Quaestio facti. Revista Internacional sobre Razonamiento Probatorio
Quaestio facti. International Journal on Evidential Legal Reasoning
Seccion: Ensayos
N. 2 | 2021 pp. 225-250
Madrid, 2021
DOI: 10.33115/udg_bib/qf.i2.22487
Marcial Pons Ediciones Jurídicas y Sociales

ISSN: 2604-6202
Recibido: 23/08/2019 | Aceptado: 15/12/2020 | Publicado: 29/01/2021

A PRIVACIDADE DIGITAL POSTA À PROVA NO PROCESSO PENAL

Paulo de Sousa Mendes[*]
Professor Catedrático da Faculdade de Direito
da Universidade de Lisboa
paulosousamendes@yahoo.com

RESUMO: o artigo 8.º da Convenção Europeia dos Direitos Humanos trata do respeito pela privacidade. O Quarto Aditamento à Constituição dos EUA trata igualmente do respeito pela privacidade. O processo penal deve assegurar a proteção da privacidade, na medida do possível, e o direito em ação deve respeitar os limites da cópia de dados eletrónicos e as restrições impostas à análise externa do acervo recolhido. Entre os aspetos críticos da análise externa de dados eletrónicos, avulta a questão do procedimento a adotar pelo investigador criminal diante dos conhecimentos fortuitos, uma questão que é analisada detalhadamente neste artigo. A jurisprudência do Tribunal Europeu dos Direitos Humanos caracteriza-se por alguma ineficácia na criação de remédios para a violação da privacidade no processo penal, designadamente no tocante à cópia de dados eletrónicos e à análise externa do acervo recolhido, desde logo porque não comina a exclusão das evidências produzidas por computador que tenham sido obtidas ilicitamente, o que deveria ser o caso, à luz do princípio do processo equitativo. O conhecimento das diretrizes e do direito jurisprudencial norte-america-

[*] O presente texto resultou da passagem a escrito de conferências proferidas pelo autor nos seguintes eventos: «The seizure of computer files and e-mails», no International Forum the Europeanization of Evidence Law in Transnational and Domestic Criminal Justice, Messina e Siracusa, Itália, 28 e 29 de maio de 2019; «La búsqueda de archivos informáticos y correos electrónicos», no Curso EJ – 1901, Las Garantías de Investigados y Acusados desde la Dimensión Europea (Buenas Prácticas Procesales), Barcelona, Espanha, 13, 14 e 15 de novembro de 2019; «Die Beschlagnahme von Computerdateien und E-Mails», organizada pelo Institut für Deutsches und Europäisches Strafprozessrecht und Polizeirecht der Universität Trier (ISP), na antiga Schwurgerichtssaal (Arbeits- und Sozialgericht, Dietrichstraße 13, Eingang Justizstraße), Trier, Alemanha, em 15 de janeiro de 2020.

no representa 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 da prática jurisprudencial.

PALAVRAS-CHAVE: conhecimentos fortuitos; doutrina jurisprudencial da visibilidade imediata; evidências produzidas por computador; mandado de busca digital; pesquisa externa; privacidade digital.

THE DIGITAL PRIVACY AT STAKE IN CRIMINAL JUSTICE

ABSTRACT: The article 8 of the European Convention on Human Rights deals with the need of respect for privacy. The 4th Amendment to the US Constitution addresses the same issue. The criminal procedure ensures the protection of privacy, as far as possible, and the praxis must recognize that, for privacy reasons, there should be limits to the seizure of computer records and to its off-site analysis. Among the critical aspects of the off-site analysis of electronic data, the approach to be adopted by the law enforcement officers in the face of serendipity findings largely remains an unanswered question. The doctrine of the European Court of Human Rights is characterized by some ineffectiveness in the creation of remedies for the violation of privacy in criminal proceedings, namely with regard to the search of data contained on computers and its off-site analysis, mainly because it does not order the exclusion of computer-generated evidence that has been illegally gathered, which should be the case, in the light of the fair trial principle. The knowledge of the North American case law and guidelines could represent a valuable contribution to the improvement of Strasbourg jurisprudence, in its decision-making role and also in its nomophylactic function, as well as to the improvement of European national legal systems at the legislative level and at the level of decision-making processes.

KEYWORDS: computer-generated evidence; digital search warrant; off-site search; plain view doctrine; privacy; seizure by chance.

RECOMMENDED CITATION: SOUSA MENDES, PAULO DE, 2020: «A privacidade digital posta à prova no processo penal», in *Quaestio facti*, 2: 225-250. Madrid: Marcial Pons Ediciones Jurídicas y Sociales. DOI: http://dx.doi.org/10.33115/udg_bib/qf.i2.22487

1. INTRODUÇÃO

A migração para o ciberespaço origina novas ameaças à privacidade, desde logo porque todas as facetas da vida ficam expostas de forma nunca antes vista no mundo físico.

O processo penal acompanha a migração para o ciberespaço, desde a desmaterialização dos autos até à audição de testemunhas por videoconferência eletrónica. No presente texto, interessa-nos sobremaneira a recolha, a custódia e a análise da prova digital. Em processos por delitos económicos e financeiros a prova é quase totalmente digital. Os documentos que servem de meios de prova são digitais. Dada a imensa informação potencialmente acumulada em bits e bytes por comparação com o mundo físico, cabe então perguntar qual é a proteção da privacidade que resta no domínio da prova digital?

A pergunta é feita tanto à luz do artigo 8.º da Convenção Europeia dos Direitos Humanos e da jurisprudência de Estrasburgo como diante do Quarto Aditamento à Constituição dos Estados Unidos da América e do correspondente direito jurisprudencial (*case law*). As soluções aí encontradas ajudarão a resolver o mesmo problema jurídico ao nível de cada ordenamento nacional, quanto mais não seja porque assistimos a uma hibridização do processo penal, ademais incrementada na ciberrealidade em que vivemos.

2. O DIREITO À PRIVACIDADE DIGITAL NA JURISPRUDÊNCIA DE ESTRASBURGO

O artigo 8.º da Convenção Europeia dos Direitos Humanos (doravante, a Convenção) impõe o respeito pela privacidade. Mais exatamente, o artigo 8.º, n.º 1, da Convenção protege o direito ao respeito da vida privada e familiar, do domicílio e da correspondência.

A privacidade é um conceito mais vasto do que parece. Realmente, o Tribunal Europeu dos Direitos Humanos (doravante, o TEDH) tem vindo a fazer uma interpretação extensiva da Convenção, aplicando o artigo 8.º à proteção da informação guardada em servidores, computadores, ficheiros informáticos e e-mails, como aconteceu nos casos *Leander v Sweden* (1987)[1], *Amann v Switzerland* (2000)[2], *Rotaru v Romania* (2000)[3], *Copland v United Kingdom* (2007)[4] e *Wieser and Bicos Beteiligungen GmbH v Austria* (2007)[5]. Além de que tem alargado o conceito de privacidade

[1] *Leander v Sweden* (queixa n.º 9248/81), de 26 de março de 1987, § 48.
[2] *Amann v Switzerland* (queixa n.º 27798/95), de 16 de fevereiro de 2000, § 65.
[3] *Rotaru v Romania* (queixa n.º 28341/95), de 4 de maio de 2000, §§ 42-43.
[4] *Copland v United Kingdom* (queixa n.º 62617/00), de 3 de abril de 2007.
[5] *Wieser and Bicos Beteiligungen GmbH v Austria* (queixa n.º 74336/01), de 16 de janeiro de 2007, § 45.

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)[6]. Geralmente, o TEDH basta-se com uma ou duas frases de fundamentação para declarar essa proteção, como aconteceu no caso *Copland v United Kingdom* (2007): «§ 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 e-mails enviados do trabalho devem igualmente ser protegidos pelo artigo 8.º, assim como as informações recolhidas através de monitoramento do uso pessoal da Internet»[7].

Seja como for, a proteção da privacidade não é absoluta. Existem situações em que a autoridade pública pode interferir no direito ao respeito pela vida privada e familiar, pelo lar e pela correspondência. Nos termos do n.º 2 do artigo 8.º da Convenção, a ingerência só é permitida, porém, quando estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, a segurança pública, o bem-estar económico do país, a defesa da ordem e a prevenção das infrações penais, 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 Convenção 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[8].

