SEPARATA RPDC N.º 4 (2024)

REVISTA PORTUGUESA DE DIREITO CONSTITUCIONAL

PORTUGUESE REVIEW OF CONSTITUTIONAL LAW

AATRIC

*Acórdãos n.os 91/2023, 314/2023 e 533/2024: Apreensão de Emails pela Autoridade da Concorrência em Processo Contraordenacional**

Paulo de Sousa Mendes

Professor Catedrático da Faculdade de Direito da Universidade de Lisboa
paulosousamendes@fd.ulisboa.pt

I. Introdução

O Tribunal Constitucional (TC), em recentes decisões[1], não julgou inconstitucional a norma contida na alínea *c*) do n.º 1 do artigo 18.º do Novo Regime Jurídico da Concorrência (NRJC), na versão aprovada pela Lei n.º 19/2012, de 8 de maio, segundo a qual, em processo contraordenacional por prática restritiva da concorrência, é permitida à Autoridade da Concorrência (AdC) a busca e apreensão de mensagens de correio eletrónico marcadas como abertas, mediante autorização judicial.

O TC julgou inconstitucional, por violação do disposto nos artigos 32.º, n.º 4, e 34.º, n.os 1 e 4, este conjugado com o artigo 18.º, n.º 2, todos da Constituição da República Portuguesa (CRP), a norma extraída das disposições conjugadas do n.º 2 do artigo 18.º e do n.º 1 do artigo 20.º do NRJC, na versão aprovada pela Lei n.º 19/2012, de 8 de maio, segundo a qual, em processo contraordenacional por prática restritiva da concorrência, é permitida à AdC a busca e apreensão de mensagens de correio eletrónico abertas mediante autorização do Ministério Público (MP).

---

* O presente texto baseia-se na apresentação realizada no VI Seminário da AATRIC no dia 11 de dezembro de 2023, mas faz referência a desenvolvimentos subsequentes relevantes para a matéria tratada.

[1] Acórdãos TC n.º 91/2023, de 16 de março, e n.º 314/2023, de 26 de maio.

Já depois da minha apresentação no VI Seminário da AATRIC, em 11 de dezembro de 2023, o TC decidiu não julgar inconstitucional o disposto no artigo 18.º, n.º 1, alínea *c*), da Lei n.º 19/2012, de 8 de maio (na redação original, anterior à conferida pela Lei n.º 17/2022, de 17 de agosto), quando interpretado: i) - No sentido de que é possível, em processo de contraordenação da concorrência, examinar, recolher e apreender mensagens de correio eletrónico; ii) - No sentido de admitir a possibilidade de exame, recolha e/ou apreensão de mensagens de correio eletrónico "abertas" ou "lidas"; iii) - No sentido de admitir o exame, recolha e apreensão de mensagens de correio eletrónico em processo de contraordenação da concorrência sem despacho judicial prévio[2]. Tal como assinalado numa das declarações de voto, é praticamente certa a interposição, pela recorrente, de recurso para o plenário, ao abrigo do n.º 1 do artigo 79.º-D da Lei do Tribunal Constitucional (LTC), ademais considerando que, neste último acórdão, estamos perante um julgamento de não inconstitucionalidade por um colégio de cinco juízes dos quais quatro estão vencidos, ou seja, um acórdão que exprime a posição de um único juiz, o Conselheiro Relator[3].

Um recente acórdão do Pleno das Secções Criminais do Supremo Tribunal de Justiça, (STJ) de uniformização de jurisprudência[4], refere-se ao processo penal, mas não deixa de ser relevante para o presente contexto. Eis a jurisprudência fixada: na fase de inquérito, compete ao juiz de instrução ordenar ou autorizar a apreensão de mensagens de correio eletrónico ou de outros registos de comunicações de natureza semelhante, independentemente de se encontrarem abertas (lidas) ou fechadas (não lidas), que se afigurem ser de grande interesse para a descoberta da verdade ou para a prova, nos termos do artigo 17.º, da Lei n.º 109/2009, de 15 de setembro (Lei do Cibercrime).

Pedem-nos uma apreciação crítica aos referidos dois acórdãos do TC (agora três acórdãos do TC), o que faremos nesta apresentação. Mas antes mesmo de nos pronunciarmos sobre esses acórdãos, impõe-se que submetamos a nossa análise ao contexto mais vasto do Direito internacional regional (Direito europeu dos direitos humanos e Direito da União Europeia) e do Direito estrangeiro (Direito norte-americano), este último enquanto termo de comparação. Só depois estaremos em condições de apreciar criticamente, de maneira suficientemente informada, os dois (agora três) recentes acórdãos do TC.

---

[2] Acórdão TC n.º 533/2024, de 4 de julho.

[3] Declaração de voto do Conselheiro Gonçalo de Almeida Ribeiro.

[4] Acórdão STJ n.º 10/2023, de 10 de novembro.

O nosso problema é complexo porque cruza o Direito comparado, a Convenção Europeia dos Direitos Humanos (CEDH ou Convenção) e a jurisprudência do Tribunal Europeu dos Direitos Humanos (TEDH), a Carta dos Direitos Fundamentais da União Europeia (CDFUE ou Carta) e a jurisprudência do Tribunal de Justiça da União Europeia (TJUE), a CRP, o Código de Processo Penal (CPP), a Lei do Cibercrime (LC), o Regime Geral das Contraordenações (RGCO) e o regime jurídico específico da concorrência.

Depois do Tratado de Lisboa, a Convenção, a Carta e as tradições constitucionais nacionais são fontes dos direitos fundamentais na ordem jurídica da União Europeia.

O Direito comparado é utilizado neste contexto como método de interpretação crítica do nosso Direito interno[5].

II. O Direito Fundamental à Privacidade Digital

1. A tutela da privacidade na Constituição dos EUA e na jurisprudência do SCOTUS

A Quarta Emenda à Constituição dos Estados Unidos da América (EUA) declara que o direito do povo à inviolabilidade de suas pessoas, domicílios, documentos e haveres contra buscas e apreensões arbitrárias não pode ser infringido; e nenhum mandado pode ser expedido a não ser baseado em indícios de culpabilidade confirmados por juramento ou declaração, e particularmente com a descrição do local da busca e a indicação das pessoas ou coisas a serem detidas ou apreendidas.

A Quarta Emenda à Constituição dos EUA limita, portanto, as possibilidades de ingerência legítima da autoridade pública na privacidade às diligências de busca e apreensão (*search and seizure*), as quais, por sua vez, dependem de haver suspeita razoável ou, literalmente, causa provável (*probable cause*), acompanhada de juramento (*oath*) ou declaração junto de um juiz competente e imparcial (que não tenha tido contacto com o caso em qualquer outro contexto), para obtenção de um mandado de busca (*search warrant*), devendo a promoção dessa diligência descrever o lugar a ser buscado (*searched*) e indicar as pessoas que aí devam, porventura, ser detidas e as coisas que devam ser apreendidas (*seized*).

O Supremo Tribunal dos EUA (*Supreme Court of the United States* – SCOTUS) adotou a regra de exclusão relativa a buscas e apreensões ilegais

[5] Sobre o Direito comparado como método de interpretação, cf. Kai Ambos, "Estado e futuro do Direito Penal comparado", *Anatomia do Crime* 6 (2017), pp. 9-42.

(*search and seizure exclusionary rule*) no caso *Weeks v United States* (1914) e tornou-a aplicável não apenas ao nível federal, mas também ao nível estadual no caso *Mapp v Ohio* (1961). Se quisermos, a regra de exclusão funciona num plano equivalente ao da proibição de valoração de prova. A proibição de produção de prova, por sua vez, encontra-se na Quarta Emenda à Constituição dos EUA, que, como vimos, proíbe as buscas e apreensões injustificadas (*unreasonable searches and seizures*) e sem mandado judicial.

2. As Diretrizes Federais para Busca e Apreensão de Computadores e a privacidade digital

Em 1994, o Departamento de Justiça (*Department of Justice* – DOJ) publicou as Diretrizes Federais para Busca e Apreensão de Computadores (*Federal Guidelines for Searching and Seizing Computers*). As Diretrizes foram atualizadas através de Suplementos (*Supplements*), em 1997 e 1999, e sujeitas a uma ampla reformulação em forma de Manual de Busca e Apreensão de Computadores e Recolha de Prova Digital em Investigações Criminais (*Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations Manual*)[6], publicado em 2001 e amplamente revisto em 2009, e foram ainda complementadas com o Manual de Persecução de Crimes Informáticos (*Prosecuting Computer Crimes Manual*), de 2010[7].

De acordo com as Diretrizes de 2009, as pesquisas informáticas em disco rígido (*hard-drive*) ou em outros ambientes informáticos (*computer media*) carecem de autorização judicial que contemple, entre outros aspetos, o modo específico de realização dessa diligência de obtenção de provas. Na grande maioria dos casos, a análise forense (*forensic analysis*) de um disco rígido (ou outro ambiente informático) leva tempo de mais para poder ser realizada no local (*on-site*) durante a execução inicial do mandado de busca e apreensão. A decisão mais importante que deve constar do mandado é se podem ser apreendidos computadores e demais equipamentos ou apenas as informações que o *hardware* contém. Na primeira hipótese, o mandado deve descrever o próprio *hardware*. Se a causa provável que justificou a diligência estiver relacionada apenas com certas informações, então o mandado deve

[6] Existem dois tipos de documentos digitais: o documento eletrónico originário, que é criado em computador com recurso a dígitos binários (*bits*), sendo transmitido e conservado em formato digital, e o documento eletrónico digitalizado, que é aquele que resulta da transposição ou reconversão da informação analógica. No presente artigo usaremos os termos "digital" e "eletrónico" como sinónimos, a benefício da simplicidade de leitura.

[7] *Online*: https://www.justice.gov/criminal/criminal-ccips/ccips-documents-and-reports (consultado em 30.09.2024).

descrever as informações a ser apreendidas e autorizar a sua apreensão em qualquer suporte em que possam ser armazenadas, seja eletrónico ou não. Neste caso, os inspetores (*officers*) devem recolher as informações que se enquadram no escopo do mandado através de cópia eletrónica de todo o dispositivo de armazenamento (*image copy*), feita ou não no local, e posteriormente devem produzir uma cópia de trabalho para poderem realizar o exame fora do local (*off-site examination*) por meio de programas de mineração de dados que lhes permitam segregar aqueles registos que correspondam (*responsive records*) aos crimes abrangidos pelo mandado judicial em execução. Mas o mandado judicial não pode simplesmente autorizar uma pesquisa e apreensão de todos os registos (*records*), sob pena de ser um mandado genérico inconstitucional (*unconstitutional general warrant*). Em vez de os inspetores fazerem uma cópia eletrónica de todo o dispositivo de armazenamento, é, pois, admissível que façam uso de técnicas forenses (*forensic techniques*) que, por exemplo, lhes permitam restringir o universo da pesquisa e apreensão apenas aos ficheiros que contenham determinadas palavras-chave (*keywords*) relacionadas com os crimes investigados ao abrigo do mandado judicial, mas esta é uma possibilidade que não deverá ser imposta pela autoridade judicial, embora deva constar da promoção que lhe for dirigida. A restrição do universo de pesquisa e apreensão pode interessar aos titulares da investigação criminal, sobretudo se pensarmos em processos que envolvam empresas e vastas quantidades de dados informáticos. Seja como for, é inadmissível impor qualquer limitação significativa (como uma restrição a pesquisas por palavras-chave) às técnicas forenses que os inspetores pretendam usar para encontrar as provas que caibam no escopo de um mandado judicial. A apreensão do equipamento, em princípio, só é possível se o mesmo for contrabando, prova, instrumento ou produto de um crime, nos termos da Regra 41(c) do Regulamento Federal de Processo Penal (*Federal Rules of Criminal Procedure*)[8]. Se o equipamento for apenas um dispositivo de armazenamento de provas, os inspetores podem, a título excecional, apreendê-lo só se não existirem alternativas menos disruptivas.

As restantes possibilidades remetem a continuação da pesquisa para fora do local da apreensão (*off-site search*). Só a possibilidade cada vez menos utilizada de impressão de ficheiros específicos implica que toda a pesquisa seja realizada no local (*on-site search*). Cabe aqui destacar que não é indiferente que a pesquisa se realize no local ou se faça ou prossiga fora

[8] As *Federal Rules of Criminal Procedure* entraram em vigor em 21 de março de 1946 e foram alteradas pela última vez em 1 de dezembro de 2019.

do local. A pesquisa no local tem um tempo limitado de duração, ao passo que a pesquisa fora do local pode durar o tempo que for necessário para ser completada (alguns juízes impõem um prazo-limite). Tal demonstra, só por si, que a pesquisa fora do local é mais invasiva da privacidade do que a pesquisa no local. Acresce que a quantidade de informação guardada em formato digital pode ser de tal maneira vasta – na ordem dos *gibabytes* ou mesmo *terabytes* – que a devassa da privacidade numa pesquisa fora do local pode suplantar largamente a que ocorreria numa simples pesquisa e apreensão no local, de duração limitada a algumas horas ou dias. Daí que seja da máxima relevância garantir que quaisquer pesquisas informáticas a prosseguir fora do local tenham a devida justificação para poderem ser consideradas legítimas.

As Diretrizes de 2009 enfatizam a importância de os titulares da investigação criminal conceberem uma estratégia minuciosa antes de promoverem junto de um juiz a obtenção de um mandado de busca e apreensão em ambiente digital. Por consequência, a garantia ajuramentada (*affidavit*) da causa provável que é necessária para a promoção do mandado junto de um juiz deve reportar quais os factos específicos que justificam a indispensabilidade de prossecução da pesquisa informática fora do local. Além de o mandado judicial ter de autorizar expressamente a pesquisa fora do local, se forem copiados elementos digitais para posterior pesquisa fora do local o auto de busca e apreensão também deve pormenorizar as circunstâncias concretas que impuseram um tal procedimento.

