



**MINISTÉRIO PÚBLICO
PORTUGAL**

PROCURADORIA-GERAL DA REPÚBLICA

GABINETE CIBERCRIME

**JURISPRUDÊNCIA SOBRE
PROVA DIGITAL**

Nota Prática nº 12/2017

2 de novembro de 2017

ÍNDICE

1. Interceções telefónicas e de comunicações	3
2. Mensagens de SMS e de correio eletrónico	5
3. Acesso ao conteúdo de telemóveis	7
4. Conversas telefónicas em <i>alta voz</i> e gravações de voz	7
5. Endereço de IP	8
6. Localização celular	10
7. Gravações de imagens de videovigilância como prova	12
8. Localizador de GPS	15
9. Uso de correio eletrónico para praticar atos processuais	16
10. Necessidade de exibição de provas em julgamento	18
11. Apreensão de dados informáticos	18
12. Retenção de dados e obtenção de dados de comunicações	19

NOTA PRÁTICA nº 12/2017

3 de novembro de 2017

Jurisprudência sobre prova digital

Pretende-se com esta nota prática atualizar as referências jurisprudenciais de tribunais superiores sobre prova digital, publicadas e disponíveis na Internet. Além dos arestos mais recentes, recuperam-se os acórdãos já incluídos em anteriores Notas Práticas.

Como aconteceu com Notas Práticas anteriores, não se faz a análise detalhada dos acórdãos, os quais se referem apenas com um curto sumário. Além deste, fazem-se apenas muito brevíssimos comentários genéricos, de enquadramento, que somente pretendem dar pistas sobre a extensão e o sentido da jurisprudência.

O período temporal coberto termina na presente data e recua até 2009, ano da publicação da Lei do cibercrime, embora se incluam algumas decisões anteriores, por se manterem pertinentes.

1. INTERCEÇÕES TELEFÓNICAS E DE COMUNICAÇÕES

A temática das interceções telefónicas tem dado origem a inúmeras decisões de tribunais superiores. Porém, aqui apenas se referenciam decisões que, de alguma forma, possam ser úteis para a compreensão do fenómeno digital, deixando-se por referenciar incontáveis acórdãos, sobre escutas telefónicas, disponibilizados no passado recente.

Acórdão da Relação do Porto de 1 de junho de 2016

As escutas telefónicas são um meio de obtenção de prova, mas as conversações recolhidas através dessas interceções constituem meio de prova. Depois de transcritas e inseridas no processo, passam a constituir prova documental submetida ao princípio da livre apreciação da prova

Acórdão da Relação de Évora de 12 de abril de 2016

Não é razoável a interpretação do nº4 do Artigo 188º do CPP, segundo a qual o prazo de 48 horas para apresentação ao JIC dos elementos referentes às interceções telefónicas se destina ao magistrado e aos dos serviços do Ministério Público: o prazo é fixado ao agente do Ministério Público e não à simbiose do agente com os respetivos serviços.

Acórdão da Relação do Porto de 13 de maio de 2015

Só podem valer como prova em julgamento as comunicações que o Ministério Público mandar transcrever ao OPC e indicar como meio de prova na acusação. A inobservância das regras do Artigo 188º, do CPP constitui nulidade que impede toda e qualquer utilização do material probatório assim obtido - esta invalidade atinge apenas essas concretas comunicações.

Acórdão da Relação de Évora de 5 de maio de 2015

A lei não impõe a pré-existência, relativamente às escutas telefónicas, de outras diligências probatórias (inconclusivas) que as abonem ou justifiquem.

Acórdão da Relação de Évora de 17 de março de 2015

É possível lançar-se mão das escutas telefónicas logo como o primeiro meio de obtenção da prova utilizado, quando - e apenas nesta hipótese - o juiz de instrução se convença, em face dos concretos dados factuais trazidos pelo Ministério Público, que ela é a única diligência capaz de fazer carrear para os autos os elementos probatórios aptos à descoberta da verdade.

Acórdão da Relação de Coimbra de 4 de fevereiro de 2015

Em inquérito, o pedido ao operador de comunicações do registo de todas as comunicações recebidas (por exemplo SMS, e MMS), num período temporal alargado, na medida em que permitem identificar os utilizadores, o relacionamento direto entre uns e outros através da rede, a localização, a frequência, a data, hora, e a duração das comunicações, deve participar das garantias a que está submetida a utilização do serviço, especialmente tudo quanto respeite ao sigilo das comunicações. Torna-se necessária a autorização do Juiz para a sua obtenção e junção aos autos.

Acórdãos da Relação de Évora de 6 de janeiro de 2015 e de 20 de janeiro de 2015

O regime processual das comunicações telefónicas previsto nos artigos 187º a 190º do Código de Processo Penal deixou de ser aplicável por extensão às “telecomunicações eletrónicas”, “crimes informáticos” e “recolha de prova eletrónica (informática)” desde a entrada em vigor da Lei do Cibercrime. Para a prova eletrónica preservada ou conservada em sistemas informáticos existe um novo sistema processual penal, o previsto nos artigos 11º a 19º da Lei do Cibercrime.

Acórdão da Relação de Évora de 6 de janeiro de 2015

O regime processual da Lei 32/2008 (designadamente o Artigo 3º, nº 1 e 2 e o Artigo 9º) está revogado e substituído pelo regime processual contido na Lei nº 109/2009 para todos os dados que não estejam especificamente previstos no Artigo 4º, nº 1 daquela lei, ou seja, dados conservados em geral; está em vigor para todos os dados que estejam especificamente previstos naquele Artigo 4º, nº 1 (por exemplo para dados conservados relativos à localização celular).

