PESQUISA E APREENSÃO DE DADOS COM CONSENTIMENTO DO TITULAR

Nota Prática nº 29/2025

21 de abril de 2025

ÍNDICE

NOTA PRÁTICA nº 29/2025
21 de abril de 2025

PESQUISA E APREENSÃO DE DADOS COM CONSENTIMENTO DO TITULAR

Esta Nota Prática tem como propósito ser um auxiliar dos magistrados do Ministério Público na compreensão da diligência processual de apreensão de dados informáticos. Trata-se de uma medida coerciva, descrita no artigo 15º da Lei do Cibercrime que pode igualmente ser efetivada com consentimento do titular dos dados em causa.
É sobre este aspeto particular – a apreensão de dados informáticos com consentimento do titular dos mesmos –, que incide esta Nota Prática.

A – PESQUISA E APREENSÃO DE DADOS

1. No Código de Processo Penal consagram-se os regimes jurídicos das buscas e apreensões, como meios de obtenção de prova (artigos 174º a 186º). Por sua vez, na Lei do Cibercrime[1], prevê-se um regime paralelo de buscas informáticas (legalmente referidas como *pesquisas*) e de apreensão de dados, o qual tem como propósito adaptar às exigências do mundo digital aqueles meios de aquisição de prova. Estas figuras processuais, descritas nos artigos 15º a 17º da Lei do Cibercrime, são naturalmente desenhadas à imagem e semelhança das suas equivalentes para o mundo físico, ou *offline*.

2. O artigo 15º da Lei do Cibercrime permite que a autoridade judiciária competente autorize uma pesquisa a um computador quando, durante o inquérito, tal se tornar necessário para a aquisição e recolha de prova.
Por sua vez, o artigo 16º regula o procedimento de apreensão dos dados informáticos que, no decurso de uma pesquisa (ou outro acesso legítimo a um sistema), se mostrarem necessários à prova da verdade dos factos. O artigo 17º regula a apreensão de um tipo muito específico de dados: as mensagens de correio eletrónico e comunicações de natureza equivalente.

3. Trata-se de uma diligência processual coerciva. Isto é, pode ser determinada pela autoridade judiciária contra a vontade do titular (*dono*) do sistema pesquisado e dos dados informáticos apreendidos – naturalmente, sem prejuízo das garantias e salvaguardas estabelecidas na lei.
Trata-se de diligências de obtenção de prova suscetíveis de pôr em causa direitos fundamentais como a privacidade, a inviolabilidade das telecomunicações ou o direito à autodeterminação informacional. Por esse motivo, a lei determina que, em geral, estas medidas processuais dependem de autorização da autoridade judiciária (Ministério Público ou juiz, consoante a fase processual). Porém, assim não acontece, no caso da pesquisa, quando "*a mesma for*

[1] Lei nº 109/2009, de 15 de setembro.

voluntariamente consentida por quem tiver a disponibilidade ou controlo desses dados" (artigo 15º, nº 3, alínea a) da Lei do Cibercrime). Quanto à apreensão, não se exige a intervenção de autoridade judiciária "*quando haja urgência ou perigo na demora*" ou no decurso de buscas / pesquisas (nºs. 1 e 2 do Artigo 16º da Lei do Cibercrime).

4. Para a apreensão de alguns tipos de dados, a lei exige expressamente a intervenção do juiz de instrução (como juiz das liberdades). É o caso da apreensão de "*dados ou documentos informáticos cujo conteúdo seja suscetível de revelar dados pessoais ou íntimos, que possam pôr em causa a privacidade do respetivo titular ou de terceiro*" (artigo 16º, nº 3 da Lei do Cibercrime) ou da apreensão de correio eletrónico ou de registos de comunicações de natureza semelhante (artigo 17º da Lei do Cibercrime).
Portanto, quando no decurso do inquérito ocorra uma destas duas situações de apreensão coerciva de dados, como salvaguarda dos direitos fundamentais em causa (privacidade / intimidade e sigilo de comunicações), além da intervenção do Ministério Público, exige-se também intervenção judicial.

B – PESQUISA E APREENSÃO COM CONSENTIMENTO

5. Porém, a pesquisa e a apreensão podem também ocorrer porque o titular do sistema informático pesquisado, ou o titular dos dados informáticos em causa, autoriza a pesquisa ou a apreensão. Neste tipo de situações, em que o *dono* dos dados (quem tiver *a disponibilidade ou controlo desses dados* – artigo 15º, nº 3 da Lei do Cibercrime) dá o seu consentimento para o acesso aos mesmos e à respetiva apreensão, não é necessário recorrer aos diversos mecanismos coercivos dos artigos 15º, 16º e 17º da Lei do Cibercrime e podem apreender-se para o processo todos os dados que se tornarem necessários à investigação.