3. Pesquise antes de apreender

Se os documentos armazenados em equipamentos informáticos estivessem em formato de papel, a seleção exigiria que os inspetores analisassem milhares de detalhes para determinar quais deles continham afinal informações que justificassem a sua apreensão ao abrigo do mandado judicial. Acresce que os inspetores poderiam precisar da orientação de um promotor de justiça (*prosecutor*) para fazer a seleção dos documentos relevantes. Essa orientação aumentaria o tempo necessário para rever os documentos e selecionar aqueles que pudessem ser legitimamente apreendidos. Se tudo isso fosse feito no local, os referidos agentes de investigação criminal poderiam ter de ocupar as instalações durante várias horas ou mesmo dias.

A migração para o ciberespaço veio, sem dúvida, facilitar a vida aos inspetores, de tal sorte, que a simples possibilidade de fazerem a pesquisa de

documentos relevantes em equipamentos informáticos em tempo real e no local da busca representa, só por si, um ganho de eficácia e de tempo.

As Diretrizes de 2009 não desaconselham que se pesquise apenas uma parte do sistema informático, eventualmente através de palavras-chave ou frases específicas, respeitando os termos do mandado judicial. Tal só é desejável, porém, se os inspetores tiverem de antemão uma perceção rigorosa das provas de que estão à procura, por exemplo, uma evidência conclusiva – vulgo, a metafórica arma fumegante (*smoking gun evidence*) – do delito sob investigação, que lhes tenha sido revelada com exatidão por um denunciante.

Nestes casos, o procedimento de utilização de palavras-chave é preferível para todos os envolvidos. Por um lado, é preferível para os inspetores, pois só trazem consigo aquilo que for essencial para a investigação e evitam trazer documentação irrelevante, a qual acabaria por se transformar em lastro processual, potenciando incidentes e demoras. Por outro lado, é preferível para os visados, pois a devassa da sua privacidade é restringida ao estritamente necessário para a investigação em curso.

4. Apreenda primeiro e pesquise depois

Não sendo possível realizar a pesquisa de documentos em ambiente digital no local da busca, então resta a alternativa de fazer uma cópia integral (*mirror-image copy*) do disco rígido ou servidor de rede ou usar palavras-chave para copiar ficheiros individuais. Mas cabe aqui enfatizar que uma cópia eletrónica de uma unidade inteira é bem diferente de uma cópia eletrónica de ficheiros individuais. Esta última reduz não só o tempo necessário para a posterior seleção de possíveis provas, mas também o risco de ultrapassagem do objeto do mandado.

As evidências geradas por computador (*computer-generated evidences*) podem ser recolhidas e custodiadas usando a automação. Os inspetores podem correr um programa para executar a apreensão de documentos em computadores independentes, servidores de rede ou armazenamento em nuvem. A utilização de palavras-chave tem a vantagem de ser relativamente célere e cirúrgica. Porém, as palavras-chave são insensíveis ao contexto e ficam muito aquém da capacidade de discriminação típica de um investigador humano. Acresce que o emprego de palavras ou frases genéricas como palavras-chave pode ajudar a localizar evidências relevantes, mas produz um número elevado de falsos positivos (*false hits*). Os falsos positivos são documentos que contêm o termo procurado, mas não têm valor probatório e escapam ao objeto do mandado judicial.

5. A pesquisa externa

A questão agora é saber se a Quarta Emenda à Constituição dos EUA autoriza a apreensão de evidências geradas por computador para pesquisa externa. Um tal procedimento implica necessariamente apreender documentos que não têm valor probatório e que estão para além do escopo do mandado. Tão-pouco dispensa a revisão de cada ficheiro (*file-by-file*) por um ou mais agentes de investigação criminal, o que significa que estes vão ter acesso a informação que, em princípio, lhes estaria vedada sob a autoridade do mandado judicial.

A maneira de lidar com este problema, especialmente se estiver ameaçado o segredo profissional entre advogado e cliente (*attorney-client privilege*), poderá passar pela nomeação de uma equipa provisória de agentes de investigação criminal (*filter team* ou *taint team*) à qual se retira o acompanhamento posterior do caso ou até mesmo a nomeação pelo tribunal de um supervisor especial (*special master*), que, por certo, oferece mais garantias de independência em relação ao poder executivo[9]. Poderá ainda tornar-se necessária a intervenção de um juiz especial (*special Magistrate Judge*).

O DOJ baseia a alegação de que as pesquisas externas são necessárias em duas premissas diferentes. A primeira é uma variante das exceções tradicionais à exigência de mandado judicial. As exceções podem ser justificadas pela necessidade de impedir a destruição de provas essenciais. Este é, certamente, um argumento válido, desde que se demonstre que a destruição de evidências estaria, de facto, iminente.

A segunda é a necessidade de envolver técnicos de informática (*computer experts*) na pesquisa para evitar a contaminação ou destruição de provas essenciais, o que normalmente só é possível fazer com segurança e tranquilidade fora das instalações buscadas.

---

[9] A figura do *special master* é regida pela Regra 53 do Regulamento Federal de Processo Civil (*Federal Rules of Civil Procedure*) e pode ser caraterizada como uma pessoa externa ao litígio, seja advogado, juiz aposentado ou professor de Direito. No âmbito da investigação criminal, as atenções viraram-se para a figura do *special master* há algum tempo por causa do caso dos documentos confidenciais que estavam na posse de Donald Trump, na sua residência de Mar-a-Lago. É facto conhecido que a defesa do ex-presidente dos EUA solicitou a nomeação de um *special master*, a fim de verificar quais daqueles documentos eram realmente confidenciais e não poderiam ter sido retirados da Casa Branca sem autorização prévia. No entanto, a atuação do *special master* em processos penais não é usual. Um dos motivos apontados para a sua fraca utilização no processo penal é a circunstância de a esmagadora maioria dos casos penais (cerca de 98%) não chegarem a julgamento, à conta da negociação da confissão (*plea bargaining*) ou outros acordos penais. Não chega, pois, a haver oportunidade de requerimentos ao juiz (*pretrial motions*) antes do julgamento, em fase de investigação criminal (*discovery*).

Nas situações que envolvam a criação no local de uma cópia forense para subsequente pesquisa externa, a promoção do mandado pelo titular da investigação criminal diante do juiz deve especificar os métodos de recolha, custódia e pesquisa que serão usados e as precauções que serão tomadas para garantir que a pesquisa respeite o objeto do mandado judicial. O próprio mandado judicial deve indicar, para além dos delitos visados, o método e, se forem recomendáveis palavras-chave, a lista dos termos a utilizar para o efeito. A autorização judicial pode estar contida no mandado original ou em mandado complementar (*supplemental warrant*). Os agentes de investigação criminal promovem o mandado complementar quando, após iniciarem a execução do mandado original, chegarem à conclusão de que uma pesquisa no local simplesmente não é viável.

6. A doutrina jurisprudencial da visibilidade imediata

À luz do direito jurisprudencial norte-americano, a recolha de evidências geradas por computador rege-se pelas normas aplicáveis às tradicionais diligências de busca e apreensão, nos termos da Quarta Emenda à Constituição dos EUA. Mas a proibição constitucional das buscas e apreensões injustificadas implica uma reelaboração de conceitos de cada vez que for aplicada ao mandado de busca digital (*digital search warrant*). Essa reelaboração é sumamente necessária quanto à questão do destino a dar aos conhecimentos fortuitos que ocorram em ambiente digital.

A doutrina jurisprudencial da visibilidade imediata (*plain view doctrine*) é uma exceção ao imperativo constitucional de mandado judicial para a realização de buscas e apreensões. A visibilidade imediata autoriza que sejam utilizados como prova de um delito quaisquer objetos apreendidos por um agente de autoridade que tenha atuado sem ou para além do mandado judicial de busca e apreensão, se forem atendidas as seguintes três condições: (1) a evidência tem de estar imediatamente à vista; (2) o agente de autoridade tem de possuir uma razão justificativa anterior para se encontrar no local a partir do qual consegue visualizar imediatamente a evidência; (3) a evidência por si mesma ou juntamente com factos conhecidos do agente de autoridade no momento da apreensão, tem de fornecer uma probabilidade razoável para se crer que exista uma conexão entre a evidência e alguma atividade criminosa.

A doutrina jurisprudencial da visibilidade imediata baseia-se na experiência empírica da perceção visual no mundo físico. No mundo cibernético, porém, não há, em princípio, analogia com a visão no mundo

físico. Um objeto pode ser imediatamente avistado no mundo físico, ao passo que um ficheiro eletrónico só pode ser visto se for aberto. Aquilo que se vê imediatamente é apenas o nome do ficheiro, que pode nem sequer ser revelador do respetivo conteúdo. Esta dificuldade tem dado azo a uma rica casuística no direito jurisprudencial norte-americano.

7. A tutela da privacidade na Convenção e na jurisprudência do TEDH

O artigo 8.º da CEDH impõe o respeito pela privacidade. Mais exatamente, o artigo 8.º, n.º 1, da CEDH protege, entre outros direitos, o direito ao respeito da vida privada e da correspondência, aparecendo estes dois direitos lado a lado. A privacidade é um conceito mais vasto do que parece.

O TEDH tem vindo a fazer uma interpretação extensiva da CEDH, aplicando o artigo 8.º à proteção da informação guardada em servidores, computadores, ficheiros informáticos e *emails*, como aconteceu nos casos Leander *v*. Sweden (1987), Amann *v*. Switzerland (2000), Rotaru *v*. Romania (2000), Copland *v*. United Kingdom (2007) e Wieser and Bicos Beteiligungen GmbH *v*. Austria (2007). Por conseguinte, o sigilo das mensagens de correio eletrónico cabe na tutela da privacidade[10].

O TEDH tem alargado o conceito de privacidade à vida profissional não só dos trabalhadores, mas também das empresas, de modo que o ambiente informático do local de trabalho acaba por estar incluído na proteção da privacidade, como aconteceu no caso Société Colas Est and other *v*. France (2002), como segue: § 41. De acordo com a jurisprudência do Tribunal, as ligações telefónicas de estabelecimentos comerciais são *prima facie* cobertas pelas noções de 'vida privada' e 'correspondência' para os fins do artigo 8.º, n.º 1 (ver Halford, já referido, § 44 e Amann *v.* Suíça [GC], n.º 27798/95, § 43, CEDH 2000 II). Segue-se logicamente que os *emails* enviados do trabalho devem igualmente ser protegidos pelo artigo 8.º, assim como as informações recolhidas através de monitoramento do uso pessoal da Internet.

A proteção da privacidade não é absoluta. Há situações em que a autoridade pública pode interferir no direito ao respeito pela vida privada e pela correspondência. Nos termos do n.º 2 do artigo 8.º da CEDH, a ingerência só é permitida, porém, quando estiver prevista em norma habilitante e constituir uma providência que, numa sociedade democrática, seja necessária para a

[10] Cf. Paulo de Sousa Mendes, "A privacidade digital posta à prova no processo penal", *Revista do Ministério Público,* 165, 2021, (pp. 109-143) pp. 110-112.

segurança nacional, a segurança pública, o bem-estar económico do país, a defesa da ordem e a prevenção ou repressão das infrações penais (*lato sensu*), a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros.

Quando é chamado a pronunciar-se sobre se o artigo 8.º da CEDH foi ou não violado, o TEDH verifica, primeiro, se houve ingerência em algum dos direitos atrás elencados; segundo, se tal ingerência estava coberta por uma norma habilitante da jurisdição em que foi praticada; e, terceiro, se a medida realizada era proporcional em ordem a satisfazer uma necessidade social premente numa sociedade democrática.

Ainda não há muitos acórdãos do TEDH que tratem da aplicação do artigo 8.º da CEDH à prova digital no processo penal (*lato sensu*)[11], mas já há os suficientes para se tirar um retrato da jurisprudência de Estrasburgo a tal respeito. A título de exemplo, recomenda-se a leitura dos seguintes acórdãos do TEDH: Robathin *v.* Austria (queixa n.º 30457/06), de 3 de julho de 2012; Bernh Larsen Holding As *v.* Norway (queixa n.º 24117/08), de 14 de março de 2013; Sérvulo *v.* Portugal (queixa n.º 27013/10), de 3 de setembro de 2015; Trabajo Rueda *v.* Spain (queixa n.º 32600/12), de 30 de maio de 2017; Ivashchenko *v.* Russia (queixa n.º 61064/10), de 13 de maio de 2018; Rook *v.* Germany (queixa n.º 1586/15), de 25 de julho de 2019.

8. A violação do direito à privacidade e o seu remédio ao nível do processo equitativo

A jurisprudência do TEDH tem contribuído, como é sua função, para a edificação de um menor denominador comum na Europa, à luz da CEDH. Mas também é verdade que a Convenção é uma carta de direitos mínimos, pois tem de abrigar ordenamentos jurídicos nacionais muito diversos entre si e tem de dar respostas para todos.

