artigo 17º). 12. O regime processual da Lei nº 32/2008 constitui relativamente aos dados «conservados» que prevê no seu artigo 4º, um regime especial relativamente ao capítulo processual penal geral que consta dos artigos 11º a 19º da Lei nº 109/2009. 13. Consequentemente devemos concluir que o regime processual da Lei 32/2008, designadamente o artigo 3º, nº 1 e 2 e o artigo 9º: - mostra-se revogado e substituído pelo regime processual contido na Lei nº 109/2009 para todos os dados que não estejam especificamente previstos no artigo 4º, n. 1 da Lei nº 32/2008 ou seja, dados conservados em geral; - revela-se vigente para todos os dados que estejam especificamente previstos no artigo 4º, n. 1 da Lei nº 32/2008, isto é, para os dados conservados relativos á localização celular. Só para este último caso ganha relevo o conceito de «crime grave». 14. Antes da entrada em vigor das Leis 32/2008 e 109/2009 podia afirmar-se que havia duas formas úteis «processualmente úteis» de usar a localização celular. Uma delas a medida cautelar de polícia prevista no artigo 252º-A do C.P.P. e a outra o meio de obtenção de prova previsto no artigo 189º, n. 2 do mesmo código, que se mantém em vigor para a localização celular em tempo real. 15. Agora co-existem três realidades distintas através do acrescento da obtenção de dados de localização celular «conservados» por via da Lei nº 32/2008.16. Os requisitos do número 3 do artigo 9º da Lei 32/2008 mostram-se de verificação alternativa. O conceito de «suspeito» dele constante exige «determinabilidade» e não «determinação». 17. A previsão do artigo 252º-A do Código de Processo Penal é claramente uma previsão de carácter excepcional para situações de carácter excepcional.

3. Ac. TRL de 22-04-2013: - A obtenção de um concreto endereço IP que esteve na origem da uma determinada comunicação efetuada é da competência do Ministério Público - e não do juiz.

Artigo 15.º

Pesquisa de dados informáticos

1 - Quando 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 autoriza ou ordena por despacho que se proceda a uma pesquisa nesse sistema informático, devendo, sempre que possível, presidir à diligência.

2 - O despacho previsto no número anterior tem um prazo de validade máximo de 30 dias, sob pena de nulidade.

3 - O órgão de polícia criminal pode proceder à pesquisa, sem prévia autorização da autoridade judiciária, quando:

a) A mesma for voluntariamente consentida por quem tiver a disponibilidade ou controlo desses dados, desde que o consentimento prestado fique, por qualquer forma, documentado;

b) Nos casos de terrorismo, criminalidade violenta ou altamente organizada, quando haja fundados indícios da prática iminente de crime que ponha em grave risco a vida ou a integridade de qualquer pessoa.

4 - Quando o órgão de polícia criminal proceder à pesquisa nos termos do número anterior:

a) No caso previsto na alínea b), a realização da diligência é, sob pena de nulidade, imediatamente comunicada à autoridade judiciária competente e por esta apreciada em ordem à sua validação;

b) Em qualquer caso, é elaborado e remetido à autoridade judiciária competente o relatório previsto no artigo 253.º do Código de Processo Penal.

5 - Quando, no decurso de pesquisa, surgirem razões para crer que os dados procurados se encontram noutro sistema informático, ou numa parte diferente do sistema pesquisado, mas que tais dados são legitimamente acessíveis a partir do sistema inicial, a pesquisa pode ser estendida mediante autorização ou ordem da autoridade competente, nos termos dos n.os 1 e 2.

6 - À pesquisa a que se refere este artigo são aplicáveis, com as necessárias adaptações, as regras de execução das buscas previstas no Código de Processo Penal e no Estatuto do Jornalista.

Jurisprudência

1. Ac. TRE de 20-01-2015 : 1. O regime processual das comunicações telefónicas previsto nos artigos 187º a 190º do Código de Processo Penal deixou de ser aplicável por extensão ás «telecomunicações electrónicas», «crimes informáticos» e «recolha de prova electrónica (informática)» desde a entrada em vigor da Lei 109/2009, de 15-09 (Lei do Cibercrime) como regime regra. 2. Esse mesmo regime processual das comunicações telefónicas deixara de ser aplicável á recolha de prova por «localização celular conservada» - uma forma de «recolha de prova electrónica - desde a entrada em vigor da Lei 32/2008, de 17-07. 3. Para a prova electrónica preservada ou conservada em sistemas informáticos existe um novo sistema processual penal, o previsto nos artigos 11º a 19º da Lei 109/2009, de 15-09, Lei do Cibercrime, coadjuvado pela Lei nº 32/2008, neste caso se estivermos face á prova por «localização celular conservada». 4. Nessa Lei do Cibercrime coexistem dois regimes processuais: o regime dos artigos 11º a 17º e o regime dos artigos 18º e 19º do mesmo diploma. O regime processual dos artigos 11º a 17º surge como o regime processual «geral» do cibercrime e da prova electrónica. Isto porquanto existe um segundo catálogo na Lei n. 109/2009, o do artigo 18º, n. 1 do mesmo diploma a que corresponde um segundo regime processual de autorização e regulação probatória. Só a este segundo regime - o dos artigos 18º e 19º - são aplicáveis por remissão expressa os artigos 187º, 188º e 190º do C.P.P. e sob condição de não contrariarem e Lei 109/2009. 5. As normas contidas nos artigos 12º a 17º da supramencionada Lei contêm um completo regime processual penal para os crimes que, nos termos das alíneas do n. 1 do artigo 11º, estão (a) previstos na lei nº 109/2009, (b) são ou foram cometidos por meio de um sistema informático ou (c) em relação aos quais seja necessário proceder á recolha de prova em suporte electrónico. 6. A diferenciação de regimes assenta na circunstância de os dados preservados nos termos dos

artigos 12º a 17º se referirem á pesquisa e recolha, para prova, de dados já produzidos mas preservados, armazenados, enquanto o artigo 18º do diploma se refere á intercepção de comunicações electrónicas, em tempo real, de dados de tráfego e de conteúdo associados a comunicações específicas transmitidas através de um sistema informático. 7. Assim, o Capítulo III da Lei 109/2009, relativo ás disposições processuais, deve ser encarado como um «escondido Capítulo V («Da prova electrónica»), do Título III («Meios de obtenção de prova») do Livro III («Da prova») do Código de Processo Penal» (Dá Mesquita). 8. Tratando-se de obter prova por «localização celular conservada», isto é, a obtenção dos dados previstos no artigo 4º, n. 1 da Lei 32/2008, de 17-07, o regime processual aplicável assume especialidade nos artigos 3º e 9º desta lei. 9. Em suma, numa interpretação conjugada das Leis 32/2008, 109/2009 e da Convenção de Budapeste sobre o Cibercrime do Conselho da Europa (aprovada pela Resolução da Assembleia da República nº 88/2009, publicada no DR de 15-09-2009), devem ter-se em consideração os seguintes catálogos de crimes quanto a dados preservados ou conservados: - o catálogo de crimes do n. 1 do artigo 11º da Lei 109/2009 como pressuposto de aplicação do regime processual contido nos artigos 11º a 17º dessa Lei; - o catálogo de crimes do n. 1 do artigo 18º da Lei 109/2009 como pressuposto de aplicação do regime processual contido nesse artigo 18º e no 19º dessa Lei aos crimes previstos na al. a) do artigo 18º; - o catálogo de crimes do n. 1 do artigo 187º do Código de Processo Penal, por remissão expressa da Lei 109/2009, como pressuposto de aplicação do regime processual contido nesse artigo 18º e no 19º dessa Lei para os crimes previstos na al. b) do artigo 18º; - o catálogo de crimes («crimes graves») do artigo 3º da Lei nº 32/2008 quanto a especiais «dados conservados» (localização celular), como requisito de aplicação dos artigos 3º e 9º da Lei nº 32/2008. 10. O artigo 189º do Código de Processo Penal nunca é aplicável a crimes informáticos, seja qual for o catálogo aplicável. 11. O objecto de ambas as leis - de 2008 e 2009 - é parcialmente coincidente. Ambas se referem e regulam «dados conservados» (Lei nº 32/2008) e «dados preservados» (Lei nº 109/2009) ou seja, depositados, armazenados, arquivados, guardados. A Lei de 2009 assume um carácter geral no seu âmbito de aplicação, não distinguindo dados arquivados pela sua natureza, o que abrange todos eles, portanto (á excepção do correio electrónico, especificamente previsto no seu artigo 17º). 12. O regime processual da Lei nº 32/2008 constitui relativamente aos dados «conservados» que prevê no seu artigo 4º, um regime especial relativamente ao capítulo processual penal geral que consta dos artigos 11º a 19º da Lei nº 109/2009. 13. Consequentemente devemos concluir que o regime processual da Lei 32/2008, designadamente o artigo 3º, nº 1 e 2 e o artigo 9º: - mostra-se revogado e substituído pelo regime processual contido na Lei nº 109/2009 para todos os dados que não estejam especificamente previstos no artigo 4º, n. 1 da Lei nº 32/2008 ou seja, dados conservados em geral; - revela-se vigente para todos os dados que estejam especificamente previstos no artigo 4º, n. 1 da Lei nº 32/2008, isto é, para os dados conservados relativos á localização celular. Só para este último caso ganha relevo o conceito de «crime grave». 14. Antes da entrada em vigor das Leis 32/2008 e 109/2009 podia afirmar-se que havia duas formas úteis «processualmente úteis» de usar a localização celular. Uma delas a medida cautelar de polícia prevista no artigo 252º-A do C.P.P. e a outra o meio de obtenção de prova previsto no artigo 189º, n. 2 do mesmo código, que se mantém em vigor para a localização celular em tempo real. 15. Agora co-existem três realidades distintas através do acrescento da obtenção de dados de localização celular «conservados» por via da Lei nº 32/2008.16. Os requisitos do número 3 do artigo 9º da Lei 32/2008 mostram-se de verificação alternativa. O conceito de «suspeito» dele constante exige «determinabilidade» e não «determinação». 17. A previsão do artigo 252º-A do Código de Processo Penal é claramente uma previsão de carácter excepcional para situações de carácter excepcional.