Ainda não há muitos acórdãos do TEDH que tratem da aplicação do artigo 8.º da Convenção à prova digital no processo penal, mas já há os suficientes para se tirar um retrato da jurisprudência de Estrasburgo a tal respeito[9]. Selecionámos um que consideramos especialmente representativo, a saber: o caso *Sérvulo v Portugal* (2015)[10].

---

[6] *Société Colas Est and other v France* (queixa n.º 37971/97), de 16 de abril de 2002, § 40.

[7] Em língua original (*Copland v United Kingdom* (2007)): «§ 41. *According to the Court's case-law, telephone calls from business premises are* prima facie *covered by the notions of 'private life' and 'correspondence' for the purposes of Article 8 § 1* (*see* Halford*, cited above,* § 44 *and* Amann v. Switzerland [*GC*]*, no. 27798/95,* § 43*, ECHR 2000 II*)*. It follows logically that e-mails sent from work should be similarly protected under Article 8, as should information derived from the monitoring of personal internet usage*».

[8] De Hert / Gutwirth, 2009: 15-17.

[9] 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; *Trabajo Rueda v Spain* (queixa n.º 32600/12), de 30 de maio de 2017; e *Ivashchenko v Russia* (queixa n.º 61064/10), de 13 de maio de 2018.

[10] *Sérvulo & Associados – Sociedade de Advogados, Rl v Portugal* (queixa n.º 27013/10), de 3 de setembro de 2015.

2.1. O caso Sérvulo & Associados – Sociedade de Advogados, RL e Outros vs. Portugal (2015)

No caso *Sérvulo v Portugal* (2015), o TEDH considerou, por maioria (6 votos contra 1), que o artigo 8.º da Convenção não foi violado. O caso dizia respeito a uma busca em escritório de advogados e à apreensão de ficheiros e mensagens alojados nos servidores da sociedade e nos computadores de secretária usados por alguns dos seus advogados, no âmbito de dois processos penais, instaurados pelo Ministério Público do Departamento Central de Investigação e Ação Penal (DCIAP), em 2006, relativamente a crimes de corrupção, participação económica em negócio, branqueamento e prevaricação conexos com a compra, em 2004, de dois submarinos pelo Governo português a um consórcio alemão [11]. Nem a sociedade, nem os respetivos advogados eram arguidos nos mencionados processos, embora um antigo advogado dessa sociedade tenha sido, de facto, constituído arguido em 29 de setembro de 2009, anteriormente às diligências de busca e apreensão [12]. O TEDH concluiu que a apreensão de ficheiros informáticos e mensagens de correio eletrónico no escritório de advocacia havia sido efetuada com garantias processuais suficientes contra eventuais abusos, arbitrariedades ou violações do sigilo profissional de advogado [13].

O despacho do juiz de instrução e respetivos mandados autorizavam o acesso aos servidores e computadores em que pudessem encontrar-se os documentos eletrónicos

---

[11] Cabe aqui antecipar que o primeiro processo terminaria arquivado pelo Ministério Público do DCIAP, em 17 de dezembro de 2014, e o segundo processo terminaria com a absolvição de todos os arguidos pelo Tribunal da Relação de Lisboa (TRL), em 19 de março de 2015, confirmando a decisão de primeira instância, de 14 de fevereiro de 2014. Veja-se, a propósito, *Sérvulo v Portugal* (queixa n.º 27013/10), de 3 de setembro de 2015, §§ 45-48.

[12] Em 6 de outubro de 2009, um dos advogados da sociedade acabaria sendo constituído arguido, após a busca e precisamente por causa desta, por se ter descoberto que também teria acompanhado as negociações que constituíam o alvo dos inquéritos criminais então em curso. Em 19 de outubro de 2009, esse mesmo advogado requereu ao juiz de instrução do Tribunal Central de Investigação Criminal (TCIC) a declaração de nulidade da sua constituição como arguido, alegando que não fora ouvido nessa qualidade, nem fora informado dos factos que lhe eram imputados, sendo que o único móbil da sua constituição como arguido teria sido justificar a apreensão dos dados armazenados no seu computador. Por despacho de 3 de novembro de 2009, o juiz de instrução do TCIC indeferiu o pedido de declaração de nulidade da constituição de arguido, tendo o advogado, na sequência, interposto recurso para o TRL. Por acórdão de 15 de abril de 2010, o TRL revogou o despacho recorrido, considerando que a constituição do advogado como arguido tinha sido ilegal, anulando essa constituição e ordenando a restituição de toda a correspondência referente a ele que havia sido apreendida. Cabe aqui reproduzir o trecho mais representativo da decisão: «[...] não é a apreensão de documentação profissional num escritório de advogados que permite fundamentar a constituição do advogado como arguido, antes sendo a constituição de um advogado como arguido que abre a possibilidade de apreensão de correspondência profissional do mesmo» (Ac. TRL 15/04/2010, proc. n.º 56/06.2TELSB-B.L1-9, Relator: Fátima Mata-Mouros). Online: http://www.dgsi.pt/jtrl.nsf/e6e1f17fa82712ff80257583004e3ddc/fdc745090a69eaa18025770b003dd2eb?OpenDocument (consultado em 03/08/2020). Este acórdão também é citado e, ademais, elogiado por Costa Ramos / Pinto de Abreu / Cordeiro, 2020: 257, n. 59.

[13] Press Release issued by the Register of the Court – ECHR 267 (2015), 03/09/2015.

relacionados com as negociações de compra dos submarinos. Os documentos eletrónicos deveriam ser selecionados através de pesquisa por meio de 35 palavras-chave indicadas na promoção do Ministério Público, tais como, por exemplo, nomes de bancos e personalidades ou palavras genéricas como *spread* ou *swap*. Os documentos eletrónicos sinalizados pelo emprego das palavras-chave deveriam ser copiados para um suporte digital autónomo e apresentados ao juiz de instrução para levantamento do sigilo profissional e validação da apreensão, se fossem relevantes para a investigação em curso. No final das contas, o juiz de instrução ordenou que se fizesse a juntada aos autos de 89.000 ficheiros de computador e 29.000 mensagens de correio eletrónico [14].

O TEDH decidiu que não ocorrera qualquer violação do artigo 8.º da Convenção, considerando que: *a)* a ingerência no direito ao respeito da vida privada ocorrida no caso concreto estava prevista por lei, ainda que nenhuma lei previsse especificamente as pesquisas e as apreensões em sistemas informáticos, o que só veio a suceder posteriormente, com a entrada em vigor da Lei n.º 109/2009, de 15 de setembro [15]; *b)* as buscas e apreensões visavam um fim legítimo, pois foram autorizadas no âmbito de um inquérito relativo à prática de crimes de corrupção, participação económica em negócio, branqueamento e prevaricação e, por conseguinte, tinham em vista a repressão de infrações penais [16]; *c)* a ingerência era necessária numa sociedade democrática, enquanto necessidade social imperiosa e proporcional ao fim legítimo visado, dado que as buscas e apreensões em escritório de advogados foram autorizadas e presididas por um juiz, foram sujeitas a controlo adicional por via da intervenção do Vice-Presidente do TRL e contaram com a presença de observadores independentes, designadamente o representante do Ordem dos Advogados (OA) [17]; *d)* apesar de entre as palavras-chave utilizadas na pesquisa informática estarem termos correntes num escritório de advocacia especializado em áreas de negócio, incluindo contratação pública, as mesmas eram proporcionais ao fim legítimo visado e a lei portuguesa contém garantias processuais suficientes contra eventuais abusos, arbitrariedades e restrições do sigilo profissional de advogado, que foram observadas no caso concreto através da autorização e intervenção do juiz de instrução e da ulterior reclamação para o Vice-Presidente do TRL [18]; *e)* ainda que apenas existisse um juiz no TCIC, o mesmo interveio apenas na qualidade de garante das liberdades individuais, para controlar a legalidade das buscas e apreensões e proteger o sigilo profissional, não tendo competência para iniciar uma investigação, sendo o alegado a este respeito pelos queixosos insuficiente para gerar dúvidas fundadas acerca da eficácia do controlo por ele exercido [19].

---

[14] *Sérvulo v Portugal* (2015), *cit.*, § 13.
[15] *Sérvulo v Portugal* (2015), *cit.*, § 96.
[16] *Sérvulo v Portugal* (2015), *cit.*, § 97.
[17] *Sérvulo v Portugal* (2015), *cit.*, § 100.
[18] *Sérvulo v Portugal* (2015), *cit.*, § 111.
[19] *Sérvulo v Portugal* (2015), *cit.*, § 119.

