3.

A recolha de prova digital através de pesquisas informáticas transfronteiriças

David Silva Ramalho

CENTRO
DE ESTUDOS
JUDICIÁRIOS

A RECOLHA DE PROVA DIGITAL ATRAVÉS DE PESQUISAS INFORMÁTICAS TRANSFRONTEIRIÇAS*

David Silva Ramalho**

1. O problema

Pense-se numa busca. Uma busca regularmente realizada ao local de trabalho de um suspeito da prática de um qualquer crime grave. No despacho do Ministério Público pode ler-se «[t]endo em conta que alguns dos elementos a apreender no decurso das buscas autorizadas podem estar contidos e armazenados em sistemas informáticos (computadores), designadamente em ficheiros de texto, bases de dados, registos de acesso e em gravações em formato vídeo e áudio, ordena-se, nos termos do disposto no n.º 1 do artigo 15º da Lei n.º 109/2009, de 15 de Setembro (Lei do Cibercrime), a pesquisa nos sistemas informáticos que venham a ser encontrados nos locais a buscar».

Assim sucede. Uma vez iniciada a pesquisa informática no computador do suspeito, percebe-se que existe muito pouca informação com relevo probatório, excepto alguns elementos que indiciam que a informação relevante há-de estar algures na *cloud*. Consultados os *Favoritos* do navegador de Internet do computador pesquisado, constata-se que aí se encontra, de facto, o *link* para um serviço de armazenamento de informação baseado na *cloud*. Ao seleccionar o *link*, percebe-se que as credenciais de acesso estão memorizadas e que, por isso, basta clicar na opção *sign in* para se poder ter acesso à informação pretendida.

O Ministério Público prepara-se para autorizar a extensão da pesquisa à conta do utilizador nessa *cloud*, ao abrigo do disposto no artigo 15.º, n.º 5, da Lei do Cibercrime, quando se apercebe que o fornecedor de serviços de armazenamento tem a sua sede na Alemanha e todos os seus servidores na Holanda, Bélgica e Irlanda. Pergunta-se: poderá clicar legitimamente na opção *sign in* para aceder e apreender[1] a informação armazenada noutro

* O presente texto corresponde, no essencial, à minha intervenção oral na acção de formação contínua sobre "Temas de Direito Penal e Processual Penal", organizada pelo Centro de Estudos Judiciários, que teve lugar no dia 9 de Março de 2018, no Tribunal da Relação do Porto. O texto conserva, por isso, o registo de oralidade que esteve na sua génese, bem como o seu propósito essencialmente expositivo.

** Assistente Convidado da Faculdade de Direito da Universidade de Lisboa, investigador do Centro de Investigação de Direito Penal e Ciências Criminais e Advogado na Morais Leitão, Galvão Teles, Soares da Silva & Associados – Sociedade de Advogados, SP, RL..

[1] De acordo com o disposto no artigo 16.º, n.º 7, da Lei do Cibercrime, a apreensão de dados informáticos poderá, consoante seja mais adequado e proporcional, revestir uma das seguintes formas: «a) Apreensão do suporte onde

Estado? Ou será que essa pesquisa e apreensão se lhe encontra vedada, sob pena de violação da soberania do Estado pesquisado, devendo por isso recorrer-se obrigatoriamente aos mecanismos de cooperação judiciária disponíveis? E se a informação pesquisada estiver, porventura, na *Dark Web*, sem que seja possível identificar o concreto Estado onde está armazenada? E se estiver armazenada em diferentes Estados em simultâneo, seja replicada, seja fragmentada? A questão não é de resolução fácil.

Com efeito, o problema do acesso transfronteiriço a prova digital vem sendo objecto de controvérsia há já pelo menos 3 décadas ([2]), quando a sua relevância era ainda diminuta, e não se antecipa que se venha a alcançar num futuro próximo uma solução satisfatória e consensual no plano internacional. Contudo, com a disseminação dos serviços de computação em nuvem e a deslocalização da informação, os obstáculos jurídicos à investigação criminal que daqui decorrem ganham um relevo muito prático e que, em certos casos, podem levar ao bloqueio da investigação criminal.

O problema jurídico-internacional tem sido, porém, desconsiderado em vários Estados pela prática judiciária, em prol de um conjunto de argumentos de natureza fundamentalmente pragmática que se prendem essencialmente com:

(i) A percepção da reduzida relevância da violação de soberania decorrente deste tipo de pesquisas e apreensões no contexto de processos-crime;

(ii) A volatilidade da prova, especialmente tendo em consideração a possibilidade de o arguido, ou alguém a seu pedido, poder eliminá-la a partir de qualquer sistema informático seu enquanto os mecanismos de cooperação judiciária são desencadeados;

(iii) A lentidão dos mecanismos de cooperação judiciária;

(iv) A ideia de que a Internet é um espaço sem fronteiras;

(v) A impossibilidade, em certos casos, de se descobrir o local onde a prova se encontra armazenada (o problema da *loss of location*) ou

(vi) A ideia de que, estando em causa a violação de normas que regulam relações entre Estados e que não visam conferir específicos direitos aos cidadãos na sua relação com o

está instalado o sistema ou apreensão do suporte onde estão armazenados os dados informáticos, bem como dos dispositivos necessários à respectiva leitura; b) Realização de uma cópia dos dados, em suporte autónomo, que será junto ao processo; c) Preservação, por meios tecnológicos, da integridade dos dados, sem realização de cópia nem remoção dos mesmos; ou d) Eliminação não reversível ou bloqueio do acesso aos dados».