2. Ac. TRG de 15-04-2012: - A transcrição de mensagens SMS do telemóvel de um queixoso que espontaneamente as fornece, pode valer como prova, apesar de não ter sido ordenada pelo juiz. Só será necessária a intervenção do JIC quando quem fornece aquelas mensagens não puder dispor delas.

3. Ac. TRP de 12-09-2012: - A jurisprudência tem equiparado as mensagens SMS ? s cartas de correio, distinguindo se ainda estão fechadas ou se foram já abertas pelo destinatário. Porém, a Lei do Cibercrime alterou esta abordagem: a leitura de mensagens guardadas num cartão de telemóvel por um agente policial sem autorização do seu dono ou do JIC é prova proibida, em nada relevando que as mesmas tivessem sido ou não abertas e lidas pelo destinatário pois que a lei não distingue entre essas duas situações.

Artigo 16.º

Apreensão de dados informáticos

1 - Quando, no decurso de uma pesquisa informática ou de outro acesso legítimo a um sistema informático, forem encontrados dados ou documentos informáticos necessários à produção de prova, tendo em vista a descoberta da verdade, a autoridade judiciária competente autoriza ou ordena por despacho a apreensão dos mesmos.

2 - O órgão de polícia criminal pode efectuar apreensões, sem prévia autorização da autoridade judiciária, no decurso de pesquisa informática legitimamente ordenada e executada nos termos do artigo anterior, bem como quando haja urgência ou perigo na demora.

3 - Caso sejam apreendidos dados ou documentos informáticos cujo conteúdo seja susceptível de revelar dados pessoais ou íntimos, que possam pôr em causa a privacidade do respectivo titular ou de terceiro, sob pena de nulidade esses dados ou documentos são apresentados ao juiz, que ponderará a sua junção aos autos tendo em conta os interesses do caso concreto.

4 - As apreensões efectuadas por órgão de polícia criminal são sempre sujeitas a validação pela autoridade judiciária, no prazo máximo de 72 horas.

5 - As apreensões relativas a sistemas informáticos utilizados para o exercício da advocacia e das actividades médica e bancária estão sujeitas, com as necessárias adaptações, às regras e formalidades previstas no Código de Processo Penal e as relativas a sistemas informáticos utilizados para o exercício da profissão de jornalista estão sujeitas, com as necessárias adaptações, às regras e formalidades previstas no Estatuto do Jornalista.

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

7 - A apreensão de dados informáticos, consoante seja mais adequado e proporcional, tendo em conta os interesses do caso concreto, pode, nomeadamente, revestir as formas seguintes:

a) Apreensão do suporte onde está instalado o sistema ou apreensão do suporte onde estão armazenados os dados informáticos, bem como dos dispositivos necessários à respectiva leitura;

b) Realização de uma cópia dos dados, em suporte autónomo, que será junto ao processo;

c) Preservação, por meios tecnológicos, da integridade dos dados, sem realização de cópia nem remoção dos mesmos; ou

d) Eliminação não reversível ou bloqueio do acesso aos dados.

8 - No caso da apreensão efectuada nos termos da alínea b) do número anterior, a cópia é efectuada em duplicado, sendo uma das cópias selada e confiada ao secretário judicial dos serviços onde o processo correr os seus termos e, se tal for tecnicamente possível, os dados apreendidos são certificados por meio de assinatura digital.

Jurisprudência

1. Ac. TRE de 20-01-2015 : 1. O regime processual das comunicações telefónicas previsto nos artigos 187º a 190º do Código de Processo Penal deixou de ser aplicável por extensão ás «telecomunicações electrónicas», «crimes informáticos» e «recolha de prova electrónica (informática)» desde a entrada em vigor da Lei 109/2009, de 15-09 (Lei do Cibercrime) como regime regra. 2. Esse mesmo regime processual das comunicações telefónicas deixara de ser aplicável á recolha de prova por «localização celular conservada» - uma forma de «recolha de prova electrónica - desde a entrada em vigor da Lei 32/2008, de 17-07. 3. Para a prova electrónica preservada ou conservada em sistemas informáticos existe um novo sistema processual penal, o previsto nos artigos 11º a 19º da Lei 109/2009, de 15-09, Lei do Cibercrime, coadjuvado pela Lei nº 32/2008, neste caso se estivermos face á prova por «localização celular conservada». 4. Nessa Lei do Cibercrime coexistem dois regimes processuais: o regime dos artigos 11º a 17º e o regime dos artigos 18º e 19º do mesmo diploma. O regime processual dos artigos 11º a 17º surge como o regime processual «geral» do cibercrime e da prova electrónica. Isto porquanto existe um segundo catálogo na Lei n. 109/2009, o do artigo 18º, n. 1 do mesmo diploma a que corresponde um segundo regime processual de autorização e regulação probatória. Só a este segundo regime - o dos artigos 18º e 19º - são aplicáveis por remissão expressa os artigos 187º, 188º e 190º do C.P.P. e sob condição de não contrariarem e Lei 109/2009. 5. As normas contidas nos artigos 12º a 17º da supramencionada Lei contêm um completo regime processual penal para os crimes que, nos termos das alíneas do n. 1 do artigo 11º, estão (a) previstos na lei nº 109/2009, (b) são ou foram cometidos por meio de um sistema informático ou (c) em relação aos quais seja necessário proceder á recolha de prova em suporte electrónico. 6. A diferenciação de regimes assenta na circunstância de os dados preservados nos termos dos artigos 12º a 17º se referirem á pesquisa e recolha, para prova, de dados já produzidos mas preservados, armazenados, enquanto o artigo 18º do diploma se refere á intercepção de comunicações electrónicas, em tempo real, de dados de tráfego e de conteúdo associados a comunicações específicas transmitidas através de um sistema informático. 7. Assim, o Capítulo III da Lei 109/2009, relativo ás disposições processuais, deve ser encarado como um «escondido Capítulo V («Da prova electrónica»), do Título III («Meios de obtenção de prova») do Livro III («Da prova») do Código de Processo Penal» (Dá Mesquita). 8. Tratando-se de obter prova por «localização celular conservada», isto é, a obtenção dos dados previstos no artigo 4º, n. 1 da Lei 32/2008, de 17-07, o regime