2. MENSAGENS DE SMS E DE CORREIO ELETRÓNICO

As mensagens curtas de texto (SMS) têm sido cada vez mais utilizadas como prova. Firmou-se jurisprudência quanto à desnecessidade de intervenção judicial na obtenção e junção ao processo dessas mensagens, se o seu destinatário (normalmente o lesado) der autorização para essa junção – por exemplo quando é ele mesmo quem faculta o telefone para a obtenção das mensagens. Já assim não será se as mensagens estão armazenadas em aparelho de quem não autoriza a obtenção das mensagens: neste caso exige-se intervenção judicial, nos termos do Artigo 17º da Lei do Cibercrime.

Contra esta orientação apenas se encontrou uma decisão (embora sobre correio eletrónico), já mais antiga, de 2011. Não está publicada, desde então, nenhuma outra decisão no sentido deste acórdão, cuja orientação tem vindo a ficar mais isolada.

O regime de apreensão de SMS tem o mesmo enquadramento legal (Artigo 17º da Lei do Cibercrime) do regime da apreensão de mensagens de correio eletrónico ou de comunicações de idêntica natureza. A jurisprudência quanto às primeiras é, pois, aplicável a estas últimas.

Nesta temática, tem sido interessante observar a jurisprudência laboral que, com interesse para as restantes jurisdições, tem incidido sobretudo sobre a possibilidade – ou não – do empregador, de aceder à correspondência eletrónica do empregado.

Acórdão do Tribunal Europeu dos Direitos do Homem de 5 de setembro de 2017 (Caso *Barbulescu vs. Roménia*)

Se uma entidade empregadora monitorizar comunicações dos seus empregados, deve respeitar o direito à privacidade e o segredo das comunicações. Para esse efeito, antes de qualquer monitorização, deve ser feita advertência aos empregados de que tal monitorização ocorrerá – e da sua extensão e grau de intrusão. Essa monitorização deve ter um fundamento, ou deve justificar-se – deverá evitar-se, se o seu propósito for atingido por qualquer outro meio, menos intrusivo.

Acórdão da Relação do Porto de 15 de dezembro de 2016

O conteúdo dos emails enviados ou rececionados pelo trabalhador que não tenham natureza profissional, estão abrangidos pela tutela dos direitos à privacidade e à confidencialidade das mensagens. Sendo disponibilizada ao trabalhador conta de correio eletrónico profissional, mas sem definição de regras quanto à sua utilização, mormente sem que seja proibida a sua utilização para efeitos pessoais, não pode o empregador aceder ao conteúdo dos emails enviados ou rececionados nessa conta. Por isso, pelo menos nas situações em que o empregador não haja regulamentado e proibido a utilização para fins pessoais de contas de correio eletrónico, o controlo dos dados de tráfego dos emails enviados ou rececionados em tais contas é sempre inadmissível.

Acórdão da Relação do Porto de 20 de janeiro de 2016

Se o arguido enviou ao ofendido mensagem por SMS, o seu destinatário pode fazer da missiva o uso que entender, nomeadamente apresentá-la às autoridades judiciais para poder servir como prova de um crime de que é vítima. A mensagem mantida em suporte digital, depois de recebida e lida, tem a mesma proteção da carta em papel que, tendo sido recebida pelo correio e aberta, foi guardada em arquivo pessoal. Sendo um mero documento escrito, aquela mensagem não goza da aplicação do regime de proteção

específico da reserva da correspondência e das comunicações previsto no Artigo 189º do CPP. A junção aos autos de transcrição de mensagem escrita guardada em telemóvel não tem de ser autorizada pelo juiz.

Acórdão da Relação de Lisboa de 24 de setembro de 2013

As mensagens de SMS deixam de ter a essência de uma comunicação em transmissão para passarem a ser uma comunicação já recebida, que terá porventura a mesma essência da correspondência», em nada se distinguindo de uma «carta remetida por correio físico»; o destinatário da correspondência tem sobre a mesma toda a disponibilidade, designadamente para divulgar o seu conteúdo ou autorizar que deste tomassem conhecimento as autoridades policiais.

Acórdão da Relação do Porto de 3 de abril de 2013

As mensagens de SMS recebidas no telemóvel da ofendida e por ela disponibilizadas de forma espontânea são um meio de prova válido, que não requiere qualquer validação judicial, por ter sido fornecido por quem é o seu legítimo detentor.

Acórdão da Relação de Guimarães de 15 de outubro de 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.

Acórdão da Relação do Porto de 12 de setembro de 2012

A jurisprudência tem equiparado as mensagens SMS às 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.

Acórdão da Relação de Lisboa de 29 de março de 2012

A junção ao processo da transcrição das mensagens SMS gravadas no telemóvel do queixoso, depois do consentimento deste, não está dependente de autorização do JIC.

Acórdão da Relação de Guimarães de 29 de março de 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.

Acórdão da Relação de Lisboa de 11 de janeiro de 2011

Quanto à 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.

3. ACESSO AO CONTEÚDO DE TELEMÓVEIS

O acórdão referenciado é pioneiro na análise da questão da obtenção de conteúdos gravados em telemóvel, não se incluindo neste conteúdo as mensagens de comunicações. Quanto a todo o restante conteúdo – incluída a lista telefónica ou o registo de chamadas efetuadas e recebidas (e presumivelmente também fotografias ou vídeos do dono do telefone), o acórdão estipula que, tendo este conteúdo a natureza de documentos, a sua apreensão não depende de ordem judicial.