[2] O tema foi suscitado, ainda que em termos genéricos, na Recomendação n.º R(89)9 do Comité de Ministros do Conselho da Europa, de 13 de Setembro de 1989, e complementada, com maior detalhe, pelo relatório sobre criminalidade informática do Comité Europeu para os Problemas Criminais, de 1990. Apesar de neste relatório se abordar já expressamente o problema da "penetração directa" em sistemas informáticos localizados no estrangeiro e de se incluírem algumas condições para a sua eventual admissibilidade a título excepcional, o Comité concluiu que a questão não se encontrava suficientemente amadurecida pelo que não seria altura de avançar uma proposta sobre a matéria - Conselho da Europa, *Computer-related crime* (prefácio de August Bequai), Estrasburgo: Council of Europe Publishing and Documentation Service, 1990, pp. 86-89.

Estado, as únicas consequências negativas que daí possam advir serão no plano supranacional e não no da invalidade da prova[3].

Por vezes a prática judiciária de aceder irrestritamente a prova armazenada no estrangeiro encontra inclusivamente esteio em disposições legais de origem nacional que, sem especial preocupação com os limites da sua jurisdição, admitem, de forma mais ou menos expressa, a extensão das pesquisas informáticas a outros territórios.

A solução assim adoptada por alguns legisladores nacionais parte do pressuposto que a mera existência de norma legal habilitante torna inconsequente, pelo menos no imediatismo do plano probatório e da respectiva validade, a violação de direito internacional. Esta solução é, todavia, um mero *remendo* para um problema mais grave, cuja solução deverá assentar num debate aberto e descomplexado quanto à eventual inaptidão do quadro jurídico vigente para fazer face a uma realidade que já não é nova mas que permanece presa às amarras da analogia com o que já não é analógico, por ser digital.

2. A Convenção sobre o Cibercrime

O Conselho da Europa procurou integrar na Convenção sobre o Cibercrime os termos em que o acesso transfronteiriço seria consensualmente admitido pelos seus membros.

Começou, porém, por assinalar que a Convenção não tornaria possível, por si só, qualquer intromissão na soberania nacional dos Estados-signatários no decurso de investigações criminais de cariz nacional, assim delimitando geograficamente, salvo disposição legal (tendencialmente) supranacional que dispusesse em sentido contrário[4], a aplicação das medidas processuais previstas na sua Secção 2, aos dados trocados, enviados ou armazenados no mesmo território em que decorre a investigação.

Deste modo, a limitação territorial do acesso a dados informáticos foi expressamente referida a propósito, não só da busca e apreensão de dados informáticos armazenados (artigo 19.º), mas também da injunção de comunicar (artigo 18.º), da recolha, em tempo real de dados de tráfego (artigo 20.º) e da intercepção de dados de conteúdo (artigo 21.º).

Apenas o acesso transfronteiriço a dados armazenados veio a merecer consagração expressa na Convenção, e não o acesso a — leia-se, a recolha ou intercepção de — dados de tráfego ou

[3] Nesse sentido, referiu recentemente o *Transborder Group*, junto do Conselho da Europa, o seguinte: «*As noted by the T-CY previously, given these limitations and in the absence of a clear, efficient and feasible international legal framework, governments increasingly pursue unilateral solutions in practice. It seems to be widespread practice that law enforcement in a specific criminal investigation access data not only on the device of the suspect but also on connected devices such as email or other cloud service accounts if the device is open or the access credentials have been obtained lawfully even if they know that they are connecting to a different, known country*» - COMITÉ DA CONVENÇÃO SOBRE O CIBERCRIME (T-CY), *Criminal Justice Access to electronic evidence in the cloud: Recommendations for consideration by the T-CY*, Estrasburgo: Conselho da Europa, Setembro de 2016, disponível em https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a495e.

[4] Dado que o objectivo da Convenção é também completar e não substituir quaisquer tratados e acordos bilaterais e multilaterais celebrados entre as Partes, é permitida a estipulação de norma em sentido contrário, a qual, naturalmente, terá um âmbito de aplicação limitado aos seus signatários — cf. artigo 39.º da Convenção e parágrafos 293, 308 e 309 do Relatório Explicativo da Convenção sobre o Cibercrime.

de conteúdo em tempo real, em relação aos quais a regra expressamente consagrada foi, sem excepções, a do recurso à cooperação internacional (cf. artigos 33.º e 34.º da Convenção). Facto que é, aliás, facilmente compreensível, tendo em conta que, se o consenso para a apreensão de dados armazenados apenas foi conseguido em situações absolutamente excepcionais, então qualquer consenso sobre a realização de intercepções transfronteiriças seria, naturalmente, inalcançável[5].