processual aplicável assume especialidade nos artigos 3º e 9º desta lei. 9. Em suma, numa interpretação conjugada das Leis 32/2008, 109/2009 e da Convenção de Budapeste sobre o Cibercrime do Conselho da Europa (aprovada pela Resolução da Assembleia da República nº 88/2009, publicada no DR de 15-09-2009), devem ter-se em consideração os seguintes catálogos de crimes quanto a dados preservados ou conservados: - o catálogo de crimes do n. 1 do artigo 11º da Lei 109/2009 como pressuposto de aplicação do regime processual contido nos artigos 11º a 17º dessa Lei; - o catálogo de crimes do n. 1 do artigo 18º da Lei 109/2009 como pressuposto de aplicação do regime processual contido nesse artigo 18º e no 19º dessa Lei aos crimes previstos na al. a) do artigo 18º; - o catálogo de crimes do n. 1 do artigo 187º do Código de Processo Penal, por remissão expressa da Lei 109/2009, como pressuposto de aplicação do regime processual contido nesse artigo 18º e no 19º dessa Lei para os crimes previstos na al. b) do artigo 18º; - o catálogo de crimes («crimes graves») do artigo 3º da Lei nº 32/2008 quanto a especiais «dados conservados» (localização celular), como requisito de aplicação dos artigos 3º e 9º da Lei nº 32/2008. 10. O artigo 189º do Código de Processo Penal nunca é aplicável a crimes informáticos, seja qual for o catálogo aplicável. 11. O objecto de ambas as leis - de 2008 e 2009 - é parcialmente coincidente. Ambas se referem e regulam «dados conservados» (Lei nº 32/2008) e «dados preservados» (Lei nº 109/2009) ou seja, depositados, armazenados, arquivados, guardados. A Lei de 2009 assume um carácter geral no seu âmbito de aplicação, não distinguindo dados arquivados pela sua natureza, o que abrange todos eles, portanto (á excepção do correio electrónico, especificamente previsto no seu artigo 17º). 12. O regime processual da Lei nº 32/2008 constitui relativamente aos dados «conservados» que prevê no seu artigo 4º, um regime especial relativamente ao capítulo processual penal geral que consta dos artigos 11º a 19º da Lei nº 109/2009. 13. Consequentemente devemos concluir que o regime processual da Lei 32/2008, designadamente o artigo 3º, nº 1 e 2 e o artigo 9º: - mostra-se revogado e substituído pelo regime processual contido na Lei nº 109/2009 para todos os dados que não estejam especificamente previstos no artigo 4º, n. 1 da Lei nº 32/2008 ou seja, dados conservados em geral; - revela-se vigente para todos os dados que estejam especificamente previstos no artigo 4º, n. 1 da Lei nº 32/2008, isto é, para os dados conservados relativos á localização celular. Só para este último caso ganha relevo o conceito de «crime grave». 14. Antes da entrada em vigor das Leis 32/2008 e 109/2009 podia afirmar-se que havia duas formas úteis «processualmente úteis» de usar a localização celular. Uma delas a medida cautelar de polícia prevista no artigo 252º-A do C.P.P. e a outra o meio de obtenção de prova previsto no artigo 189º, n. 2 do mesmo código, que se mantém em vigor para a localização celular em tempo real. 15. Agora co-existem três realidades distintas através do acrescento da obtenção de dados de localização celular «conservados» por via da Lei nº 32/2008.16. Os requisitos do número 3 do artigo 9º da Lei 32/2008 mostram-se de verificação alternativa. O conceito de «suspeito» dele constante exige «determinabilidade» e não «determinação». 17. A previsão do artigo 252º-A do Código de Processo Penal é claramente uma previsão de carácter excepcional para situações de carácter excepcional.

2. Ac. TRP de 05.04.2017 I ? O Facebook é uma rede social que funciona através da internet, operando no âmbito de um sistema informático pelo que a recolha de prova está sujeita ? Lei do Cibercrime - DL 109/2009 de 15/9.II ? Constitui prova legal a cópia de informação que alguém publicita no seu mural do Facebook sem restrição de acesso.III ? Só esta sujeita ? disciplina do art.º 16º 1 e 3 da Lei do Cibercrime a apreensão da informação original inserta na plataforma, esteja ou não disponível.

3. Ac. TRL de 11-05-2023:
I A Lei do Cibercrime é uma legislação especial que veio estabelecer disposições penais materiais e processuais relativas ao domínio do cibercrime e da recolha de prova em suporte electrónico (secundarizando o Código de Processo Penal) para fazer face a novas realidades e inerentes especificidades, tais como dos dados informáticos e do correio electrónico, justificando-se o sacrifício do interesse individual numa comunicação livre de interferências alheias, em prol do exercício do ?ius puniendi? estadual.
II - Mas, a apreensão (mesmo gozando de legitimidade formal pela existência de prévia autorização ou ordem judicial de apreensão) não legitima, ?per si?, a valoração dos elementos probatórios assim conseguidos. Para o efeito, é ainda necessário que o Juiz seja a primeira pessoa a tomar conhecimento do conteúdo apreendido, conhecimento esse que não tem de ser obrigatoriamente completo/total. Depois, os elementos apreendidos podem ser enviados pelo Juiz ao Ministério Público para que este emita proposta/parecer sobre a relevância, ou não, para a descoberta da verdade ou para a prova dos factos em investigação (pelo mesmo (Ministério Público face ? estrutura acusatória de qualquer processo penal).Então o Juiz estará em condições de melhor aferir qual o conteúdo relevante e ponderar da necessidade, ou não, da sua junção aos autos como meios de prova e, em caso afirmativo, com a inerente compressão de direitos constitucionais.
III - O Juiz de instrução é um garante dos direitos fundamentais dos diversos intervenientes no processo penal, porém não controla o exercício da ação penal.A intervenção do Juiz de Instrução Criminal em sede de inquérito deve pautar-se por um princípio da intervenção enquanto Juiz das liberdades (e não como Juiz de investigação), respeitando o modelo constitucional de divisão de funções entre a magistratura judicial e a magistratura do Ministério Público.

Artigo 17.º

Apreensão de correio electrónico e registos de comunicações de natureza semelhante

Quando, no decurso de uma pesquisa informática ou outro acesso legítimo a um sistema informático, forem encontrados, armazenados nesse sistema informático ou noutro a que seja permitido o acesso legítimo a partir do primeiro, mensagens de correio electrónico ou registos de comunicações de natureza semelhante, o juiz pode autorizar ou ordenar, por despacho, a apreensão daqueles que se afigurem ser de grande interesse para a descoberta da verdade ou para a prova, aplicando-se correspondentemente o regime da apreensão de correspondência previsto no Código de Processo Penal.