Os ordenamentos jurídicos nacionais abrangidos ainda estão longe de partilhar na prática os mesmos princípios e garantias penais. Sempre que é chamado a decidir quaisquer casos de violação da CEDH, o TEDH usa de alguma contenção, dado que tem de lidar, à vez, com os diferentes ordenamentos jurídicos nacionais. Não admira, pois, que as decisões e os remédios sejam minimalistas. Tal poderá ser dececionante para quem for

[11] O TEDH estabeleceu uma definição ampla de acusação criminal (*criminal charge*) e de ilícito criminal (*criminal offence*) para efeitos de aplicação das garantias da CEDH que abrange os processos administrativos sancionadores e todos os processos sancionadores de caráter público, já desde os casos Engel and Others *v.* The Netherlands (queixas n.os 5100/71, 5101/71, 5102/71, 5354/72 e 5370/72), de 8 de junho de 1976 (§ 81), e Öztürk *v.* Germany (queixa n.º 8544/79), de 21 de fevereiro de 1984 (§ 53).

atrás de soluções jurídicas vanguardistas na jurisprudência do TEDH, já que estaria a procurá-las no lugar errado. Paradoxalmente, a jurisprudência do TEDH ganha, afinal, uma importância acrescida por causa do seu caráter moderado. Podemos, assim, dar por adquirido que, onde o TEDH viu uma violação à CEDH, é difícil de dizer o contrário. Mas, onde o TEDH deixou passar uma eventual violação de direitos humanos, é sempre possível discordar. Neste caso, a fundamentação do acórdão em causa é tão importante como os votos dissidentes. Um voto dissidente de hoje pode ser a jurisprudência de amanhã, como todos sabemos desde que o Chief Justice Oliver Wendell Holmes Jr. ficou famoso como protagonista de votos dissidentes.

No tocante à violação do artigo 8.º da CEDH, a jurisprudência do TEDH, valendo-se de um raciocínio de ponderação de interesses (*balancing approach*), acaba não extraindo consequências dessa violação para o funcionamento do processo equitativo como um todo (*fair as a whole*), à luz do artigo 6.º da CEDH, desde que ao acusado, no caso concreto, tenham sido dadas oportunidades de contestar a prova em questão, tenham sido respeitados os seus outros direitos de defesa e não haja dúvidas sobre a fiabilidade da prova – o que é, genericamente, o caso para as provas obtidas em violação do artigo 8.º da CEDH. A jurisprudência do TEDH parece não fornecer quaisquer regras de exclusão da prova, as quais, enquanto critérios operativos a nível nacional, possam constituir remédios efetivos contra a utilização de provas obtidas em violação do artigo 8.º da CEDH. Mas, dizemos nós, a utilização de provas obtidas através da lesão do direito à privacidade não deveria ser indiferente para a noção do processo equitativo como um todo.

Pelo contrário, deveríamos esperar do TEDH que impusesse aos Estados, quando fosse o caso, remédios efetivos contra a violação da equidade processual (*fairness*), devolvendo assim o acusado à posição processual em que se encontraria se não fosse a lesão da sua privacidade. Muito embora a jurisdição do TEDH não funcione como última instância face aos ordenamentos jurídicos nacionais, aquele Tribunal até já tem decretado a *restitutio in integrum*, em conformidade com a Recomendação do Comité de Ministros do Conselho Europa N.º R(2000)2, de 19 de janeiro, obrigando à reabertura do processo-crime no ordenamento de origem, sem que isso implique, naturalmente, que o acusado tenha de ser absolvido.

Vamos esperar que a evolução da jurisprudência do TEDH se dê no sentido de um estreitamento da conexão entre o direito substantivo à

privacidade e o direito processual ao processo equitativo, ambos direitos convencionais, ainda que o campo de aplicação do direito à privacidade e a sua violação ocorram muitas vezes fora do processo penal. Mas essa evolução é improvável enquanto o TEDH se mantiver apegado a um raciocínio de ponderação de interesses que contrapõe, fundamentalmente, o interesse do Estado na preservação de uma prova fiável aos olhos do juiz-julgador para poder produzir uma decisão robusta do ponto de vista factual e o interesse do acusado em defender-se, estando este último interesse assegurado, na perspetiva do TEDH, se o acusado tiver tido a oportunidade no processo penal para contestar essa prova.

9. A tutela da privacidade na UE e na jurisprudência do TJUE e (ex-)TJCE

O estado da arte na legislação da União Europeia (UE) é o seguinte: por um lado, estão previstas salvaguardas específicas para o acesso aos dados retidos pelos fornecedores de serviços telefónicos e de Internet (e entre essas salvaguardas, a avaliação prévia sobre a proporcionalidade do acesso por uma autoridade independente e imparcial desempenha um papel fundamental), enquanto, por outro lado, não são expressamente impostas quaisquer limitações às autoridades judiciárias e órgãos de polícia criminal no que diz respeito às pesquisas e apreensões de dados informáticos. Com efeito, a Diretiva 2002/58/CE[12] está atualmente em vigor e determina a competência da UE apenas no domínio da retenção de dados, deixando de lado o tema aqui considerado. Tal traduz-se numa falta de garantias substantivas e processuais para o suspeito ou arguido, uma vez que a questão nunca foi tratada pelo legislador da UE. Embora esta imagem seja claramente inconsistente com a jurisprudência relevante do TEDH, vale a pena recordar que a ausência de regras da UE neste domínio decorre da falta de consenso político numa área muito sensível do processo penal[13].

10. Conclusões intermédias

A Quarta Emenda à Constituição dos EUA trata do respeito pela privacidade. O artigo 8.º da CEDH trata também do respeito pela privacidade.

---

[12] Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas).

[13] Lorenzo Bernardini e Francesco Sanvitale, "Searches and Seizures of Electronic Devices in European Criminal Proceedings: A New Pattern For Independent Review?", *Revista Ítalo-Española de Derecho Procesal,* 1, 2023, (pp. 73-119), p. 110.

O respeito pela privacidade abrange a privacidade digital, no contexto da desmaterialização crescente dos registos e das comunicações das empresas e dos indivíduos.

Ao contrário da Quarta Emenda à Constituição dos EUA, o artigo 8.º da CEDH não exige causa provável, nem mandado judicial, mas exige, mais vagamente, que qualquer ingerência da autoridade pública na privacidade venha prevista na lei e constitua uma providência necessária numa sociedade democrática.

A jurisprudência do TEDH caracteriza-se por alguma ineficácia na criação de remédios para a violação da privacidade no processo penal, incluindo a privacidade digital, desde logo porque não comina a exclusão das evidências eletrónicas que extravasem do objeto da investigação criminal em curso.

O Direito da UE, por sua vez, é totalmente omisso nesta matéria, dada a falta de consenso político numa área muito sensível do processo penal.

O conhecimento das leis, das diretrizes e do direito jurisprudencial norte-americano deveria representar um contributo valioso para o aprofundamento da jurisprudência de Estrasburgo, na sua dupla função decisória e nomofilácica, assim como para o aperfeiçoamento dos ordenamentos jurídicos nacionais europeus ao nível legislativo e ao nível jurisprudencial. A comparação com o direito norte-americano permite destacar que a devassa nas pesquisas e colheitas informáticas decorre sobremaneira da vastidão e da falta de precisão do acervo eletrónico recolhido, o que deveria implicar a nomeação de equipas *ad hoc* de analistas especializados (juristas, economistas e informáticos) cuja função se limitasse à triagem das evidências relevantes para o processo penal em curso, sinalizando os documentos eletrónicos cobertos por privilégios de sigilo profissional ou segredo de negócio e eliminando os documentos eletrónicos irrelevantes. A equipa *ad hoc* deveria ser afastada da prossecução da investigação criminal logo que terminasse a tarefa para que foi designada, dado que ficou contaminada pelo conhecimento de informação que, por definição, não poderia conhecer sob a autoridade dos mandados de busca e apreensão digital.

Não basta a nomeação *ad hoc* de uma equipa de investigação, à qual faltará sempre a suficiente imparcialidade para assegurar a proteção da privacidade digital dos visados ou de terceiras partes. A maneira mais eficaz de mitigar, na prática, a manipulação abusiva da doutrina da visibilidade imediata quando os investigadores tenham de analisar grandes

acervos de documentos eletrónicos é através da intervenção de um juiz especial (dependendo dos ordenamentos jurídicos que o prevejam, essa é função do juiz das garantias ou das liberdades)[14]. O juiz especial deve validar as evidências produzidas por computador e confirmar a respetiva correspondência com as autorizações e os mandados de busca e apreensão digital.

Mas não é essencial, do ponto de vista das garantias do processo penal, que a apreensão de documentos eletrónicos, incluindo *emails* ou outros registos de comunicações de natureza semelhante, seja autorizada previamente por um juiz especial, cuja intervenção nesta fase da investigação criminal tenderia a ser meramente formal e ineficaz para a tutela da privacidade digital dos visados ou de terceiras partes.

III. Os Poderes das Agências de Concorrência

1. A deteção e a repressão de cartéis no Direito federal e estadual norte-americano

Nos EUA, as principais leis relativas aos cartéis são as seguintes:

- A Secção 1 da Lei Sherman (*Sherman Antitrust Act* – Sherman Act), de 1890, que proíbe qualquer contrato, acordo ou outra combinação, ou conspiração, para restringir a concorrência ou o comércio entre os vários estados ou com nações estrangeiras (15 U.S.C. § 1);

- A Secção 5(a) da Lei da Comissão Federal do Comércio (*Federal Trade Commission Act* – FTC Act), de 1914, que proíbe métodos desleais de concorrência e atos ou práticas desleais ou enganosas (15 U.S.C. §§ 41–58).

A Lei Sherman pode ser aplicada criminal, administrativa ou civilmente pela Divisão de Concorrência (*Antitrust Division* – AT) do DOJ. A aplicação criminal é reservada para violações graves (*hard core*) da Secção 1: fixação de preços, fraude em licitações e esquemas de repartição de mercado entre concorrentes horizontais. O DOJ pode processar civilmente os casos menos graves.

A Comissão Federal de Comércio (*Federal Trade Commission* – FTC) não aplica a Lei Sherman, mas pode instaurar investigações administrativas ou civis (*administrative or civil investigations*) ao abrigo da Secção 5(a) da Lei FTC. Entretanto, o SCOTUS reconheceu que todas as violações da Lei Sherman também violam a Lei FTC, permitindo assim que a FTC persiga

[14] Entre nós, é o juiz de instrução, que cumula a função de juiz das garantias com a função de juiz da fase de instrução com poderes autónomos de investigação e competência de pronúncia sobre o mérito da conclusão produzida na fase de inquérito em processo comum, o que não abona a favor da sua desejável imparcialidade.

através da Lei FTC o mesmo tipo de condutas que violam a Lei Sherman. A Lei FTC também abrange outras práticas que não preenchem todos os elementos previstos na Lei Sherman (por exemplo, propostas que não se concretizaram em colusão efetiva).

Os procuradores-gerais estaduais (*state attorneys general*) também podem aplicar a Lei Sherman em nome dos cidadãos de um estado ou do próprio estado. Para o efeito atuam geralmente em redes pluri-estaduais e coordenam-se com o DOJ e a FTC.

Todos os estados norte-americanos possuem leis de concorrência ou de concorrência desleal, que são interpretadas em conformidade com as leis federais. Os procuradores-gerais estaduais têm competência para a aplicação pública dessas leis (*public enforcement*). Os procuradores-gerais estaduais também podem perseguir criminalmente as infrações de concorrência previstas e punidas pela lei estadual, se for o caso (geralmente, casos de fraude em licitações ao nível estadual)[15].

2. A interceção de comunicações

A Lei Ónibus relativa ao Controlo do Crime e às Ruas Seguras (*Omnibus Crime Control and Safe Streets Act*), de 1968, limita o poder do governo de intercetar comunicações presenciais, telefónicas e eletrónicas. No contexto do controlo das práticas restritivas da concorrência, o governo só poderá intercetar comunicações no âmbito de investigações criminais de cartéis e mediante mandado judicial de busca e apreensão[16].

3. O acesso a dados informáticos através de terceiras partes

O Título II da Lei de Privacidade das Comunicações Eletrónicas (*Electronic Communications Privacy Act* – ECPA) regula o como e o quando qualquer agência de aplicação da lei dos EUA, incluindo a Divisão, poderá obter acesso, através dos fornecedores (*providers*), a comunicações eletrónicas armazenadas, tais como *emails* ou registos telefónicos, durante uma investigação criminal. A ECPA foi projetada para fornecer às agências de aplicação da lei ferramentas para investigar eficazmente a prática de crimes, embora respeitando a privacidade das empresas e dos indivíduos e garantindo-lhes proteção contra buscas e apreensões injustificadas, um conceito consagrado na Quarta Emenda da Constituição dos EUA. Uma característica fundamental da

[15] *Online*: https://www.globallegalinsights.com/practice-areas/cartels-laws-and-regulations/usa (consultado em 01.04.2024).

[16] *Ibid*

ECPA é a distinção entre dados de conteúdo (*content data*) e outros registos ou informações relacionadas com a conta (*non-content data*), incluindo informações de identificação do cliente e registos de transações comerciais, que não são considerados dados de conteúdo. As informações definidas como dados de conteúdo estão sujeitas a um nível mais elevado de proteção de privacidade. Na maioria dos casos, os promotores de justiça terão de obter um mandado de busca e apreensão para qualquer informação de conteúdo, o que requer autorização judicial e demonstração da causa provável de que o conteúdo da comunicação visada contém evidências de um crime. A noção de dados de conteúdo inclui, por exemplo, o corpo de uma mensagem de *email* ou o texto de uma mensagem SMS. Em 2018, o Congresso dos EUA promulgou a Lei de Esclarecimento do Uso Legítimo de Dados Armazenados no Estrangeiro (*Clarifying Legal Overseas Use of Data* – Cloud Act), que alterou a ECPA para deixar claro que uma empresa sujeita à jurisdição dos EUA deve facultar quaisquer dados que controle. Por consequência, agora é indiscutível que os fornecedores de comunicações eletrónicas sujeitos à ECPA são obrigados a produzir provas na sua posse, custódia ou controlo, independentemente de os dados estarem armazenados nos EUA ou no estrangeiro[17].