Assim, refere-se no parágrafo 195 do Relatório Justificativo da Convenção sobre o Cibercrime que o artigo 19.º, dedicado à *busca e apreensão de dados informáticos armazenados*, «não aborda a "busca e apreensão transfronteiriça" que confere aos Estados a possibilidade de busca e apreensão de dados no seio do território de outras Partes, sem que seja necessário recorrer às modalidades tradicionais de assistência jurídica mútua», uma vez que este meio de obtenção de prova se encontra regulado no capítulo da cooperação internacional. Duas excepções a esta regra são, porém, contempladas no artigo 32.º da Convenção, a saber:

> (i) Quando os dados forem publicamente acessíveis, ou,
>
> (ii) Se os dados se encontrarem armazenados no território de uma outra Parte da Convenção, quando for obtido o consentimento legal e voluntário da pessoa com legitimidade para divulgar os dados através desse sistema informático.

Nesta matéria, como se refere no parágrafo 293 do Relatório Justificativo da Convenção, «[f]oram examinadas em pormenor todas as situações nas quais se considera admissível que os Estados actuem de forma unilateral, bem como as situações nas quais tal não será aceitável» até que "[o]s redactores chegaram […] à conclusão de que, nesta fase, não seria ainda possível elaborar um regime global, legalmente vinculativo, que regulamentasse esta matéria», devido «em parte, à inexistência, até à data, de uma experiência objectiva relativamente a este tipo de situações, ao que se acrescenta o facto de se considerar que a resolução adequada está, frequentemente, ligada à conjuntura do caso em concreto, pelo que se torna difícil estipular regras gerais», pelo que, em conclusão, «os redactores decidiram que apenas seriam definidas, ao abrigo do artigo 32.º da Convenção, as situações nas quais, por unanimidade, a acção unilateral se mostrasse aceitável».

A regra geral configurada na Convenção é, então, a do recurso à cooperação internacional, sempre que os dados estejam armazenados em território estrangeiro, salvo acordo supranacional em sentido diferente, entre os Estados envolvidos, e exceptuando os dois casos que se analisarão de seguida.

Todavia, por força da tendencial lentidão dos mecanismos de cooperação internacional tradicionais, especialmente agravada em virtude do carácter altamente volátil da prova digital, o Conselho da Europa, inspirado na rede de pontos de contacto estabelecida em 1998, por

[5] Assim, PAUL DE HERT, «Cybercrime and jurisdiction in Belgium and the Netherlands. Lotus in cyberspace — whose sovereignty is at stake?», em *Cybercrime and Jurisdiction* (ed. Susan Brenner/Bert-Jaap Koops), Haia: T.M.C. Asser Press, 2006 , p. 83.

iniciativa do G8, criou a Rede 24/7[6], composta por pontos de contacto, em cada Parte, disponíveis vinte e quatro horas por dia, sete dias por semana, a fim de assegurar de imediato a prestação de auxílio nas investigações e nos procedimentos relativos a infracções penais relacionadas com sistemas informáticos, ou na recolha de provas sob a forma electrónica, da prática de infracções penais[7].

2.1. O acesso transfronteiriço a dados publicamente acessíveis

Dispõe o artigo 32.º, alínea *a)*, da Convenção sobre o Cibercrime, que uma Parte pode, sem autorização de uma outra Parte, «aceder a dados informáticos acessíveis ao público (fonte aberta), independentemente da sua localização geográfica». Assim, sempre que seja necessário recolher dados[8] num *website* ao qual o público pode ter acesso, ainda que mediante subscrição ou registo prévio[9] — pense-se numa rede social[10], num *blog*, ou mesmo numa pasta *Dropbox* acessível através de um *link* público[11] —, podem as autoridades fazê-lo sem necessidade de recurso aos mecanismos de cooperação internacional, procedendo ao *download* dos documentos relevantes ou mesmo realizando *screenshots* da página em questão[12].

---

[6] A Rede viria a ser alargada ao contexto da União Europeia por via da Decisão-Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro de 2005, relativa a ataques contra sistemas de informação — cf. PEDRO VERDELHO, *The effectiveness of international co-operation against cybercrime: examples of good practice,* 2008, Conselho da Europa, pp. 15, disponível em: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/567%20study4-Version7%20provisional%20_12%20March%2008_.pdf.

[7] Referindo-se essencialmente a actos de espionagem mas com relevo para esta matéria, refere JOHANN-CHRISTOPH WOLTAG o seguinte: «[i]*f these operations are undertaken by merely accessing publicly available data, the performing State does not substitute the target State's sovereignty on its own. Consequently only those operations that access data not readily available to a foreign State can be considered in their effects to be infringe on the target State's sovereignty and political independence*» — CHRISTOPH WOLTAG, *Cyber Warfare — Military Cross-Border Computer Network Operations under International Law*, Cambridge: Intersentia, 2014, p. 127.

[8] A circunstância de o artigo 32.º, n.º 1, alínea a), da Convenção sobre o Cibercrime falar em "acesso" e não em "aceder a, ou receber", como faz a alínea b), poderia indicar que aquele acesso não permitiria uma apreensão de prova. A distinção parece, porém, ser inconsequente, permitindo também a apreensão da prova. Assim, cf. o excelente e incontornável artigo de ULRICH SIEBER / CARL-WENDELIN NEUBERT, «Transnational Criminal Investigations in Cyberspace: Challenges to National Sovereignty», em *Max Planck Yearbook of United Nations Law* (ed. Frauke Lachenmann et al.), Vol. 20, Leiden | Boston: Brill, Nijhoff, 2016, pp. 267-268.