Jurisprudência

1. Ac. TRE de 20-01-2015 : 1. O regime processual das comunicações telefónicas previsto nos artigos 187º a 190º do Código de Processo Penal deixou de ser aplicável por extensão ás «telecomunicações electrónicas», «crimes informáticos» e «recolha de prova electrónica (informática)» desde a entrada em vigor da Lei 109/2009, de 15-09 (Lei do Cibercrime) como regime regra. 2. Esse mesmo regime processual das comunicações telefónicas deixara de ser aplicável á recolha de prova por «localização celular conservada» - uma forma de «recolha de prova electrónica - desde a entrada em vigor da Lei 32/2008, de 17-07. 3. Para a prova electrónica preservada ou conservada em sistemas informáticos existe um novo sistema processual penal, o previsto nos artigos 11º a 19º da Lei 109/2009, de 15-09, Lei do Cibercrime, coadjuvado pela Lei nº 32/2008, neste caso se estivermos face á prova por «localização celular conservada». 4. Nessa Lei do Cibercrime coexistem dois regimes processuais: o regime dos artigos 11º a 17º e o regime dos artigos 18º e 19º do mesmo diploma. O regime processual dos artigos 11º a 17º surge como o regime processual «geral» do cibercrime e da prova electrónica. Isto porquanto existe um segundo catálogo na Lei n. 109/2009, o do artigo 18º, n. 1 do mesmo diploma a que corresponde um segundo regime processual de autorização e regulação probatória. Só a este segundo regime - o dos artigos 18º e 19º - são aplicáveis por remissão expressa os artigos 187º, 188º e 190º do C.P.P. e sob condição de não contrariarem e Lei 109/2009. 5. As normas contidas nos artigos 12º a 17º da supramencionada Lei contêm um completo regime processual penal para os crimes que, nos termos das alíneas do n. 1 do artigo 11º, estão (a) previstos na lei nº 109/2009, (b) são ou foram cometidos por meio de um sistema informático ou (c) em relação aos quais seja necessário proceder á recolha de prova em suporte electrónico. 6. A diferenciação de regimes assenta na circunstância de os dados preservados nos termos dos artigos 12º a 17º se referirem á pesquisa e recolha, para prova, de dados já produzidos mas preservados, armazenados, enquanto o artigo 18º do diploma se refere á intercepção de comunicações electrónicas, em tempo real, de dados de tráfego e de conteúdo associados a comunicações específicas transmitidas através de um sistema informático. 7. Assim, o Capítulo III da Lei 109/2009, relativo ás disposições processuais, deve ser encarado como um «escondido Capítulo V («Da prova electrónica»), do Título III («Meios de obtenção de prova») do Livro III («Da prova») do Código de Processo Penal» (Dá Mesquita). 8. Tratando-se de obter prova por «localização celular conservada», isto é, a obtenção dos dados previstos no artigo 4º, n. 1 da Lei 32/2008, de 17-07, o regime processual aplicável assume especialidade nos artigos 3º e 9º desta lei. 9. Em suma, numa interpretação conjugada das Leis 32/2008, 109/2009 e da Convenção de Budapeste sobre o Cibercrime do Conselho da Europa (aprovada pela Resolução da Assembleia da República nº 88/2009, publicada no DR de 15-09-2009), devem ter-se em consideração os seguintes catálogos de crimes quanto a dados preservados ou conservados: - o catálogo de crimes do n. 1 do artigo 11º da Lei 109/2009 como pressuposto de aplicação do regime processual contido nos artigos 11º a 17º dessa Lei; - o catálogo de crimes do n. 1 do artigo 18º da Lei 109/2009 como pressuposto de aplicação do regime processual contido nesse artigo 18º e no 19º dessa Lei aos crimes previstos na al. a) do artigo 18º; - o catálogo de crimes do n. 1 do artigo 187º do Código de Processo Penal, por remissão expressa da Lei 109/2009, como pressuposto de aplicação do regime processual contido nesse artigo 18º e no 19º dessa Lei para os crimes previstos na al. b) do artigo 18º; - o catálogo de crimes («crimes graves») do artigo 3º da Lei nº 32/2008 quanto a especiais «dados conservados» (localização celular), como requisito de aplicação dos artigos 3º e 9º da Lei nº 32/2008. 10. O artigo 189º do Código de Processo Penal nunca é aplicável a crimes informáticos, seja qual for o catálogo aplicável. 11. O objecto de ambas as leis - de 2008 e 2009 - é parcialmente coincidente. Ambas se referem e regulam «dados conservados» (Lei nº 32/2008) e «dados preservados» (Lei nº 109/2009) ou seja, depositados, armazenados, arquivados, guardados. A Lei de 2009 assume um carácter geral no seu âmbito de aplicação, não distinguindo dados arquivados pela sua natureza, o que abrange todos eles, portanto (á excepção do correio electrónico, especificamente previsto no seu artigo 17º). 12. O regime processual da Lei nº 32/2008 constitui relativamente aos dados «conservados» que prevê no seu artigo 4º, um regime especial relativamente ao capítulo processual penal geral que consta dos artigos 11º a 19º da Lei nº 109/2009. 13. Consequentemente devemos concluir que o regime processual da Lei 32/2008, designadamente o artigo 3º, nº 1 e 2 e o artigo 9º: - mostra-se revogado e substituído pelo regime processual contido na Lei nº 109/2009 para todos os dados que não estejam especificamente previstos no artigo 4º, n. 1 da Lei nº 32/2008 ou seja, dados conservados em geral; - revela-se vigente para todos os dados que estejam especificamente previstos no artigo 4º, n. 1 da Lei nº 32/2008, isto é, para os dados conservados relativos á localização celular. Só para este último caso ganha

relevo o conceito de «crime grave». 14. Antes da entrada em vigor das Leis 32/2008 e 109/2009 podia afirmar-se que havia duas formas úteis «processualmente úteis» de usar a localização celular. Uma delas a medida cautelar de polícia prevista no artigo 252º-A do C.P.P. e a outra o meio de obtenção de prova previsto no artigo 189º, n. 2 do mesmo código, que se mantém em vigor para a localização celular em tempo real. 15. Agora co-existem três realidades distintas através do acrescento da obtenção de dados de localização celular «conservados» por via da Lei nº 32/2008.16. Os requisitos do número 3 do artigo 9º da Lei 32/2008 mostram-se de verificação alternativa. O conceito de «suspeito» dele constante exige «determinabilidade» e não «determinação». 17. A previsão do artigo 252º-A do Código de Processo Penal é claramente uma previsão de carácter excepcional para situações de carácter excepcional.

2. Ac. TRG de 15-04-2012: - A transcrição de mensagens SMS do telemóvel de um queixoso que espontaneamente as fornece, pode valer como prova, apesar de não ter sido ordenada pelo juiz. Só será necessária a intervenção do JIC quando quem fornece aquelas mensagens não puder dispor delas.

3. Ac. TRP de 12-09-2012: - A jurisprudência tem equiparado as mensagens SMS ? s cartas de correio, distinguindo se ainda estão fechadas ou se foram já abertas pelo destinatário. Porém, a Lei do Cibercrime alterou esta abordagem: a leitura de mensagens guardadas num cartão de telemóvel por um agente policial sem autorização do seu dono ou do JIC é prova proibida, em nada relevando que as mesmas tivessem sido ou não abertas e lidas pelo destinatário pois que a lei não distingue entre essas duas situações.

4. Ac. TRG de 29-03-2011: - A apreensão de mensagens de telemóvel (SMS), mesmo que resultante de uma pesquisa de dados informáticos validamente ordenada pelo Ministério Público, deve depois ser autorizada pelo JIC. Embora o MP deva tomar conhecimento em primeira das mensagens, ordenando a apreensão provisória, deve depois ser o juiz a ordenar a apreensão definitiva - Artigo 17º da Lei do Cibercrime. A lei não estabelece distinção entre mensagens por abrir e abertas.

5. Ac. TRL de 11-01-2011: - Quanto ? apreensão de mensagens de correio eletrónico ou registos de comunicações de natureza semelhante, a Lei do Cibercrime, ao remeter para o regime geral previsto no Código de Processo Penal, determina a aplicação deste regime na sua totalidade, sem redução do seu âmbito - tais apreensões têm de ser autorizadas ou determinadas por despacho judicial, devendo ser o juiz a primeira pessoa a tomar conhecimento do conteúdo da correspondência apreendida, sob pena de nulidade.

6. Ac. TRL de 06.02.2018 Correio electrónico. Apreensão de correspondência. A Lei do Cibercrime, lei nº 109/2009, de 15 de Setembro, a qual transpõe para a ordem jurídica interna a Decisão Quadro nº 2005/222/JAI, do Conselho da Europa, de 24 de Fevereiro, relativa a ataques contra sistemas de informação e adapta o direito interno ? Convenção sobre Cibercrime do Conselho da Europa, determina no seu art.º 17º, sob a epígrafe da ?apreensão de correio electrónico e registo de comunicações de natureza semelhante?, dispõe que, quando no decurso de uma pesquisa informática ou outro acesso legítimo a um sistema informático, forem encontrados armazenados nesse sistema informático ou noutro que seja permitido o acesso legítimo a partir do primeiro, mensagens de correio electrónico ou registos de comunicações de natureza semelhante, o juiz pode autorizar ou ordenar, por despacho, a apreensão daqueles que se afigurem de grande interesse para a descoberta da verdade ou para a prova, aplicando-se correspondentemente o regime de apreensão de correspondência previsto no Código de Processo Penal.Aplicando-se assim o regime de apreensão de correspondência previsto no Código de Processo Penal, este encontra-se disciplinado no art.º 179º, o qual estabelece desde logo no n.º 1 que tais apreensões sejam determinadas por despacho judicial, ?sob pena de nulidade? expressa (n.º 1), e que ?o juiz que tiver autorizado ou ordenado a diligência é a primeira pessoa a tomar conhecimento do conteúdo da correspondência apreendida?, o que se aplica ao correio electrónico já convertido em ficheiro legível, o que constitui acto da competência exclusiva do Juiz de Instrução Criminal, nos termos do art.º 268º n.º 1 alínea d) do CPP, o qual estabelece que ?compete exclusivamente ao juiz de instrução, tomar conhecimento, em primeiro lugar, do conteúdo da correspondência apreendida?, o que se estendeu ao conteúdo do correio electrónico, por força da subsequente Lei nº 109/2009, de 15 de Setembro, constituindo a sua violação nulidade expressa absoluta e que se reconduz, a final, ao regime de proibição de prova.A falta de exame da correspondência pelo juiz constitui uma nulidade prevista no art.º 120º n.º 2 alínea d) do CPP, por se tratar de um acto processual legalmente obrigatório.