4. A obtenção direta de dados informáticos

Uma ferramenta amplamente utilizada pelas agências de concorrência para detetar e processar cartéis é a inspeção não anunciada ou "incursão matutina" ("*dawn raid*"), realizada tanto em empresas como em domicílios de sócios, dirigentes ou trabalhadores[18]. A versão da incursão matutina que é praticada pela AT consiste na execução de uma busca e apreensão em conformidade com um mandado judicial. A Regra 41 do Regulamento Federal de Processo Penal determina o procedimento de promoção e execução de um mandado de busca e apreensão, o qual deverá ser emitido por um agente de justiça imparcial, geralmente um juiz federal, mediante a demonstração de que há motivos sérios para acreditar que foi cometido um crime e que as evidências do mesmo provavelmente serão encontradas no local concretamente especificado no mandado.

Para os promotores da AT importa garantir que as buscas e apreensões são conduzidas de acordo com a lei e respeitando as garantias proporcionadas pela Quarta Emenda da Constituição dos EUA para evitar a potencial exclusão

[17] *Online*: https://one.oecd.org/document/DAF/COMP/LACF(2020)14/en/pdf (consultado em 01.04.2024).

[18] A designação inglesa dessas operações é expressiva, pois alude à circunstância de começarem sempre de madrugada (*at dawn*).

das provas pelo tribunal durante o eventual julgamento. A AT trabalha em estreita colaboração com os parceiros federais de aplicação da lei, tanto na promoção como na execução dos mandados de busca e apreensão.

As buscas promovem o medo de deteção que é essencial à desestabilização dos cartéis e incentiva a autodenúncia com vista à participação em programas de clemência (*leniency programs*). O Manual da AT (*Division Manual*) menciona a importância das buscas para a obtenção de evidências de cartéis graves (*hardcore*).

A realização de uma busca numa empresa ou local privado poderá implicar a apreensão de documentos digitais que estejam armazenados em terminais, servidores e *smartphones*. Tais equipamentos poderão conter provas de colusão entre empresas, mas também informações não relacionadas com a investigação em curso. Em princípio, é impraticável analisar durante a operação de busca no local os ficheiros eletrónicos um por um para determinar quais são os documentos realmente relevantes. Quando tal revisão for impraticável, a Regra 41(e)(2)(B) estabelece um procedimento em duas etapas para a apreensão de evidências eletrónicas. Os meios eletrónicos são apreendidos ou copiados no local (*on-site*) durante a execução do mandado de busca e analisados posteriormente para determinar os conteúdos que se enquadram no escopo do mandado.

A proteção do sigilo entre advogado-e-cliente (*attorney-client privilege*) significa que, se houver motivos para crer que os materiais apreendidos incluem documentos privilegiados, a AT tomará medidas para retirar esses documentos antes de a equipa de investigação poder analisá-los. Tal poderá ser feito de várias maneiras: (i) a AT poderá realizar a sua própria análise utilizando uma equipa independente, ou seja, uma equipa de triagem, que separará quaisquer materiais potencialmente privilegiados e, em seguida, fornecerá à equipa da investigação acesso aos materiais restantes; (ii) alternativamente, a análise de materiais privilegiados poderá ser feita pelo advogado da empresa ou do indivíduo visado, após a apreensão e antes que a equipa de investigação analise os materiais apreendidos, devendo a equipa de investigação analisar apenas os materiais considerados não privilegiados pelo advogado da empresa ou do indivíduo visado.

Muitos ordenamentos de direito legislado que não reconhecem o sigilo entre advogado-e-cliente editaram regras legais de confidencialidade que obrigam os advogados a não divulgar informações confidenciais que o cliente lhes tenha fornecido. Mas tal geralmente só se aplica ao advogado, não ao cliente, e pode incluir apenas advogados externos. Como resultado,

uma busca aos escritórios do cliente, ou um pedido de documento dirigido ao cliente, mas não ao advogado, pode não proporcionar qualquer proteção às informações confidenciais de um cliente. E embora esta abordagem fosse viável numa época em que os clientes visitavam os escritórios dos seus advogados para obter aconselhamento e trocar informações, num mundo de comunicação digital e negócios globais esta é uma lacuna fundamental nas proteções de segredos. A AT apoia o trabalho em prol de práticas comuns relativamente ao sigilo entre advogado-e-cliente para promover os padrões básicos do devido processo.

5. A deteção e a repressão de cartéis no Direito da UE

O TEDH e o TJUE têm vindo a contribuir decisivamente para a definição dos poderes de investigação da Comissão Europeia (Comissão) e das Autoridades Nacionais de Concorrência (ANC).

A Comissão e as ANC realizam frequentemente incursões matutinas nas empresas. Mas qual é, exatamente, a natureza jurídica dessas operações? São buscas judicialmente autorizadas? São inspeções administrativas anunciadas? São inspeções administrativas de surpresa?

6. A jurisprudência do TEDH

Já existe um razoável acervo de jurisprudência do TEDH sobre buscas e inspeções das ANC: Société Colas Est *v.* France (2002), Societé Canal Plus *v.* France (2010), Compagnie des Gas de Pétrole Primagaz *v.* France (2010), Société Métallurgique Liotard Frères *v.* France (2011), entre outros.

Importa considerar especialmente o caso Delta Pekárny A.S. *v.* Czech Republic (2014). A Delta Pelkárny apresentara uma queixa junto do TEDH, alegando que a incursão matutina efetuada pela ANC checa nas suas instalações sem mandado violara o seu direito ao respeito da privacidade, domicílio e correspondência, tal como disposto no artigo 8.º, n.º 1, da CEDH. Numa decisão muito disputada (4 contra 3), o TEDH condenou a República Checa por violação do artigo 8.º, n.º 1, da CEDH. Segundo o TEDH, a tutela conferida pelo artigo 8.º, n.º 1, da CEDH à privacidade, ao domicílio e à correspondência também abrange as pessoas coletivas, ainda que fique aquém da proteção concedida às pessoas singulares[19].

Em 19.11.2003, a ANC checa, no âmbito de um processo administrativo sancionatório contra a Delta Pekárny, fundado em suspeitas razoáveis de

[19] Entre nós, as sedes e instalações das pessoas coletivas não têm sido enquadradas pela jurisprudência no conceito de domicílio.

cartelização, realizara uma incursão matutina de surpresa nas instalações dessa empresa. Embora os inspetores da ANC quisessem copiar *emails* dos trabalhadores da Delta Pelkárny, estes avisaram-nos que alguns desses *emails* não tinham nenhuma relação com a investigação em curso e que outros eram sigilosos (*i.e.*, segredos de advogado e segredos de negócio) ou privados (*i.e.*, mensagens pessoais). Assim, os trabalhadores não permitiram o acesso aos respetivos *emails*. A ANC condenou a Delta Pelkárny por obstrução ao exercício dos poderes de inspeção, aplicando-lhe uma sanção pecuniária de CZK 300,000 (EUR 11,500). No processo administrativo sancionatório principal, a ANC acabaria, mais tarde, condenando a Delta Pelkárny por prática de cartel, aplicando-lhe uma sanção pecuniária de CZK 2.129,000. A Delta Pelkárny interpôs recurso junto do Tribunal Administrativo Regional de Brno, o qual anulou a decisão da ANC por insuficiência da matéria de facto. A ANC repetiria a decisão de condenação, especificando agora que se deveria presumir que os documentos encontrados numa empresa são de natureza comercial, e não de outra natureza. A Delta Pelkárny recorreu também desta decisão, invocando a jurisprudência do TEDH, em especial o caso Société Colas Est *v.* France (2002). A Delta Pelkárny alegou que a base jurídica da inspeção de surpresa, nomeadamente o artigo 21.º, n.º 4, da Lei da Concorrência checa, não respeitava os requisitos estabelecidos na CEDH. A Delta Pelkárny argumentou que essa ação de inspeção carecia de prévia autorização judicial. O Tribunal Administrativo Regional de Brno negou provimento ao recurso, em 27.09.2007, afirmando que o procedimento da ANC era similar ao da Comissão Europeia, o que, neste último caso, já fora aceite pelo TJUE, no caso Hoechst *v.* Comission (1989). A Delta Pelkárny interpôs subsequentemente recurso perante o Supremo Tribunal Administrativo checo, novamente citando o caso Société Colas Est. Ademais contestou a aplicação da jurisprudência Hoechst à sua própria situação, uma vez que a entrada da República Checa na União Europeia ocorrera em 2004. O recurso foi rejeitado em 29.05.2009. A Delta interpôs ainda recurso de constitucionalidade perante o Tribunal Constitucional checo, alegando que a inspeção carecia de prévia autorização judicial. O recurso de constitucionalidade foi rejeitado em 26.08.2010. Paralelamente, a Delta arguiu a nulidade da inspeção por via de recurso no processo principal. O Tribunal Administrativo Regional de Brno confirmou, porém, a legalidade do procedimento inspetivo. A Delta seria depois absolvida da prática da infração de cartel pelo Supremo Tribunal Administrativo checo.

A queixa da Delta junto do TEDH começou a ser apreciada em dezembro de 2010. O TEDH reconheceu que a inspeção fora levada a cabo nos termos da Lei da Concorrência checa. Mas cuidou ainda de apreciar se era uma restrição à privacidade necessária numa sociedade democrática. Em casos anteriores, o TEDH analisara diligências previamente autorizadas por juiz e com mandados devidamente fundamentados. No entendimento do TEDH, a falta de autorização judicial prévia teria de ser contrabalançada por um controlo judicial efetivo *ex post facto*. No caso vertente, os tribunais checos não escrutinaram os factos que justificaram a inspeção, pelo que a decisão quanto à sua oportunidade, duração e amplitude nunca foi objeto de controlo jurisdicional. O TEDH notou que a inspeção tinha sido ordenada por um Diretor da ANC checa, logo no primeiro dia de abertura do processo administrativo sancionatório, baseada em meras suspeitas de práticas restritivas da concorrência. A notificação da Delta acerca da existência do processo administrativo sancionatório foi feita antes da inspeção, mas era vaga. Incluía a autorização para a inspeção e as credenciais dos inspetores. Em suma, o TEDH concluiu que a inspeção realizada pela ANC checa violava o artigo 8.º, n.º 1, CEDH porque faltava a prévia autorização judicial, faltava o controlo jurisdicional *a posteriori* e faltava a garantia de destruição das cópias dos documentos apreendidos desnecessários.

Em suma, o TEDH exige um conjunto de garantias em tema de buscas e inspeções que importa reter:

I. A exigência de fundadas suspeitas que justifiquem a busca ou inspeção;

II. A existência de mandado ou, pelo menos, a possibilidade de controlo jurisdicional efetivo *ex post facto*;

III. A delimitação precisa do objeto da diligência;

IV. A presença dos ocupantes das instalações durante as diligências;

V. O levantamento de auto no final da diligência, elencando os documentos apreendidos;

VI. A colocação num envelope selado dos documentos controvertidos (*e.g.*, documentos protegidos pelo sigilo entre advogado-e-cliente);

VII. A presença de um representante da Ordem, no caso de busca em escritório de advogados[20].

[20] Para desenvolvimentos, cf. Helena Gaspar Martinho, "Acórdão do Tribunal Europeu dos Direitos Humanos de 2 de outubro de 2014, Petição n.º 97/11, Delta Pekárny A.S. c. República Checa", *C&R*, 17 (jan./mar. 2014), (pp. 279-304) p. 295. Também, cf. Paulo de Sousa Mendes, "Poderes de busca e inspeção: O caso especial dos *dawn raids*", in: Carla Amado Gomes/Ana Fernanda Neves (coord.), *Estudos sobre a Actividade Inspectiva*, Lisboa: AAFDL, 2018, (pp. 151-165) pp. 153-156.

7. O Regulamento n.º 1/2003 e a jurisprudência do TJUE e (ex-) TJCE

Nos termos do Regulamento (CE) n.º 1/2003 do Conselho, de 16 de dezembro de 2002, relativo à execução das regras de concorrência estabelecidas nos artigos 81.º e 82.º do Tratado (atuais artigos 101.º e 102.º do Tratado sobre o Funcionamento da União Europeia – TFUE), a Comissão Europeia pode realizar inspeções nas instalações das empresas sem mandado judicial, ou sequer judiciário (*i.e.*, não judicial), estando as empresas e associações de empresas obrigadas a sujeitar-se a tais diligências, desde que ordenadas através de decisão da Comissão (artigo 20.º, n.º 4, do Regulamento n.º 1/2003). Poderá, porém, ser solicitado um mandado às autoridades judiciárias nacionais competentes, de acordo com o ordenamento jurídico do local da inspeção, se tal for necessário para vencer a eventual oposição da empresa em causa, inclusive com recurso à força pública (artigo 20.º, n.ºs 6 e 7, do Regulamento n.º 1/2003), o que tem vindo a ser feito pela Comissão, a título preventivo (as mais das vezes, as empresas acabam dando o seu acordo à realização da inspeção). Neste contexto, a autoridade judiciária nacional controla a autenticidade da decisão da Comissão, bem como o carácter não arbitrário e não excessivo das medidas coercivas relativamente ao objeto da inspeção, mas o controlo de legalidade da decisão da Comissão está reservado ao Tribunal de Justiça (artigo 20.º, n.º 8, do Regulamento n.º 1/2003).

No caso das buscas ao domicílio dos administradores, diretores e outros trabalhadores das empresas ou associações de empresas em causa, a decisão da Comissão que ordena as buscas não poderá ser executada sem mandado da autoridade judiciária nacional competente do Estado-Membro em causa (artigo 21.º, n.º 3, do Regulamento n.º 1/2003).

Apenas 14 Estados-Membros da União Europeia (UE) exigem mandado das autoridades judiciárias para serem realizadas buscas ou inspeções no âmbito de investigações por práticas restritivas da concorrência[21].

O Acórdão do Tribunal Geral (TG), de 6 de setembro de 2013, Deutsche Bahn AG e outros v Comissão Europeia, processos apensos T-289/11, T-290/11 e T-521/11, pronunciou-se sobre as garantias de defesa que devem nortear as inspeções realizadas pela Comissão, inspirando-se expressamente na jurisprudência do TEDH.

