Jurisprudência Temática de Direito Processual Penal
N.º 148 – Abril de 2026

PESQUISA E APREENSÃO DE DADOS INFORMÁTICOS

JURISPRUDÊNCIA DO TRIBUNAL CONSTITUCIONAL

Acórdão de 20 de Junho de 2024 (Processo n.º 304/2024)
Consentimento – Pesquisa - Apreensão

Teria bastado a leitura atenta de todo o artigo 15.º para se deparar com alínea a) do seu número 3, onde se lê "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".

Assim sendo, e assumindo o recorrente o seu "consentimento", não seria necessário adivinhar a possível relevância desse consentimento, para efeitos de consideração da prova obtida.

O assim delineado arco normativo (…), não corresponde à *ratio decidendi* da decisão recorrida, pois que, o tribunal a quo em nenhum momento afirmou a possibilidade de valoração probatória sem autorização do JIC, em derrogação dos artigos 179.º, n.º 1, alínea a), ambos do CPP; antes afirmou a validade da perícia com base no consentimento do visado, previsto no artigo 15.º, n.º 3, alínea a), da LCC, tendo sido precisamente esse o critério normativo de decisão.

Acórdão de 4 de Outubro de 2017 (Processo n.º 89/2017)
Conteúdo de mensagens de correio eletrónico – Pesquisa de sistema informático – Dados informáticos - Lei do Cibercrime

Ora, é um dado seguro que o acesso ao conteúdo de mensagens de correio eletrónico não integra o conceito de pesquisa de sistema informático, para efeitos de delimitação da norma aplicada na decisão recorrida e sindicada junto deste Tribunal. Se é certo que uma pesquisa genérica permite identificar a eventual presença de correio eletrónico e de outros dados informáticos suscetíveis de revelar dados pessoais ou íntimos que estejam armazenados num sistema informático, é igualmente claro que a mesma não abrange o acesso ao conteúdo ou mesmo a autorização para apreender esses elementos.

Com efeito, não foi com o sentido e alcance que lhes atribui o recorrente que os artigos 11.º, n.º 1, alínea c) e 15.º, n.º 1, ambos da Lei n.º 109/2009, de 15 de setembro, foram interpretados e aplicados pelo Supremo Tribunal de Justiça. No acórdão recorrido, ainda que por remissão para o acórdão do Tribunal da Relação do Porto, de 7 de julho de 2016, distinguiram-se com nitidez os âmbitos objetivos de aplicação das disposições dos artigos 15.º, 16.º e 17.º da Lei n.º 109/2009, de 15 de setembro. Aí se interpretou o artigo 15.º como regulando apenas a pesquisa de um sistema informático — o mesmo é dizer: a determinação do que lá se encontra armazenado —, mas não a apreensão de qualquer elemento cuja presença seja revelada pela pesquisa (sobre a qual dispõe o artigo 16.º), nem o caso especial das mensagens de correio eletrónico ou registos de comunicações de natureza semelhante (sobre o qual dispõe o artigo 17.º, ainda que por lapso manifesto a decisão refira o artigo 18.º).

JURISPRUDÊNCIA DO SUPREMO TRIBUNAL DE JUSTIÇA

Acórdão de 3 de Abril de 2025 (Processo n.º 5722/22.2T9AVR-A.P1-A.S1)
Recurso para fixação de jurisprudência – Pressupostos – Identidade dos factos – Busca – Correio eletrónico - Admissibilidade de recurso