Acórdão da Relação de Évora de 7 de abril de 2015

O exame pericial a um telemóvel e seu cartão SIM, para identificação da respetiva lista telefónica, dos registos das chamadas recebidas e atendidas, das recebidas e não atendidas e, das chamadas efetuadas, não carece da prévia autorização do Juiz de Instrução. Embora as comunicações por telemóvel tenham uma dinâmica entre a realização da chamada e o termo da mesma que perdura durante determinado lapso de tempo, ultrapassado este, deixa de haver comunicação telefónica - nos termos da lei penal, nomeadamente do Artigo 187º, do Código de Processo Penal - e o registo que delas fica passa a constituir um mero documento demonstrativo dessas mesmas comunicações telefónicas.

4. CONVERSAS TELEFÓNICAS EM ALTA VOZ E GRAVAÇÕES DE VOZ

A (não) admissibilidade de testemunho sobre conversas telefónicas que se escutaram no telefone de outrem, em alta voz, provocou forte discussão jurisprudencial no passado. A orientação da jurisprudência mais recente é serena no sentido da admissibilidade deste tipo de prova, nalgumas circunstâncias.

Acórdão da Relação de Évora de 11 de maio de 2017

Por constituir meio de prova obtido de forma ilícita, não pode ser admitida a junção, em processo civil, de gravações não consentidas de comunicações orais, por telefone ou de viva voz, não destinadas ao público, mesmo que sejam dirigidas a quem fez a gravação.

Acórdão da Relação de Évora de 25 de novembro de 2014

A prova por depoimento de testemunha que escutou conversação telefónica por intermédio de sistema alta voz, em geral, não é prova livre, podendo cair nas proibições de prova. Porém, a mesma pode ser admissível, desde que se mostre imprescindível, atentas as circunstâncias do caso concreto, designadamente, ocorrer causa de justificação,

consistente numa legítima defesa - obter testemunho do crime praticado pelo arguido para o enfrentar e obstar a que prossiga na agressão - ou num direito de necessidade (probatório) - agir para obter prova para o perseguir criminalmente.

Acórdão da Relação de Coimbra de 10 de julho de 2013

Quando a vítima é a destinatária da comunicação telefónica (ou outra), considera-se justificada a divulgação do teor da conversa pelo sistema de alta voz, quando essa comunicação é o meio utilizado para cometer um crime de ameaças, ou injúrias, se a vítima consentir na divulgação; como tal não constitui prova proibida.

Acórdão da Relação de Coimbra de 6 de março de 2013

A divulgação, pelo sistema de alta voz, de uma conversa telefónica, quando essa precisa comunicação telefónica é o meio utilizado para cometer um crime de ameaças ou injúrias é lícita, sendo permitido a quem a escutou testemunhar sobre ela, se a vítima consentir na divulgação, como forma de se proteger de tais ameaças ou injúrias.

5. ENDEREÇO DE IP

Na nota prática nº 2/2013 (de 3 de abril de 2013) concluía-se que a jurisprudência dominante sustentava que o pedido de identificação do utilizador de um determinado endereço IP, num dado dia e hora, não devia ser submetido ao regime dos dados de tráfego, por se entender que este pedido não se refere a informação sobre o percurso dessa comunicação nem sobre outro eventual tráfego comunicacional da pessoa em causa. Por isso, concluía-se que pertencia ao Ministério Público a competência para pedir, a um operador de comunicações, a identificação do seu cliente que utilizou um determinado endereço IP num determinado dia e hora.

Todos os acórdãos agora referenciados, posteriores à emissão daquela nota prática confirmam esta orientação.

Acórdão do Tribunal de Justiça da UE de 19 de outubro de 2016

O endereço IP é um dado pessoal e, por isso, a sua recolha e tratamento não pode ser livremente efetuada. Porém, é legítima a guarda de endereços IP dos visitantes de sites web, mesmo após o termo das sessões: um site possa armazenar os IPs dos seus visitantes para fins de defesa de um ataque informático, ou para fins de queixa-crime contra os eventuais atacantes

Acórdão da Relação do Porto de 17 de setembro de 2014

No serviço de telecomunicações a obtenção dos dados de base (isto é, dos dados de conexão à 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.

Acórdão da Relação de Lisboa de 19 de junho de 2014

Estando 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 respetiva obtenção é do MP. 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.

Acórdão da Relação de Évora de 22 de abril de 2014

A identificação completa, morada e endereço de correio eletrónico do titular de determinado *blog*, Facebook ou outra rede social, bem como o IP de criação dessa rede social e o IP onde foi efetuado determinado *post* constituem dados de base, que embora cobertos pelo sistema de confidencialidade, podem ser comunicados a pedido de uma autoridade judiciária.

Acórdão da Relação de Lisboa de 22 de janeiro de 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.

Acórdão da Relação de Évora de 22 de dezembro de 2012

Obtenção de endereço IP - legitimidade do MP - embora o objeto da decisão seja outro, este aresto cita despacho de JIC sobre a temática em epígrafe.

Acórdão da Relação de Évora de 7 de dezembro de 2012

Quando o MP pretende apenas aceder ao IP de origem de uma comunicação não está a querer aceder a dados de tráfego (quer saber apenas a identificação e a morada do utilizador do serviço - isto é, quer saber dados de base).

Acórdão da Relação de Évora de 13 de novembro de 2012

A identificação completa, morada e endereço de correio eletrónico do titular de determinado *blogue*, bem como o IP de criação desse *blogue* e o IP de onde foi efetuado determinado *post*, constituem dados de base - os elementos ou dados funcionais (de tráfego), necessários ou produzidos pelo estabelecimento da ligação (...) são a direção, o destino (*adressage*) e a via, o trajeto (*route*).