[21] Cf. ECN Working Group Cooperation Issues and Due Process, 2012. Online: http://ec.europa.eu/competition/ecn/investigative_powers_report_en.pdf (consultado em 29.07.2018).

Em poucas palavras, o caso versava sobre uma inspeção realizada sem autorização judicial, ou sequer judiciária, durante a qual a Comissão encontrara documentos relacionados com outra infração para a qual até já tinha sido anteriormente alertada por via de uma denúncia, tendo os inspetores sido informados também sobre o conteúdo desta denúncia, mas somente para conhecimento do historial da empresa visada. Dado que os documentos fortuitamente descobertos extravasavam o objeto da decisão da Comissão que ordenara a inspeção, a mesma adotou uma segunda decisão de inspeção em tempo real.

Essas duas decisões, assim como uma terceira decisão de inspeção, foram alvo de recurso para o TG. O acórdão do TG confirmou que a Comissão detém ampla margem de manobra em matéria de inspeções, não carecendo de obter autorização judicial, ou sequer judiciária, antes de uma operação intrusiva e que os documentos casualmente descobertos que indiciem a prática de uma infração separada podem ser usados como prova dessa violação, desde que respeitados os devidos requisitos processuais. Não obstante, os amplos poderes da Comissão devem ser utilizados com parcimónia e a sua utilização abusiva deve poder ser sujeita a fiscalização jurisdicional efetiva. Neste caso, a fiscalização *ex post* por parte dos Tribunais da UE já oferece um nível adequado de proteção dos direitos fundamentais.

O TG verificou se o regime instituído pelo Regulamento n.º 1/2003 e a forma como foi aplicado no caso concreto expressavam garantias de defesa adequadas e suficientes para as empresas, assim delimitando rigorosamente os poderes da Comissão.

Em particular, o artigo 20.º, n.º 4, do Regulamento n.º 1/2003 dispõe:

"As empresas e as associações de empresas são obrigadas a sujeitar-se às inspeções que a Comissão tenha ordenado mediante decisão. A decisão deve indicar o objeto e a finalidade da inspeção, fixar a data em que esta tem início e indicar as sanções previstas nos artigos 23.º e 24.º, bem como a possibilidade de impugnação da decisão perante o Tribunal de Justiça. A Comissão toma essas decisões após consultar a autoridade responsável em matéria de concorrência do Estado-Membro em cujo território se deve efetuar a inspeção".

O TG salientou a existência de seis espécies de garantias de defesa:

a) A necessidade de fundamentação das decisões de inspeção:

"Com vista a garantir à empresa a possibilidade de fazer uso do seu direito de oposição, a decisão de inspeção, além dos elementos formais enumerados no artigo 20.°, n.° 4, do Regulamento n.° 1/2003, deve conter

uma descrição das características essenciais da infração objeto de suspeita, mediante a indicação do mercado presumido em causa e da natureza das restrições de concorrência objeto de suspeita, bem como os setores abrangidos pela pretensa infração a que diz respeito o inquérito, explicações sobre a forma como a empresa visada pela inspeção está supostamente implicada nessa infração, da matéria investigada e dos elementos sobre os quais a verificação deve incidir" (§ 77);

b) Os limites impostos à realização da inspeção:

Os documentos de natureza não profissional ficam excluídos da investigação. As empresas-alvo de uma inspeção gozam dos direitos a assistência jurídica e à proteção do sigilo da correspondência entre advogados e clientes (embora este último direito não se aplique à correspondência com os advogados internos). O dever de cooperação não implica que as empresas tenham de fornecer respostas através das quais sejam levadas a confessar a prática da infração, cuja prova cabe à Comissão. Devem ser notificadas às empresas as decisões de inspeção acompanhadas de notas explicativas, expondo assim o procedimento que a Comissão se autodetermina a respeitar na realização da diligência em causa (§§ 79 a 84);

c) A proibição de uso da força (§§ 85 a 90);

d) A intervenção das instâncias formais de controlo nacionais:

"No tocante às garantias proporcionadas pelo processo de oposição previsto no artigo 20.°, n.º 6, do Regulamento n.º 1/2003, há que constatar que a Comissão se encontra na obrigação de recorrer à assistência das autoridades nacionais do Estado em cujo território a inspeção deve ser efetuada. Este processo desencadeia a execução dos mecanismos de fiscalização, eventualmente judicial, próprios ao Estado-Membro em causa" (§ 91).

e) O direito de recurso *a posteriori* (§§ 95 a 99), que permita uma fiscalização tanto de direito como de facto (§§ 103 a 114);

f) A eventual anulação da decisão de inspeção acarreta a proibição de utilização das provas e informações obtidas durante as diligências controvertidas (§ 113).

Foi interposto recurso desta decisão junto do Tribunal de Justiça (TJ), processo C-583/13 P. A decisão do TJ, de 18 junho de 2015, constitui um marco importante nesta matéria.

Sobre a necessidade de autorização judicial, o TJ buscou arrimo na jurisprudência do TEDH relativa ao direito fundamental à inviolabilidade do domicílio, referindo expressamente que: (i) a falta de prévia autorização judicial pode ser contrabalançada por uma revisão pós-inspeção que abranja

tanto as questões de facto como de direito; (ii) a legitimidade dos poderes inspetivos da Comissão é assegurada pelo facto incontestável de os Tribunais da UE realizarem uma revisão aprofundada de facto e de direito, o que é reconhecido até pela jurisprudência do TEDH; (iii) a necessidade de prévia autorização judicial apenas se verifica quando, nos termos do artigo 20.º, n.os 6 e 7, do Regulamento n.º 1/2003, a empresa se opuser à inspeção, o que não aconteceu no caso em apreço.

O TJ explicou ainda por que razão este sistema é também compatível com o direito fundamental à fiscalização jurisdicional efetiva, improcedendo assim o segundo fundamento do recurso da empresa visada, ora recorrente.

Sobre as descobertas fortuitas "não totalmente surpreendentes", a questão perante o TJ centrou-se em saber se a Comissão tinha tido razões válidas para informar os seus funcionários sobre a existência de suspeitas relativas à segunda infração independente, mas anterior à inspeção, o que fora contestado pela recorrente. Não era de presumir que o TJ conhecesse desta questão, que – como argumentado pela Comissão – poderia ser definida mais como uma questão de facto do que de direito, sendo certo que as questões de facto não podem ser objeto de revisão pelo TJ. No entanto, o TJ realçou que a Deutsche Bahn (DB) argumentara que o TG cometera um erro de direito ao considerar que a Comissão tinha razões válidas para informar os seus funcionários sobre a existência de suspeitas relativas à segunda infração independente (§ 54). O TJ não chega a explicar por que razão a alegação era realmente jurídica e não factual, mas aceitou imediatamente a admissibilidade do fundamento alegado, talvez para não ter de lidar com previsíveis críticas nos círculos de especialistas de concorrência.

Quanto ao mérito, o TJ rememorou a jurisprudência relevante nessa matéria e sublinhou que a Comissão só pode pesquisar documentos que se enquadrem no âmbito do objeto da inspeção, tal como definido na própria decisão de inspeção (§ 60), alertando que a Comissão poderá iniciar novas investigações se deparar com novas provas genuinamente fortuitas (§ 59), tendo concluído – tal como o Advogado-Geral (AG) Nils Wahl – que, embora os inspetores necessitem de receber informações básicas sobre cada caso em apreço, "toda essa informação deve, no entanto, referir-se exclusivamente ao objeto da inspeção ordenada pela decisão" (§ 62). Em conformidade, o TJ concluiu que a primeira inspeção padecia de invalidade, "uma vez que os agentes da Comissão, estando anteriormente na posse de informação alheia ao objeto daquela inspeção, procederam à apreensão de documentos que não se enquadram no âmbito da inspeção, tal como circunscrito pela primeira

decisão" (§ 66). O TJ decidiu, portanto, proferir o acórdão final nos termos do artigo 61.º do Estatuto do Tribunal e anulou a segunda e terceiras decisões de inspeção, em vez de reenviar o processo para o TG.

8. Conclusões intermédias

A referida decisão do TJ, de 18 junho de 2015, baseia-se na jurisprudência do TEDH, que é abundantemente citada, bem como na opinião do AG Wahl, que também é repetidamente citada. Já não constitui surpresa para ninguém que as normas processuais do Direito da Concorrência da UE tenham vindo a convergir com o princípio do processo equitativo e outros princípios convencionais, tal como interpretados pelo TEDH, cuja grande influência no Luxemburgo se tornou cada vez mais visível, já mesmo antes da adesão da UE à CEDH.

A dispensa de autorização prévia (judicial ou judiciária) para a realização de operações intrusivas de surpresa por parte da Comissão nas sedes e outras instalações das empresas é legítima porque a revisão judicial *ex post* das decisões da Comissão está disponível para todas as empresas visadas. Na medida em que o TJ assume que a revisão judicial se estende tanto a questões de facto como de direito, o que inclui o poder de avaliar provas e anular decisões, o controlo judicial acaba por ser suficientemente intenso. Mas é preciso confiar que a jurisprudência do TJ se venha a tornar cada vez mais concreta e esclarecida do ponto de vista dos direitos e garantias processuais das empresas visadas.

A pesquisa e a apreensão de mensagens de correio eletrónico durante uma operação intrusiva de surpresa por parte da Comissão também não carece de autorização prévia (judicial ou judiciária), pois essas mensagens são consideradas como documentos eletrónicos iguais a quaisquer outros, a menos que sejam documentos de natureza não profissional (*i.e.*, pessoal), caso em que não podem ser apreendidos, nem usados com prova contra as empresas visadas em processos por práticas restritivas da concorrência.

A Comissão poderá solicitar um mandado às autoridades judiciárias nacionais competentes, de acordo com o ordenamento jurídico do local da inspeção, se tal for necessário para vencer a eventual oposição das empresas em causa.

No caso concreto, a decisão do TJ merece aplauso, mas a situação apreciada era anómala e não se percebe a razão por que a Comissão, gozando de tão amplos poderes – que os Tribunais da UE normalmente amparam –, sentiu necessidade de se envolver em práticas de inspeção menos consistentes, quando poderia, sem problemas, ter adotado uma única decisão de inspeção

para as duas suspeitas de infração independentes ou então duas decisões de inspeção simultâneas. A especificidade do caso torna-o uma lição para a futura prática decisória da Comissão, mas também torna o interesse do caso neste aspeto residual e, porventura, irrepetível.

IV. As Inspeções e as Buscas da Autoridade da Concorrência Portuguesa

Os procedimentos para a aplicação das regras de concorrência da UE pelas ANC são regidos, em larga escala, pela legislação nacional, sujeita aos princípios gerais do Direito da UE, em especial os princípios de eficácia e equivalência. Isto significa que as ANC aplicam as regras de concorrência da UE com base em diferentes procedimentos[22].

Em Portugal, a Lei n.º 19/2012, de 8 de maio[23], que contém o atual regime jurídico da concorrência, distingue as inspeções e auditorias (artigo 63.º) das buscas (artigos 18.º e 19.º).

1. As inspeções

A previsão dos estudos, inquéritos, inspeções ou auditorias já constava dos anteriores Estatutos da Autoridade da Concorrência (AdC). À parte essa previsão, cabe ainda referir uma norma geral, muito vaga e remissiva para o Código do Procedimento Administrativo (CPA), sobre poderes de supervisão, no artigo 20.º da velha Lei n.º 18/2003, de 11 de junho.

O atual NRJC dedica agora um capítulo inteiro à matéria dos estudos, inspeções e auditorias. Nesse capítulo, o artigo 63.º, n.º 4, prevê a emissão de recomendações de caráter comportamental ou estrutural se, em resultado de inspeções ou auditorias, a AdC detetar situações que afetam a concorrência nos mercados em causa.

Não diz, porém, se é possível o aproveitamento dos elementos recolhidos em inspeções e auditorias para efeitos de processos sancionatórios, caso surjam indícios de alguma infração às normas de concorrência neste contexto. O artigo 31.º, n.º 5, do NRJC autoriza agora expressamente o aproveitamento como meio de prova num processo sancionatório da informação e documentação obtida no âmbito da supervisão.

---

[22] Cf. Paulo de Sousa Mendes, *O Sancionamento das Práticas Restritivas da Concorrência*, Coimbra: Almedina, 2022, p. 55. Para desenvolvimentos, veja-se a Comunicação da Comissão ao Parlamento Europeu e ao Conselho, de 9 de julho de 2014, sobre os Dez anos de aplicação da legislação antitruste ao abrigo do Regulamento n.º 1/2003: Progressos alcançados e perspetivas {SWD(2014) 230 final} e {SWD(2014) 231 final}. *Online*: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52014DC0453 (consultado em 08/10/2024).

[23] 4.ª versão – a mais recente (Lei n.º 17/2022, de 17/08).

As diligências de supervisão e, em especial, as inspeções e auditorias são atos administrativos de conteúdo verificativo, no âmbito de uma relação institucional em que o dever de colaboração do inspecionado ou auditado tem como contrapartida a comunicação prévia por parte da AdC do como e quando serão realizadas as diligências, de maneira a assegurar o máximo resultado das mesmas. Tais diligências não visam a descoberta de ilícitos, sob pena de se transformarem em buscas encapotadas (em manifesta fraude à lei), mas o controlo ou fiscalização do cumprimento da lei. É natural, portanto, que, em caso de descoberta de irregularidades ou indícios de infrações, a AdC deva emitir preferencialmente recomendações para adoção de medidas de correção, códigos de conduta e criação ou aperfeiçoamento de sistemas de cumprimento normativo (*compliance*) nas empresas. Pode até, neste contexto e ao abrigo do princípio da oportunidade (prioridades) consagrado no artigo 7.º, n.º 2, do NRJC decidir não abrir inquérito em processo de contraordenação por práticas restritivas da concorrência.