7. Ac. TRL de 11-05-2023:
I A Lei do Cibercrime é uma legislação especial que veio estabelecer disposições penais materiais e processuais relativas ao domínio do cibercrime e da recolha de prova em suporte electrónico (secundarizando o Código de Processo Penal) para fazer face a novas realidades e inerentes especificidades, tais como dos dados informáticos e do correio electrónico, justificando-se o sacrifício do interesse individual numa comunicação livre de interferências alheias, em prol do exercício do ?ius puniendi? estadual.
II - Mas, a apreensão (mesmo gozando de legitimidade formal pela existência de prévia autorização ou ordem judicial de apreensão) não legitima, ?per si?, a valoração dos elementos probatórios assim conseguidos. Para o efeito, é ainda necessário que o Juiz seja a primeira pessoa a tomar conhecimento do conteúdo apreendido, conhecimento esse que não tem de ser obrigatoriamente completo/total. Depois, os elementos apreendidos podem ser enviados pelo Juiz ao Ministério Público para que este emita proposta/parecer sobre a relevância, ou não, para a descoberta da verdade ou para a prova dos factos em investigação (pelo mesmo (Ministério Público face ? estrutura acusatória de qualquer processo penal).Então o Juiz estará em condições de melhor aferir qual o conteúdo relevante e ponderar da necessidade, ou não, da sua junção aos autos como meios de prova e, em caso afirmativo, com a inerente compressão de direitos constitucionais.
III - O Juiz de instrução é um garante dos direitos fundamentais dos diversos intervenientes no processo penal, porém não controla o exercício da ação penal.A intervenção do Juiz de Instrução Criminal em sede de inquérito deve pautar-se por um princípio da intervenção enquanto Juiz das liberdades (e não como Juiz de investigação), respeitando o modelo constitucional de divisão de funções entre a magistratura judicial e a magistratura do Ministério Público.

Jurisprudência obrigatória

1. Ac. STJ n.º 10/2023, de 10 de novembro: «Na fase de inquérito, compete ao juiz de instrução ordenar ou autorizar a apreensão de mensagens de correio eletrónico ou de outros registos de comunicações de natureza semelhante, independentemente de se encontrarem abertas (lidas) ou fechadas (não lidas), que se afigurem ser de grande interesse para descoberta da verdade ou para a prova, nos termos do art. 17.º, da Lei n.º 109/2009, de 15/09 (Lei do Cibercrime)»

Artigo 18.º

Intercepção de comunicações

1 - É admissível o recurso à intercepção de comunicações em processos relativos a crimes:

a) Previstos na presente lei; ou

b) Cometidos por meio de um sistema informático ou em relação aos quais seja necessário proceder à recolha de prova em suporte electrónico, quando tais crimes se encontrem previstos no artigo 187.º do Código de Processo Penal.

2 - A intercepção e o registo de transmissões de dados informáticos só podem ser autorizados 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.

3 - A intercepção pode destinar-se ao registo de dados relativos ao conteúdo das comunicações ou visar apenas a recolha e registo de dados de tráfego, devendo o despacho referido no número anterior especificar o respectivo âmbito, de acordo com as necessidades concretas da investigação.

4 - Em tudo o que não for contrariado pelo presente artigo, à intercepção e registo de transmissões de dados informáticos é aplicável o regime da intercepção e gravação de conversações ou comunicações telefónicas constante dos artigos 187.º, 188.º e 190.º do Código de Processo Penal.

Jurisprudência

1. Ac. TRL de 19-06-2014 : I. estando apenas em causa a obtenção da identificação de um utilizador de um endereço IP ou o número de IP usado por um determinado indivíduo, em circunstâncias temporais determinadas, a competência para a respectiva obtenção é do M°P° II. a identificação de um determinado endereço de IP conjugada com a identidade de quem o utilizou num dado dia e hora não revela informação sobre o percurso da comunicação nem sobre outro eventual tráfego comunicacional da pessoa em causa III. os direitos constitucionais dos arguidos não são absolutos, face aos direitos dos restantes cidadãos, mormente das vítimas em processo penal, e as entidades públicas, ao enquadrar o uso dos diversos meios de prova têm de considerar os direitos dos vários intervenientes processuais

2. Ac. TRC, de 04.02.2015 Em inquérito, o pedido ao operador de comunicações do registo de todas as comunicações recebidas (por exemplo SMS, MMs), num período temporal alargado, na medida em que permitem identificar, em tempo real ou ? posterior, os utilizadores, o relacionamento directo entre uns e outros através da rede, a localização, a frequência, a data, hora, e a duração da comunicação, devem participar das garantias a que está submetida a utilização do serviço, especialmente tudo quanto respeite ao sigilo das comunicações. Desde que os dados de base estejam em interligação com dados de tráfego ou dados de conteúdo, torna-se necessária a autorização do Juiz para a sua obtenção e junção aos autos