O juiz *ad-hoc* português (Saragoça da Matta), discordando da maioria, considerou que ocorrera uma violação do artigo 8.º da Convenção, por várias razões, que disse não se basearem na avaliação da lei portuguesa, mas resultarem antes da aplicação da Convenção aos factos do caso, a saber, entre outras: *a)* não ser admissível que, para recuperar os documentos desaparecidos do Ministério da Defesa, as autoridades judiciárias escolhessem uma diligência intrusiva, ademais muito ampla, contra um escritório de advocacia e sem agirem contra os responsáveis pela irregularidade praticada dentro do próprio Ministério[20]; *b)* não ser admissível a realização de uma pesquisa informática com base numa lista de 35 palavras-chave que incluía palavras que fazem parte do jargão de escritórios de advocacia, para além de nomes de bancos e personalidades, pois o objeto da pesquisa de dados informáticos deveria ter sido delimitado de uma forma muito mais rigorosa, ponderando as necessidades da investigação e os contrapostos direitos dos advogados e dos seus clientes[21]; *c)* ainda que as garantias processuais contra eventuais arbitrariedades e restrições excessivas do sigilo profissional de advogado previstas pela lei portuguesa sejam adequadas, em abstrato, apenas ficou demonstrado que o procedimento previsto na lei foi seguido, mas não que as garantias tenham sido efetivas (designadamente quanto à salvaguarda do sigilo profissional) quanto a outros clientes do escritório cujos documentos, ficheiros informáticos e e-mails foram apreendidos e posteriormente transferidos para utilização noutro processo[22]; *d)* tendo em conta o elevado número de mensagens de correio eletrónico apreendidas, só se poderia concluir que a pesquisa fora, de facto, desproporcional em relação ao fim prosseguido[23]; *e)* não se poderia dizer que, no caso concreto, os receios manifestados pelos queixosos contra o juiz de instrução fossem infundados, dado que a sua intervenção teria sido, na melhor das hipóteses, meramente formal[24]; *f)* os elementos apreendidos irrelevantes não foram devolvidos aos queixosos, mas foram abusivamente emprestados para valoração noutros processos[25]. Assim sendo, o juiz dissidente concluiu que o TEDH deveria ter reconhecido a violação do artigo 8.º da Convenção.

O caso *Sérvulo v Portugal* tem características que o tornam notado, mas não necessariamente por a decisão de Estrasburgo concitar o aplauso da doutrina académica, antes pelo contrário. Alguma doutrina refere que a presente decisão de Estrasburgo é ilustrativa da necessidade de estabelecer padrões e proteções adequados à salvaguarda da confidencialidade entre o advogado e o cliente (*lawyer-client confidentiality*)[26]. O privilégio da confidencialidade entre o advogado e o seu cliente é um domínio especial do direito à privacidade, à luz da jurisprudência de Estrasburgo. Por isso

---

[20] *Sérvulo v Portugal* (2015), *cit.*, Opinião Dissidente, III/1.
[21] *Sérvulo v Portugal* (2015), *cit.*, Opinião Dissidente, III/2.
[22] *Sérvulo v Portugal* (2015), *cit.*, Opinião Dissidente, III/3.
[23] *Sérvulo v Portugal* (2015), *cit.*, Opinião Dissidente, III/3.
[24] *Sérvulo v Portugal* (2015), *cit.*, Opinião Dissidente, III/6.
[25] *Sérvulo v Portugal* (2015), *cit.*, Opinião Dissidente, III/7.
[26] Bachmaier Winter / Thaman, 2020: 57.

mesmo, estranhamos que a decisão do caso Sérvulo *vs.* Portugal (2015) espelhe uma tão grande tolerância do TEDH com a devassa em larga escala de ficheiros informáticos e mensagens de correio eletrónico cobertos pelo segredo profissional da advocacia. A propósito, cabe aqui a comparação com o procedimento adotado no mundo anglo-saxónico. Em Inglaterra e Gales, assim como nos Estados Unidos da América (doravante, os EUA), existe um procedimento especial para buscas em escritórios de advocacia quando o objetivo seja a apreensão de documentos protegidos por segredo profissional[27]. Nestes casos, a preferência das autoridades vai para a solicitação dos documentos sob cominação de desobediência (*subpoena*)[28]. Tão-somente em situações de emergência, seja porque o advogado recuse o envio dos documentos requisitados ou porque atue em colusão com o cliente na prática de factos puníveis, é legítimo promover a obtenção de um mandado de busca (*search warrant*) junto de um juiz (*Magistrate Judge*) com vista à entrada no escritório de advocacia. Ainda assim, os inspetores devem começar por informar o advogado de que poderá entregar os documentos antes de se iniciarem as diligências de busca e apreensão no seu escritório[29].

À parte a questão do segredo profissional do advogado, a decisão de Estrasburgo no caso *Sérvulo v Portugal* surpreende também pela tolerância com a utilização da lista de 35 palavras-chave de uso corrente num escritório de advocacia especializado em áreas de negócio e contratação pública. Parece que a mera utilização de palavras-chave é considerada pelo TEDH como uma garantia contra abusos e arbitrariedades, ao reduzir o universo da pesquisa informática. Mas a utilização de palavras-chave garante sobretudo a eficientização da mineração de dados do ponto de vista das autoridades de investigação criminal. Seja como for, a utilização de palavras-chave não permite, só por si, joeirar as falsas correspondências, trazendo dados irrelevantes para o acervo probatório acolhido nos autos do processo. Acresce que a possibilidade de falsas correspondências aumenta na razão direta da maior vagueza das palavras-chave escolhidas. Não se deve, pois, perder de vista que os dados irrelevantes para a investigação configuram, do mesmo passo, uma devassa abusiva e arbitrária para os visados. Tão-pouco a utilização de palavras-chave elimina a possibilidade de conhecimentos fortuitos. Neste contexto, os conhecimentos fortuitos acabam sendo acreditados ilimitadamente para utilização em outros processos, em curso ou a instaurar. Foi, aliás, o que aconteceu no caso *Sérvulo v Portugal*, em que —tal como foi destacado no voto dissidente— os elementos apreendidos que eram irrelevantes para a investigação que justificara a diligência intrusiva no escritório da advocacia não foram devolvidos aos queixosos, mas foram emprestados para valoração noutros processos. Cabe aqui perguntar se não devem existir regras estritas quanto à possibilidade do aproveitamento de conhecimentos fortuitos por parte das autoridades de investigação criminal. O requisito da previsão legal do aproveitamento de conhecimentos fortuitos, enquanto ingerência das autoridades de investigação criminal na esfera do direito à privacidade

[27] Bachmaier Winter / Thaman, 2020: 57-58.
[28] Bachmaier Winter / Thaman, 2020: 57.
[29] Bachmaier Winter / Thaman, 2020: 57-58.

de qualquer pessoa, nos termos do n.º 2 do artigo 8.º da Convenção, não se verificava à data das buscas no escritório de advocacia, uma vez que o regime legal das buscas e apreensões é omisso a tal respeito[30]. O TEDH revela insensibilidade quanto à excecionalidade do aproveitamento de conhecimentos fortuitos.

2.2. 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 garantístico na Europa, à luz da Convenção[31]. 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[32]. Na verdade, 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 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[33].

No tocante à violação do artigo 8.º da Convenção, 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*)[34], à luz do artigo 6.º da Convenção, desde que ao acusado, no caso concreto, tenham sido dadas oportunidades de contestar a prova

---

[30] Veja-se os artigos 174.º a 186.º do Código de Processo Penal (CPP) português. A possibilidade do aproveitamento de conhecimentos fortuitos só está contemplada para as escutas telefónicas e respetivas extensões, nos termos do n.º 7 do artigo 187.º do CPP, na redação da Lei n.º 48/2007, de 29 de agosto. Na atual Lei n.º 109/2009, de 15 de setembro (vulgo: Lei do Cibercrime), também não há previsão do aproveitamento de conhecimentos fortuitos fortuitos, salvo por remissão do n.º 4 do artigo 18.º para o regime das escutas telefónicas.

[31] Kostoris, 2014: 44-60.

[32] Os atuais 47 Estados-Membros do Conselho da Europa.

[33] Sousa Mendes, 2020: 2365.

[34] Costa Ramos, 2017: 742.

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 Convenção[35]. Sendo assim, 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 Convenção[36]. 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[37]. Vamos, pois, 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[38]. 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[39].