Não pode, porém, a AdC ignorar a descoberta desses indícios. Por conseguinte, os mesmos servem de notícia da infração e, por força do artigo 31.º, n.º 5, do NRJC, também como meio de prova em processos sancionatórios em curso ou a instaurar.

Neste tocante, o NRJC não pode ser mais restritivo do que a Lei n.º 18/2003, que não continha limitações nesta matéria. De resto, a jurisprudência do Tribunal do Comércio de Lisboa (TCL) já se vinha pronunciando no sentido de um aproveitamento como prova em processos sancionatórios dos elementos recolhidos na supervisão. Veja-se a Sentença do TCL, de 8 de maio de 2007, no chamado caso das Moageiras[24], decidindo um recurso de decisões da AdC que aplicaram coimas às empresas por não terem prestado a informação e os elementos por esta solicitados: "Dentro da AdC e independentemente da natureza dos procedimentos a informação deve circular. O que para uns é informação, para outros podem ser meios de prova incriminatórios"[25].

Esta orientação também foi confirmada pelo TC, que, em acórdão de 11 de outubro de 2011, referente a um processo de contraordenação com

[24] Sentença do Tribunal de Comércio de Lisboa, de 8 de maio de 2007, proc. n.º 205/06.0TYLSB, p. 72.

[25] A Lei n.º 18/2003 não continha qualquer norma relativa ao aproveitamento dos elementos recolhidos no âmbito da supervisão para efeitos de processos sancionatórios. O artigo 17.º da Lei n.º 18/2003 tinha por epígrafe "Poderes de inquérito e inspeção" e no corpo do n.º 1 abrangia "poderes sancionatórios e de supervisão", sem fazer outras distinções. Ainda que se possa apontar a falta de clareza desta disposição, a mesma legitimava, porém, a interpretação de que a AdC gozava dos mesmos poderes em sede de supervisão e em sede contraordenacional, não havendo limitações à passagem de informação de uma para outra sede.

origem na AdC, expressamente considerou que «[…] nenhuma dúvida haverá quanto à possibilidade de utilização de elementos coligidos pela Autoridade da Concorrência, no âmbito dos poderes de supervisão, em ulterior procedimento contraordenacional»[26].

Não podemos deixar passar a oportunidade de tecer uma nota crítica em relação à Lei-Quadro das Entidades Administrativas Independentes com funções de regulação da atividade económica dos setores privado, público e cooperativo (Lei n.º 67/2013, de 28 de agosto)[27]. Não se percebe a necessidade de uma disposição avulsa sobre poderes em matéria de inspeção e auditoria, nem, sobretudo, o regime instituído, o qual permite a realização de inspeções e auditorias sem pré-aviso aos inspecionados e, aparentemente, o uso da força (artigo 42.º da Lei-Quadro). Trata-se, a nosso ver, de uma norma que confunde poderes de inspeção e poderes de busca, o que mostra o quanto ainda há para esclarecer entre nós nesta matéria. Felizmente, é norma que não interfere com os poderes da AdC, na medida em que a própria Lei-Quadro exceciona o NRJC na parte em que contenha normas especiais, nos termos do artigo 1.º, n.º 2, da Lei-Quadro.

O NRJC estabelece uma separação entre as funções de supervisão e de sancionamento, mas, como vimos, consagra vasos comunicantes entre ambas, no quadro de um princípio de lealdade na relação da AdC com as empresas e as pessoas afetadas por quaisquer diligências.

2. As buscas

As buscas ocorrem no âmbito de processos sancionatórios por práticas restritivas da concorrência. A busca é um meio de obtenção de prova que implica a entrada em locais vedados ao público, tais como as sedes e demais instalações e terrenos de empresas e associações de empresas, e, eventualmente, a restrição ao próprio direito fundamental de inviolabilidade de domicílio (artigo 24.º, n.º 1, da CRP). Como tal, estamos perante um meio de obtenção de prova relativamente proibido (artigo 34.º, n.º 2, da CRP).

Apenas são permitidas se houver previsão legal, o que é o caso, nos termos do artigo 18.º, n.º 1, do NRJC. Note-se que o artigo 19.º acrescenta ainda a permissão de buscas ao domicílio de sócios, de membros de órgãos de administração e de trabalhadores e colaboradores de empresas ou associações

[26] Acórdão do TC n.º 461/2011, exarado no processo n.º 366/11, em recurso interposto por Abbott – Laboratórios, Lda., publicado in: *Diário da República*, 2.ª Série, n.º 243, 21 de dezembro 2011.

[27] 4.ª versão – a mais recente (Lei n.º 75-B/2020, de 31/12).

de empresas. Acresce que a busca depende de autorização da autoridade judiciária competente, devendo ter-se em especial atenção o princípio da proporcionalidade, em sentido amplo. Isto é, a ideia de que nenhum direito poderá ser restringido sem que esteja em causa assegurar um direito ou interesse de valor superior. É preciso, pois, atender à necessidade, adequação e proporcionalidade em sentido estrito da diligência, no caso concreto. Por sua própria natureza de meio de obtenção de prova, é diligência realizada sem pré-aviso e pode implicar o uso da força, se tal estiver contemplado no despacho que a autoriza, sendo, de resto, por isso mesmo que a lei prevê a possibilidade de a AdC recorrer à colaboração de entidades policiais, nos termos do artigo 18.º, n.º 1, alínea *g*), do NRJC.

3. Conclusões intermédias

O NRJC veio clarificar a distinção entre poderes de busca e de inspeção, a saber:

- Separa os procedimentos de inspeção e auditoria dos procedimentos sancionatórios;

- Mas não estabelece barreiras entre ambos os domínios;

- Admite o aproveitamento da informação e da documentação obtida no âmbito dos procedimentos de inspeção e auditoria não apenas como notícia da infração, mas até como meio de prova em processo sancionatório em curso ou a instaurar;

- Favorece a obtenção de informação e de documentação por parte da AdC junto das empresas através da consagração de deveres de colaboração, estabelecidos sob cominação de coimas para a desobediência;

- Não concede imunidades às empresas ao abrigo do cumprimento desse dever de colaboração;

- Mas impõe à AdC um dever de lealdade em relação às empresas, na medida em que o aproveitamento probatório da informação e da documentação assim obtida depende de prévio esclarecimento da possibilidade dessa utilização;

- No âmbito das ações inspetivas e auditorias a realizar pela AdC impõe-se que seja dada a informação necessária sobre o caráter da diligência (que não se confunde com uma busca no quadro de um processo sancionatório), mediante notificação prévia da sua realização;

- Não obstante o dever de colaboração, todas as pessoas notificadas pela AdC gozam da prerrogativa de não autoinculpação, no sentido de não serem obrigadas a confessar a prática de quaisquer ilícitos (ou seja, de não

terem de prestar declarações que por si só e independentemente de outros meios de prova e valorações sejam equivalentes à admissão da prática de uma infração), mas apenas de deverem fornecer as informações estritamente factuais que lhes forem pedidas e os documentos preexistentes referenciados pela AdC (jurisprudência Orkem);

- E têm garantida a possibilidade de revisão das decisões da AdC por via de recurso judicial de jurisdição plena.

O NRJC estabelece, pois, uma separação entre as funções de supervisão e sancionatórias, mas consagra vasos comunicantes entre ambas, no quadro de um princípio de lealdade na relação da AdC com as empresas e as pessoas afetadas por quaisquer diligências.

O sistema de separação relativa entre as funções puramente supervisoras e as funções repressivas pode ser sintetizado da seguinte forma: a AdC pode executar de modo próprio e sem qualquer autorização externa todas as funções de pura supervisão (por exemplo, inspeções e auditorias), mas, ainda que possa também realizar autonomamente algumas das diligências de investigação das práticas restritivas da concorrência (por exemplo, solicitação de informações e inquirições), a AdC depende de autorização externa para aquelas diligências de investigação que são mais invasivas, precisamente por serem lesivas da privacidade das empresas e dos respetivos dirigentes e demais colaboradores (por exemplo, buscas a instalações, terrenos, meios de transporte, dispositivos ou equipamentos de empresas, buscas domiciliárias, buscas em escritórios de advogados, consultórios médicos ou escritórios de revisores oficiais de contas, apreensões, incluindo em bancos ou outras instituições de crédito de documentos abrangidos por sigilo bancário).

A autorização externa para as diligências invasivas, quando necessária, será, em algumas situações, da competência do MP e, noutras situações, do Juiz de Instrução (JI). A promoção junto do MP é necessária, designadamente, quanto à busca, exame, recolha e apreensão de documentos nas instalações e outros locais relativos às empresas visadas (artigo 18.º, n.º 1, alíneas *a*) a *d*), do NRJC). A promoção junto do JI é necessária, designadamente, quanto à busca domiciliária (artigo 19.º do NRJC). Tratando-se de busca em escritório de advogado, em consultório médico ou em escritório de revisor oficial de contas, esta é realizada, sob pena de nulidade, na presença do JI, o qual avisa previamente o presidente do conselho regional ou, na sua falta, do conselho geral, da Ordem dos Advogados, da Ordem dos Médicos ou da Ordem dos Revisores Oficiais de Contas, respetivamente, para que o mesmo ou um representante seu possa estar presente (artigo 19.º, n.º

7, do NRJC). A apreensão em bancos ou outras instituições de crédito de documentos abrangidos por sigilo bancário é efetuada pelo JI, quando tiver fundadas razões para crer que eles estão relacionados com uma infração e se revelam de grande interesse para a descoberta da verdade ou para a prova, mesmo que não pertençam ao visado (artigo 20.º, n.º 6, do NRJC). Por conseguinte, o JI autoriza, preside ou realiza diretamente as diligências, consoante os casos.

A razão para o NRJC ostentar um sistema de divisão de competências decorre da sintonia com o regime das buscas previsto no CPP (artigos 174.º, n.º 3, 177.º. n.º 1, 268.º, n.º 1, alínea *c*), 269.º, n.º 1, alínea *c*), do CPP), dada a relação estreita com o CPP (artigo 59.º, n.º 2, do NRJC), ainda que intermediada pelo artigo 41.º, n.º 1, do RGCO. Não sendo um caso de aplicação subsidiária do CPP porque o NRJC contém uma previsão própria do regime das buscas, a sintonia de regimes não é indesejável numa matéria que pode afetar direitos, liberdades e garantias dos visados. Mas é uma questão que fica na memória para analisar *infra*, nas conclusões gerais.

V. A Apreensão de Mensagens de Correio Eletrónico

A questão da apreensão de mensagens de correio eletrónico no decurso de pesquisas informáticas era um irritante (*vexata quaestio*) do processo penal doméstico, até que ficou relativamente pacificada na doutrina e na jurisprudência após a publicação da Lei n.º 109/2009, de 15 de setembro[28]. O regime previsto na LC, apesar das suas múltiplas imperfeições de que não cabe aqui tratar, ainda assim permitiu ultrapassar muitas das dúvidas práticas nesta matéria[29].

As mesmas dúvidas práticas renasceram, porém, com acrescida intensidade no domínio da apreensão de correio eletrónico no decurso de buscas realizadas pela AdC em processos de contraordenação relativos a práticas restritivas da concorrência.

1. A apreensão de mensagens de correio eletrónico à luz do NRJC

O NRJC não exibe quaisquer semelhanças com a LC, embora o legislador pudesse ter seguido essa via. É manifesto que não o fez. O legislador deixou a questão da apreensão de correio eletrónico e registos de comunicações de

[28] 2.ª versão – a mais recente (Lei n.º 79/2021, de 24/11).

[29] Para desenvolvimentos, cf. Ricardo Witter Contardo, "A apreensão de correio eletrónico em Portugal: Presente e futuro de uma questão de 'manifesta simplicidade'", Paulo de Sousa Mendes/Rui Soares Pereira (coord.), *Novos Desafios da Prova Penal*, Coimbra: Almedina, 2020, pp. 277-313.

natureza semelhante subentendida no trecho: "[...] apreensões de documentos, independentemente da sua natureza ou do seu suporte [...]" (artigo 20.º, n.º 1, do NRJC).

O legislador teve pressa de aprovar o NRJC por causa do Memorando de Entendimento (MdE) celebrado entre o Estado Português e o Fundo Monetário Internacional, o Banco Central Europeu e a Comissão Europeia (a então chamada *Troika*), em 17 de maio de 2011, que incluía uma secção relativa à concorrência, contratação pública e ambiente de negócios, na qual se destacava a necessidade de, através da aplicação das regras de concorrência e de regulação setorial, se conseguir minorar a economia rentista. Se o NRJC, porventura, tivesse incluído a previsão expressa da apreensão de *emails* no âmbito das diligências de obtenção de prova das práticas restritivas da concorrência, então, provavelmente, tal obrigaria a suscitar a sua fiscalização preventiva pelo TC, o que atrasaria a entrada em vigor do diploma e violaria o compromisso estabelecido no MdE. Mas, ainda assim, já à época tínhamos entendido que seria preferível enfrentar imediatamente a questão de constitucionalidade, em vez de se procrastinar a resolução do problema, bem sabendo que era inevitável o seu surgimento. De resto, o Parecer do Conselho Superior da Magistratura (CSM) sobre a Proposta de Lei n.º 45/XII/1.ª (GOV) sinalizou oportunamente a "falta [de] uma norma habilitante da apreensão de mensagens de correio ele[t]rónico durante as buscas nas instalações das empresas, a qual deveria replicar o regime previsto na Lei do Cibercrime"[30]. Aproveita-se para referir que, longe de representar uma imposição externa, a intenção de propor uma revisão da Lei n.º 18/2003, em função da experiência dos primeiros anos de aplicação, partiu da própria AdC, muito antes da crise financeira que levou à intervenção da Troika[31].