Não existe identidade fáctica quando no acórdão recorrido se aprecia situação em que o MP tinha ordenado a realização de buscas e de pesquisas informáticas em material informático existente nas instalações das sociedades investigadas sem que tivesse sido determinada a apreensão de correio eletrónico e o tribunal entendeu que, tendo o correio eletrónico sido encontrado na sequência das diligências legitimamente autorizadas pelo MP (busca e pesquisa informática), nos termos do arts. 15.º e 16.º, n.ºs 1 e 3, da Lei do Cibercrime, tais dados podiam ter sido extraídos e selados para que o juiz de instrução, após análise, inteirando-se do respetivo conteúdo, decidisse se os mesmos deveriam ou não ser apreendidos para junção ao processo, considerando que tal extração e selagem dos dados constituía uma medida cautelar de preservação dos dados e não uma apreensão; e por seu turno, no acórdão fundamento se aprecia situação em que o MP ordenou a busca e pesquisa informática ao conteúdo dos sistemas informáticos que viessem a ser encontrados na posse dos buscados, com a advertência de que, caso fosse encontrado correio eletrónico, deveria ser efetuada uma cópia cega, sem visualização de conteúdo a fim de ser exibida à mm.ª juíza de instrução, entendendo o tribunal que se o MP, quando ordenou as diligências, pretendia que fosse apreendida ou extraída correspondência de qualquer tipo, nomeadamente eletrónica, teria que requerer a prévia autorização judicial para essa apreensão, por só no caso de inadvertidamente encontrada correspondência eletrónica no decurso de uma busca devidamente autorizada ser possível apresentá-la judicialmente sem autorização prévia e por essa razão julgou verificada a nulidade, por força do art. 17.º da Lei do Cibercrime e do art. 179.º, n.º 1, do CPP.

As soluções encontradas em cada um daqueles acórdãos divergem por serem diferentes as situações fácticas verificadas nos inquéritos, o que foi determinante para que naqueles acórdãos se fizesse uma diferente interpretação do direito aplicável.

Acórdão de 11 de Outubro de 2023 (Processo n.º 184/12.5TELSB-R.L1-A.S1)
Acórdão de fixação de jurisprudência – Inquérito – Juiz de instrução – Competência – Apreensão de correio eletrónico e registo de comunicações de natureza semelhante – Lei do Cibercrime

Uma adequada compreensão dos regimes previstos nos artigos 15.º e 17.º da Lei do Cibercrime afasta a alegação de idênticas dificuldades práticas dessa intervenção prévia de um juiz, na medida em que a pesquisa de dados informáticos tem em vista a obtenção de "dados informáticos específicos e determinados" e só deverá ser apreendida a correspondência eletrónica "de grande interesse para a descoberta da verdade ou para a prova", devendo, sempre que possível, ser presidida pela autoridade judiciária que a autorizou ou ordenou.

Acórdão de 27 de Agosto de 2021 (Proc. n.º 1/20.2F1PDL.S1)
Tráfico de estupefacientes – Apreensão – Autoridade judiciária – Correio de droga – atenuação especial da pena – medida da pena

No regime processual especial da Lei do Cibercrime, a tradicional busca deu lugar à pesquisa em sistemas informáticos da representação de factos, informações ou conceitos sob uma forma suscetível de processamento naqueles sistemas, incluindo os programas aptos a fazê-lo executar uma função.

A pesquisa livremente consentida pelo titular dos dados ou documentos, pode ser efetuada por OPC, sem autorização da autoridade judiciária.

O consentimento dispensa, salvo disposição em contrário, o controlo e validação posterior da autoridade judiciária, porque, nessas circunstâncias, a intromissão na privacidade ou na correspondência não é abusiva.

O facto de se tratar de chats e sms, em suma, de comunicações eletrónicas (que podem incluir textos, imagens, vídeos, áudios, etc.) não obsta a que o titular consinta, livremente, na respetiva pesquisa.

O OPC pode, no decurso de pesquisa informática, legitimamente executada, - designadamente mediante consentimento documentado -, apreender para os autos dados ou documentos informáticos, em suma, prova eletrónica necessária à demonstração de um crime e do seu agente, também sem prévia autorização da autoridade judiciária – art. 16.º, n.º 2 da Lei do Cibercrime.

Quando assim suceder, tem sempre de submeter a apreensão efetuada a validação da autoridade judiciária competente no prazo máximo de 72 horas.

Quando os dados ou documentos apreendidos tenham conteúdo suscetível de revelar dados pessoais ou íntimos, que possam pôr em causa a privacidade do titular ou de terceiro são, sob pena de nulidade, apresentados ao juiz, que ponderará da junção aos autos tendo em conta os interesses do caso – art. 16.º, n.º 3 da citada Lei.

A nulidade resultante da não apresentação ao juiz de instrução dos dados e documentos apreendidos em suporte ou sistema informático, que tenham aquele conteúdo particular, consubstancia a proibição de obtenção de prova, estatuída nos arts. 32.º, n.º 8 da Constituição da República e 126.º do CPP.