3. Ac. TRE de 20-01-2015 : 1. O regime processual das comunicações telefónicas previsto nos artigos 187º a 190º do Código de Processo Penal deixou de ser aplicável por extensão ás «telecomunicações electrónicas», «crimes informáticos» e «recolha de prova electrónica (informática)» desde a entrada em vigor da Lei 109/2009, de 15-09 (Lei do Cibercrime) como regime regra. 2. Esse mesmo regime processual das comunicações telefónicas deixara de ser aplicável á recolha de prova por «localização celular conservada» - uma forma de «recolha de prova electrónica - desde a entrada em vigor da Lei 32/2008, de 17-07. 3. Para a prova electrónica preservada ou conservada em sistemas informáticos existe um novo sistema processual penal, o previsto nos artigos 11º a 19º da Lei 109/2009, de 15-09, Lei do Cibercrime, coadjuvado pela Lei nº 32/2008, neste caso se estivermos face á prova por «localização celular conservada». 4. Nessa Lei do Cibercrime coexistem dois regimes processuais: o regime dos artigos 11º a 17º e o regime dos artigos 18º e 19º do mesmo diploma. O regime processual dos artigos 11º a 17º surge como o regime processual «geral» do cibercrime e da prova electrónica. Isto porquanto existe um segundo catálogo na Lei n. 109/2009, o do artigo 18º, n. 1 do mesmo diploma a que corresponde um segundo regime processual de autorização e regulação probatória. Só a este segundo regime - o dos artigos 18º e 19º - são aplicáveis por remissão expressa os artigos 187º, 188º e 190º do C.P.P. e sob condição de não contrariarem e Lei 109/2009. 5. As normas contidas nos artigos 12º a 17º da supramencionada Lei contêm um completo regime processual penal para os crimes que, nos termos das alíneas do n. 1 do artigo 11º, estão (a) previstos na lei nº 109/2009, (b) são ou foram cometidos por meio de um sistema informático ou (c) em relação aos quais seja necessário proceder á recolha de prova em suporte electrónico. 6. A diferenciação de regimes assenta na circunstância de os dados preservados nos termos dos artigos 12º a 17º se referirem á pesquisa e recolha, para prova, de dados já produzidos mas preservados, armazenados, enquanto o artigo 18º do diploma se refere á intercepção de comunicações electrónicas, em tempo real, de dados de tráfego e de conteúdo associados a comunicações específicas transmitidas através de um sistema informático. 7. Assim, o Capítulo III da Lei 109/2009, relativo ás disposições processuais, deve ser encarado como um «escondido Capítulo V («Da prova electrónica»), do Título III («Meios de obtenção de prova») do Livro III («Da prova») do Código de Processo Penal» (Dá Mesquita). 8. Tratando-se de obter prova por «localização celular conservada», isto é, a obtenção dos dados previstos no artigo 4º, n. 1 da Lei 32/2008, de 17-07, o regime processual aplicável assume especialidade nos artigos 3º e 9º desta lei. 9. Em suma, numa interpretação conjugada das Leis 32/2008, 109/2009 e da Convenção de Budapeste sobre o Cibercrime do Conselho da Europa (aprovada pela Resolução da Assembleia da República nº 88/2009, publicada no DR de 15-09-2009), devem ter-se em consideração os seguintes catálogos de crimes quanto a dados preservados ou conservados: - o catálogo de crimes do n. 1 do artigo 11º da Lei 109/2009 como pressuposto de aplicação do regime processual contido nos artigos 11º a 17º dessa Lei; - o catálogo de crimes do n. 1 do artigo 18º da Lei 109/2009 como pressuposto de aplicação do regime processual contido nesse artigo 18º e no 19º dessa Lei aos crimes previstos na al. a) do artigo 18º; - o catálogo de crimes do n. 1 do artigo 187º do Código de Processo Penal, por remissão expressa da Lei 109/2009, como pressuposto de aplicação do regime processual contido nesse artigo 18º e no 19º dessa Lei para os crimes previstos na al. b) do artigo 18º; - o catálogo de crimes («crimes graves») do artigo 3º da Lei nº 32/2008 quanto a especiais «dados conservados» (localização celular), como requisito de aplicação dos artigos 3º e 9º da Lei nº 32/2008. 10. O artigo 189º do Código de Processo Penal nunca é aplicável a crimes informáticos, seja qual for o catálogo aplicável. 11. O objecto de ambas as leis - de 2008 e 2009 - é parcialmente coincidente. Ambas se referem e regulam «dados conservados» (Lei nº 32/2008) e «dados preservados» (Lei nº 109/2009) ou seja, depositados, armazenados, arquivados, guardados. A Lei de 2009 assume um carácter geral no seu âmbito de aplicação, não distinguindo dados arquivados pela sua natureza, o que abrange todos eles, portanto (á excepção do correio electrónico, especificamente previsto no seu artigo 17º). 12. O regime processual da Lei nº 32/2008 constitui relativamente aos dados «conservados» que prevê no seu artigo 4º, um regime especial relativamente ao capítulo processual penal geral que consta dos artigos 11º a 19º da Lei nº 109/2009. 13. Consequentemente devemos concluir que o regime processual da Lei 32/2008, designadamente o artigo 3º, nº 1 e 2 e o artigo 9º: - mostra-se revogado e substituído pelo regime processual contido na Lei nº 109/2009 para todos os dados que não estejam especificamente previstos no artigo 4º, n. 1 da Lei nº 32/2008 ou seja, dados conservados em geral; - revela-se vigente para todos os dados que estejam especificamente previstos no artigo 4º, n. 1 da Lei nº 32/2008, isto é, para os dados conservados relativos á localização celular. Só para este último caso ganha relevo o conceito de «crime grave». 14. Antes da entrada em vigor das Leis 32/2008 e 109/2009 podia afirmar-se que havia duas formas úteis «processualmente úteis» de usar a localização celular. Uma delas a medida cautelar de polícia prevista no artigo 252º-A do C.P.P. e a outra o meio de obtenção de prova previsto no artigo 189º, n. 2 do mesmo código, que se mantém em vigor para a localização celular em tempo real. 15. Agora co-existem três realidades distintas através do acrescento da obtenção de dados de localização celular «conservados» por via da Lei nº 32/2008.16. Os requisitos do número 3 do artigo 9º da Lei 32/2008 mostram-se de verificação alternativa. O conceito de «suspeito» dele constante exige «determinabilidade» e não «determinação». 17. A previsão do artigo 252º-A do Código de Processo Penal é claramente uma previsão de carácter excepcional para situações de carácter excepcional.

4. Ac. TRP de 17-09-2014: - No serviço de telecomunicações a obtenção dos dados de base (isto é, dos dados de conexão ? rede, tais como a identidade do titular do telefone o seu número e a sua morada, ainda que cobertos pelo sistema de confidencialidade a solicitação do assinante) não contendem com a privacidade do seu titular pelo que devem ser comunicados a pedido de qualquer autoridade judiciária.

5. Ac. TRC de 03-10-2012: - O endereço IP é um dado de tráfego, sendo a sua obtenção dependente de autorização do JIC - no despacho recorrido, de JIC, a posição assumida no despacho recorrido era a oposta.

Artigo 19.º

Ações encobertas

1 - É admissível o recurso às ações encobertas previstas na Lei n.º 101/2001, de 25 de agosto, nos termos aí previstos, no decurso de inquérito relativo aos seguintes crimes:

a) Os previstos na presente lei;

b) Os cometidos por meio de um sistema informático, quando lhes corresponda, em abstrato, pena de prisão de máximo superior a 5 anos ou, ainda que a pena seja inferior, e sendo dolosos, os crimes contra a liberdade e autodeterminação sexual nos casos em que os ofendidos sejam menores ou incapazes, a burla qualificada, a burla informática e nas comunicações, o abuso de cartão de garantia ou de cartão, dispositivo ou dados de pagamento, a discriminação racial, religiosa ou sexual, as infrações económico-financeiras, bem como os crimes consagrados no título iv do Código do Direito de Autor e dos Direitos Conexos.

2 - Sendo necessário o recurso a meios e dispositivos informáticos observam-se, naquilo que for aplicável, as regras previstas para a interceção de comunicações.

Contém as alterações dos seguintes diplomas:

- Lei n.º 79/2021, de 24/11

Consultar versões anteriores deste artigo:

-1ª versão: Lei n.º 109/2009, de 15/09

Jurisprudência

1. Ac. TRE de 20-01-2015 : 1. O regime processual das comunicações telefónicas previsto nos artigos 187º a 190º do Código de Processo Penal deixou de ser aplicável por extensão ás «telecomunicações electrónicas», «crimes informáticos» e «recolha de prova electrónica (informática)» desde a entrada em vigor da Lei 109/2009, de 15-09 (Lei do Cibercrime) como regime regra. 2. Esse mesmo regime processual das comunicações telefónicas deixara de ser aplicável á recolha de prova por «localização celular conservada» - uma forma de «recolha de prova electrónica - desde a entrada em vigor da Lei 32/2008, de 17-07. 3. Para a prova electrónica preservada ou conservada em sistemas informáticos existe um novo sistema processual penal, o previsto nos artigos 11º a 19º da Lei 109/2009, de 15-09, Lei do Cibercrime, coadjuvado pela Lei nº 32/2008, neste caso se estivermos face á prova por «localização celular conservada». 4. Nessa Lei do Cibercrime coexistem dois regimes processuais: o regime dos artigos 11º a 17º e o regime dos artigos 18º e 19º do mesmo diploma. O regime processual dos artigos 11º a 17º surge como o regime processual «geral» do cibercrime e da prova electrónica. Isto porquanto existe um segundo catálogo na Lei n. 109/2009, o do artigo 18º, n. 1 do mesmo diploma a que corresponde um segundo regime processual de autorização e regulação probatória. Só a este segundo regime - o dos artigos 18º e 19º - são aplicáveis por remissão expressa os artigos 187º, 188º e 190º do C.P.P. e sob condição de não contrariarem e Lei 109/2009. 5. As normas contidas nos artigos 12º a 17º da supramencionada Lei contêm um completo regime processual penal para os crimes que, nos termos das alíneas do n. 1 do artigo 11º, estão (a) previstos na lei nº 109/2009, (b) são ou foram cometidos por meio de um sistema informático ou (c) em relação aos quais seja necessário proceder á recolha de prova em suporte electrónico. 6. A diferenciação de regimes assenta na circunstância de os dados preservados nos termos dos artigos 12º a 17º se referirem á pesquisa e recolha, para prova, de dados já produzidos mas preservados, armazenados, enquanto o artigo 18º do diploma se refere á intercepção de comunicações electrónicas, em tempo real, de dados de tráfego e de conteúdo associados a comunicações específicas transmitidas