Acórdão da Relação de Coimbra de 3 de outubro de 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.

Acórdão da Relação de Évora de 12 de julho de 2012

A identidade de um cidadão que se liga a determinado *blogue* ou sítio da Internet não está coberta pelo segredo das conversações ou comunicações, regulado pelos Artigos 187º a 190º do CPP. O mesmo sucede com os dados de conexão à rede, elementos necessários

ao estabelecimento de uma base para comunicação, aquém da comunicação; são prévios em relação a ela e constituem, na perspetiva dos utilizadores, os elementos necessários ao acesso à rede, designadamente através da ligação individual e para utilização própria do respetivo serviço. A eventual confidencialidade desses dados (por exemplo, por força dos termos do contrato de fornecimento do serviço) traduz um simples interesse pessoal do utilizador, que de modo algum contende com a sua esfera pessoal íntima, podendo ser comunicados a pedido de qualquer autoridade judiciária para fins de investigação criminal.

Acórdão da Relação de Évora de 5 de junho de 2012

Quando o Ministério Público pretende obter "todos os dados do utilizador de IP" num determinado período de tempo, está-se perante dados de tráfego, dependendo a sua obtenção de autorização judicial e só sendo possível quando a um limitado catálogo de crimes. Estando em causa investigação por crime de difamação através da internet, não é admissível o acesso a dados de tráfego, por via de autorização judicial, dado que tal ilícito não consta, nem do catálogo previsto no Artigo 187º do CPP, nem da definição de crime grave do Artigo 2º da Lei nº 32/2008.

Acórdão da Relação de Évora de 27 de janeiro de 2011

A mera identificação de um titular de um número fixo ou móvel não pertence ao sigilo das comunicações. Quanto a endereços IP fixos, o acesso à identificação do seu utilizador faz-se sem recurso a dados de tráfego, mas quanto a endereços dinâmicos supõe, simultaneamente, aceder a dados de tráfego e depende de autorização judicial.

Acórdão da Relação de Lisboa de 18 de janeiro de 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.

6. LOCALIZAÇÃO CELULAR

A jurisprudência sobre localização celular incide, na sua maioria, sobre a possibilidade legal, ou não, de se proceder à identificação indiscriminada de todas as comunicações efetuadas por via de uma determinada antena repetidora de sinal de telemóvel, num certo período de tempo, na esperança de se encontrarem eventuais registos de comunicações de autores de crimes. Sem exceção, a jurisprudência pronuncia-se no sentido da inadmissibilidade legal desta medida.

Acórdão da Relação de Lisboa de 7 de março de 2017

Em inquérito, a obtenção, em tempo real, de dados sobre localização celular, funda-se nos Artigos 187º a 189º do Código de Processo Penal, enquanto a obtenção de dados que concernem a comunicações relativas ao passado, ou seja, arquivadas, se baseia no quadro da Lei nº 32/2008.

Acórdão da Relação de Lisboa de 22 de junho de 2016

Solicitar a operadoras de telemóveis todos os dados de tráfego dos cartões SIM que operaram num determinado período de tempo em 19 antenas, mas não estando concretizados alvos determináveis, e atingindo a diligência pretendida um universo ilimitado e indiferenciado de cidadãos que não se integram no conceito jurídico-penal de “suspeitos” é proibido por lei e não os princípios constitucionais da proporcionalidade e da adequação

Acórdão da Relação de Lisboa de 22 de junho de 2016

Solicitar a operadoras de telemóveis todos os dados de tráfego dos cartões SIM que operaram num determinado período de tempo em 19 antenas, mas não estando concretizados alvos determináveis, e atingindo a diligência pretendida um universo ilimitado e indiferenciado de cidadãos que não se integram no conceito jurídico-penal de “suspeitos” é proibido por lei e não respeita os princípios constitucionais da proporcionalidade e da adequação.

Acórdão da Relação de Lisboa de 3 de maio de 2016

Não é permitido, em inquérito, solicitar às operadoras de comunicações que forneçam todos os números de telefone que num determinado período de tempo, se conectaram a uma determinada antena, sem que, previamente, se determinem previamente os suspeitos o que, em caso de desconhecimento da respetiva identificação, pressupõe a existência de dados factuais tendentes à sua individualização, não sendo admissível que sejam consideradas suspeitas de determinada ação criminosa, todas as pessoas que se encontrassem naquele local e tempo.

Acórdão da Relação de Évora de 19 de maio de 2015

A falta de suspeito determinado contra quem dirigir as escutas telefónicas, os pedidos de obtenção de dados de tráfego ou os pedidos de localização celular, é obstáculo intransponível à realização deste tipo de meios de obtenção de prova. Recolher informações de pessoas inocentes, na esperança de, de entre estas, se “apanhar” algum suspeito, é desproporcional aos fins visados, sendo, pois, uma compressão inconstitucional e ilícita do direito à privacidade e à inviolabilidade das comunicações.

Acórdão da Relação do Porto de 11 de fevereiro de 2015

Não é admissível solicitar-se a um operador de comunicações que forneça os dados de localização celular relativos a um número indeterminado de pessoas, uma vez que a obtenção indiscriminada de dados de localização celular afronta o direito à inviolabilidade das telecomunicações.

Acórdão da Relação de Évora de 25 de maio de 2013

A localização celular não pode ser usada já depois de se ter consumado uma situação de perigo; supõe a séria possibilidade da existência dessa situação de perigo para a vida e a integridade física grave de alguém e supõe que a localização celular possa obviar à

concretização desse perigo. Não pode ser autorizada quando está apenas em causa a investigação de perigo que já se consumou.