As provas obtidas com intromissão na vida privada, na correspondência e nas telecomunicações não são nulas se o seu titular nisso consentir, livre e esclarecidamente - art. 126.º, n.º 3 do CPP – porque não são obtidas por método proibido, não advindo ao processo por "abusiva intromissão" naqueles direitos fundamentais.

Nas demais situações a validação da apreensão efetuada pelo OPC em inquérito, compete ao Ministério Público.

A não validação da apreensão de dados ou documentos informáticos que não tenham conteúdo suscetível de respeitar à privacidade ou intimidade, porque obrigatória, configura a nulidade cominada no art. 120.º, n.º 2 al. d) do CPP.

Nulidade que resulta sanada se não for arguida nos prazos estipulados no seu n.º 3.

JURISPRUDÊNCIA DO TRIBUNAL DA RELAÇÃO DE LISBOA

Acórdão de 21 de Novembro de 2024 (Processo n.º 85/18.3TELSB-F.L1-9)
Lei do Cibercrime – Correio eletrónico

A Lei do Cibercrime, Lei n.º 109/2009 de 15 de Setembro transpôs para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI do Conselho da Europa de 24 de Fevereiro relativa a ataques contra sistemas de informação e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa adotada em Budapeste em 23 de novembro de 2001 (aprovada pela Resolução da Assembleia da República n.º 88/2009 de 10 de Julho de 2009 publicada no DR. I série, de 15 de Setembro de 2009 e ratificada pelo Decreto n.º 91/2009 de 15 de Setembro).

A lei n.º 109/2009 instituiu pela primeira vez regras jurídicas (disposições penais materiais e processuais) específicas referentes à recolha de prova em suporte eletrónico, sendo nos termos do n.º 1 do art. 11.º, as disposições dela constantes aplicáveis a todo e qualquer crime, desde que se mostre necessária a recolha da prova em suporte eletrónico, encontrando-se nos art. 15.º a 17.º a regulamentação relativa à pesquisa (art. 15.º) e apreensão de dados ou documentos informáticos previamente armazenados num sistema informático (arts. 16.º e 17.º), estabelecendo o art.º 17.º um regime especial para a apreensão de correio eletrónico e registos de comunicações de natureza semelhante.

Por regra é a autoridade judiciária competente – o Juiz ou o Ministério Público-, consoante a fase processual, que autoriza ou ordena a realização da pesquisa e apreensão sempre que tal seja indispensável para a prova (n.º 1 do art. 16.º).

A lei individualiza duas situações específicas cuja sensibilidade e relevância jurídico-constitucional justifica a previsão de um regime normativo particular relativo à apreensão de dados sensíveis (dados pessoais ou íntimos que possam pôr em causa a privacidade do respetivo titular ou de terceiros) (art. 16.º) e de correio eletrónico e registos de natureza semelhante (art. 17.º).

Decorre do art. 17.º que compete ao juiz autorizar ou ordenar por despacho a apreensão de mensagens de correio eletrónico ou registos de comunicações de natureza semelhante encontrados no decurso de pesquisas informáticas ou outro acesso legítimo a um sistema informático que se afigurem ser de grande interesse para a descoberta da verdade ou para a prova, aplicando-se o regime de apreensão de correspondência previsto nos artigos 178.º e 179.º do Código de Processo penal.

O n.º 3 do art. 179.º, do CPP impõe que seja o Juiz de Instrução Criminal, enquanto juiz das liberdades, direitos e garantias, enquanto e garante dos direitos fundamentais, mesmo na fase de inquérito, a tomar em primeiro lugar conhecimento, em primeira visualização, do correio eletrónico aprendido, sob pena de nulidade prevista no art. 120.º, n.º 2 al. d) do CPP, que não tem que ser obrigatoriamente completo.

Compete igualmente ao Juiz de Instrução Criminal ordenar ou autorizar a junção aos autos das mensagens de correio eletrónico que se afigurem relevantes para a prova, através de despacho fundamentado e recorrível.