6. Em termos processuais, este consentimento tem de ser traduzido em expressa declaração, formalizada de alguma maneira: o artigo 15º, nº 3, alínea a) da Lei do Cibercrime exige que o consentimento "*fique, por alguma forma, documentado*". Esta documentação pode ser traduzida num registo constante, por exemplo, do próprio auto de pesquisa e apreensão. Ou então, de uma declaração avulsa. Porém, o seu teor deve ser claro, esclarecido e inequívoco.
Junta-se em Anexo a esta Nota Prática um modelo de formulário de declaração de consentimento.

7. Havendo consentimento do titular dos dados, como regra não se aplicam ao caso concreto as limitações legais e as formalidades da apreensão. Isto é, quando o titular dos dados autoriza o acesso aos mesmos e a sua apreensão, não têm aplicação as garantias e salvaguardas legais que rodeiam as pesquisas e as apreensões de dados. Designadamente, não é exigida qualquer autorização de autoridade judiciária, quer para o acesso aos dados (pesquisa), quer para a apreensão e tomada de conhecimento dos mesmos.
Assim, por exemplo um órgão de polícia criminal, munido de consentimento documentado no processo, pode proceder à pesquisa de dados num sistema ao qual foi autorizado a aceder. Da mesma forma, pode nele apreender dados, seja fisicamente, apreendendo o respetivo suporte, seja por realização de uma cópia dos mesmos (artigo 16º, nº 7, alíneas a) e b) da Lei do Cibercrime).

8. Esta conclusão é também válida para dados em relação aos quais, nos casos de apreensão coerciva (portanto sem consentimento), se requere intervenção judicial. É o caso dos chamados dados pessoais ou íntimos (artigo 16º, nº 3 da Lei do Cibercrime) e do correio eletrónico ou registos de natureza semelhante (artigo 17º). Quando se torna necessário apreender dados destas naturezas e não há consentimento de acesso aos dados em causa, é exigida intervenção judicial; porém, caso seja prestado consentimento e o mesmo documentado, não se torna a necessária intervenção judicial. A intervenção judicial é uma garantia processual adicional que a lei confere aos cidadãos. Porém, não estando em causa direitos indisponíveis, podem esses mesmos cidadãos prescindir na mesma, consentindo o acesso aos dados.

C – APREENSÃO POR CÓPIA

9. A apreensão de dados com consentimento do respetivo titular pode também efetuar-se por mera cópia dos mesmos. Este mecanismo da apreensão por cópia (permitido pela alínea b do nº 7 do artigo 16º da Lei do Cibercrime) tem como propósito permitir ir ao encontro das necessidades da investigação no caso concreto e, ao mesmo tempo, evitar que a apreensão de dados prejudique interesses legítimos, do próprio titular dos dados ou de terceiros. Assim, permite facultar à investigação dados informáticos necessários à mesma (designadamente por razões probatórias), evitando a apreensão de computadores ou servidores imprescindíveis a atividades legítimas.
Esta possibilidade, de apreensão por cópia, é uma manifestação dos princípios da necessidade e da adequação, permitindo que a mesma se execute através do método que se afigure mais adequado às finalidades investigatórias – descoberta da verdade e obtenção da prova – e que se revele o menos lesivo para os direitos do visado com a diligência.

10. Como se disse, nada obsta a que se proceda a apreensão por cópia dos dados, quando há consentimento do respetivo titular. Porém, se assim acontecer, terá que ser observado o disposto no número 8 do artigo 16º da Lei do Cibercrime. Isto é, a cópia terá que ser "*efetuada em duplicado, sendo uma das cópias selada e confiada ao secretário judicial*". Além disso, "*se tal for tecnicamente possível, os dados apreendidos são certificados por meio de assinatura digital*". A primeira destas regras é imperativa, enquanto a segunda é observada se no caso concreto for tecnicamente possível fazê-lo.
A realização de duas cópias dos dados apreendidos, além de garantia processual para casos de apreensão coerciva, tem também como objetivo preservar a fidelidade dos dados, no seu conjunto, para que os mesmos possam ser objeto de ulterior análise mais alargada, por exemplo, por assim o exigir o direito de defesa do suspeito ou arguido. Trata-se pois de uma imposição que vai ao encontro das boas melhores práticas processuais, que recomendam sempre a realização de uma cópia dos dados apreendidos em duplicado, sendo apenas uma delas intervencionada pelos investigadores.

D – VALIDAÇÃO DA APREENSÃO POR AUTORIDADE JUDICIÁRIA

11. É regra geral que as apreensões de dados efetuadas "*por órgão de polícia criminal são sempre sujeitas a validação pela autoridade judiciária, no prazo máximo de 72 horas*" – artigo 16º, nº 4, da Lei do Cibercrime. Não existe norma expressa que dispense a validação de apreensão de dados quando há consentimento do titular dos mesmos. Portanto, havendo apreensão de dados com consentimento do titular dos mesmos, deve observar-se a regra geral de validação.

