# BUSCAS INFORMÁTICAS (PESQUISAS) NA "CLOUD"

## Nota Prática nº 28/2025

***2 de abril de 2025***

# ÍNDICE

**NOTA PRÁTICA nº 28/2025**
**2 de abril de 2025**

# BUSCAS INFORMÁTICAS (PESQUISAS) NA "CLOUD"

***Esta Nota Prática tem como propósito ser um auxiliar dos magistrados do Ministério Público na compreensão da diligência processual descrita no artigo 15º da Lei do Cibercrime e, em particular, da extensão de pesquisas a sistemas informáticos remotos, a que se refere o seu nº 5.***
***Além de descrever brevemente o regime legal, faz também o seu enquadramento no direito internacional. Por se tratar de uma medida inovadora, que afasta princípios do direito internacional tradicional, refere também a jurisprudência existente sobre a mesma.***

## A – PESQUISA DE DADOS

**1.** O Código de Processo Penal consagra o bem conhecido regime de buscas e apreensões, como meios de obtenção de prova (artigos 174º a 186º). São institutos jurídicos comuns na generalidade dos regimes processuais de todo o mundo. Porém, as normas respeitantes às buscas foram previstas para espaços físicos, identificáveis por via sensorial. Por sua vez, as regras quanto às apreensões visam coisas ou objetos tangíveis. Nem umas nem outras se adaptam às realidades tecnológicas. Não são suscetíveis de aplicação na realização de buscas em sistemas informáticas ou na apreensão de dados informáticos: os sistemas informáticos não são espaços físicos e os dados não são objetos tangíveis.

**2.** Porque a investigação da criminalidade moderna exige que se realizem umas e outras, a busca, ou pesquisa, num sistema informático e a apreensão de dados informáticos, veio a Lei do Cibercrime[1] a consagrar estas figuras processuais, como meios de aquisição ou obtenção de prova, nos respetivos artigos 15º a 17º. Estas figuras processuais são naturalmente desenhadas à imagem e semelhança das suas equivalentes para o mundo físico, ou *offline*, adaptando-as, porém, ao mundo digital.
No artigo 15º, a Lei do Cibercrime regula aquilo a que chama pesquisa de dados informáticos, transpondo e adaptando para o ciberespaço a generalidade das regras previstas das buscas em processo penal[2]. Além disso, introduz no nº 5 uma norma específica para o ambiente digital.

## B – EXTENSÃO DA PESQUISA

**3.** O artigo 15º, nº 1, permite que a autoridade judiciária competente autorize uma busca (pesquisa) a um computador quando, durante o inquérito, tal se tornar necessário para a recolha de prova,

[1] Lei nº 109/2009, de 15 de setembro.
[2] Veja-se, nesse expresso sentido o artigo 15º, nº 6.

a fim de apurar a verdade. Além disso, o nº 5 do mesmo artigo permite que, no decurso de uma pesquisa, se estenda essa mesma a um outro computador ou sistema informático, se existirem razões para crer que a prova que pretende obter-se está armazenada nesse outro sistema, mas é legalmente acessível a partir do sistema inicialmente pesquisado.
Nesta norma permitem-se as buscas, ou pesquisas, à distância. Isto é, **a lei permite que se aceda, por via da busca informática, a computadores remotos**, desde que este acesso se faça a partir de um computador que legitimamente possa aceder ao outro. Trata-se de uma previsão legal de enorme amplitude e utilidade prática. Por exemplo, permite o acesso a servidores de uma empresa, a partir de terminais colocados em dependências dessa mesma empresa, física ou geograficamente distantes. Ou permite o acesso a contas de *webmail*, ou de redes sociais, desde que o dispositivo de onde se acede tenha legitimamente acesso às mesmas.
Os dados informáticos que venham a ser apreendidos por esta via constituem prova válida, por aplicação da regra geral do Artigo 125º do Código de Processo Penal (que determina ser admissível toda a prova que não seja proibida por lei).