Após a abertura e primeira visualização pelo juiz de Instrução Criminal e exclusão daqueles que possam contender com a reserva da vida privada e não tenham relevância para a prova, o Juiz de Instrução Criminal autoriza o Ministério Público, enquanto titular, a quem compete a direção do inquérito e da investigação, e por emanação do princípio do acusatório previsto no art. 32.º, n.º 5 da Constituição da República Portuguesa, a selecionar as mensagens de correio eletrónico que se lhe afigurem relevantes para descoberta da verdade e para a prova, apresentando-a ao Juiz de Instrução Criminal em ordem a determinar a junção aos autos.

Acórdão de 25 de Janeiro de 2024 (Processo n.º 1/21.5ICLSB-A.L1-9)
Lei do Cibercrime – Dados informáticos – Buscas – Cópia cega – Crime continuado

O legislador da Lei do Cibercrime, com a menção feita no seu art. 15.º, n.º 1, à obtenção de dados informáticos específicos e determinados, não pretendeu certamente abarcar uma exigência legal de pré-identificação exata e rigorosa dos dados informáticos a pesquisar, no decurso de buscas, mas tão-só pretendeu que houvesse uma interligação entre os dados informáticos pesquisados e a sua relevância probatória para a descoberta da verdade material.

O procedimento que tem vindo a ser genericamente denominado de "cópia cega", não é, só por si e de forma imediata, reprovável ou inadmissível, podendo encontrar-se justificada a necessidade de se proceder à pesquisa dos dados informáticos (art. 15.º da LCC), em local externo, relativamente ao local buscado, por recurso, excecional, à "cópia cega" de tais ficheiros.

É que, a "cópia cega" a que apenas se lançou mão na sequência da grande extensão dos ficheiros a pesquisar, não constitui uma apreensão, em sentido estrito, mas, antes, uma diligência prévia necessária, uma atuação meramente "facilitadora", com vista a permitir um extenso trabalho posterior: a efetivação da pesquisa devida e autorizada pelo JIC - a qual, pela circunstância excecional referida, deverá ter lugar num local externo.

Acórdão de 11 de Maio de 2023 (Processo n.º 215/20.5T9LSB-C.L1-9)
Cibercrime – Recolha de prova – Procedimento – Valoração – Juiz de instrução

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 eletrónico (secundarizando o Código de Processo Penal) para fazer face a novas realidades e inerentes especificidades, tais como dos dados informáticos e do correio eletrónico, justificando-se o sacrifício do interesse individual numa comunicação livre de interferências alheias, em prol do exercício do "*ius puniendi*" estadual.

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 à 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.

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 DO TRIBUNAL DA RELAÇÃO DO PORTO

Acórdão de 11 de Dezembro de 2024 (Processo n.º 5722/22.2T9AVR-A.P1)
Convenção de Budapeste – Lei do Cibercrime – Interpretação da lei – Elementos essenciais – Jurisprudência internacional – Princípio da territorialidade – Sistema informático – Dados pessoais – Acesso a dados – Legalidade

Contextualizando-se a interpretação com um sentido atualista dos arts. 19.º, 22.º e 32.º da Convenção sobre o Cibercrime, adotada em Budapeste em 23 de novembro de 2001, à luz dos respetivos objeto e fim, tendo-se devidamente em conta os elementos sistemático e teleológico, assim como a jurisprudência internacional relevante, nomeadamente os Acórdão do Supremo Tribunal Federal Suíço, de 24/05/2017, e do Supremo Tribunal da Noruega, de 29/03/2019 (caso Tidal), cujos países são Partes naquela Convenção, não haverá violação do princípio da territorialidade no acesso e recebimento de dados informáticos armazenados em *Cloud Computing*, num servidor localizado em território estrangeiro, quando, de harmonia com a legislação interna, os dados pesquisados, ainda que localizados fora do respetivo território, o foram através de credenciais que em si permitiam o acesso legítimo a esses mesmos dados por parte da entidade investigada, a partir do seu próprio território, não assumindo ademais a busca informática realizada uma dimensão que pudesse materialmente pôr em causa o princípio da soberania de outro Estado.