através de um sistema informático. 7. Assim, o Capítulo III da Lei 109/2009, relativo ás disposições processuais, deve ser encarado como um «escondido Capítulo V («Da prova electrónica»), do Título III («Meios de obtenção de prova») do Livro III («Da prova») do Código de Processo Penal» (Dá Mesquita). 8. Tratando-se de obter prova por «localização celular conservada», isto é, a obtenção dos dados previstos no artigo 4º, n. 1 da Lei 32/2008, de 17-07, o regime processual aplicável assume especialidade nos artigos 3º e 9º desta lei. 9. Em suma, numa interpretação conjugada das Leis 32/2008, 109/2009 e da Convenção de Budapeste sobre o Cibercrime do Conselho da Europa (aprovada pela Resolução da Assembleia da República nº 88/2009, publicada no DR de 15-09-2009), devem ter-se em consideração os seguintes catálogos de crimes quanto a dados preservados ou conservados: - o catálogo de crimes do n. 1 do artigo 11º da Lei 109/2009 como pressuposto de aplicação do regime processual contido nos artigos 11º a 17º dessa Lei; - o catálogo de crimes do n. 1 do artigo 18º da Lei 109/2009 como pressuposto de aplicação do regime processual contido nesse artigo 18º e no 19º dessa Lei aos crimes previstos na al. a) do artigo 18º; - o catálogo de crimes do n. 1 do artigo 187º do Código de Processo Penal, por remissão expressa da Lei 109/2009, como pressuposto de aplicação do regime processual contido nesse artigo 18º e no 19º dessa Lei para os crimes previstos na al. b) do artigo 18º; - o catálogo de crimes («crimes graves») do artigo 3º da Lei nº 32/2008 quanto a especiais «dados conservados» (localização celular), como requisito de aplicação dos artigos 3º e 9º da Lei nº 32/2008. 10. O artigo 189º do Código de Processo Penal nunca é aplicável a crimes informáticos, seja qual for o catálogo aplicável. 11. O objecto de ambas as leis - de 2008 e 2009 - é parcialmente coincidente. Ambas se referem e regulam «dados conservados» (Lei nº 32/2008) e «dados preservados» (Lei nº 109/2009) ou seja, depositados, armazenados, arquivados, guardados. A Lei de 2009 assume um carácter geral no seu âmbito de aplicação, não distinguindo dados arquivados pela sua natureza, o que abrange todos eles, portanto (á excepção do correio electrónico, especificamente previsto no seu artigo 17º). 12. O regime processual da Lei nº 32/2008 constitui relativamente aos dados «conservados» que prevê no seu artigo 4º, um regime especial relativamente ao capítulo processual penal geral que consta dos artigos 11º a 19º da Lei nº 109/2009. 13. Consequentemente devemos concluir que o regime processual da Lei 32/2008, designadamente o artigo 3º, nº 1 e 2 e o artigo 9º: - mostra-se revogado e substituído pelo regime processual contido na Lei nº 109/2009 para todos os dados que não estejam especificamente previstos no artigo 4º, n. 1 da Lei nº 32/2008 ou seja, dados conservados em geral; - revela-se vigente para todos os dados que estejam especificamente previstos no artigo 4º, n. 1 da Lei nº 32/2008, isto é, para os dados conservados relativos á localização celular. Só para este último caso ganha relevo o conceito de «crime grave». 14. Antes da entrada em vigor das Leis 32/2008 e 109/2009 podia afirmar-se que havia duas formas úteis «processualmente úteis» de usar a localização celular. Uma delas a medida cautelar de polícia prevista no artigo 252º-A do C.P.P. e a outra o meio de obtenção de prova previsto no artigo 189º, n. 2 do mesmo código, que se mantém em vigor para a localização celular em tempo real. 15. Agora co-existem três realidades distintas através do acrescento da obtenção de dados de localização celular «conservados» por via da Lei nº 32/2008.16. Os requisitos do número 3 do artigo 9º da Lei 32/2008 mostram-se de verificação alternativa. O conceito de «suspeito» dele constante exige «determinabilidade» e não «determinação». 17. A previsão do artigo 252º-A do Código de Processo Penal é claramente uma previsão de carácter excepcional para situações de carácter excepcional.

CAPÍTULO IV
Cooperação internacional

Artigo 20.º
Âmbito da cooperação internacional

As autoridades nacionais competentes cooperam com as autoridades estrangeiras competentes para efeitos de investigações ou procedimentos respeitantes a crimes relacionados com sistemas ou dados informáticos, bem como para efeitos de recolha de prova, em suporte eletrónico, de um crime, de acordo com as normas sobre transferência de dados pessoais previstas na Lei n.º 59/2019, de 8 de agosto.

Contém as alterações dos seguintes diplomas:
- Lei n.º 79/2021, de 24/11

Consultar versões anteriores deste artigo:
-1ª versão: Lei n.º 109/2009, de 15/09

Artigo 21.º
Ponto de contacto permanente para a cooperação internacional

1 - Para fins de cooperação internacional, tendo em vista a prestação de assistência imediata para os efeitos referidos no artigo anterior, a Polícia Judiciária assegura a manutenção de uma estrutura que garante um ponto de contacto disponível em permanência, vinte e quatro horas por dia, sete dias por semana.

2 - Este ponto de contacto pode ser contactado por outros pontos de contacto, nos termos de acordos, tratados ou convenções a que Portugal se encontre vinculado, ou em cumprimento de protocolos de cooperação internacional com organismos judiciários ou policiais.

3 - A assistência imediata prestada por este ponto de contacto permanente inclui:

a) A prestação de aconselhamento técnico a outros pontos de contacto;

b) A preservação expedita de dados nos casos de urgência ou perigo na demora, em conformidade com o disposto no artigo seguinte;

c) A recolha de prova para a qual seja competente nos casos de urgência ou perigo na demora;

d) A localização de suspeitos e a prestação de informações de carácter jurídico, nos casos de urgência ou perigo na demora;

e) A transmissão imediata ao Ministério Público de pedidos relativos às medidas referidas nas alíneas b) a d), fora dos casos aí previstos, tendo em vista a sua rápida execução.

4 - Sempre que atue ao abrigo das alíneas b) a d) do número anterior, a Polícia Judiciária dá notícia imediata do facto ao Ministério Público e remete-lhe o relatório previsto no artigo 253.º do Código de Processo Penal.

5 - O Ministério Público deve, de modo a responder prontamente a pedidos de assistência imediata, assegurar a disponibilidade de magistrados e meios técnicos para levar a cabo quaisquer intervenções processuais urgentes da sua competência.

Contém as alterações dos seguintes diplomas:
- Lei n.º 79/2021, de 24/11

Consultar versões anteriores deste artigo:
-1ª versão: Lei n.º 109/2009, de 15/09

Artigo 22.º
Preservação e revelação expeditas de dados informáticos em cooperação internacional

1 - Pode ser solicitada a Portugal a preservação expedita de dados informáticos armazenados em sistema informático aqui localizado, relativos a crimes previstos no artigo 11.º, com vista à apresentação de um pedido de auxílio judiciário para fins de pesquisa, apreensão e divulgação dos mesmos.

2 - A solicitação especifica:

a) A autoridade que pede a preservação;

b) A infracção que é objecto de investigação ou procedimento criminal, bem como uma breve exposição dos factos relacionados;

c) Os dados informáticos a conservar e a sua relação com a infracção;

d) Todas as informações disponíveis que permitam identificar o responsável pelos dados informáticos ou a localização do sistema informático;

e) A necessidade da medida de preservação; e

f) A intenção de apresentação de um pedido de auxílio judiciário para fins de pesquisa, apreensão e divulgação dos dados.

3 - Em execução de solicitação de autoridade estrangeira competente nos termos dos números anteriores, a autoridade judiciária competente ordena a quem tenha disponibilidade ou controlo desses dados, designadamente a fornecedor de serviço, que os preserve.

4 - A preservação pode também ser ordenada pela Polícia Judiciária mediante autorização da autoridade judiciária competente ou quando haja urgência ou perigo na demora, sendo aplicável, neste último caso, o disposto no n.º 4 do artigo anterior.

5 - A ordem de preservação especifica, sob pena de nulidade:

a) A natureza dos dados;
b) Se forem conhecidos, a origem e o destino dos mesmos; e
c) O período de tempo pelo qual os dados devem ser preservados, até um máximo de três meses.
6 - Em cumprimento de ordem de preservação que lhe seja dirigida, quem tem disponibilidade ou controlo desses dados, designadamente o fornecedor de serviço, preserva de imediato os dados em causa pelo período de tempo especificado, protegendo e conservando a sua integridade.
7 - A autoridade judiciária competente, ou a Polícia Judiciária mediante autorização daquela autoridade, podem ordenar a renovação da medida por períodos sujeitos ao limite previsto na alínea c) do n.º 5, desde que se verifiquem os respectivos requisitos de admissibilidade, até ao limite máximo de um ano.
8 - Quando seja apresentado o pedido de auxílio referido no n.º 1, a autoridade judiciária competente para dele decidir determina a preservação dos dados até à adopção de uma decisão final sobre o pedido.
9 - Os dados preservados ao abrigo do presente artigo apenas podem ser fornecidos:
a) À autoridade judiciária competente, em execução do pedido de auxílio referido no n.º 1, nos mesmos termos em que poderiam sê-lo, em caso nacional semelhante, ao abrigo dos artigos 13.º a 17.º;
b) À autoridade nacional que emitiu a ordem de preservação, nos mesmos termos em que poderiam sê-lo, em caso nacional semelhante, ao abrigo do artigo 13.º
10 - A autoridade nacional à qual, nos termos do número anterior, sejam comunicados dados de tráfego identificadores de fornecedor de serviço e da via através dos quais a comunicação foi efectuada, comunica-os rapidamente à autoridade requerente, por forma a permitir a essa autoridade a apresentação de nova solicitação de preservação expedita de dados informáticos.
11 - O disposto nos n.os 1 e 2 aplica-se, com as devidas adaptações, aos pedidos formulados pelas autoridades portuguesas.