---

[35] Costa Ramos, 2017: 756. Segundo a autora citada, o único caso em que o TEDH teria decidido no sentido de ser excluída a prova obtida em violação do artigo 8.º da Convenção (embora este artigo não fosse expressamente mencionado), por a sua utilização ser violadora do artigo 6.º da Convenção, foi o caso *Lisica v Croatia* (queixa n.º 20100/06), de 25 de fevereiro de 2010, §§ 60-62.

[36] Costa Ramos, 2017: 757.

[37] Jahn, 2014: 5-9.

[38] Costa Ramos, 2017: 760, n. 72.

[39] Diversamente, a recolha de prova em processo penal que viole a proibição convencional da tortura (artigo 3.º da Convenção) deve, na ótica do TEDH, implicar a impossibilidade de utilização dessa prova, abstraindo de quaisquer ponderações de interesses. Assim, a utilização de prova ilicitamente obtida em violação do artigo 3.º da Convenção tem levado o TEDH à consideração de que o processo em causa foi desleal (*unfair*). Neste sentido, Costa Ramos, 2017: 760.

3. O DIREITO À PRIVACIDADE DIGITAL NO DIREITO JURISPRUDENCIAL DOS ESTADOS UNIDOS DA AMÉRICA

O Quarto Aditamento à Constituição dos EUA declara que o direito do povo à inviolabilidade de suas pessoas, casas, papéis e haveres contra busca e apreensão arbitrárias não poderá ser infringido; e nenhum Mandado será expedido a não ser mediante 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 apreendidas[40].

O Quarto Aditamento à Constituição dos EUA oferece uma proteção substantiva maior do que a do artigo 8.º da Convenção, porquanto limita 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 uma probabilidade razoável de descoberta de provas relacionadas com um crime (*probable cause*) e haver uma promoção formal 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 indicando qual o fundamento daquela probabilidade razoável[41]. O artigo 8.º da Convenção não exige causa provável, nem mandado, mas exige, mais vagamente, que qualquer ingerência da autoridade pública na privacidade venha prevista na lei e constitua uma providência necessária numa sociedade democrática.

O Supremo Tribunal dos EUA (*Supreme Court of the United States*) adotou a regra de exclusão relativa a buscas e apreensões ilegais (*search and seizure exclusionary rule*) no caso *Weeks v United States* (1914)[42] e tornou-a aplicável não apenas ao nível federal, mas também ao nível estadual no caso *Mapp v Ohio* (1961)[43]/[44]. Se quisermos, a regra de exclusão funciona num plano equivalente ao da proibição de valoração de prova[45]. A proibição de produção de prova, por sua vez, encontra-se no Quarto Aditamento à Constituição dos EUA, que, como vimos, proíbe as buscas e apreensões injustificadas (*unreasonable searches and seizures*) e sem mandado judicial. Compare-se com a violação do artigo 8.º da Convenção, relativamente à qual a jurisprudência do TEDH, lamentavelmente, não comina quaisquer regras de exclusão da prova.

---

[40] Em língua original (*Fourth Amendment of the U.S. Constitution*): «*The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized*».

[41] Há várias exceções à exigência de mandado judicial, mas não relevam imediatamente para a discussão. Oportunamente voltaremos a este ponto no próprio texto.

[42] *Weeks v United States*, 232 U.S. 383, 34 S.Ct. 341, 58 L.Ed. 652 (1914).

[43] *Mapp v Ohio*, 367 U.S. 643 (1961).

[44] Sobre os antecedentes, a evolução e o conteúdo da regra de exclusão relativa a buscas e apreensões ilegais, LaFave, 2004 (vol. 1): 3-26, LaFave, 2011-2012 (Pocket Part): 1-101 e Kamisar, 2003: 121-140.

[45] Ambos, 2010: 19.

3.1. As Diretrizes Federais para Busca e Apreensão de Computadores (2009)

Em 1994, o Departamento de Justiça publicou as Diretrizes Federais para Busca e Apreensão de Computadores (*Federal Guidelines for Searching and Seizing Computers*) [46]. As Diretrizes foram atualizadas através de Suplementos (*Supplements*), em 1997 e 1999, e foram 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*), publicado em 2001 e amplamente revisto em 2009 [47].

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 (*search warrant*) [48]. 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* [49]. Se a causa provável que justificou a diligência estiver relacionada apenas com certas informações, então o mandado deve descrever as informações a ser apreendidas e autorizar a sua apreensão em qualquer suporte em que possam ser armazenadas, seja eletrónico ou não [50]/[51]. 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*) [52],

---

[46] *Online*: https://epic.org/security/computer_search_guidelines.txt (consultado em 11/08/2020).

[47] *Online*: https://www.justice.gov/criminal-ccips/ccips-documents-and-reports (consultado em 11/08/2020).

[48] *Guidelines* 2009, p. 72.

[49] Naturalmente, o mandado judicial não precisa de ser excessivamente técnico (*overly technical*), podendo seguir uma visão de senso comum (*commonsensical*) e uma abordagem prática (*practical*) para descrever genericamente o tipo de equipamentos que podem ser apreendidos. Veja-se *United States v Ventresca*, 380 U.S. 102, 108 (1965).

[50] As anteriores Diretrizes de 2001 recomendavam, como um dos modos possíveis de executar pesquisas em computadores (II.B.1. *Basic Strategies for Executing Computer Searches*), a pesquisa no local e a impressão de ficheiros específicos nesse momento («[s]earch the computer and print out a hard copy of particular files at that time»), mas as Diretrizes de 2009 já não mencionam expressamente esta possibilidade.

[51] *Guidelines* 2009, p. 70.

[52] «[A copy that] duplicates every bit and byte on the target drive including all files, the slack space, Master File Table, and metadata in exactly the order they appear on the original». Veja-se *United States v Vilar*, 2007 WL 1075041, *35 n.22 (S.D.N.Y. Apr. 4, 2007) e *United States v Stierhoff*, 477 F. Supp. 2d 423, 439 & n.8 (D.R.I. 2007). Do ponto de vista técnico, o curso de ação recomendável implica que se comece por preservar uma cópia forense do ambiente informático antes de se iniciar qualquer pesquisa, a fim de prevenir a contaminação ou destruição de evidências. As ferramentas forenses convencionais

feita ou não no local[53], 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[54]. Mas o mandado judicial não pode simplesmente autorizar uma pesquisa e apreensão de «todos os registos» («all records»)[55], sob pena de ser um mandado genérico inconstitucional (*unconstitutional general warrant*)[56]. 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-crime 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 evidências que caibam no escopo de um mandado judicial[57].

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)[58] do Regulamento Federal de Processo Penal (*Federal Rules of Criminal Procedure*)[59]. Se o equipamento for apenas um dispositivo de armazenamento de evidências, os agentes de autoridade pública podem, a título excecional, apreendê-lo só se não existirem alternativas menos disruptivas[60].

---

oferecem a capacidade de criar cópias precisas e infalseáveis (graças à atribuição de valores *hash*), contendo todas as características do ambiente original, incluindo a informação sobre os ficheiros excluídos e o espaço no disco rígido ou no servidor de rede ainda não alocado a qualquer ficheiro.

[53] Em alguns casos, os agentes de autoridade pública fazem a cópia de imagem no local; em outros, apreendem o *hardware* do computador e fazem a cópia da imagem fora do local, mas tal é admissível somente se constar da promoção quais os constrangimentos práticos e técnicos que requerem este procedimento, conforme é referido nas *Guidelines* 2009, p. 78.

[54] *Guidelines* 2009, p. 76.

[55] *United States v Ford*, 184 F.3d 566, 576 (6th Cir. 1999), citando casos, e *In re Grand Jury Investigation Concerning Solid State Devices, Inc.*, 130 F.3d 853, 857 (9th Cir. 1997). Também relevante: *United States v Fleet Management Ltd.*, 521 F. Supp. 2d 436, 443-44 (E.D. Pa. 2007).

[56] *Guidelines* 2009, p. 73.

[57] *Guidelines* 2009, pp. 80-81.

[58] Em língua original (*Fed. R. Crim. P.* 41(c). Persons or Property Subject to Search or Seizure): «*A warrant may be issued for any of the following: (1) evidence of a crime; (2) contraband, fruits of crime, or other items illegally possessed; (3) property designed for use, intended for use, or used in committing a crime; or (4) a person to be arrested or a person who is unlawfully restrained*».