O princípio da territorialidade, nos termos previstos na Convenção de Budapeste, assim como o princípio do primado do direito internacional convencional sobre o direito ordinário interno, não terão possibilidade de aplicação quando a busca informática a realizar tiver por objeto dados de um sistema informático situado num "espaço virtual" relativamente ao qual se desconhece o local geográfico das máquinas ou dos materiais físicos de suporte onde tal sistema informático e respetivos dados se encontram guardados, ou, conhecendo-se esse local, o respetivo país não tenha ratificado, aceitado ou aprovado aquela Convenção, nos termos dos arts. 2.º da Convenção de Viena sobre o Direito dos Tratados e 36.º da Convenção sobre o Cibercrime.

Concomitantemente não haverá qualquer questão de ilegalidade por confrontação de normas de direito internacional convencional com as normas de direito ordinário interno, e assim também qualquer violação do art. 8.º, n.º 2, da Constituição da República Portuguesa.

A determinação pelo Ministério Público, na qualidade de autoridade judiciária, no sentido de se proceder cautelarmente à realização de cópias digitalmente encriptadas, devidamente seladas, sendo uma delas para entregar ao Juiz de instrução criminal, de cujo conteúdo virá este a ter conhecimento em primeiro lugar, tendo em vista a apreciação da existência ou não de grande interesse da mesma para a descoberta da verdade ou para a prova, harmoniza-se com o regime legalmente previsto na Lei do Cibercrime, nomeadamente no seu art. 17.º, relativo à apreensão de correio eletrónico, mostrando-se ademais devidamente salvaguardado o sigilo da correspondência, bem como a garantia de reserva de juiz na tutela dos direitos fundamentais com ela relacionados, tal como sucederá quando no decurso de uma busca informática venham a ser detetados dados suscetíveis de revelar informação de natureza pessoal ou íntima dos visados, nos termos do artigo 16.º, n.º 3, daquela Lei.

A envergadura da investigação, a sua dimensão e a quantidade de dados a pesquisar, torna proporcional e justificada a pesquisa informática sem a utilização de "palavras-chave", sob pena de ficar inabalavelmente prejudicada a pesquisa a realizar e com ela a descoberta da verdade.

Acórdão de 5 de Abril de 2017 (Processo n.º 671/14.0GAMCN.P1)
Lei do Cibercrime – Facebook – Prova

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 à Lei do Cibercrime - DL n.º 109/2009 de 15/9.

Constitui prova legal a cópia de informação que alguém publicita no seu mural do Facebook sem restrição de acesso.

Só esta sujeita à disciplina do art. 16.º, n.ºs 1 e 3 da Lei do Cibercrime a apreensão da informação original inserta na plataforma, esteja ou não disponível.

Acórdão de 7 de Junho de 2016 (Processo n.º 2039/14.0JAPRT.P1)
Agente encoberto – Informador – Busca – Flagrante delito – Lei do Cibercrime – Exame de computador – Correio eletrónico – Dados de navegação na internet

A busca em casa habitada pode ser realizada pela autoridade policial nos casos de flagrante delito (abrangendo o flagrante delito em sentido restrito, o quase flagrante delito e a presunção de flagrante delito) desde que por crime a que corresponda pena de prisão – art. 174.º, nºs 2, 3 e 5, al. c), do CPP.

As buscas subsequentes ao flagrante delito não estão limitadas ao local e ao momento do crime (não existe um limite temporal para tal diligência), devendo exigir-se apenas que não se trate do decurso de um prazo desproporcionado para o efeito ou inadequado ao caso, de acordo com as regras da proporcionalidade, adequação e razoabilidade face à necessidade da mínima intromissão/intervenção na vida do arguido e tendo em vista o crime em análise e seus contornos.

A busca de onde resulte a apreensão de um computador é regulada pelas normas do Cód. Proc. Penal.
VII A pesquisa no computador dos dados informáticos que dele constam, bem como a apreensão desses dados é regulada na Lei do Cibercrime, em cujo âmbito definido logo no art. 1.º se encontram "as disposições penais materiais e processuais (…), relativas ao domínio (…) da recolha de prova em suporte eletrónico".

Apreendido um computador com acesso à internet, a autoridade judiciária pode ordenar ou autorizar a pesquisa desse sistema informático (art. 15.º n.º 1) e se no seu decurso foram encontrados dados ou documentos informáticos a autoridade judiciária ordena ou autoriza essa apreensão (art. 16.º n.º 1) – sem prejuízo da apreensão pela polícia criminal sujeita a validação (art. 16.º n.ºs 2 e 4), apreensão essa sujeita às formas do n.º 7 do mesmo art..