## C – PESQUISA NA "*CLOUD*"

**4.** Esta disposição, do nº 5 do artigo 15º da Lei do Cibercrime pretende assumidamente transpor para o direito interno português o conteúdo do artigo 19º, nº 2 da Convenção de Budapeste[3], fonte direta da Lei do Cibercrime.
No texto da Convenção, esta possibilidade de extensão da pesquisa está apenas prevista para sistemas remotos nacionais, ou dados armazenados no território de cada Estado. Pelo contrário, o quadro jurídico português vai mais longe, permitindo às autoridades de justiça criminal **aceder a dados armazenados num sistema remoto, mesmo que tal sistema esteja fisicamente no estrangeiro**.

**5.** A investigação de crimes que se relacionam com redes de comunicações, ou as utilizam, supõe quase sempre obter provas digitais armazenadas em sistemas informáticos fisicamente localizados fora das fronteiras de Portugal. Este é um dos mais difíceis obstáculos a superar nas investigações criminais modernas. Por vezes, é impossível ao investigador determinar o local e país onde estão fisicamente alojados os dados informáticos que se procuram. E sendo impossível determinar o local dos dados, desde logo não pode determinar-se a lei aplicável à obtenção desses dados nem a autoridade nacional a quem devam solicitar-se tais dados, por via dos canais da cooperação internacional.

**6.** Foi neste contexto que o legislador português (como muitos outros) introduziu a possibilidade legal do acesso a dados remotos em investigações criminais. Nesta regulamentação afloram novos conceitos e novos princípios dos direitos modernos, introduzidos com o intuito de ultrapassar as dificuldades práticas e operacionais que as tecnologias colocaram à justiça criminal.
Um deles é o princípio da aplicação ao caso concreto do direito do lugar onde está quem tem a disponibilidade dos dados. Crescentemente, as legislações e a doutrina internacional vêm acolhendo a regra segundo a qual a obtenção de dados informáticos deve ser regulada pela lei do

[3] A Convenção sobre o Cibercrime do Conselho da Europa, conhecida como Convenção de Budapeste, foi adotada nesta cidade a 23 de novembro de 2001. Foi aprovada pela Resolução da Assembleia da República nº 88/2009 e ratificada pelo Decreto do Presidente da República nº 91/2009, ambos publicados no Diário da República, Iª Série I de 15 de setembro de 2009 (https://files.diariodarepublica.pt/1s/2009/09/17900/0635406378.pdf).

lugar onde está aquele que tem o efetivo acesso a dados informáticos e o direito de deles dispor – contrariamente, no passado o princípio vigente era o da aplicação do direito da localização física do sistema informático onde estavam armazenados os dados.
Esta linha de evolução vai ao encontro das exigências das investigações que requerem provas armazenadas na chamada *cloud*, ou "nuvem". Trata-se de informação que, pela sua própria natureza está deslocalizada e pode ser acedida a partir de qualquer local – o que torna irrelevante a localização física do servidor onde se aloja aquela informação. **A aplicação do princípio da disponibilidade legitima o acesso a estes dados (provas) às autoridades da jurisdição onde se encontra quem tem o poder e disponibilidade sobre os dados em causa** (o chamado "*data controller*").

**7.** Importa recordar que este acesso transfronteiriço a dados, de acordo com as regras conformadoras do sistema processual português, depende de decisão do Ministério Público (a quem pertencem todos os poderes de investigação, incluindo os poderes para autorizar buscas e apreensão de dados informáticos – artigos 15º e 16 da Lei do Cibercrime). No entanto, se no decurso destas diligências forem encontradas comunicações de correio eletrónico ou registos de comunicações de natureza semelhante) por imposição do artigo 17º da Lei do Cibercrime, é exigida a intervenção do juiz de instrução. A mesma exigência se impõe se o acesso remoto se deparar com dados cujo conteúdo seja suscetível de revelar informações pessoais ou íntimas e que coloquem em risco a privacidade do seu titular ou de terceiro (artigo 16º, nº 3 da Lei do Cibercrime). Em ambos os casos, a apresentação das provas obtidas ao juiz de instrução é necessária, sob pena de nulidade.

**8.** A possibilidade de aceder remotamente a dados informáticos pode ser utilizada na investigação da generalidade dos tipos de crimes: de acordo com o artigo 11º, número 1, da Lei do Cibercrime, pode recorrer-se a esta medida de investigação quando estiverem em causa crimes cometidos por meio de um sistema informático ou crimes em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico.