Com respeito à pesquisa de dados, que também é permitida mediante consentimento, a lei (nºs 3 e 4 do artigo 15 da Lei do Cibercrime) determina que quando a pesquisa "*for voluntariamente consentida por quem tiver a disponibilidade ou controlo desses dados*", é "*elaborado e remetido à autoridade judiciária competente o relatório previsto no artigo 253º do Código de Processo Penal*". Nesse relatório, o órgão de polícia criminal "*menciona, de forma resumida, as investigações levadas a cabo, os resultados das mesmas, a descrição dos factos apurados e as provas recolhidas*" – artigo 253º, nº 1, do Código de Processo Penal.

12. A experiência e a natureza das coisas têm revelado que é comum a apreensão de dados demorar muito tempo a processar-se, podendo este tempo ser de muitas horas ou até mesmo de vários dias. Esta situação é muito frequente nos casos de apreensão por cópia: a execução material da cópia pode demorar mais que as 72 horas conferidas ao órgão de polícia criminal para sujeitar a apreensão à validação da autoridade judiciária.
A interpretação da lei não pode ignorar a realidade a que se aplica. Por isso, tem que aceitar-se que este prazo de 72 horas tem como referência o momento em for concluída a cópia dos dados. Isto é, a obrigação de, em 72 horas, o órgão de polícia criminal apresentar os dados apreendidos ao Ministério Público começa no momento em que terminar efetivamente *o ato da apreensão*.

E – APREENSÃO FÍSICA DOS SUPORTES

13. O direito processual penal português não regula de forma expressa a obtenção de elementos probatórios livremente entregues às autoridades.
Apenas quanto a documentos que possam constituir prova, caso o seu dono ou detentor livremente os faculte à investigação, a lei determina que são oficiosamente "*juntos*" (artigo 164º, nº 2 do Código de Processo Penal). Esta regra é também aplicável a documentos digitais, por força do artigo 255º, alínea a) do Código de Processo Penal. Caso, quem *tiver a disponibilidade ou controlo* de dados informáticos, voluntariamente consentir no acesso aos mesmos, estes poderão ser *juntos* ao processo. Esta junção de documento não carece de validação.

14. Já quanto a suportes onde os dados possam estar registados (computadores, discos externos, unidades de armazenamento de dados USB…), não existe regra expressa quanto à sua *apreensão*, quando haja consentimento do titular dos dados que porventura ali estejam gravados. Porém, a apreensão de equipamentos físicos – portanto de *coisas* –, processa-se de acordo com as regras gerais do regime de apreensões, previsto no Código de Processo Penal (artigos 178º e seguintes).

ANEXO - MODELO DE FORMULÁRIO

DECLARAÇÃO DE CONSENTIMENTO DE ACESSO, PESQUISA E APREENSÃO DE DADOS

Comarca	
NUIPC	
Referenciação no OPC	

NOME	
DOCUMENTO DE IDENTIFICAÇÃO	

Declaro, de minha livre vontade, que autorizo os órgãos de polícia criminal e as autoridades judiciárias a aceder ao meu equipamento seguinte:

Descrever a marca, modelo, cor e números de referenciação (tais como, se for o caso, o número de série, o IMEI, o número de cartão SIM, o PIN ou outra credencial de acesso)

Estou ciente de que este acesso se destina à obtenção de prova para ser utilizada em processo penal, no inquérito acima referenciado. Declaro que o acesso compreende a pesquisa de dados e a sua visualização, bem como a recolha dos mesmos, por apreensão. Abrange todos os dados registados no dispositivo (incluindo textos, fotografias, vídeos, ficheiros de áudio, registos de mensagens ou conversações de correio eletrónico ou outras comunicações de natureza semelhante, lista de contactos, agenda), dados de acesso e utilização de aplicações de mensagens (tais como *Whatsapp*, *Messenger*, *Telegram* ou outras), dados de acesso e utilização de redes sociais (tais como *Facebook*, *Instagram*, *TikTok* ou outras).
A autorização que concedo também confere permissão para acesso e apreensão de dados noutros sistemas informáticos remotos, aos quais seja permitido o acesso legítimo a partir do meu dispositivo acima identificado, tais como redes sociais, serviços de correio eletrónico ou dados armazenados em sistemas remotos (na chamada *cloud*, ou nuvem).

Data		
Assinaturas	Declarante	
	Defensor[2]	
	Autoridade judiciária ou órgão de polícia criminal	

[2] Caso esteja presente, por assim o pretender o declarante, ou seja exigido, nos termos do artigo 64º, nº 1, alínea d) do Código de Processo Penal (arguido cego, surdo, mudo, analfabeto, desconhecedor da língua portuguesa, menor de 21 anos, ou se suscitar a questão da sua inimputabilidade ou da sua imputabilidade diminuída)