Se, no decurso da pesquisa, for encontrado correio eletrónico ou registo de comunicações de natureza semelhantes, o juiz ordena ou autoriza a sua apreensão (art. 18.º), seguindo-se o regime da apreensão de correspondência do CPP (art. 179.º).

Acórdão de 12 de Setembro de 2012 (Processo n.º 787/11.5PWPRT.P1)
Prova proibida – SMS

O órgão de polícia criminal pode proceder a pesquisa em telemóvel ou outro suporte informático, sem prévia autorização da autoridade judiciária, para que decida da conveniência da sua apreensão. Porém, essa possibilidade está limitada aos casos em que a mesma seja voluntariamente consentida por quem tiver a disponibilidade ou o controlo desses dados – desde que o consentimento prestado fique, por qualquer forma, documentado – ou, 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.

Não sendo essa a situação, se as SMS (*short message service*) guardadas no telemóvel do arguido foram lidas e transcritas pelo órgão de polícia criminal sem o seu consentimento nem foi autorizada a sua apreensão pelo juiz de instrução criminal, autoridade judiciária naquele momento competente para o efeito, estamos perante um caso de prova proibida.

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.

JURISPRUDÊNCIA DO TRIBUNAL DA RELAÇÃO DE COIMBRA

Acórdão de 26 de Abril de 2023 (Processo n.º 840/22.0T9LRA-A.C1)
Pesquisa informática – Apreensão de equipamento informático – Extração de material recolhido em equipamento informático – Validação da junção aos autos dos dados recolhidos – Prazo para a apresentação dos dados recolhidos ao juiz

A pesquisa informática a que se refere o artigo 15.º, n.º 1, da Lei do Cibercrime consiste numa pesquisa sumária ao equipamento eletrónico suspeito para averiguar se nele existem dados armazenados que interessem à prova; se a resposta for positiva, o equipamento é apreendido com vista à extração dos dados.

É distinto o apuramento da existência de dados informáticos específicos e determinados que se encontrem armazenados num sistema informático, obtido através de pesquisa informática sumária, e a extração dos dados relevantes do equipamento informático onde foram encontrados, bem como a sua junção ao processo, razão pela qual aquela pesquisa nunca pode ser confundida com a "junção" do material aos autos.

O prazo a que se refere o artigo 15.º, n.º 2, da Lei do Cibercrime respeita àquela pesquisa sumária, não à extração dos dados relevantes do equipamento informático para efeitos da sua junção ao processo, que se encontra previsto no art. 16.º da mesma lei.

Quando forem apreendidos 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, devem ser apresentados ao juiz antes da sua junção aos autos, sob pena de nulidade, para prolação do despacho a que se refere no n.º 3 do artigo 16.º da Lei do Cibercrime.

JURISPRUDÊNCIA DO TRIBUNAL DA RELAÇÃO DE ÉVORA

Acórdão de 25 de Fevereiro de 2025 (Processo n.º 1064/22.1PAOLH-A.E1)

Lei do Cibercrime – Pesquisa de dados em sistema informático – Apreensão de dados ou documentos Informáticos – Prazo de 30 dias – Nulidade dependente de arguição

A pesquisa de dados num sistema informático (no caso um telemóvel), em inquérito, realizada ao abrigo do disposto no artigo 15.º da Lei do Cibercrime, pode ser ordenada pelo Ministério Público, competindo a essa autoridade ordenar a apreensão dos dados ou documentos informáticos necessários à produção de prova revelados nessa pesquisa.

Se os dados ou documentos informáticos apreendidos pelo Ministério Público tiverem conteúdo suscetível de revelar dados pessoais ou íntimos, que possam pôr em causa a privacidade do respetivo titular ou de terceiro, compete ao juiz de instrução decidir se devem ser juntos aos autos, tendo em conta os interesses do caso concreto.

Quando, no decurso da mesma pesquisa, forem encontrados, armazenados no sistema informático, mensagens de correio eletrónico ou registos de comunicações de natureza semelhante, é ao juiz de instrução que compete ordenar a apreensão daqueles que se afigurem ser de grande interesse para a descoberta da verdade ou para a prova.