## D – JURISPRUDÊNCIA

**9.** Trata-se de uma possibilidade legal recente e a jurisprudência nacional a este respeito é ainda escassa. Porém, como a fonte do artigo 15º da Lei do Cibercrime é um tratado internacional (a Convenção de Budapeste, ratificada por quase todos os Estados europeus), é possível colher inspiração na jurisprudência de outros países.
A discussão principal a este respeito tem sido a da admissibilidade, à luz do direito internacional, da extensão da pesquisa informática para sistemas de computadores fisicamente localizados fora das fronteiras do território nacional.

**10.** Sobre este aspeto específico a jurisprudência internacional é marcada por dois casos: a deliberação do Supremo Tribunal Federal Suíço de 24 de maio de 2017[4] e a deliberação do Supremo Tribunal da Noruega de 28 de março de 2019[5] (no chamado caso *Tidal*). Ambos os países ratificaram a Convenção de Budapeste e introduziram nas respetivas leis internas a possibilidade

[4] Disponível aqui.
[5] Disponível em inglês aqui

de extensão de pesquisas informáticas. Nas duas decisões, a questão que motivou a decisão foi a da validade legal do acesso a dados informáticos armazenados fora do território nacional dos países em causa.
No caso suíço, as autoridades aceram ao Facebook de um suspeito com as legítimas credenciais do mesmo. O Supremo Tribunal Federal Suíço entendeu que o acesso pela Internet, a partir de computadores na Suíça, a dados *online* (na *cloud*), mesmo que alojados no estrangeiro, não era considerado como um ato praticado fora dos limites territoriais do país – e portanto era válido, sendo igualmente válida a prova dele resultante.
Quanto ao caso norueguês, no decurso de uma busca física, foi feita uma pesquisa em computadores existentes no local, verificando-se que a informação que importava obter (e que foi efetivamente obtida) estava alojada num serviço de alojamento remoto (na *cloud*). O Supremo Tribunal da Noruega considerou não ser relevante esta localização remota, uma vez que o acesso foi feito a partir da Noruega, local onde tinha sede a sociedade comercial em causa e onde estava a ser desenvolvida a investigação. Portanto, a pesquisa e a apreensão de dados no servidor remoto foi válida.

**11.** Em Portugal, pronunciou-se sobre esta específica questão o Tribunal da Relação do Porto que, no Acórdão de 11 de dezembro de 2024[6], citando e acolhendo a doutrina das duas decisões acima referidas, entendeu que o acesso transfronteiriço a dados, nos termos do nº 5 do artigo 15º da Lei do Cibercrime é conforme à Lei e à Constituição. Além disso, não contraria o direito internacional, mormente os princípios da territorialidade e da soberania nacional.
Esta decisão de um tribunal português acolhe, tal como as outras duas acima citadas, a doutrina moderna segundo a qual é importante "*quem e a partir de onde é que se tem acesso as dados*" e não o local de armazenamento daqueles dados que "*por sua natureza, se encontram num «espaço virtual», sendo a maioria das vezes desconhecido para o titular do acesso aos dados o local geográfico das máquinas ou dos materiais físicos de suporte onde os mesmos se encontram guardados*".

## E – ACESSO A DADOS EM FONTE ABERTA OU COM CONSENTIMENTO

**12.** O regime que acima se descreveu regula o acesso a dados que não estão publicamente disponíveis. Por isso não se confunde com o acesso aos chamados dados *em fonte aberta*. E também não se confunde com o acesso a dados com consentimento.
Em ambos estes casos é permitido o acesso a dados alojados na *cloud*, mesmo que no estrangeiro. Legitima este acesso, no direito português, o artigo 125º do Código de Processo Penal e no direito internacional, o artigo 32º da Convenção de Budapeste. Este último permite às autoridades nacionais de investigação criminal a obtenção direta, fora do território nacional, de informações *open source*. Esta mesma norma permite também a obtenção de dados informáticos "não abertos", se for obtida a autorização da pessoa com permissão legal para a conceder.

**13.** Este regime legal, que permite às autoridades portuguesas aceder a informação alojada no estrangeiro, tem uma contrapartida importante no artigo 25º da Lei do Cibercrime, que confere idêntica permissão a autoridades congéneres estrangeiras, quanto a dados fisicamente alojados em Portugal.

[6] Disponível aqui.