Artigo 23.º

Motivos de recusa

1 - A solicitação de preservação ou revelação expeditas de dados informáticos é recusada quando:
a) Os dados informáticos em causa respeitarem a infracção de natureza política ou infracção conexa segundo as concepções do direito português;
b) Atentar contra a soberania, segurança, ordem pública ou outros interesses da República Portuguesa, constitucionalmente definidos;
c) O Estado terceiro requisitante não oferecer garantias adequadas de protecção dos dados pessoais.
2 - A solicitação de preservação expedita de dados informáticos pode ainda ser recusada quando houver fundadas razões para crer que a execução de pedido de auxílio judiciário subsequente para fins de pesquisa, apreensão e divulgação de tais dados será recusado por ausência de verificação do requisito da dupla incriminação.

Artigo 24.º

Acesso a dados informáticos em cooperação internacional

1 - Em execução de pedido de autoridade estrangeira competente, a autoridade judiciária competente pode proceder à pesquisa, apreensão e divulgação de dados informáticos armazenados em sistema informático localizado em Portugal, relativos a crimes previstos no artigo 11.º, quando se trata de situação em que a pesquisa e apreensão são admissíveis em caso nacional semelhante.
2 - A autoridade judiciária competente procede com a maior rapidez possível quando existam razões para crer que os dados informáticos em causa são especialmente vulneráveis à perda ou modificação ou quando a cooperação rápida se encontre prevista em instrumento internacional aplicável.
3 - O disposto no n.º 1 aplica-se, com as devidas adaptações, aos pedidos formulados pelas autoridades judiciárias portuguesas.

Artigo 25.º

Acesso transfronteiriço a dados informáticos armazenados quando publicamente disponíveis ou com consentimento

As autoridades estrangeiras competentes, sem necessidade de pedido prévio às autoridades portuguesas, de acordo com as normas sobre transferência de dados pessoais previstas na Lei n.º 59/2019, de 8 de agosto, podem:
a) Aceder a dados informáticos armazenados em sistema informático localizado em Portugal, quando publicamente disponíveis;
b) Receber ou aceder, através de sistema informático localizado no seu território, a dados informáticos armazenados em Portugal, mediante consentimento legal e voluntário de pessoa legalmente autorizada a divulgá-los.

Contém as alterações dos seguintes diplomas:
- Lei n.º 79/2021, de 24/11

Consultar versões anteriores deste artigo:
-1ª versão: Lei n.º 109/2009, de 15/09

Artigo 26.º

Intercepção de comunicações em cooperação internacional

1 - Em execução de pedido da autoridade estrangeira competente, pode ser autorizada pelo juiz a intercepção de transmissões de dados informáticos realizadas por via de um sistema informático localizado em Portugal, desde que tal esteja previsto em acordo, tratado ou convenção internacional e se trate de situação em que tal intercepção seja admissível, nos termos do artigo 18.º, em caso nacional semelhante.
2 - É competente para a recepção dos pedidos de intercepção a Polícia Judiciária, que os apresentará ao Ministério Público, para que os apresente ao juiz de instrução criminal da comarca de Lisboa para autorização.
3 - O despacho de autorização referido no artigo anterior permite também a transmissão imediata da comunicação para o Estado requerente, se tal procedimento estiver previsto no acordo, tratado ou convenção internacional com base no qual é feito o pedido.
4 - O disposto no n.º 1 aplica-se, com as devidas adaptações, aos pedidos formulados pelas autoridades judiciárias portuguesas.

CAPÍTULO V
Disposições finais e transitórias

Artigo 27.º

Aplicação no espaço da lei penal portuguesa e competência dos tribunais portugueses

1 - Para além do disposto no Código Penal em matéria de aplicação no espaço da lei penal portuguesa, e salvo tratado ou convenção internacional em contrário, para efeitos da presente lei, a lei penal portuguesa é ainda aplicável a factos:

a) Praticados por Portugueses, se aos mesmos não for aplicável a lei penal de nenhum outro Estado;
b) Cometidos em benefício de pessoas colectivas com sede em território português;
c) Fisicamente praticados em território português, ainda que visem sistemas informáticos localizados fora desse território; ou
d) Que visem sistemas informáticos localizados em território português, independentemente do local onde esses factos forem fisicamente praticados.
2 - Se, em função da aplicabilidade da lei penal portuguesa, forem simultaneamente competentes para conhecer de um dos crimes previstos na presente lei os tribunais portugueses e os tribunais de outro Estado membro da União Europeia, podendo em qualquer um deles ser validamente instaurado ou prosseguido o procedimento penal com base nos mesmos factos, a autoridade judiciária competente recorre aos órgãos e mecanismos instituídos no seio da União Europeia para facilitar a cooperação entre as autoridades judiciárias dos Estados membros e a coordenação das respectivas acções, por forma a decidir qual dos dois Estados instaura ou prossegue o procedimento contra os agentes da infracção, tendo em vista centralizá-lo num só deles.
3 - A decisão de aceitação ou transmissão do procedimento é tomada pela autoridade judiciária competente, tendo em conta, sucessivamente, os seguintes elementos:
a) O local onde foi praticada a infracção;
b) A nacionalidade do autor dos factos; e
c) O local onde o autor dos factos foi encontrado.
4 - São aplicáveis aos crimes previstos na presente lei as regras gerais de competência dos tribunais previstas no Código de Processo Penal.
5 - Em caso de dúvida quanto ao tribunal territorialmente competente, designadamente por não coincidirem o local onde fisicamente o agente actuou e o local onde está fisicamente instalado o sistema informático visado com a sua actuação, a competência cabe ao tribunal onde primeiro tiver havido notícia dos factos.

Artigo 28.º
Regime geral aplicável

Em tudo o que não contrarie o disposto na presente lei, aplicam-se aos crimes, às medidas processuais e à cooperação internacional em matéria penal nela previstos, respectivamente, as disposições do Código Penal, do Código de Processo Penal e da Lei n.º 144/99, de 31 de Agosto.

Artigo 29.º
Competência da Polícia Judiciária para a cooperação internacional

A competência atribuída pela presente lei à Polícia Judiciária para efeitos de cooperação internacional é desempenhada pela unidade orgânica a quem se encontra cometida a investigação dos crimes previstos na presente lei.

Artigo 30.º
Proteção de dados pessoais

O tratamento de dados pessoais ao abrigo da presente lei efetua-se nos termos da Lei n.º 59/2019, de 8 de agosto, sendo aplicável, em caso de violação, o disposto nos respetivos capítulos vii e viii.

Contém as alterações dos seguintes diplomas:
- Lei n.º 79/2021, de 24/11

Consultar versões anteriores deste artigo:
-1ª versão: Lei n.º 109/2009, de 15/09

Artigo 31.º
Norma revogatória

É revogada a Lei n.º 109/91, de 17 de Agosto.
Consultar a Lei da Crminalidade Informática(revogado face ao diploma em epígrafe)

Artigo 32.º
Entrada em vigor

A presente lei entra em vigor 30 dias após a sua publicação.
Aprovada em 23 de Julho de 2009.
O Presidente da Assembleia da República, Jaime Gama.
Promulgada em 29 de Agosto de 2009.
Publique-se.
O Presidente da República, Aníbal Cavaco Silva.
Referendada em 31 de Agosto de 2009.
O Primeiro-Ministro, José Sócrates Carvalho Pinto de Sousa.

Diversos

1. Entrou em vigor em 15.09.2009.