O despacho que autoriza ou ordena a pesquisa no sistema informático tem um prazo de validade máximo de 30 dias, sob pena de nulidade. A contagem desse prazo inicia-se no momento em que o órgão de polícia criminal está em condições de realizar a pesquisa e não no momento em que o despacho é proferido. A violação do prazo determina a nulidade do ato, sujeita ao regime de arguição previsto no artigo 120.º do Código de Processo Penal, e não uma proibição de prova.

Acórdão de 7 de Maio de 2024 (Processo n.º 338/23.9JAFAR-B.E1)
Cibercrime - Recolha de Prova – Procedimento – Juiz de Instrução Criminal

Sendo determinada, pelo Ministério Público, a pesquisa em sistema informático, a apreensão, nesse âmbito, de mensagens de correio eletrónico ou registos de comunicações de natureza semelhante tem de ser previamente autorizada pelo Juiz de Instrução Criminal, nos termos das disposições conjugadas dos artigos 17.º da Lei do Cibercrime, 179.º, n.º 1, e 269.º, n.º 1, al. d), ambos do C. P. Penal.

No caso dos autos, tendo sido ordenada pelo Ministério Público a pesquisa ao sistema informativo dos equipamentos eletrónicos, designadamente telemóveis apreendidos, e tendo no decurso dessa pesquisa sido encontrados registo de comunicações via "*chat*" na aplicação "*Telegram*", da agenda e registo de chamadas, que foram extraídos e gravados em CD´s conquanto estes hajam sido selados e os dados encriptados, o facto é que não existiu despacho prévio do Juiz de Instrução Criminal a determinar ou a autorizar a apreensão desses registos de comunicações.

A consequência dessa omissão não pode deixar de ser a nulidade da apreensão das mensagens de correio eletrónico e registos de comunicações de natureza semelhante determinada no despacho recorrido (cfr. artigo 179.º, n.º 1, do C. P. Penal), com a consequente proibição de utilização dessa prova (cfr. artigo 126.º, n.º 3, do mesmo diploma legal).

Acórdão de 20 de Janeiro de 2015 (Processo n.º 648/14.6GCFAR-A.E1)
Crime informático – Cibercrime – Prova eletrónica

O regime processual das comunicações telefónicas previsto nos artigos 187.º a 190.º 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 n.º 109/2009, de 15-09 (Lei do Cibercrime) como regime regra.
Esse mesmo regime processual das comunicações telefónicas deixara de ser aplicável à recolha de prova por "localização celular conservada" – uma forma de "recolha de prova eletrónica – desde a entrada em vigor da Lei n.º 32/2008, de 17-07.

Para a prova eletrónica preservada ou conservada em sistemas informáticos existe um novo sistema processual penal, o previsto nos artigos 11.º a 19.º da Lei n.º 109/2009, de 15-09, Lei do Cibercrime, coadjuvado pela Lei nº 32/2008, neste caso se estivermos face à prova por "localização celular conservada".

Nessa Lei do Cibercrime coexistem dois regimes processuais: o regime dos artigos 11.º a 17.º e o regime dos artigos 18.º e 19.º do mesmo diploma. O regime processual dos artigos 11.º a 17.º surge como o regime processual "geral" do cibercrime e da prova eletrónica. Isto porquanto existe um segundo catálogo na Lei n.º 109/2009, o do artigo 18.º, n.º 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 19.º - são aplicáveis por remissão expressa os artigos 187.º, 188.º e 190.º do C.P.P. e sob condição de não contrariarem e Lei n.º 109/2009.

As normas contidas nos artigos 12.º a 17.º da supramencionada Lei contêm um completo regime processual penal para os crimes que, nos termos das alíneas do n.º 1 do artigo 11.º, estão (a) previstos na lei n.º 109/2009, (b) são ou foram cometidos por meio de um sistema informático ou (c) em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico.

A diferenciação de regimes assenta na circunstância de os dados preservados nos termos dos artigos 12.º a 17.º se referirem à pesquisa e recolha, para prova, de dados já produzidos, mas preservados, armazenados, enquanto o artigo 18.º do diploma se refere à interceção de comunicações eletrónicas, em tempo real, de dados de tráfego e de conteúdo associados a comunicações específicas transmitidas através de um sistema informático.