[9] Assim, cf. a recente obra incontornável de ULRICH SIEBER / CARL-WENDELIN NEUBERT, «Transnational Criminal Investigations in Cyberspace: Challenges to National Sovereignty», em *Max Planck Yearbook of United Nations Law* (ed. Frauke Lachenmann et al.), Vol. 20, Leiden | Boston: Brill, Nijhoff, 2016, pp. 267-268 e COMITÉ DA CONVENÇÃO SOBRE O CIBERCRIME (T-CY), *T-CY Guidance Note #3 — Transborder access to Data (Article 32)*, Estrasburgo: Conselho da Europa, p. 4., disponível em: http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/Guidance_Notes/T-CY(2013)7REV_GN3_transborder_V11.pdf.

[10] Nesse sentido, veja-se o recente acórdão do Tribunal da Relação do Porto, de 5 de Abril de 2017, Proc. 671/14: «A recolha ou cópia de informação que alguém disponibiliza ou publicita no seu mural de Facebook sem restrição de acesso, não impede a sua utilização como prova para efeitos de procedimento criminal. Deste modo, a utilização da cópia da publicação pela qual o arguido divulgou factos pouco abonatórios e falsos no mural do Facebook sobre a conduta dos assistentes no âmbito da parceria de trabalho que tinham em Angola, sem restrição de acesso, constitui prova perfeitamente válida».

[11] Cf. BERT-JAAP KOOPS / MORAG GOODWIN, *Cyberspace, the cloud and cross-border criminal investigation – The limits and possibilities of international law*, Tilburg: Universiteit van Tilburg, 2014, p.53.

[12] Cf. PEDRO VERDELHO, *The effectiveness of international co-operation against cybercrime: examples of good practice*, cit., pp. 12-15, e CRISTOS VELASCO SAN MARTÍN, *La jurisdicción y competencia sobre delitos cometidos a través de sistemas de cómputo e internet*, Valencia: Tirant lo blanch, 2012, pp. 155-160.

Trata-se, porém, de uma permissão cuja ausência tende a ser considerada como relativamente inócua tendo em conta que já se encontraria a coberto de um costume internacional[13], em virtude de se tratar de uma prática geral (*consuetudo*), considerada juridicamente vinculativa (*opinio iuris sive necessitatis*)[14].

2.2. O acesso transfronteiriço a dados informáticos com o consentimento da pessoa legalmente autorizada

Por outro lado, consta do artigo 32.º, alínea b), da Convenção sobre o Cibercrime que «[u]ma Parte pode, sem autorização de uma outra Parte […] [a]través de um sistema informático situado no seu território, aceder a dados informáticos no território de uma outra Parte, ou recebê-los, se obtiver o consentimento legal e voluntário da pessoa com legitimidade para lhe divulgar os dados através desse sistema informático».

A primeira questão que cumpre clarificar prende-se com o significado de *pessoa com legitimidade para divulgar os dados*, cujo significado poderá variar em função da legislação de cada Estado-signatário. Nesta matéria, esclarece o Relatório Justificativo da Convenção sobre o Cibercrime, no parágrafo 294, que «a pessoa "legalmente autorizada" a divulgar os dados poderá variar em função das circunstâncias, da natureza jurídica da pessoa e da respectiva legislação aplicável», avançando o seguinte exemplo, «uma mensagem de correio electrónico de uma dada pessoa poderá ser armazenada num outro país por um fornecedor de serviços, ou a pessoa poderá intencionalmente armazenar os dados num outro país. Estas pessoas poderão, assim, recuperar os dados e, visto que dispõem de uma autoridade legal, proceder voluntariamente à divulgação dos dados junto dos serviços competentes para a aplicação da lei, ou permitir a estes últimos o acesso aos dados em conformidade com as disposições contidas neste artigo»[15].

A segunda questão a dirimir prende-se com o conceito de *consentimento legal e voluntário*. Nesta matéria, cabe não esquecer que, não só a pessoa legalmente autorizada a divulgar os dados tem de querer, livremente, facultar o acesso aos mesmos, como, no momento em que

[13] Sendo certo que existem algumas vozes que tendem a atribuir relevo apenas ao critério do local de armazenamento, sem distinção quanto à eventual publicidade dos dados. Assim, de acordo com a opinião do Conselho de Estado da Bélgica, «*most of the member States tend to consider a cross-border search on the web carried out by the competent authorities entrusted with the inquiry without the authorization of the competent authorities to be a violation of their sovereignty and of international law*» — cf. PAUL DE HERT / GERTJAN BOULET, «Report for Belgiu»", *Révue Internationale de Droit Pénale*, Ano 84 (1.º e 2.º trimestres de 2013), p. 36 e BERT-JAAP KOOPS, "Police investigations in Internet open sources: Procedural-law issues, *Computer Law & Security Review*, n.º 29 (2013), p. 658.