[59] 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.

[60] *United States v Tamura*, 694 F.2d 591, 595 (9th Cir. 1982).

As restantes possibilidades remetem a pesquisa do equipamento 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 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. 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 à luz das Diretrizes de 2009.

As Diretrizes de 2009 enfatizam a importância de os agentes 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[61]. Por consequência, a garantia (*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[62]. Independentemente de o mandado judicial permitir expressamente a pesquisa fora do local, se forem copiados elementos digitais para posterior pesquisa fora do local, o auto de busca e apreensão deve então pormenorizar os factos e as circunstâncias que impuseram um tal procedimento.

3.2. Pesquise antes de apreender ou…

Se os documentos armazenados em equipamentos informáticos estivessem em formato de papel, a seleção exigiria que os inspetores (*officers*) analisassem milhentos 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 da investigação criminal poderiam ter de ocupar as instalações durante várias horas ou mesmo dias[63].

A migração para o ciberespaço veio, sem dúvida, facilitar a vida às autoridades públicas, de tal sorte que a simples possibilidade de fazerem a pesquisa de documentos

---

61 *Guidelines* 2009: 61-86.
62 Berman, 2018: 53.
63 Brenner / Frederiksen, 2002: 59.

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 viável, porém, se as autoridades públicas tiverem de antemão uma perceção rigorosa das evidências de que estão à procura, uma espécie de evidência conclusiva —vulgo, a «*smoking gun evidence*»— do delito sob investigação, que, por exemplo, lhes tenha sido revelada com exatidão por um denunciante. Nestes casos, o procedimento de utilização de palavras-chave é preferível para todos. Por um lado, é preferível para as autoridades públicas, 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.

Do ponto de vista técnico, o curso de ação recomendável implica que se comece por preservar uma cópia forense do ambiente informático antes de se iniciar qualquer pesquisa, a fim de prevenir a contaminação ou destruição de evidências. As ferramentas forenses convencionais oferecem a capacidade de criar *back-ups* precisos e infalseáveis, graças à atribuição de valores *hash*, que contenham todas as características do ambiente original, incluindo a informação sobre os ficheiros excluídos e o espaço no disco rígido ou no servidor de rede ainda não alocado a qualquer ficheiro[64].

3.3. Apreenda primeiro e depois logo se vê

Não sendo possível realizar a pesquisa de documentos em equipamentos informáticos em tempo real e no local da busca, então resta a alternativa entre usar palavras-chave (*key-words*) para copiar ficheiros individuais ou fazer uma cópia integral (*mirror-image copy*) do disco rígido ou do servidor de rede[65]. Mas as Diretrizes de 2009 enfatizam que fazer uma cópia eletrónica de uma unidade inteira é bem diferente de fazer uma cópia eletrónica de ficheiros individuais. Esta última reduz não só o tempo necessário para a posterior seleção de possíveis evidências, 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, por intermédio de palavras-chave, a apreensão de documentos em computadores independentes, servidores de rede ou armazenamento em nuvem. A utilização de palavras-chave automatizadas tem a vantagem de ser relativamente célere e cirúrgica. Porém, as palavras-chave são insensíveis ao contexto e ficam muito

[64] Brenner / Frederiksen, 2002: 63-65.
[65] Bartholomew, 2014: 1034-1036 e Berman, 2018: 92-93.

aquém da capacidade de discriminação típica de um investigador humano[66]. 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[67].

3.4. A pesquisa externa

A questão agora é saber se o Quarto Aditamento 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[68]. 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*)[69], que, por certo, oferece mais garantias de independência em relação ao poder executivo[70]/[71]. Poderá ainda tornar-se necessária a intervenção de um juiz especial (*special Magistrate Judge*)[72].

O Departamento de Justiça 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 evidências essenciais. Este é, certamente, um argumento válido, desde que se demonstre que a destruição de evidências estaria, de facto, iminente[73]. A segunda é a necessidade de envolver técnicos de informática (*computer experts*) na pesquisa para evitar a contaminação ou destruição de evidências essenciais, o que normalmente só é possível fazer com segurança e tranquilidade fora das instalações buscadas[74].

---

[66] Moshirnia, 2010: 624-626.

[67] Brenner / Frederiksen, 2002: 60-62.

[68] Berman, 2018: 52.

[69] Veja-se o Manual do Procurador dos Estados Unidos (*United States Attorney's Manual* – USAM, section 9-13.420).

[70] Veja-se o recente caso *United States v Gallego*, No. 4:18- cr-01537, 2018 U.S. (Dist. Ariz.).

[71] Assinalando, porém, as dificuldades postas pela criação destas equipas provisórias, designadamente relacionadas com a sua falta de acurácia, veja-se Mantei, 2011: 1000.

[72] Brenner / Frederiksen, 2002: 105.

[73] Brenner / Frederiksen, 2002: 68.

[74] Brenner / Frederiksen, 2002: 69.

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 usadas e as precauções que serão tomadas para garantir que a pesquisa respeite o objeto do mandado judicial. O próprio mandado judicial deve indicar os delitos visados, revelando o máximo de pormenores e, se forem necessárias palavras-chave, listando os 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[75].

3.5. 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 do Quarto Aditamento à Constituição dos EUA[76]. 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*)[77]. 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[78]. 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 deve 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, [deve fornecer] uma probabilidade razoável para crer que exista uma conexão entre a evidência e alguma atividade criminosa"»[79].

---

[75] Brenner / Frederiksen, 2002: 102-104.

[76] Clancy, 2005: 208 e Kerr, 2005: 532.

[77] Brenner / Frederiksen, 2002: 41, Chang, 2007: 33-34, Ward, 2011: 1170-1179, Bartholomew, 2014: 1033, Silva Ramalho, 2014: 93-146, Berman, 2018: 53 e Wittler Contardo, 2020: 305-306.

[78] Veja-se os casos *Coolidge v New Hampshire*, 403 U.S. 443, 465 (1971) e *Horton v California*, 496 U.S. 128, 134 (1990).

[79] Em língua original (*State v Guy*, 172 Wis.2d 86, 101-02, 492 N.W.2d 311 (1992), citando *State v Washington*, 134 Wis.2d 108, 121, 396 N.W.2d 156 (1986), que citava *Bies v State*, 76 Wis.2d 457, 464, 251 N.W.2d 461 (1977)): «(1) *the evidence must be in plain view;* (2) *the officer must have a*

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 informático só pode ser visto se for aberto. Aquilo que se vê imediatamente é apenas o nome do ficheiro, que pode nem ser revelador do respetivo conteúdo. Esta dificuldade tem dado azo a uma rica casuística no direito jurisprudencial norte-americano [80]. De seguida, oferecemos uma imagem, a voo de pássaro, da referida casuística através de dois casos paradigmáticos.

3.6. O caso Estados Unidos vs. Carey (1999)

O caso *United States v Carey* (1999) é paradigmático das dificuldades de aplicação da doutrina jurisprudencial da visibilidade imediata às evidências geradas por computador [81].

Patrick J. Carey foi acusado de posse de um disco rígido de computador que continha três ou mais imagens de pornografia infantil resultantes de materiais adquiridos no mercado ilícito. Após um reconhecimento parcial de culpabilidade (*conditional plea of guilty*), o réu recorreu da decisão do tribunal distrital que indeferira a sua moção para exclusão do material retirado do seu computador, alegando que o mesmo fora apreendido como resultado de uma busca geral sem mandado. O Tribunal de Apelação do Décimo Circuito dos Estados Unidos da América (*United States Court of Appeals, Tenth Circuit*) decidiu, em 14 de abril de 1999, que a moção do réu devia ser deferida e reverteu a decisão do tribunal recorrido [82].

Carey estava sob investigação, havia já algum tempo, por possível venda e posse de cocaína. A polícia obteve um mandado para detê-lo em sua residência. Durante a execução do mandado de detenção, os agentes de autoridade observaram, bem à vista no apartamento do visado, um dispositivo normalmente utilizado para fumar marijuana (*bong*) e o que parecia ser droga. Alertado por esses itens, um dos agentes solicitou a Carey que consentisse na busca domiciliária. O agente disse que conseguiria um mandado de busca se Carey recusasse a permissão. Após uma discussão considerável com o agente, Carey consentiu verbalmente e mais tarde assinou um consentimento formal na esquadra de polícia. Receando que os agentes «destruíssem» o seu apartamento durante a busca, Carey deu-lhes indicações sobre onde poderiam encontrar evidências da venda e posse de drogas. Os agentes também apreenderam dois computadores, pois acreditavam que poderiam conter evidências

---

prior justification for being in the position from which [*he or*] *she discovers the evidence in 'plain view';* (3) *the evidence seized* '*in itself or itself with facts known to the officer at the time of the seizure,* [*must provide*] *probable cause to believe there is a connection between the evidence and criminal activity*'».