Não há dúvida de que as mensagens de correio eletrónico são documentos[32], embora em formato eletrónico (quanto aos anexos) e especificamente digital (quanto às próprias mensagens)[33]. Mas são documentos

[30] *Online*: https://www.parlamento.pt/ActividadeParlamentar/Paginas/DetalheIniciativa.aspx?BID=36753 (consultado em 09.10.2024).

[31] Neste sentido, Miguel Moura e Silva, "As práticas restritivas da concorrência na Lei n.º 19/2012: Novos desenvolvimentos", *Revista do Ministério Público,* 137, 2014, (pp. 9-45) p. 4.

[32] Para efeitos do Código Penal (CP), considera-se documento "a declaração corporizada em escrito, ou registada em disco, fita gravada ou qualquer outro meio técnico, inteligível para a generalidade das pessoas ou para um certo círculo de pessoas, que, permitindo reconhecer o emitente, é idónea para provar facto juridicamente relevante, quer tal destino lhe seja dado no momento da sua emissão, quer posteriormente" (artigo 255.º, alínea *a*), do CP).

[33] Estamos habituados a imaginar um documento por referência a um suporte físico de papel. Mas já não é novidade para ninguém que passámos a viver numa época que privilegia a desmaterialização dos

que beneficiam de um regime especial de proteção por razões de tutela da privacidade e do próprio meio de comunicação.

Os acórdãos do TC n.os 91/2023 e 314/2023 vieram agora aproximar a aplicação do NRJC ao regime da LC, no tocante ao regime de busca, exame, recolha e apreensão previsto nos artigos 18.º, 19.º e 20.º do NRJC, na versão aprovada pela Lei n.º 19/2012[34], exigindo a autorização do JI para casos em que o NRJC se basta com a autorização do MP. Recordamos que a LC aceita a autorização do MP para as pesquisas informáticas (artigo 15.º, n.º 1, da LC) e apreensões de dados informáticos (artigo 16.º, n.º 1, da LC), mas exige a validação do JI para a 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 16.º, n.º 3, da LC), além de que exige a autorização do JI para a apreensão de correio eletrónico e registos de comunicações de natureza semelhante (artigo 17.º da LC), até parecendo que esta apreensão nunca poderá ser contemplada à partida no despacho que autoriza a pesquisa informática.

Repare-se, porém, que nenhum JI aceitaria a promoção da AdC fora dos casos previstos no NRJC. A resposta que daria à AdC seria sempre: bateu à porta errada! Será que, no final do dia, temos de aceitar que a única interpretação do NRJC conforme à CRP seja aquela que, na prática, não poderia ser seguida por incompetência legal do JI? Agora a AdC promove as buscas junto do JI, mas já tem o conforto dos acórdãos do TC. Dantes, enquanto autoridade administrativa, não tinha competência para desaplicar o NRJC com fundamento em suposta inconstitucionalidade.

---

documentos. A desmaterialização vale para os documentos eletrónicos, que admitem a distinção entre o original e a sua reprodução. É o caso dos documentos digitalizados que tiveram origem num formato físico. Não faz sentido falar de desmaterialização no caso de documentos eletrónicos originários, desde logo porque foram pristinamente codificados em dígitos binários e acedidos por meio de um sistema computacional. Nos documentos eletrónicos originários, o original é igual à cópia, pois trata-se de pura informação codificada em *bits* e *bytes*. Ainda assim, é possível falar de cópias digitais (ou seja, reproduções), já que podem ser guardados em arquivo digital, sendo assegurada a integridade da informação através da atribuição de um valor *hash* criptográfico, que resulta da implementação de uma função algorítmica que transforma a informação num conjunto alfanumérico com comprimento fixo de caracteres. A própria lei, para assegurar a cadeia de custódia na apreensão de dados informáticos, recomenda, consoante seja mais adequado e proporcional, a realização de uma cópia dos dados, em duplicado, sendo uma das cópias selada e confiada ao secretário judicial dos serviços onde o processo correr os seus termos e, se tal for tecnicamente possível, certificando os dados apreendidos por meio de assinatura digital (ou seja, *hash*), nos termos do artigo 16.º, n.º 7, alínea *b*), e n.º 8, da LC.

[34] O NRJC foi alterado, a partir de 16 de setembro de 2022, pela Lei n.° 17/2022 de 17 de agosto, que transpõe a Diretiva 2019/1. Esta lei aditou um n.º 4 ao artigo 18.º do NRJC, nos termos do qual da recusa, por parte da autoridade judiciária competente, em conceder à AdC a autorização referida nesse artigo cabe "*a*) [n]o caso de decisão do Ministério Público, reclamação para o superior hierárquico imediato; *b*) [n]o caso de decisão do juiz de instrução, recurso para o tribunal da relação competente, que decide em última instância".

Mas percebe-se que o TC tenha acentuado o respeito pelas fontes, especialmente pela CRP. Não podia o TC ignorar o artigo 34.º, n.º 4, da CRP com o argumento de que não é assim noutros países europeus, só em Portugal. A menos que a questão esteja vinculada ao Direito da UE, o que é difícil de defender numa matéria processual, embora esteja em causa a eficácia de uma política essencial da UE, ou seja, a defesa da concorrência.

O artigo 34.º da CRP é uma idiossincrasia nacional porque separa a tutela das comunicações da tutela da reserva da intimidade da vida privada estabelecida no artigo 26.º, n.º 1, da CRP, ao contrário do artigo 8.º, n.º 1, da CEDH, que inclui a tutela da correspondência no âmbito do respeito pela vida privada e familiar. Ao ter uma norma autónoma para a ingerência das autoridades públicas na correspondência, nas telecomunicações e nos demais meios de comunicação, a CRP reserva o artigo 34.º, n.º 4, para a tutela do próprio meio de comunicação, em si mesmo, independentemente da reserva da privacidade. Passa a ser uma proteção formal do veículo de comunicação, contenha ou não informação privada. Para este efeito, tanto vale uma mensagem publicitária como uma mensagem íntima. É um absurdo, mas é assim. A combinação de um cartel pode não ser uma mensagem privada, enquanto conspiração ilícita, mas o meio usado garante-lhe a proteção constitucional. Custa-nos a aceitar uma proteção formal do meio de comunicação, que só não é absoluta porque são excecionados os casos previstos na lei em matéria de processo criminal. Mas o artigo 34.º, n.º 4, da CRP existe.

O TC fez um trabalho notável para não o tornar um obstáculo intransponível à apreensão de mensagens de correio eletrónico nos processos por práticas restritivas da concorrência, que são de natureza contraordenacional. Ou seja, o TC conseguiu aplicar a exceção dos casos previstos na lei em matéria de processo criminal também aos casos de processo contraordenacional por práticas restritivas da concorrência, com apelo a um conceito material de crime. Podemos acompanhar o argumento do conceito material de crime, mas até se chegaria ao mesmo resultado mais diretamente através da jurisprudência do TEDH. Não devemos esquecer que o TEDH estabeleceu uma definição ampla de ilícito criminal (*criminal offence*) para efeitos de aplicação das garantias da CEDH, que abrange os processos administrativos sancionadores e todos os processos sancionadores de carácter público[35].

[35] Já desde os casos Engel and Others *v.* The Netherlands (1976), § 81, e Öztürk *v.* Germany (1984), § 53. O mesmo entendimento foi recentemente reafirmado em Jesus Pinhal *v.* Portugal (2024), § 152 ss.

O problema dos acórdãos do TC n.os 91/2023 e 314/2023 é a dificuldade de agradar a Gregos e Troianos[36]. Os referidos acórdãos convocam o JI, em vez do MP, para autorizar a apreensão de *emails*, por parte da AdC, ao aceder aos dispositivos ou equipamentos das empresas visadas durante as buscas a todas as suas instalações. Afastaram-se assim da lógica do NRJC, que tem regime próprio, embora equívoco quanto à apreensão de *emails*. Mas permitem que a AdC doravante promova junto do JI as diligências de busca que envolvam – ou previsivelmente envolvam – a apreensão de mensagens de correio eletrónico que constituam prova da prática de infrações de concorrência, o que dantes seria difícil por falta de previsão legal de uma tal diligência junto do JI. A AdC facilmente se adaptou a essa nova exigência, mas ficaram por resolver os processos antigos e agora temos os reenvios prejudiciais que podem comprometer a validade da prova eletrónica apreendida em processos de contraordenação por práticas restritivas da concorrência pendentes no TCRS.

2. Os pedidos de reenvio prejudicial enviados pelo TCRS ao TJUE e as Conclusões da Advogada-Geral Laila Medina

No dia 20 de junho de 2024, foram publicadas as Conclusões da AG Laila Medina sobre três pedidos de decisão prejudicial (reenvio prejudicial) dirigidos pelo TCRS ao TJ relacionados com a compatibilidade das leis nacionais com o artigo 7.º da Carta dos Direitos Fundamentais da UE (Carta) no que concerne à apreensão de *emails* realizada pela AdC no decurso de buscas às instalações de empresas, no âmbito de três processos contraordenacionais por práticas restritivas da concorrência devidamente identificados[37]. Os três pedidos do órgão jurisdicional de reenvio surgiram na sequência dos dois acórdãos do TC de 2023, que declararam inconstitucional a regra relativa ao artigo 18.º, n.º 1, alínea *c*), e n.º 2 e ao artigo 20.º, n.º 1, do NRJC, com base na qual a AdC procedia à pesquisa e apreensão de mensagens de correio eletrónico abertas, ou seja, mensagens de correio eletrónico marcadas como lidas, mediante mera autorização do MP. Dado

[36] Mas há também quem discorde totalmente das posições avançadas pelo TC, tanto na parte respeitante à definição do âmbito normativo do direito à autodeterminação comunicativa, como na parte atinente à ressalva feita à matéria de processo criminal. Neste sentido, cf. Nuno Brandão, "Apreensão de webmail em processo contraordenacional e reserva de processo criminal – Contraponto a uma nova jurisprudência constitucional duplamente equivocada", *Revista Portuguesa de Direito Constitucional* 3 (2023), (pp. 215-238) p. 220.

[37] *Online*: https://curia.europa.eu/juris/document/document.jsf;jsessionid=875B5FD7AA350F5768A16A75E7DB3CDA?text=&docid=287318&pageIndex=0&doclang=PT&mode=req&dir=&occ=first&part=1&cid=7628636 (consultado em 09.10.2024).

que as questões foram submetidas no âmbito de três processos pendentes de julgamento, o TCRS decidiu suspender a instância e aguardar pela decisão do TJ em cada um dos processos principais. As conclusões da AG valem por si mesmas, mas não vinculam o TJ. Importa, em qualquer caso, destacar que a decisão final que vier a ser proferida nestes processos prejudiciais balizará os poderes de investigação das ANC defronte das exigências impostas pela tutela da vida privada e do sigilo das comunicações, especialmente no nosso país, considerando o risco iminente de anulação das decisões da AdC e das coimas aplicadas às empresas.

As três questões prejudiciais são as seguintes:

1. Os documentos profissionais em causa, veiculados através de correio eletrónico, são "correspondência" na aceção do artigo 7.º da Carta?

2. O artigo 7.º da Carta opõe-se à apreensão de documentação profissional, resultante de comunicações estabelecidas entre administradores e colaboradores de empresas através de endereços de correio eletrónico, quando esteja em causa a investigação de acordos e práticas proibidas nos termos do artigo 101.º do TFUE (ex-artigo 81.º do TCE) ou, no processo C-260/23, do artigo 102.º do TFUE (ex-artigo 82.º do TCE)?

3. O artigo 7.º da Carta opõe-se à apreensão daquela documentação profissional, mediante prévia autorização de autoridade judiciária, *in casu*, o MP, a quem compete representar o Estado, defender os interesses que a lei determinar, exercer a ação penal orientado pelo princípio da legalidade e defender a legalidade democrática, nos termos da Constituição e que atua com autonomia em relação aos demais órgãos do poder central, regional e local?

As Conclusões da AG Laila Medina dão resposta às três questões que sustentaram os três pedidos de decisão prejudicial.

Quanto à primeira questão, a opinião dada vai no sentido de que: "[...] as apreensões de mensagens de correio eletrónico efetuadas no decurso das visitas domiciliárias às instalações profissionais ou comerciais de uma pessoa singular ou às instalações de uma sociedade comercial constituem ingerências no exercício do direito ao respeito pela correspondência garantido pelo artigo 8.º, n.º 1, da CEDH e, logo, em aplicação do artigo 52.º, n.º 3, da Carta, no exercício do direito correspondente consagrado no artigo 7.º desta. Esta afirmação aplica-se às apreensões efetuadas quer no quadro de um processo penal quer no quadro de um processo administrativo. Além disso, a qualificação das mensagens de correio eletrónico enquanto 'correspondência' na aceção do artigo 8.º, n.º 1, da CEDH e 'comunicações' na aceção do artigo 7.º da Carta é independente da circunstância de essas mensagens já terem sido recebidas pelo

seu destinatário, lidas, não lidas ou suprimidas, do facto de a comunicação ter sido enviada a partir das instalações ou equipamentos profissionais ou através de uma caixa de correio eletrónico profissional ou de a morada do remetente ou do destinatário ser a de uma pessoa coletiva, ou, ainda, da questão de saber se o seu conteúdo tem ou não um caráter privado. Assim, o facto de, à luz do seu conteúdo, uma mensagem de correio eletrónico poder ser qualificada de 'documento profissional' não permite privá-la da proteção que o artigo 7.º da Carta garante às comunicações. Por fim, esta proteção não respeita apenas ao conteúdo das mensagens de correio eletrónico, estendendo-se também aos dados de caráter pessoal relativos ao tráfego por elas gerados, que são também protegidos pelo artigo 8.º da Carta" (§ 31).