[14] Assim, NICOLAI SEITZ, «Transborder Search: a new perspective in law enforcement?», *Yale Journal of Law and Technology*, Vol. 7 (2005), p. 38, e, SUB-GRUPO AD-HOC SOBRE JURISDIÇÃO E ACESSO TRANSFRONTEIRIÇO A DADOS E FLUXOS DE DADOS JUNTO DO COMITÉ DA CONVENÇÃO SOBRE O CIBERCRIME (T-CY), *Transborder access and Jurisdiction: What are the options?*, Conselho da Europa, 2012, disponível em http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/T-CY/TCY_2012_3_transborder_rep_V30public_7Dec12.pdf, p. 20. Nesta matéria, na doutrina portuguesa, cf. BENJAMIM SILVA RODRIGUES, *Da Prova Penal — Tomo IV — Da Prova -Electrónico- Digital e da Criminalidade Informático-Digital* (com prefácio de Catarina dos Santos Gomes), Lisboa: Rei dos Livros, 2011, p. 376 e PEDRO VERDELHO et al., *Leis do Cibercrime — Volume 1*, Lisboa: Centro Atlântico, 2003, p. 20.

[15] Cf. SUB-GRUPO AD-HOC SOBRE JURISDIÇÃO E ACESSO TRANSFRONTEIRIÇO A DADOS E FLUXOS DE DADOS JUNTO DO COMITÉ DA CONVENÇÃO SOBRE O CIBERCRIME (T-CY), *Transborder access and Jurisdiction: What are the options?*, cit., pp. 23-24. Para maior desenvolvimento sobre este tema, veja-se o nosso *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, Coimbra: Almedina, 2017, pp. 73-75.

decide fazê-lo, tem de estar cabalmente esclarecida e informada do teor e consequências do seu consentimento[16]. A estes requisitos tem de juntar-se o da admissibilidade legal de concessão válida do consentimento, nos termos da legislação interna do Estado no qual o mesmo é prestado, designadamente em casos de menoridade ou de anomalia psíquica do visado.

A alínea *b)* do artigo 32.º, embora tenha entretanto sido praticamente replicada noutras disposições supranacionais[17], foi, e continua a ser, uma das disposições mais controversas da Convenção sobre o Cibercrime[18], por poder implicar uma cedência de soberania nacional[19], ao permitir — sem, contudo, definir procedimentos para o efeito — que um Estado execute actos processuais materialmente incidentes sobre o território de outro Estado sem recorrer aos mecanismos de auxílio mútuo[20], para que esta faculte o acesso aos dados[21].

Assim, tendo em conta que a norma em apreço é aplicável apenas às Partes da Convenção, se, por hipótese, os dados visados estiverem armazenados num sistema informático localizado num Estado que não seja Parte, ou, se for impossível descobrir a localização dos dados, o artigo 32.º, alínea b), da Convenção não será aplicável[22].

---

[16] Acerca da eventual revogabilidade deste consentimento cf. o relatório elaborado por JOSEPH J. SCHWERHA IV, *Law Enforcement Challenges in Transborder Acquisition of Electronic Evidence from "Cloud Computing Providers"*, Estrasburgo: Conselho da Europa, 2010, p. 12, disponível em: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/reports-presentations/2079_reps_IF10_reps_joeschwerha1a.pdf

[17] Assim sucede com o artigo 40.º, n.º 2, da Convenção Árabe sobre o Combate a Infracções Informáticas, de 2010, ou com o artigo 49.º da Lei Modelo sobre Cibersegurança da *Common Market for Eastern and Southern Africa* (COMESA).

[18] Aliás, como se pode ver nos Relatórios da 2.ª Consulta Multilateral das Partes da Convenção sobre o Cibercrime [CM/Inf(2007)38], de 2007, na qual consta que a Federação Russa teve uma aproximação positiva à Convenção mas entendeu que teria de ser feita uma análise adicional ao artigo 32b, «*em particular à luz da experiência recolhida do uso deste artigo*» — disponível em https://wcd.coe.int/ViewDoc.jsp?id=1167033&Site=COE, acedido e consultado em 5 de Agosto de 2012 —, bem como ao Relatório da 4.ª Consulta Multilateral no qual consta que uma «*delegação de observadores fez uma declaração a expressar preocupação acerca das incertezas relativas à aplicação do artigo 32 (b) da Convenção e sugerindo que o T-CY deveria iniciar um processo que resultaria na emenda desta previsão. O T-CY não aceitou esta sugestão*» — disponível em: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/T-CY/TC-Y_2009_06.pdf, acedido e consultado em 5 de Agosto de 2012. Sobre este assunto cf. MICHEÁL O'FLOINN, «It wasn't all white light before Prism: Law enforcement practices in gathering data abroad, and proposals for further transnational access at the Council of Europe», *Computer Law & Security Review*, n.º 29 (2013), p. 611.

[19] Cf. MARCO GERCKE, «10 years Convention on Cybercrime», *Computer Law Review International*, Vol. 5/2011 (Outubro de 2011), p. 149, e *Understanding Cybercrime: A Guide for Developing Countries*, Genebra: ITU, 2011, pp. 277-278.

[20] Foi, aliás, em grande medida, devido a esta norma que a Rússia, apesar de ser membro do Conselho da Europa, se recusa, até à data, a assinar a Convenção sobre o Cibercrime, porquanto, no seu entendimento, o artigo 32.º, alínea b), «poderia danificar a soberania e a segurança dos Estados membros e os direitos dos seus cidadãos» — cf. CNEWS (2008), «Putin defies Convention on Cybercrime», 27 de Março, disponível em http://eng.cnews.ru/news/top/indexEn.shtml?2008/03/27/293913.