Acórdão da Relação de Évora de 18 de outubro de 2011

A obtenção de dados de localização celular de uma determinada área geográfica, sem que haja um suspeito concreto, além de ferir os ditames legais, é desprovida de razoabilidade, desproporcionada e inadequada, não sendo justificada face à devassa intolerável que constituiria.

Acórdão da Relação de Évora de 23 de setembro de 2010

Não é permitida a obtenção de dados sobre a localização celular ou de registos da realização de comunicações, genericamente relativos a uma determinada área geográfica e a determinado intervalo temporal, porque essa diligência vai necessariamente abranger um leque muito alargado de cidadãos e não visa um suspeito determinado, como exige a lei.

7. GRAVAÇÕES DE IMAGENS DE VIDEOVIGILÂNCIA COMO PROVA

A consideração, como prova válida, de imagens gravadas por indivíduos (privados), não está expressamente regulada na lei processual penal. Porém, a jurisprudência é consistente a esse propósito, permitindo essa mesma utilização, desde que, na sua origem, não esteja um propósito ilícito. No caso de gravações ocasionais feitas por cidadãos, esta ilicitude tem sido aferida, caso a caso, segundo as suas peculiares circunstâncias. Quanto à gravação por via de sistemas de vigilância, esta licitude (e, portanto, a validade da prova delas resultante), não é beliscada por eventual falta formal ou burocrática, por exemplo, de não submissão prévia de pedido anterior à CNPD. Referenciam-se alguns acórdãos da jurisdição laboral que versam sobre a licitude, ou não, de empregadores usarem meios de vigilância eletrónica sobre os seus trabalhadores.

Acórdão da Relação de Coimbra de 20 de setembro de 2017

Em processo penal é permitida a utilização de imagens previamente obtidas através de um sistema de videovigilância de um estabelecimento comercial. Tais imagens não respeitam ao “núcleo duro da vida privada” das pessoas visionadas e existe justa causa (prova de uma infração criminal), razão pela qual não se trata de método proibido de prova (ainda que, porventura, não tenha sido obtida autorização da CNPD para a instalação do sistema de recolha de imagens).

Acórdão da Relação de Guimarães de 11 de julho de 2017

São válidas como prova, em processo penal, as filmagens recolhidas pelo sistema de videovigilância de um condomínio, independentemente de ter ou não havido comunicação à CNPD e de ter ou não anúncio do seu acionamento, por existir justa causa para a captação das imagens (documentar um crime de furto), não sendo atingidos dados sensíveis da pessoa visionada nem o “núcleo duro” da sua vida privada.

Parecer nº 10/2017 do Conselho Consultivo da Procuradoria-Geral da República de 8 de junho de 2017

A utilização de câmaras de vídeo ao abrigo da Lei nº 1/2005 permite a captação de imagens e sons, sendo certo que quanto aos sons, apenas quando se verifique perigo concreto para a segurança de pessoas e bens. Tal utilização carece de autorização judicial se abranger interior de casa ou edifício habitado ou sua dependência, quando não exista consentimento dos proprietários e de quem o habite legitimamente. Existindo notícia de crime relativamente ao qual a gravação possa compreender elementos de investigação e/ou prova, o suporte original das imagens e sons deve ser transmitido ao Ministério Público para que pondere os valores em causa (por um lado, a tutela da privacidade, proteção da imagem e palavra; por outro, aos interesses e fins do processo penal, nomeadamente de recolha e preservação de meios de prova).

Acórdão da Relação do Porto de 26 de junho de 2017

A lei não obsta à instalação de meios de vigilância à distância, incluindo a captação de imagem, nos locais de trabalho. Contudo, essa vigilância apenas poderá ser utilizada quando vise a proteção e segurança de pessoas e bens ou quando particulares exigências inerentes à natureza da atividade o justifiquem, não podendo nunca ter a finalidade de controlar o desempenho profissional do trabalhador.

As imagens captadas por sistema de videovigilância podem ser usadas como meio de prova em processo disciplinar e na subsequente ação judicial, desde que sejam observados os pressupostos que decorrem da legislação sobre a proteção de dados.

Acórdão da Relação de Coimbra de 18 de maio de 2016

São lícitas as imagens obtidas através de câmaras de vigilância, em espaços destinados à vida estritamente privada, como o interior de habitações, pelos legítimos utilizadores de tais espaços, visando a defesa dos seus bens pessoais e patrimoniais. Sendo obtidas imagens da prática de crimes por estranhos ao espaço em causa e que nele se introduziram ilegalmente, é indiferente que não tenha havido autorização do visado ou aprovação da CNPD, uma vez que, por natureza, no caso, as imagens não podem dizer respeito ao núcleo duro da vida privada e mais sensível daquele visado.

Acórdão da Relação de Lisboa de 10 de maio de 2016

Imagens captadas em local de acesso público, mesmo na falta de consentimento do visado, não correspondem a qualquer método proibido de prova, por não violarem o núcleo duro da vida privada, avaliado numa ideia de proporcionalidade e por existir uma justa causa na sua obtenção e utilização, que é a prova de uma infração criminal. A falta de parecer prévio favorável da CNPD, só por si, não torna a gravação ilícita, nos termos da lei penal.

Acórdão da Relação de Évora de 29 de março de 2016

É, em princípio, admissível a valoração das fotografias ou filmes que não tenham sido obtidos de forma penalmente ilícita. Filmar a materialidade de autoria de um crime e de utilizar posteriormente o vídeo como prova do facto, embora possa eventualmente preencher a factualidade típica do crime de gravações e fotografias ilícitas (Artigo 199º do

Código Penal), pode ser lícito, por exemplo, se quem filmou agiu ao abrigo do direito de necessidade (Artigo 34º do Código Penal), o que vale tanto para a obtenção do vídeo como para a sua posterior utilização em processo crime, pois esta utilização constitui a concretização daquele mesmo fim.