Quanto à segunda questão, a opinião dada vai no sentido de que: "[...] o artigo 7.º da Carta não se opõe à revista e à apreensão, por uma [ANC], de mensagens de correio eletrónico trocadas através da caixa de correio interna de uma empresa sujeita a uma inspeção nas suas instalações profissionais ou comerciais no quadro de um inquérito por infração às regras da concorrência, desde que essas mensagens sejam pertinentes para o objeto da inspeção" (§ 39).

Quanto à terceira questão, onde, pensando bem, tudo se joga, a opinião dada vai no sentido de que: "[recordando a jurisprudência do TEDH no que respeita ao artigo 8.º da CEDH, assim como a jurisprudência do TJUE no que respeita ao artigo 7.º da Carta,] não havendo autorização judicial prévia, a proteção dos indivíduos contra as infrações arbitrárias do poder público aos direitos garantidos por esse artigo exige um enquadramento legal e limites estritos dessa apreensão. [P]or um lado, [que] esta apreensão só é compatível com o referido artigo 7.º se a legislação e a prática internas oferecerem garantias adequadas e suficientes contra os abusos e a arbitrariedade e, por outro, que a não existência de um mandado judicial prévio pode, em certa medida, ser contrabalançada pela possibilidade de a pessoa visada na apreensão solicitar *a posteriori* a fiscalização jurisdicional quer da legalidade quer da necessidade desta, devendo essa fiscalização ser eficaz nas circunstâncias particulares do processo em causa" (§ 44).

Que fazer, porém, se: "[...] um Estado-Membro apli[car] um nível nacional de proteção do direito fundamental ao respeito pelas comunicações garantido pelo artigo 7.º da Carta mais elevado do que o previsto por essa disposição, como interpretada pelo [TJUE], nomeadamente ao impor à autoridade nacional da concorrência que obtenha uma autorização judicial

prévia para poder proceder a inspeções e apreensões nas instalações de uma sociedade" (§ 46)?

A resposta é que: "[o TJUE] afirmou repetidamente que, quando, numa situação em que a ação dos Estados-Membros não é inteiramente determinada pelo direito da União, uma disposição ou uma medida nacional aplique este direito na aceção do artigo 51.º, n.º 1, da Carta, as autoridades e os órgãos jurisdicionais nacionais podem aplicar padrões nacionais de proteção dos direitos fundamentais, desde que essa aplicação não comprometa nem o nível de proteção previsto na Carta, conforme interpretada pelo [TJUE], nem o primado, a unidade e a efetividade do direito da União" (§ 48).

"Ora, no caso em apreço, por um lado, [a AG Laila Medina] consider[a] que incumbe ao órgão jurisdicional de reenvio, quando da apreciação das consequências a retirar dos Acórdãos de 2023, ter em conta a necessidade de assegurar uma aplicação efetiva das regras de concorrência da União, recorrendo a todas as possibilidades oferecidas pelo direito nacional – incluindo, sendo caso disso, a de sanar, em circunstâncias como as dos litígios nos processos principais, a inexistência de autorização judicial prévia através de uma fiscalização judicial *a posteriori* – para assegurar que o desrespeito dessas regras seja punido" (§ 61).

"Por outro lado, a fim de dar plena execução aos artigos 101.º e 102.º TFUE, os tribunais portugueses podem ser levados a não aplicar uma regra nacional que reconhece à interpretação adotada nos Acórdãos de 2023 um efeito retroativo que tem como consequência pôr em causa a responsabilidade das empresas em questão em situações em que uma infração ao direito da concorrência da União foi definitivamente constatada pela AdC, gerando um risco sistémico de impunidade para tais infrações" (§ 62).

Assim, a AG Laila Medina sugere ao TJ que responda como segue à terceira questão prejudicial submetida pelo TCRS em cada um dos processos apensos C-258/23 a C-260/23:

"O artigo 7.º da Carta dos Direitos Fundamentais da União Europeia deve ser interpretado no sentido de que não se opõe à legislação de um Estado-Membro ao abrigo da qual, durante uma inspeção nas instalações de uma empresa, conduzida no quadro de uma investigação por violação do artigo 101.º ou 102.º TFUE, a autoridade nacional da concorrência procede à busca e à apreensão de mensagens de correio eletrónico cujo conteúdo está relacionado com o objeto da inspeção sem dispor de uma autorização judicial prévia, desde que estejam previstos um enquadramento legal estrito dos poderes dessa autoridade, bem como garantias adequadas e suficientes

contra os abusos e a arbitrariedade, nomeadamente uma fiscalização judicial *ex post* completa das medidas em causa".

VI. Conclusões Gerais

A AG Laila Medina entende que as autoridades e os órgãos jurisdicionais nacionais podem aplicar padrões nacionais de proteção dos direitos fundamentais, desde que essa aplicação não comprometa nem o nível de proteção previsto na Carta, conforme interpretada pelo TJUE, nem o primado, a unidade e a efetividade do direito da União.

A primeira questão é saber se a necessidade de autorização judicial prévia para proceder a pesquisas e apreensões de mensagens de correio eletrónico concede um nível de proteção superior ao de uma autorização judiciária prévia, ou seja, do MP[38].

Importa destacar que tanto o MP como o JI são independentes do poder executivo. Será que o MP pode ser considerado menos independente do que o JI? À primeira vista, dir-se-ia que sim porque o MP assume as vestes de acusador público, em caso de recurso de impugnação judicial da decisão condenatória da AdC (artigo 62.º, n.º 1, do RGCO)[39]. Essa função, porém, só se manifesta se houver recurso da decisão condenatória da AdC, não havendo até lá nada que ligue a titularidade da investigação pela AdC na fase organicamente administrativa do processo de contraordenação à atuação do MP. Nem o MP perde, em fase judicial, a independência perante a AdC. Embora seja discutível, do ponto de vista da igualdade de armas, a solução legal de a AdC ter atuação autónoma no tribunal, acrescendo à atuação do MP.

Mas a independência do JI também pode ser questionada, uma vez que não é um autêntico juiz das garantias. O sistema português do JI, em declínio na maior parte dos ordenamentos jurídicos de estrutura acusatória, confia ao JI as funções antagónicas de juiz garantidor, na fase de inquérito, e de juiz investigador, na fase de instrução, com poderes autónomos de investigação e competência para pronunciar o arguido, se for o caso, antecipando-se assim ao julgamento da causa[40]. Dir-se-ia que as suas funções de juiz investigador

---

[38] Cf. Rui Cardoso, "A Apreensão de correio eletrónico após o Acórdão do Tribunal Constitucional n.º 687/2021: Do Juiz das Liberdades ao Juiz Purificador Investigador?", *Revista Portuguesa de Direito Constitucional,* 1 (2021), (pp. 141-170) p. 153.

[39] DL n.º 433/82, de 27 de outubro (Ilícito de Mera Ordenação Social), cuja 7.ª versão, a mais recente, foi dada pela Lei n.º 109/2001, de 24 de dezembro.

[40] Questionando a independência dos juízes de instrução europeus (*e.g.*, belgas), cf. Clémence Van Muylder, "La conservation des données de télécommunication à des fins de poursuites pénales – Influence de la jurisprudence européenne sur le droit belge", *Rev. dr. pén. entr.,* 4 (2022), pp. 343-365.

só relevam no processo penal, não tendo, por isso mesmo, qualquer expressão no processo contraordenacional. O JI seria, pois, uma figura independente, ademais totalmente imparcial no processo contraordenacional, designadamente no processo especial por práticas restritivas da concorrência. Mesmo concedendo que a ambivalência das funções do JI possa deixar intocada a sua função de garante dos direitos fundamentais, a surpresa advém agora da convocação de uma figura alheia ao processo contraordenacional para intervir em procedimentos e matérias que lhe são completamente estranhos. Será que o JI poderá então fazer mais do que chancelar as promoções da AdC? Não se antolha, pois, que as diligências de investigação das práticas restritivas da concorrência que carecem de autorização externa sejam mais eficazmente controladas pelo JI do que pelo MP.

Seja como for, o TC não pode impor um efeito retroativo em casos em que a AdC não teria alternativa para cumprir a sua missão de defesa da concorrência, a não ser procurando obter uma autorização judiciária para pesquisas e apreensões de mensagens de correio eletrónico em equipamentos informáticos situados na sede ou em outras instalações de uma empresa. Enquanto autoridade administrativa, a AdC não podia desaplicar a lei com fundamento em inconstitucionalidade.

Manifestamente, os acórdãos do TC n.os 91/2023 e 314/2023 redundam na imposição de uma solução meramente formalista (*i.e.*, a chancela do JI), que não é mais garantidora de direitos fundamentais do que a consagrada no NRJC (*i.e.*, a autorização do MP), até pelo contrário.

Acresce, como segunda questão, que a interpretação do artigo 34.º, n.º 4, da CRP como se contivesse uma remissão implícita para o regime da apreensão de correio eletrónico estabelecido no artigo 17.º da LC, enquanto regime de referência em matéria de processo criminal e agora – na perspetiva adotada nos acórdãos do TC n.os 91/2023 e 314/2023 – também tornado aplicável ao processo de contraordenação por práticas restritivas da concorrência, tem de ser entendida com as maiores cautelas quanto ao papel do JI. Cabe destacar que o artigo 17.º da LC não impõe a autorização prévia do JI para a apreensão de correio eletrónico, mas exige, isso sim, a autorização posterior do JI se forem encontradas durante a pesquisa informática mensagens de correio eletrónico, o que significa que as mesmas podem ser apresentadas em suporte autónomo juntamente com requerimento fundamentado, que o JI apreciará, tomando conhecimento do seu conteúdo, e decidirá autorizar

ou não autorizar a apreensão formal[41] e, se for o caso, a junção aos autos, o que corresponde a um controlo judicial *a posteriori* da apreensão[42]. Esta interpretação teria, pelo menos, a vantagem de não comprometer nem o nível de proteção previsto na Carta, conforme interpretada pelo TJUE, nem o primado, a unidade e a efetividade do direito da União. De maneira nenhuma se pode aceitar que o juízo de (in)constitucionalidade normativa comprometa nem o nível de proteção previsto na Carta, conforme interpretada pelo TJUE, nem o primado, a unidade e a efetividade do direito da União.

O acórdão do TC n.º 533/2024 reconhece que o Direito interno não pode constituir um obstáculo à efetividade do Direito europeu na jurisdição nacional e a CRP não pode ser interpretada em sentido que represente a obstrução da vigência e efetividade prática do Direito da Concorrência em Portugal, ademais sublinhando o caráter crucial das medidas de busca e apreensão de documentos eletrónicos contendo mensagens no âmbito de infrações contra a concorrência, bem como a sua centralidade para a punição deste tipo de infrações. De resto, o sistema português excede o padrão de garantias europeu, que reside na exigência de controlo jurisdicional *ex post facto*, ao passo que a lei portuguesa estabelece um quadro de duplo controlo judiciário (MP, prévio à operação e controlo por Juiz, subsequente). Dos três analisados, o acórdão do TC n.º 533/2024 afigura-se, assim, o mais alinhado com o princípio da interpretação conforme ao Direito da Concorrência da União Europeia, o que merece aplauso, desde que seja respeitado o padrão de garantias europeu (CEDH e Carta), o que é o caso.

Tirando a questão de constitucionalidade, que, obviamente, não é de somenos importância, a questão remanescente – ou seja, a terceira e mais relevante de todas as questões – é saber se o modelo doméstico de apreensão de mensagens de correio eletrónico em processos de contraordenação por práticas restritivas da concorrência está bem pensado e construído.

Cremos que a resposta deve ser negativa, designadamente à luz do Direito internacional regional (Direito europeu dos direitos humanos e Direito da União Europeia)[43] e do Direito estrangeiro (Direito norte-americano),

---

[41] Cf. Rui Cardoso, "Apreensão de correio eletrónico e registos de comunicações de natureza semelhante – artigo 17.º da Lei n.º 109/2009, de 15.IX", *Revista do Ministério Público,* 153 (2018), (pp. 167-214) p. 214.

[42] Cf. Rui Cardoso, *Revista Portuguesa de Direito Constitucional* 1 (2021), cit., pp. 157-161 e 165.

[43] Cf. Manuel Pelicano Antunes, "Prática restritiva da concorrência – busca e apreensão de mensagens de correio eletrónico pela Autoridade da Concorrência nas instalações das empresas por mandado do Ministério Público – o Acórdão do Tribunal Constitucional n.º 91/2023", *Revista do Ministério Público,* 176 (2023), (pp. 105-139) p. 105.

este último enquanto termo de comparação, salvaguardadas as diferenças entre todos e evitando soluções de puro transplante legal avulso[44]. Faz falta sobremaneira um regime legal que estabeleça a necessidade de controlo e triagem judicial *a posteriori* do conjunto das mensagens de correio eletrónico apreendidas, mas com nomeação pelo tribunal de um supervisor especial que ofereça garantias de independência em relação à AdC e às empresas visadas. Do ponto de vista técnico, importa que o controlo e a triagem judicial obedeçam aos requisitos da pesquisa eletrónica (*e-discovery*) assistida por ferramentas de inteligência artificial, designadamente para codificação preditiva (*predictive coding*) baseada em aprendizagem automática (*machine learning*) e suportada por modelos de linguagem de grande escala (*large language models*), quando o acervo digital apreendido assim o justificar em função de grandes volumes de dados (*big data*)[45].

[44] A designação de transplante legal (*legal transplant*), que refere um fenómeno indesejável por si mesmo, foi criada pelo especialista de história do Direito Alan Watson (1974) e adotada por todos os comparatistas a partir daí.

[45] Cf. Sean Broderick, Donna Lee Elm. Andrew Goldsmith, John Haried e Kiran Raj, *Criminal E-Discovery – A Pocket Guide for Judges*, 2.ª ed., Washington, DC: Federal Judicial Center, 2015, pp. 13-14 e *passim*.