[21] Há, inclusivamente, quem questione a admissibilidade jurídica da criação desta excepção, alegando para tal que a soberania nacional de um Estado não está à disposição de um indivíduo — sobre esta matéria, cf. NICOLAI SEITZ, «Transborder Search: a new perspective in law enforcement?», cit., p. 40.

[22] A menos que, como refere NICOLAI SEITZ, também aqui possamos reconhecer, quanto à procura do consentimento da pessoa legalmente autorizada, a existência de um costume internacional que permita estender esta excepção a Estados não-signatários da Convenção — *Idem,* p. 45. Cabe, porém, sublinhar, que, o facto de não se aplicar esta disposição da Convenção, não impede que a medida tenha lugar relativamente a outros Estados, mas antes significa que não será este o supedâneo jurídico habilitante dessa medida.

3. Possíveis vias de solução

A admissibilidade da realização de pesquisas informáticas transfronteiriças sem suporte em instrumentos jurídicos de cariz supranacional tem sido amplamente discutida na doutrina, sem que se tenha, até à data, encontrado uma solução que satisfaça simultaneamente, por um lado, os interesses dos Estados em perseguir eficazmente os agentes da prática de crimes cujo suporte probatório se encontre em ambiente digital e, por outro, os interesses dos Estados *pesquisados* em não sofrerem ingerências directas em sistemas informáticos localizados nos seus territórios, sem suporte jurídico internacional.

As soluções têm sido procuradas, naturalmente, em três frentes:

– A primeira, o direito vigente dos tratados, a jurisprudência internacional e as excepções comummente admitidas às ingerências na soberania de outros Estados;

– A segunda, na eventual formação de um costume internacional que permita legitimar este meio de obtenção de prova;

– A terceira, na eventual criação de um protocolo adicional à Convenção sobre o Cibercrime que permita alargar aos seus signatários uma nova permissão de acesso.

No plano do direito internacional vigente, entendem SIEBER e NEUBERT que a única solução juridicamente sustentável, no contexto da investigação criminal, que permitiria excepcionar a necessidade de cumprimento da obrigação de não ingerência na soberania de outros Estados seria o caso em que a pesquisa transfronteiriça respeitasse a um Estado desconhecido pelo Estado actuante e fosse necessária a salvaguardar um interesse essencial contra um perigo grave e iminente. Entre esses interesses, entendem os Autores, pode encontrar-se o de garantir o exercício efectivo da jurisdição executiva contra criminosos que afectem o seu território. Não se trata aqui, naturalmente, de garantir o exercício da jurisdição executiva em casos isolados ou perante qualquer tipo de crimes, mas sim de permitir um funcionamento continuado do sistema de aplicação coerciva do direito, enquanto serviço essencial do Estado, em relação a certo tipo de crimes cuja gravidade o justifique e em circunstâncias particularmente exigentes. Uma vez identificado um interesse essencial, será necessário verificar se o mesmo enfrenta um perigo grave e iminente, o que, de acordo com os Autores, depende da circunstância de a impossibilidade de identificação do local onde se encontra a prova impedir as autoridades de executar qualquer investigação em ambiente digital em relação a áreas importantes da criminalidade. Subjacente a esta ideia está a criação de *paraísos digitais do crime*, para onde os agentes do crime se deslocariam impunemente, perante o olhar impotente do Estado, que se veria colocado perante uma «impossibilidade sistemática de investigar o crime relacionado com a Internet»[23].

[23] Cf. ULRICH SIEBER / CARL-WENDELIN NEUBERT, «Transnational Criminal Investigations in Cyberspace: Challenges to National Sovereignty», cit., pp. 296-302.

Mesmo nestes casos, porém, seria necessário que o meio utilizado fosse o *único* apto a proteger o interesse essencial contra o perigo grave e iminente. Daqui retiram os autores uma consequência relevante nos casos de impossibilidade (ou extrema dificuldade, quando aplicadas todas as medidas razoavelmente exigíveis, dentro dos constrangimentos de recursos e tempo existentes) de identificação do local onde se encontra a prova: é que se for possível, através do acesso transfronteiriço, identificar a localização dos dados informáticos pesquisados, então deverá o Estado actuante notificar o Estados pesquisado do acesso, requerendo a obtenção da prova através dos canais existentes em matéria de cooperação internacional. Em caso de recusa por parte do Estado pesquisado, os dados deveriam ser imediatamente eliminados pelo Estado actuante. Será apenas no caso de não ser possível, de todo, mesmo após aceder à informação visada, identificar o Estado onde a mesma se encontra armazenada, que o Estado actuante poderá copiá-la e utilizá-la em processo penal[24].

As dificuldades que esta interpretação do regime vigente gera para a investigação criminal em ambiente digital tem levado certa doutrina a procurar identificar lugares paralelos no direito internacional que outrora tenham justificado a criação de excepções à impossibilidade de ingerência em território estrangeiro. O objectivo é o de, por essa via, procurar descortinar se os fundamentos que levaram à gradual permissividade dos Estados perante ingerências pouco relevantes na sua soberania poderão alargar-se a casos como os da pesquisa transfronteiriça de dados informáticos[25].