[80] Brenner / Frederiksen, 2002: 94, Moshirnia, 2010: 612, Berman, 2018: 59-60 e Wittler Contardo, 2020: 302-306.

[81] *United States v Carey*, 172 F.3d 1268 (10th Cir. 1999).

[82] *United States v Carey* (1999), *cit*., § I.

de tráfico de drogas. Os computadores foram levados para a esquadra da polícia e os agentes obtiveram um mandado judicial que lhes permitia pesquisar ficheiros nos computadores em busca de nomes, números de telefone, recibos de contabilidade, endereços e outras evidências documentais relativas à venda e distribuição de substâncias proibidas. Nos diretórios estavam vários ficheiros com títulos sexualmente sugestivos, em formato JPG. O inspetor Lewis inseriu os discos em outro computador e começou a pesquisar os ficheiros copiados dos computadores de Carey. O seu método consistia em inserir palavras-chave como «dinheiro, contas, pessoas, etc.» na função de pesquisa para encontrar ficheiros baseados em texto (*text-based*) contendo essas palavras. Esta pesquisa não produziu qualquer correspondência relativa a drogas (*related to drugs*). O inspetor Lewis continuou a explorar os diretórios e encontrou alguns ficheiros com os quais, disse, «não estava familiarizado». Incapaz de visualizá-los no computador que estava usando, copiou-os para um disco externo e colocou-os em outro computador. Então foi «imediatamente» capaz de visualizar o que mais tarde descreveria como um ficheiro em formato JPG (*JPG file*). Ao abrir este ficheiro, descobriu que continha pornografia infantil. O inspetor Lewis abriu aproximadamente duzentos e quarenta e quatro ficheiros JPG ou de imagem [83].

Carey entrou com uma moção requerendo a exclusão dos ficheiros que continham pornografia infantil. Durante a audiência judicial sobre a moção, o inspetor Lewis afirmou que, embora a descoberta dos ficheiros JPG tenha sido completamente fortuita, logo que vira a primeira foto contendo pornografia infantil desenvolveu uma causa provável para acreditar que o mesmo tipo de material estaria presente nos restantes ficheiros de imagem. Quando perguntado por que razão não promovera, afinal, um mandado complementar para pesquisa dos demais ficheiros de imagem, o inspetor Lewis respondeu que a questão fora equacionada e o seu superior hierárquico, supostamente, tratara disso através do gabinete do promotor de justiça local (*county attorney's office*). Não foi, porém, obtido qualquer mandado complementar, mas o inspetor Lewis, mesmo assim, continuou a explorar os ficheiros de imagem. Na opinião do governo, «uma pesquisa em computador como a realizada neste caso equivale a procurar documentos em um arquivo físico, de acordo com um mandado de busca e apreensão válido, acabando por se encontrar pornografia infantil» [84].

Na sua decisão, o Tribunal de Apelação recordou que o Supremo Tribunal (*Supreme Court*) fixara o entendimento de que «a doutrina jurisprudencial da visibilidade imediata não pode ser usada para estender uma pesquisa exploratória geral de um objeto para outro até que algo de incriminador finalmente apareça» (*Coolidge v New Hampshire*, 403 U.S. at 466, 91 S.Ct. 2022) [85]. O mandado obtido para um propó-

---

[83] *United States v Carey* (1999), *cit.*, § I.

[84] Em língua original (*United States v Carey* (1999), § II): «*a computer search such as the one undertaken in this case is tantamount to looking for documents in a file cabinet, pursuant to a valid search warrant, and instead finding child pornography*».

[85] Em língua original (*United States v Carey* (1999), § II): «*the plain view doctrine may not be used to extend a general exploratory search from one object to another until something incriminating at last emerges*».

sito específico de pesquisa nos computadores do visado permitiria apenas a busca de ficheiros por nomes, números de telefone, livros, recibos, endereços e outras provas documentais relativas à venda e distribuição de substâncias proibidas. O escopo da busca foi, portanto, circunscrito a evidências pertencentes ao tráfico de drogas. Lewis havia abandonado temporariamente essa pesquisa para procurar mais pornografia infantil e apenas voltou a pesquisar documentos relativos a drogas depois de conduzir uma pesquisa de cinco horas nos ficheiros de pornografia infantil [86].

O Tribunal de Apelação não aceitou a alegação do governo de que a imagem sexualmente sugestiva que repentinamente surgiu à «vista de todos» (*plain view*) na tela do computador tornara os ficheiros acessíveis como se fosse um «jogo justo» (*fair game*) baseado numa busca consensual, desde logo porque o consentimento do visado referia-se apenas à busca no respetivo apartamento e nada mais. A consideração crítica a este respeito é que os agentes nunca anunciaram, antes que o visado desse o seu consentimento, que estavam investigando uma suspeita de posse de pornografia infantil [87].

O Tribunal de Apelação concluiu, por unanimidade (com voto de concordância separado do juiz Porfilio), que o inspetor Lewis excedera o escopo do mandado no caso em apreço. A apreensão de evidências em que se baseara a acusação foi consequência de uma busca geral inconstitucional e, por conseguinte, o tribunal distrital cometera um erro ao recusar-se a excluir tais evidências [88].

O caso *United States v Carey* (1999) apresenta uma característica singular que ajuda a explicar a decisão do Tribunal de Apelação, a saber: o mandado judicial autorizava a pesquisa nos computadores do visado através de palavras-chave, o que tornava os ficheiros de imagem inacessíveis ao tipo de pesquisa autorizado, a menos que os títulos desses ficheiros correspondessem a alguma das palavras-chave, o que não era o caso. Uma correta pesquisa através de palavras-chave não consentiria sequer que o inspetor Lewis vasculhasse livremente os diretórios dos computadores do visado [89]. Neste contexto, é compreensível que a doutrina jurisprudencial da visibilidade imediata não tenha aplicação, tanto mais que o acesso ao conteúdo dos ficheiros de imagem só ocorreu após sucessivas transferências do material informático apreendido para distintos computadores de trabalho. Que a doutrina jurisprudencial da visibilidade imediata não tenha aplicação neste contexto não significa, porém, que nunca tenha aplicação às evidências geradas por computador.

---

[86] *United States v Carey* (1999), *cit.*, § II.
[87] *United States v Carey* (1999), *cit.*, § II.
[88] *United States v Carey* (1999), *cit.*, § III.
[89] Moshirnia, 2010: 623-624 e Mantei, 2011: 993-996.

3.7. O caso State vs. Schroeder (2000)

O caso *State v Schroeder* (2000)[90] é, por sua vez, paradigmático da possibilidade de aplicação da doutrina jurisprudencial da visibilidade imediata às evidências geradas por computador.

Keith Schroeder recorreu da sentença que o condenara por dezoito acusações de posse de pornografia infantil, assim como da decisão de recusa de atenuação do regime de cumprimento da pena. Entre outras, suscitou a questão da violação do Quarto Aditamento à Constituição dos EUA durante a pesquisa ao seu computador pelo laboratório de polícia científica. Durante a pesquisa foram descobertos fortuitamente ficheiros de pornografia infantil, embora o mandado judicial fosse destinado à pesquisa de evidências relativas a crimes de assédio online (*harassment*) e conduta desordeira (*disorderly conduct*). Logo que deparou com os primeiros ficheiros pornográficos, o analista interrompeu a pesquisa e aguardou a obtenção de novo mandado judicial de busca digital, o qual viria, de facto, a ser emitido. Mas Schroeder manteve a alegação de que faltava um mandado judicial de busca e apreensão válido e alegou que as imagens de pornografia infantil deveriam ser eliminadas como fruto da árvore venenosa (*fruit of the poisonous tree*). O Tribunal de Apelação de Wisconsin (*Court of Appeals of Wisconsin*), em 24 de maio de 2000, rejeitou este (e os demais) argumento(s) trazido(s) pelo recurso[91].