Acórdão da Relação de Évora de 29 de março de 2016

É prova válida a gravação de filme, com telemóvel, de situação de conflito na qual vem a ocorrer um crime. Já será prova proibida a que resulta de fotografias tiradas já depois de o crime ter ocorrido, ao autor deste, para demonstrar a respetiva presença no local.

Acórdão da Relação de Coimbra de 24 de fevereiro de 2016

A captação de imagens por particulares, em locais públicos ou de livre acesso ao público, não estando ferida de qualquer ilegalidade nem violando os direitos de personalidade que compreendem o direito à imagem, é meio admissível de prova. As imagens assim captadas não constituem nenhuma violação do “núcleo duro da vida privada” nem do direito à imagem. Por conseguinte, não é necessário o consentimento do visado para essa filmagem, nos termos exigidos pelo Artigo 79º, nº 2, do Código Civil, porquanto a imagem do suspeito se encontra justificada por razões de justiça, nem tão pouco a referida recolha de imagens integra o crime do Artigo 199º, nº 2, do Código Penal. Os depoimentos que reproduzem as ditas filmagens, não estando afetados por qualquer proibição de prova, devem ser livremente apreciados e valorados pelo tribunal.

Acórdão da Relação do Porto de 25 de fevereiro de 2015

A obtenção de fotografias ou de filmagens sem o consentimento do visado, sempre que exista justa causa nesse procedimento, nomeadamente quando as mesmas estejam enquadradas em lugares públicos, visem a realização de interesses públicos ou hajam ocorrido publicamente não constitui ilícito típico. Nessas circunstâncias mesmo que haja falta de licenciamento da CNPD podem ser usadas como meio de prova.

Acórdão da Relação de Coimbra de 6 de fevereiro de 2015

Apesar de o Artigo 20º, nº 1 do Código do Trabalho proibir a utilização de meios de vigilância à distância para controlar de forma dedicada e permanente o desempenho profissional do trabalhador, esta utilização é lícita se cumprir os requisitos de fim e publicidade previstos nos nºs 2 e 3 do mesmo artigo e for obtida a autorização da Comissão Nacional de Proteção de Dados. Neste último caso, os dados obtidos podem servir de meio de prova em procedimento disciplinar e no controlo jurisdicional da licitude da decisão disciplinar.

Acórdão da Relação do Porto de 17 de dezembro de 2014

Não é admissível como meio de prova, em processo laboral, a captação de imagens por sistema de videovigilância; a consequência legal dessa utilização ilícita dos meios de vigilância à distância é a invalidade da prova obtida para efeitos disciplinares.

Acórdão do Tribunal de Justiça da União Europeia de 11 de dezembro de 2014

A gravação, por um sistema de videovigilância, de imagens de pessoas, por uma pessoa singular, na sua casa familiar, para proteger os seus bens, a saúde e a vida dos proprietários dessa casa e que vigia igualmente o espaço público, não constitui um tratamento de dados efetuado no exercício de atividades exclusivamente pessoais ou domésticas, na aceção do Artigo 3º, nº 2, da Diretiva 95/46/CE.

Acórdão da Relação de Guimarães de 29 de abril de 2014

Não constituem provas ilegais, podendo ser valoradas pelo tribunal, as imagens gravadas por particulares em locais públicos ou acessíveis ao público, se se destinarem a documentar uma infração criminal e não disserem respeito ao «núcleo duro da vida privada» da pessoa visionada.

Acórdão da Relação do Porto de 23 de outubro de 2013

São válidas, não constituindo métodos proibidos de prova e podendo ser valoradas pelo julgador, as imagens gravadas por particular, sendo a gravação direcionada para um local público, particularmente dirigida para o seu veículo automóvel, estacionado na via pública, apenas com vista a apurar quem era o autor dos danos, por neste caso existir justa causa para essa captação de imagens (por não serem atingidos dados sensíveis da pessoa visionada). A imagem captada nas circunstâncias deste caso concreto, por um lado não constitui nenhuma violação do “núcleo duro da vida privada”, nem do direito à imagem do visionado.

Acórdão da Relação de Évora de 28 de junho de 2011

A obtenção das imagens através de sistema, tendo em vista a identificação de autores de crimes, visa documentar infrações e não diz respeito ao «núcleo duro da vida privada» da pessoa visionada; é um meio necessário e apto ao exercício do direito de defesa, pelo que está excluída a ilicitude do mesmo. Não constitui um método proibido de prova, dado que existe uma causa de justificação para a sua obtenção.

Acórdão da Relação de Lisboa de 14 de maio de 2009

Apesar de o Artigo 199º, nº4, do Código Penal proibir e punir a recolha de imagens, por fotografia ou por filmagem, este direito apenas é reconhecido a quem pode legitimamente ostentá-lo e defendê-lo; não é esse o caso de quem entra num espaço vedado e não livremente acessível ao público e dali retira e faz seus bens que sabe não lhe pertencerem - neste caso, são lícitas e válidas como prova as imagens obtidas por câmara de videovigilância oculta.