Assim, KOOPS e GOODWIN começam por explorar a possibilidade de o ciberespaço poder configurar património comum da Humanidade, à semelhança do que prescreve a Convenção das Nações Unidas sobre Direito do Mar e o Acordo Relativo à Aplicação da Parte XI da mesma Convenção a propósito do leito do mar, dos fundos marinhos e oceânicos e do seu subsolo que se situam para além dos limites da jurisdição nacional. A comparação é ainda alargada ao regime constante do Tratado sobre os Princípios Que Regem as Actividades dos Estados na Exploração e Utilização do Espaço Exterior, Incluindo a Lua e Outros Corpos Celestes, assinado em Washington, Londres e Moscovo em 27 de Janeiro de 1967, comparando o ciberespaço ao espaço exterior. A comparação, que serve como mero exercício introdutório, é rapidamente abandonada pelos Autores, na medida em que a generalidade dos Estados pretende, evidentemente, reclamar soberania sobre os sistemas informáticos que se localizem no seu território[26].

Os Autores prosseguem a sua análise, convocando, já não o regime do património da Humanidade, mas sim o da *navegação* em alto mar. Referem que, apesar de o alto mar não se

[24] *Idem*, pp. 303-307.
[25] «*A critical approach to international law, as espoused by David Kennedy and Martti Koskenniemi among others, is that international law is permanently caught in the need to compromise between the positivist (i.e., that law is the outcome of an authoritative process, regardless of its content) and naturalist (i.e., that law is only law if it is both made in the right (authoritative) process and speaks to some broader goal of the international order, such as justice or fairness) traditions of law. What this means is that international law has to make a claim to being something more than simply state interests – otherwise it is just brute power; yet at the same time it needs to reflect the actual practice of states – otherwise it is just wishful thinking*» - BERT-JAAP KOOPS / MORAG GOODWIN, *Cyberspace, the cloud and cross-border criminal investigation – The limits and possibilities of international law*, cit., p. 65.
[26] *Idem*, pp. 67-68.

encontrar sujeito a qualquer reivindicação territorial, o mesmo não sucede com os navios que dele fazem uso, os quais se encontrarão sujeitos à jurisdição do país da sua bandeira.

Entre as limitações à liberdade de navegação encontram-se um conjunto de cenários contemplados pelo direito consuetudinário internacional, que incluem:

(i) O envolvimento dos barcos em actos de pirataria;

(ii) O tráfico de pessoas;

(iii) Ameaças ao Estado (que incluem actos de terrorismo e tráfico de droga) e

(iv) Casos de perseguição em curso (*hot pursuit*), ou seja, casos em que um navio persegue outro desde águas territoriais até ao alto mar. A ideia explorada pelos autores seria a de comparar a *cloud* ao alto mar e os fornecedores de serviços a navios, abrangidos pela jurisdição do seu país, mas sujeitos a *abordagens* decorrentes de excepções análogas às que acima se identificaram[27].

Por fim, os Autores referem-se ao caso da aquisição remota de imagens por teledetecção, através de satélite. A ideia é a de que também na década de 60 a utilização de satélites para recolha remota de imagens era vista por alguns como uma ingerência na soberania dos Estados, para o que seria necessária a sua autorização. O que torna esta comparação especialmente interessante é o facto de, à semelhança do que se refere quanto às pesquisas transfronteiriças, também a recolha de imagens implicava um grau de ingerência mensurável nos Estados. Ao passo que as pesquisas transfronteiriças despoletam reacções físicas, ainda que insignificantes, em sistemas informáticos localizados noutros Estados, a recolha de imagens por satélite implicava a emissão de radiação para identificar o relevo do terreno. Esta concepção viria a ser afastada pela criação do princípio céu aberto, que previa, em termos sumários, a liberdade de recolher e distribuir imagens através de satélite e de disseminá-las de forma não discriminatória[28].

Com este excurso, pretendem os Autores assinalar que também noutras alturas houve necessidade de consensualmente adaptar os quadros jurídicos vigentes em prol de um interesse comum entendido como benéfico. Poderia, questionam, ponderar-se se solução semelhante poderia ocorrer com este tema.

Também o Conselho da Europa tem procurado explorar uma solução para o problema do acesso transfronteiriço a dados informáticos. Assim, o Comité da Convenção sobre o Cibercrime junto do Conselho da Europa estabeleceu, na sua reunião plenária de 23 e 24 de Novembro de 2011, o sub-grupo *ad-hoc* sobre jurisdição e acesso transfronteiriço a dados e fluxos de dados (*Transborder Group)*, com o objectivo de «desenvolver um instrumento jurídico — como uma adenda à Convenção, um Protocolo ou Recomendação — que regule o acesso transfronteiriço a dados e fluxo de dados, bem como o uso de medidas de investigação

[27] *Idem*, pp. 68-71.
[28] *Idem*, pp. 71-72.

transfronteiriças na Internet e assuntos conexos, e para apresentar um relatório com as conclusões do Comité»[29].