Tudo começou com a execução do primeiro mandado judicial de busca e apreensão. O delegado de polícia (*County Sheriff's Sergeant*) Harry Sokel procurou instalar no computador de Schroeder um programa para preservar (*to freeze*) o sistema de modo a que os respetivos conteúdos não pudessem ser alterados. Enquanto procurava os equipamentos periféricos do computador, Sokel deparou com um disco compacto que parecia pela respetiva capa de invólucro conter pornografia. Sokel perguntou a Schroeder se guardava pornografia adulta no computador e ele respondeu afirmativamente. Sokel perguntou ainda a Schroeder se guardava pornografia infantil no computador, ao que este retorquiu não saber o que era tal coisa. Sokel acrescentou que se referia a fotografias de crianças despidas com idade inferior a dezasseis anos. Schroeder respondeu que deveria haver algumas[92].

O computador foi enviado ao laboratório de polícia científica para análise. Sokel disse ao inspetor (*investigator*) que levou o computador para o laboratório, Steve Malchow, que poderia haver pornografia infantil no computador. Malchow, por sua vez, disse a Marty Koch, o analista forense (*crime lab analyst*), que se encontrasse qualquer pornografia infantil no computador deveria interromper a pesquisa e ligar para Malchow. Em sua busca de evidências de assédio online, Koch encontrou, de facto, algumas fotos pornográficas de crianças[93].

---

[90] *State v Schroeder*, 613N.W.2d911 (Wis. App. 2000).
[91] *State v Schroeder* (2000), *cit.*, § 1.
[92] *State v Schroeder* (2000), *cit.*, § 2.
[93] *State v Schroeder* (2000), *cit.*, § 4.

Em recurso, Schroeder alegou que Koch abrira indevidamente alguns ficheiros cujos nomes sugeriam conteúdos de pornografia infantil. Segundo Schroeder: «[e]ste passo adicional de abrir e ver a pasta para verificar se continha pornografia infantil torna a pesquisa ilegal»[94]. Schroeder parece, portanto, desafiar a aplicação da doutrina jurisprudencial da visibilidade imediata, ao referir que os ficheiros não estavam à vista[95].

O Tribunal de Apelação, porém, não aceitou a alegação de Schroeder. Koch testemunhara que, ao pesquisar um computador, costumava vasculhar sistematicamente e abrir os ficheiros independentemente dos seus nomes. Tal faz sentido, pois um utilizador é livre de nomear um ficheiro com qualquer nome. Se Koch limitasse sua pesquisa a ficheiros cujos nomes sugerissem o tipo de evidência que ele buscava, seria muito fácil para os visados esconderem as evidências no computador: – Nomeie o seu ficheiro de pornografia infantil como «1986.taxreturn» e ninguém poderá abri-lo! Ao abrir sistematicamente todos os ficheiros criados pelo utilizador, Koch deparou com um que continha imagens que ele considerava serem de pornografia infantil. Neste momento, Koch interrompeu a pesquisa e chamou Malchow. Não retomou a pesquisa, nem encontrou o resto das imagens de pornografia infantil antes de obter o segundo mandado de busca digital. Assim, a sua descoberta inicial de pornografia infantil ocorreu quando ele abriu um ficheiro e viu a foto de uma criança nua aparecendo na tela. Estava bem à vista. Segundo o Tribunal de Apelação: «[i]sto não era diferente de um investigador abrir uma gaveta enquanto procurava por drogas e ver a foto de uma criança nua em cima de uma pilha de meias»[96]. O primeiro requisito do teste da visibilidade imediata está satisfeito. Com relação ao segundo e terceiro requisitos, é indiscutível que Koch tinha um mandado para pesquisar o computador em busca de evidências de assédio online e que a primeira imagem que Koch encontrou poderia ser razoavelmente vista, de caras, como pornografia infantil. Por consequência, a doutrina jurisprudencial da visibilidade imediata, segundo o Tribunal de Apelação, aplicava-se ao caso[97].

A situação é diferente da ocorrida no caso *United States v Carey* (1999), onde o tribunal de recurso considerara a pesquisa irrazoável a partir do momento em que o inspetor abandonara a sua procura original por evidências de tráfico de drogas e passara a procurar pornografia infantil, após a descoberta inadvertida da primeira imagem de pornografia infantil. A diferença significativa é que, em Carey, o investigador abandonara a sua pesquisa original e começara a procurar apenas mais pornografia infantil, sem obter um novo mandado de busca digital. Assim, nenhuma das imagens pornográficas descobertas posteriormente caiu sob a alçada da doutrina jurispru-

---

[94] Em língua original (*State v Schroeder* (2000), § 13): «*This additional step of opening and reviewing the folder to verify it contained child porn makes the search illegal*».

[95] *State v Schroeder* (2000), *cit.*, § 13.

[96] Em língua original (*State v Schroeder* (2000), § 14): «*This was no different than an investigator opening a drawer while searching for drugs and seeing a nude picture of a child on top of a pile of socks*».

[97] *State v Schroeder* (2000), *cit.*, § 14.

dencial da visibilidade imediata. No presente caso, pelo contrário, o analista parou de pesquisar e obteve um segundo mandado. A pesquisa por pornografia infantil só prosseguiu depois de autorizada pelo segundo mandado[98].

Em suma, a doutrina jurisprudencial da visibilidade imediata justifica apenas apreensões, não buscas[99]. O investigador criminal deve, por isso, ignorar as descobertas fortuitas? A resposta é negativa. Se tiver uma causa provável para acreditar que os ficheiros que sobram contêm evidências de atividade criminosa não abrangida pelo mandado de busca digital, então deverá solicitar um mandado de busca digital complementar que o autorize a prosseguir a pesquisa.

4. CONCLUSÕES

O artigo 8.º da Convenção Europeia dos Direitos Humanos trata do respeito pela privacidade. O Quarto Aditamento à Constituição dos EUA trata igualmente do respeito pela privacidade.

A migração da vida contemporânea para o ciberespaço deve preservar o respeito pela privacidade, inclusivamente ao nível do processo penal. Para assegurar este desiderato, o direito em ação deve definir com mais rigor os limites da cópia de dados eletrónicos e as restrições impostas à análise externa do acervo recolhido.

Entre os aspetos críticos da análise externa de dados eletrónicos, avulta a questão do procedimento a adotar pelo investigador criminal diante dos conhecimentos fortuitos. A descoberta inadvertida de evidências produzidas por computador relacionadas com uma atividade criminosa não abrangida pelo mandado de busca digital primitivo obriga o investigador criminal a interromper a visualização dos ficheiros eletrónicos e a promover a obtenção de um mandado de busca digital complementar com base em indícios razoáveis da prática do crime detetado. A falta de mandado de busca digital complementar determina a exclusão das evidências porventura descobertas através da indevida continuação da análise externa do acervo recolhido.

Consoante a vastidão do acervo eletrónico recolhido, a análise externa pode implicar a necessidade de nomeação *ad hoc* de uma equipa de promotores de justiça, inspetores de polícia criminal e analistas informáticos cuja função se limite à triagem das evidências relevantes para o processo criminal, em curso ou a instaurar, sinalizando os documentos eletrónicos cobertos por privilégios de sigilo profissional ou segredo de negócio e eliminando os documentos eletrónicos irrelevantes. A equipa *ad hoc* deve ser afastada da prossecução da investigação criminal logo que termine a tarefa para que foi designada, dado que ficou contaminada pelo conhecimento de

---

[98] *State v Schroeder* (2000), *cit.*, § 16.

[99] Mas cada nova visualização de dados na tela do computador é uma busca, não uma apreensão, segundo Kerr, 2005: 534.

informação que, por definição, não poderia conhecer sob a autoridade do(s) mandado(s) de busca digital.

Não basta a nomeação *ad hoc* de uma equipa de investigação criminal, à qual faltará sempre a suficiente imparcialidade para assegurar a proteção da privacidade do visado. A única maneira eficaz de mitigar, na prática, a manipulação abusiva da doutrina da visibilidade imediata quando os investigadores criminais 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 de instrução). O juiz especial deve examinar todas as evidências produzidas por computador e confirmar a respetiva correspondência com o mandado de busca digital.

A jurisprudência do Tribunal Europeu dos Direitos Humanos caracteriza-se por alguma ineficácia na criação de remédios para a violação da privacidade no processo penal, designadamente no tocante à cópia de dados eletrónicos e à análise externa do acervo recolhido, desde logo porque não comina a exclusão das evidências produzidas por computador que tenham sido obtidas ilicitamente, o que deveria ser o caso, à luz do princípio do processo equitativo.