8. LOCALIZADOR DE GPS

Tal como acontece com outras tecnologias, a informação providenciada por aparelhos de GPS também tem sido indicada em sede probatória, apesar de não existirem normas que refiram expressamente esta nova tecnologia como prova. Mais que a sua utilização – ou não – têm sido discutidas as condições legais em que essa utilização é permitida. Tal como acontece com o uso de imagens, também a este

propósito é relevante considerar jurisprudência da jurisdição laboral, sobre o recurso a meios de vigilância eletrónica sobre trabalhadores.

Acórdão da Relação de Lisboa de 13 de abril de 2016

O aparelho conhecido como *GPS tracker* permite saber, em tempo real, onde está o mesmo – por exemplo, onde está o veículo onde foi instalado, bem como o respetivo percurso, os tempos e locais de paragem, o período de funcionamento do motor e a velocidade a que o automóvel circula. Este meio de obtenção de prova é diferente da interceção de comunicações e não existe lei que o preveja, bem como aos seus limites e às garantias inerentes à sua aplicação. É um meio oculto de investigação que, por isso mesmo, só poderia ser admitido se existisse lei que o consagrasse como um meio de obtenção de prova legítimo e regulasse todos os aspetos do seu regime. Assim é, porque a utilização destes aparelhos, pelo sistemático e permanente registo de dados que propicia e pela natureza dos mesmos, é suscetível de violar a vida privada dos utilizadores dos veículos em que se encontrem instalados.

Acórdão do Supremo Tribunal de Justiça de 13 de novembro de 2013

O dispositivo de GPS instalado, pelo empregador, em veículo automóvel utilizado pelo seu trabalhador no exercício das respetivas funções, não pode ser qualificado como meio de vigilância à distância no local de trabalho, porquanto apenas permite a localização do veículo em tempo real, não permitindo saber o que faz o respetivo condutor. Encontrando-se o GPS instalado numa viatura exclusivamente afeta às necessidades do serviço, não permitindo a captação ou registo de imagem ou som, o seu uso não ofende os direitos de personalidade do trabalhador, nomeadamente a reserva da intimidade da sua vida privada e familiar.

Acórdão da Relação do Porto de 21 de março de 2013

A colocação de um localizador de GPS no veículo de um suspeito está sujeita a autorização judicial - por aplicação analógica do Artigo 187º do CPP.

9. USO DE COMUNICAÇÕES ELETRÓNICAS PARA PRATICAR ATOS PROCESSUAIS

A legislação processual penal desconhece o correio eletrónico como forma de praticar atos processuais, tendo como referência os documentos em papel. O mesmo não acontece com o processo civil, que vai muito mais adiantado neste tema. Por essa razão, a jurisprudência referenciada é maioritariamente da jurisdição civil; mesmo aquela que se reporta expressamente a processo penal, apela igualmente às normas processuais civis. Uma vez que se trata de matéria vizinha, incluem-se ainda decisões quanto ao Cítius.

Acórdão da Relação de Lisboa de 26 de setembro de 2017

O correio eletrónico não é meio adequado para apresentar ato processual escrito em Tribunal da Relação, nem para proceder à notificação do mandatário da parte contrária. Contudo a utilização de tal meio para esses efeitos não implica a desconsideração de tal ato ou notificação. A consequência da não utilização do meio legalmente estabelecido de

apresentação em juízo de atos processuais é tão somente a de o apresentante ficar desprovido de qualquer garantia, quanto à efetiva chegada e à fixação do momento da chegada desse ato ao tribunal. Mas, uma vez chegado o ato ao tribunal, a existência e relevância desse ato é inelutável.

Acórdão da Relação do Porto de 24 de junho de 2017

Os serviços do portal Citius de alertas via SMS e/ou correio eletrónico, não foram objeto de qualquer regulação normativa, não constituem meios ou formas de notificação de atos processuais e não são geridos pela secretaria judicial onde corre o processo em relação ao qual é prestada a informação. Por isso, a falta a um ato judicial de pessoa para ele convocada em virtude de haver recebido um alerta via SMS de haver sido alterada a data é injustificada.

Acórdão da Relação de Lisboa de 13 de dezembro de 2016

Podem ser remetidas peças processuais de processo penal através de correio eletrónico, se tiverem aposta assinatura digital qualificada e se estiverem cronologicamente validadas com utilização da marca do dia eletrónica.

Acórdão da Relação de Coimbra de 15 de setembro de 2015

É obrigatória a apresentação a juízo dos atos processuais através do sistema Citius, para os profissionais forenses. Apenas o não será em caso de justo impedimento que, no entanto, tem que ser expressamente invocado.

Acórdão da Relação de Coimbra de 30 de junho de 2015

Não é admitida a prova testemunhal para demonstração da prática de ato processual por transmissão eletrónica de dados, prova que só é admissível por documento eletrónico - ou através da representação escrita de que é suscetível - i.e., através de uma declaração de validação cronológica, que ateste a data da expedição ou receção do documento eletrónico correspondente. Não integra justo impedimento a avaria do computador do Sr. Advogado subscritor da peça processual, impeditiva da expedição ou remessa da peça processual por transmissão eletrónica de dados.

Acórdão do Supremo Tribunal de Justiça de 21 de janeiro de 2014

Tendo o ato processual - apresentação de requerimento probatório - sido praticado antes do termo do prazo, mas junto tardiamente aos autos, devido a uma gralha no endereço eletrónico do tribunal, não é justificado o seu desentranhamento e desconsideração, com as gravíssimas consequências ao nível da prova e da decisão do mérito da causa.

Acórdão da Relação de Évora de 26 de novembro de 2013

É permitida a remessa a juízo de peças processuais por via de correio eletrónico.

Acórdão da Relação de Évora de 19 de março de 2013

O correio eletrónico pode ser usado para a prática de atos processuais, em processo penal.