Assim, o Capítulo III da Lei n.º 109/2009, relativo às disposições processuais, deve ser encarado como um «escondido Capítulo V ("Da prova eletrónica"), do Título III ("Meios de obtenção de prova") do Livro III ("Da prova") do Código de Processo Penal …» (Dá Mesquita).

Tratando-se de obter prova por "localização celular conservada", isto é, a obtenção dos dados previstos no artigo 4.º, n.º 1 da Lei 32/2008, de 17-07, o regime processual aplicável assume especialidade nos artigos 3.º e 9.º desta lei.

Em suma, numa interpretação conjugada das Leis n.ºs 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.º 1 do artigo 11.º da Lei 109/2009 como pressuposto de aplicação do regime processual contido nos artigos 11.º a 17.º dessa Lei;
- o catálogo de crimes do n.º 1 do artigo 18.º da Lei n.º 109/2009 como pressuposto de aplicação do regime processual contido nesse artigo 18.º e no 19.º dessa Lei aos crimes previstos na al. a) do artigo 18.º;
- o catálogo de crimes do n.º 1 do artigo 187.º do Código de Processo Penal, por remissão expressa da Lei n.º 109/2009, como pressuposto de aplicação do regime processual contido nesse artigo 18.º. e no 19.º dessa Lei para os crimes previstos na al. b) do artigo 18.º;
- o catálogo de crimes ("crimes graves") do artigo 3.º da Lei nº 32/2008 quanto a especiais "dados conservados" (localização celular), como requisito de aplicação dos artigos 3.º e 9.º da Lei nº 32/2008.

O artigo 189.º do Código de Processo Penal nunca é aplicável a crimes informáticos, seja qual for o catálogo aplicável.

O objeto 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 (à exceção do correio eletrónico, especificamente previsto no seu artigo 17.º).
O regime processual da Lei nº 32/2008 constitui relativamente aos dados "conservados" que prevê no seu artigo 4.º, um regime especial relativamente ao capítulo processual penal geral que consta dos artigos 11.º a 19.º da Lei nº 109/2009.

Consequentemente devemos concluir que o regime processual da Lei n.º 32/2008, designadamente o artigo 3.º, nºs 1 e 2 e o artigo 9.º:
- 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 4.º, n.º 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 4.º, n.º 1 da Lei n.º 32/2008, isto é, para os dados conservados relativos à localização celular. Só para este último caso ganha relevo o conceito de "crime grave".

Antes da entrada em vigor das Leis n.ºs 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 252.º-A do C.P.P. e a outra o meio de obtenção de prova previsto no artigo 189.º, n.º 2 do mesmo código, que se mantém em vigor para a localização celular em tempo real.

Agora coexistem três realidades distintas através do acrescento da obtenção de dados de localização celular "conservados" por via da Lei n.º 32/2008.

Os requisitos do n.º 3 do artigo 9.º da Lei n.º 32/2008 mostram-se de verificação alternativa. O conceito de "suspeito" dele constante exige "determinabilidade" e não "determinação".

A previsão do artigo 252.º-A do Código de Processo Penal é claramente uma previsão de carácter excecional para situações de carácter excecional.

JURISPRUDÊNCIA DO TRIBUNAL DA RELAÇÃO DE GUIMARÃES

Acórdão de 15 de Abril de 2012 (Processo n.º 68/10.1GCBRG.G1)
Transcrição – Mensagens SMS – Autorização judicial – Juiz – Prova

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 de 29 de Março de 2011 (Processo n.º 735/10.0GAPTL-A.G1)
Telecomunicações – Cibercrime – Cartão de telemóvel – Mensagens SMS

Tendo o Ministério Público determinado a pesquisa de dados informáticos supostamente guardados no telemóvel da denunciante, a apreensão das mensagens (SMS) ali encontradas deve ser autorizada pelo juiz de instrução -artigo 17º da Lei do Cibercrime (Lei n.º 109/2009, de 15/9).

A lei não estabelece qualquer distinção entre mensagens por abrir ou já abertas.

Carlos Pinto de Abreu
André Gil Dias