Os ordenamentos jurídicos nacionais europeus caracterizam-se por um regime legal geral e abstrato em matéria de prova digital. A distância entre as normas legais habilitantes da cópia de dados eletrónicos e respetiva análise externa, por um lado, e a atuação no terreno das autoridades de investigação criminal, por outro, não é colmatada pela existência de diretrizes mandatórias para tais autoridades, ademais divulgadas publicamente, que contenham a descrição detalhada das boas práticas. Naturalmente, a mera existência de manuais de procedimentos internos, indicativos e secretos não é garantia suficiente das boas práticas.

O conhecimento das diretrizes e do direito jurisprudencial norte-americano representa 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 da prática jurisprudencial.

Alguns dirão que as conclusões deste artigo são contraproducentes porque não anunciam formas de eficientização da recolha das evidências produzidas por computador em ordem ao deslindamento dos factos puníveis investigados, antes estabelecem limites à atividade de investigação criminal no ciberespaço. A crítica é pertinente, mas a sociedade democrática tem de pagar um preço para que a vida dos indivíduos e das empresas não se torne um livro aberto à absoluta devassa, nem mesmo quando as autoridades públicas andem legitimamente à procura das evidências dos crimes investigados.

5. BIBLIOGRAFIA

Ambos, Kai, (2010: *Beweisverwertungsverbote: Grundlagen und Kasuistik – internationale Bezüge – ausgewählte Probleme*, Berlin: Duncker & Humblot.

Bachmaier Winter, Lorena, Thaman, Stephen C., 2020: «A Comparative View of the Right to Counsel and the Protection of Attorney-Client Communications», in: Lorena Bachmaier Winter, Stephen C. Thaman e Veronica Lynn (eds.), *The Right to Counsel and the Protection of Attorney-Client Privilege in Criminal Proceedings – A Comparative View*, Cham: Springer, pp. 7-73.

Bartholomew, Paige, 2014: «Seize First, Search Later: The Hunt for Digital Evidence», 30 *Touro Law Review* 4, pp. 1027-1052.

Berman, Emily, 2018: «Digital Searches, the Fourth Amendment, and the Magistrates' Revolt», 68 *Emory Law Journal*, pp. 49-94.

Brenner, S. W., Frederiksen, B. A., 2002: «Computer Searches and Seizures: Some Unresolved Issues», 8 *Mich. Telecomm. Tech. L. Rev*. 39, pp. 39-114.

Chang, RayMing, 2007: «Why the Plain View Doctrine Should Not Apply to Digital Evidence», *Suffolk Journal of Trial and Appellate Advocacy* 12, pp. 31-67.

Clancy, Thomas K., 2005: «The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer», *Mississippi Law Journal* 75, pp. 193-286.

Costa Ramos, Vânia, 2017: «Os problemas em matéria de proibições de prova—a dimensão internacional—regras de exclusão da prova obtida em violação da Convenção Europeia dos Direitos Humanos na jurisprudência do Tribunal Europeu dos Direitos Humanos», in: J. Faria Costa *et al.* (eds.), *Estudos em Homenagem ao Prof. Doutor Manuel da Costa Andrade*, vol. II (Direito Penal, Direito Processual Penal), Coimbra: Universidade de Coimbra, pp. 740-773.

Costa Ramos, Vânia, Pinto de Abreu, Carlos, Cordeiro, João Valente, 2020: «Confidentiality of Correspondence with Counsel as a Requirement of a Fair Trial in Portugal», in: Lorena Bachmaier Winter, Stephen C. Thaman e Veronica Lynn (eds.), *The Right to Counsel and the Protection of Attorney-Client Privilege in Criminal Proceedings – A Comparative View*, Cham: Springer, pp. 235-271.

De Hert, Paul, Gutwirth, Serge, 2009: «Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action», in: Serge Gutwirth, Yves Poullet, Paul de Hert, Cécile de Terwangne e Sjaak Nouwt (eds.), *Reinventing Data Protection?* Brussel / Namur / Utrecht: Springer, p. 3-44.

Jahn, Jannika, 2014: «Ruling (In)directly through Individual Measures? Effect and Legitimacy of the ECtHR's New Remedial Power», *ZaöRV* 74, pp. 1-39.

Kamisar, Yale, 2003: «In Defense of the Search and Seizure Exclusionary Rule», 26 *Harv. J. L. & Pub. Pol'y* 119, pp. 119-140.

Kerr, Orin S., 2005: «Searches and Seizures in a Digital World», 119 *Harvard Law Review* 2, pp. 531-569.

Kostoris, Roberto E., 2014: «Diritto europeo e giustizia penale», in: Roberto E. Kostoris (ed.), *Manuale di Procedura Penale Europea*, Milano: Giuffrè, pp. 1-62.

LaFave, Wayne R., 2004: *Search and Seizure – A Treatise on the Fourth Amendment*, vol. 1 (Sections 1.1 through 2.7: The Exclusionary Rule and Other Remedies & Protected Areas and Interests), 4.ª ed., New York: Thomson Reuters, (1.ª ed., 1978).

—, 2011-2012: *Search and Seizure – A Treatise on the Fourth Amendment*, vol. 1 (Sections 1.1 through 2.7), 4.ª ed., New York: Thomson Reuters, Pocket Part (1.ª ed., 1978).

Mantei, Corey J., 2011: «Pornography and Privacy in Plain View: Applying the Plain View Doctrine to Computer Searches», 53 *Arizona Law Review*, pp. 984-1012.

Moshirnia, Andrew Vahid, 2010: «Separating Hard Fact from Hard Drive: A Solution for Plain View Doctrine in the Digital Domain», 23 *Harvard Journal of Law & Technology* 2, pp. 609-634.

Silva Ramalho, David, 2017: *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, Coimbra: Almedina.

Sousa Mendes, Paulo de, 2020: «O princípio do processo equitativo na jurisprudência do TEDH», in: Anabela Antunes *et al.* (eds.), *Estudos de Homenagem ao Professor Doutor Germano Marques da Silva*, vol. II, Lisboa: Universidade Católica Editora, pp. 2325-2339.
Ward, Kate Brueggemann, 2011: «The Plain (or Not So Plain) View Doctrine: Applying the Plain View Doctrine to Digital Seizures», *University of Cincinnaty Law Review* 79, pp. 1163-1187.
Wittler Contardo, Ricardo, 2020: «Apreensão de correio eletrónico em Portugal: Presente e futuro de uma questão de "manifesta simplicidade"», in: Paulo de Sousa Mendes e Rui Soares Pereira (eds.), *Novos Desafios da Prova Penal*, Coimbra: Almedina, pp. 277-313.

JURISPRUDÊNCIA DO TRIBUNAL EUROPEU DOS DIREITOS HUMANOS

Leander v Sweden (queixa n.º 9248/81), de 26 de março de 1987.
Amann v Switzerland (queixa n.º 27798/95), de 16 de fevereiro de 2000.
Rotaru v Romania (queixa n.º 28341/95), de 4 de maio de 2000.
Société Colas Est and other v France (queixa n.º 37971/97), de 16 de abril de 2002.
Wieser and Bicos Beteiligungen GmbH v Austria (queixa n.º 74336/01), de 16 de janeiro de 2007.
Copland v United Kingdom (queixa n.º 62617/00), de 3 de abril de 2007.
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 & Associados – Sociedade de Advogados, Rl 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.

DIRETRIZES E JURISPRUDÊNCIA DOS ESTADOS UNIDOS DA AMÉRICA

Federal Rules of Criminal Procedure (1946, 2019).
Federal Guidelines for Searching and Seizing Computers (1994) e *Supplements* (1997, 1999).
Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations (2001, 2009).
Weeks v United States, 232 U.S. 383, 34 S.Ct. 341, 58 L.Ed. 652 (1914).
Mapp v Ohio, 367 U.S. 643 (1961).
Coolidge v New Hampshire, 403 U.S. 443 (1971).
Bies v State, 76 Wis.2d 457, 464, 251 N.W.2d 461 (1977).
State v Washington, 134 Wis.2d 108, 121, 396 N.W.2d 156 (1986).
Horton v California, 496 U.S. 128 (1990).
State v Guy, 172 Wis. 2d 86, 492 N.W.2d 311 (1992).
United States v Carey, 172 F.3d 1268 (10th Cir. 1999).
State v Schroeder, 613N.W.2d911 (Wis. App. 2000).