10. NECESSIDADE DE EXIBIÇÃO DE PROVAS EM JULGAMENTO

Os acórdãos referenciados neste ponto, sem se referirem especificamente a prova digital, sublinham uma importante orientação sobre a produção de prova em julgamento (aliás comum na jurisprudência), quando essa prova não está, na sua origem, plasmada em papel. Essa orientação vai no sentido da desnecessidade de ver ou ouvir, em julgamento, elementos de prova não impressos se, de alguma forma, esses elementos de prova estão já documentados em papel no processo.

Acórdão da Relação do Porto de 8 de julho de 2015

As escutas telefônicas, regularmente efetuadas durante o inquérito, uma vez transcritas em auto, passam a constituir prova documental, que o tribunal de julgamento pode valorar de acordo com as regras da experiência; essa prova documental não carece de ser lida em audiência e, no caso de o tribunal dela se socorrer, não é necessário que tal fique a constar da ata.

Acórdão da Relação de Évora de 17 de março de 2015

Tendo os filmes de carácter pornográfico sido objeto de perícia, a sua exibição/visualização em audiência torna-se tarefa sem utilidade detetável. A concreta identificação de vítimas não constitui elemento do tipo de pornografia de menores, previsto no artigo 176º, nº 1, alíneas c) e d) do Código Penal.

11. APREENSÃO DE DADOS INFORMÁTICOS

No decurso do último ano foram publicadas algumas decisões jurisprudenciais respeitantes a este aspeto processual da Lei do Cibercrime. Em geral, as decisões referenciadas discutem a forma como o regime da apreensão de dados informáticos previsto naquela lei se aplica ao caso concreto, quer quanto a dados livremente acessível a todos, quer, também, quanto a dados reservados.

Acórdão da Relação do Porto de 5 de abril de 2017

Constitui prova legal a cópia de informação que alguém publicita no seu mural do Facebook sem restrição de acesso – só está sujeita à disciplina do Artigo 16º da Lei do Cibercrime a apreensão da informação original inserta na plataforma, não acessível a terceiros, esteja ou não disponível. Ou seja, em processo penal, nada impede a impressão de informação livremente acessível a todos, no Facebook, ou noutra plataforma na Internet.

Acórdão da Relação do Porto de 7 de dezembro de 2016

Compete ao juiz de instrução determinar que as entidades bancárias prestem informação, sobre dados informáticos, a ser extraída de um sistema informático pertencente àquelas entidades, face ao disposto no Artigo 14º, nº 6 da Lei do Cibercrime.

Acórdão da Relação do Porto de 7 de julho de 2016

A busca de onde resulte a apreensão de um computador é regulada pelas normas do Código de Processo Penal. A pesquisa dos dados informáticos, num computador, bem como a apreensão desses dados, é regulada na Lei do Cibercrime.

12. RETENÇÃO DE DADOS E OBTENÇÃO DE DADOS DE COMUNICAÇÕES

A temática da retenção de dados sofre grande discussão, na Europa, após decisões, de 2014 e 2016, do Tribunal de Justiça da União Europeia sobre a diretiva que inspirou as diversas leis nacionais a este propósito. Nalguns dos Estados Membros da União Europeia, em consequência daquelas decisões do TJUE, as leis nacionais foram revogadas ou declaradas inconstitucionais. Noutros, tem-se considerado que as leis se mantêm em vigor. É este o caso de Portugal, onde se tem considerado que a Lei nº 32/2008, que define o quadro legal da retenção de dados, está em vigor.

Até muito recentemente, os tribunais apenas se pronunciaram sobre essa vigência de forma indireta, referindo-a a propósito de outras questões. Muito recentemente, porém, o Tribunal Constitucional analisou expressamente esta problemática, da vigência, ou não da Lei nº 32/2008, deliberando não a julgar inconstitucional.

Acórdão do Tribunal Constitucional de 13 de julho de 2017

Não julga inconstitucional a obrigação de retenção de dados pelos operadores de comunicações, nos termos previstos na Lei nº 32/2008. Nesta deliberação, o tribunal tomou em consideração a recente jurisprudência europeia que anulou a Diretiva nº 2006/24/CE (relativa à conservação de dados comunicações eletrónicas), transposta para a ordem jurídica portuguesa por aquela Lei nº 32/2008.

Acórdão da Relação de Évora de 2 de maio de 2017

Os dados, preservados ou conservados em sistemas informáticos só podem ser acedidos, em inquérito, por injunção do Ministério Público e em instrução pelo juiz de instrução. Tendo a prova em causa sido obtida pela Polícia Judiciária, sem prévio despacho do Magistrado do Ministério Público, deve ter-se por inválida.

Acórdão da Relação de Lisboa de 7 de março de 2017

Em inquérito, a obtenção, em tempo real, de dados sobre localização celular, funda-se nos Artigos 187º a 189º do Código de Processo Penal, enquanto a obtenção de dados que concernem a comunicações relativas ao passado, ou seja, arquivadas, se baseia no quadro da Lei nº 32/2008.

Acórdão da Relação de Évora de 25 de outubro de 2016

Em processo penal, a obtenção de dados de comunicações “conservadas” ou “preservadas” não é feita ao abrigo do Artigo 189º do Código de Processo Penal, mas antes nos termos dos Artigos 11º a 19º da Lei do Cibercrime e dos Artigos 3º a 11º da Lei nº 32/2008 (neste último case, se tratarem de dados previstos nesta última lei).

(O Gabinete Cibercrime fica grato pela indicação, para cibercrime@pgr.pt de outras decisões sobre prova digital que não tenham sido elencadas)