Em 9 de Abril de 2013, o *Transborder Group* apresentou uma proposta com os elementos preliminares para um Protocolo Adicional à Convenção de Budapeste sobre o Cibercrime[30], no qual fez constar cinco propostas para enfrentar o problema da *loss of location*, a saber:

a) A aplicabilidade da excepção prevista no artigo 32.º, alínea *b)*, da Convenção a qualquer Estado, ainda que não signatário da Convenção sobre o Cibercrime, quando não seja claro o local de armazenamento dos dados ou quando os mesmos se encontrem em *movimento*[31], ainda que seguida de notificação do Estado no qual os dados se encontrem armazenados, uma vez descoberta a sua localização;

b) O acesso transfronteiriço mediante credenciais legitimamente obtidas, seguido da notificação do Estado no qual se encontrem armazenados os dados;

c) O acesso transfronteiriço em certos casos, com o objectivo de evitar a concretização de um perigo iminente, ofensa à integridade física, a fuga de um suspeito ou o perigo de destruição de elementos probatórios relevantes, novamente seguido de notificação ao Estado no qual se encontrassem armazenados os dados. Adicionalmente poderia ser criada uma disposição destinada a cobrir as situações de *boa fé*, em que, durante uma pesquisa, a autoridade competente não saiba se o sistema informático pesquisado se encontra em território estrangeiro, ou, mesmo que o saiba, não saiba em que território estrangeiro se encontra, ou tenha inadvertidamente obtido prova digital armazenada em território estrangeiro (em todos estes casos não seria necessário que o Estado em causa fosse parte da Convenção);

d) A simples remoção da limitação territorial da pesquisa informática, embora, neste caso, a medida apenas possa ocorrer em relação a Estados que sejam Partes na Convenção;

e) A utilização do critério do poder de disposição[32] (*power of disposal*), e que, em síntese, se traduz na ligação existente entre os dados visados e a pessoa ou pessoas que a eles têm, exclusiva ou colectivamente, acesso e que preservam o direito de os alterar,

[29] Cf. SUB-GRUPO AD-HOC SOBRE JURISDIÇÃO E ACESSO TRANSFRONTEIRIÇO A DADOS E FLUXOS DE DADOS JUNTO DO COMITÉ DA CONVENÇÃO SOBRE O CIBERCRIME (T-CY), *Transborder access and Jurisdiction: What are the options?*, cit., p. 4.

[30] Cf. SUB-GRUPO AD-HOC SOBRE JURISDIÇÃO E ACESSO TRANSFRONTEIRIÇO A DADOS E FLUXOS DE DADOS JUNTO DO COMITÉ DA CONVENÇÃO SOBRE O CIBERCRIME, *(Draft) elements of an Additional Protocol to the Budapest Convention on Cybercrime regarding transborder access to data*, T-CY(2013)14, 2013, disponível em: http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/T-CY(2013)14transb_elements_protocol_V2.pdf.

[31] Sendo certo que, como consta da proposta, esta opção poderia conflituar com o artigo 34.º da Convenção de Viena sobre o Direito dos Tratados, nos termos do qual «um tratado não cria obrigações nem direitos para um terceiro Estado sem o consentimento deste».

[32] Cf. JAN SPOENLE, «Cloud Computing and cybercrime investigations: Territoriality vs. the power of disposal», pp. 10-12, disponível em: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/internationalcooperation/2079_Cloud_Computing_power_disposal_31Aug10a.pdf.

eliminar, suprimir ou tornar inutilizáveis, bem como o direito de excluir o seu acesso e a sua utilização de qualquer modo a terceiros[33].

Com base no referido documento, o T-CY, na sua 9.ª reunião plenária, ocorrida em 4 e 5 de Junho de 2013, deliberou começar a preparação de um protocolo adicional à Convenção sobre o Cibercrime, com vista à regulação do acesso transfronteiriço[34], a começar após reflexão e diálogo com as partes interessadas, incluindo intervenientes do sector privado e autoridades de protecção de dados[35].

Por vicissitudes várias, até à data, não existe uma solução oficial adoptada e o grupo permanece a trabalhar nesse sentido.

4. A resposta nacional

Perante as dificuldades colocadas pela impossibilidade de aceder remotamente a informação armazenada no estrangeiro, e dada a tendencial ausência de consequências no foro diplomático e probatório deste tipo de práticas, certos Estados têm optado por prever o acesso transfronteiriço nas suas legislações nacionais.

É o caso, desde logo, da Bélgica, onde o legislador previu, no artigo 39*bis* do Código de Processo Penal, a possibilidade de ser alargada a pesquisa informática a outros Estados, independentemente da sua localização, desde que, quando se suspeite que a informação não esteja armazenada na Bélgica, a informação não seja eliminada mas apenas copiada e sob condição de o Ministro da Justiça informar o Estado pesquisado, quando este possa ser identificado (embora, segundo conste, esta notificação nunca tenha ocorrido)[36].

Em Portugal o legislador adoptou uma solução mais discreta na formulação mas, ao que tudo indica, mais ousada do que a belga. Ao suprimir, por comparação com a norma homóloga da Convenção sobre o Cibercrime, a limitação territorial à extensão da pesquisa informática a sistemas informáticos acessíveis através do primeiro sistema pesquisado (por exemplo, no caso dado no início desta apresentação), o investigador poderia, nos termos do artigo 15.º, n.º

[33] O legislador português incluiu um conceito semelhante no artigo 15.º, n.º 3, alínea a), da Lei do Cibercrime, ao prever a desnecessidade de recurso a autorização da autoridade judiciária para a realização de uma pesquisa informática quando «[a] mesma for voluntariamente consentida por quem tiver **a** disponibilidade ou controlo desses dados […]».

[34] Cf. SUB-GRUPO AD-HOC SOBRE JURISDIÇÃO E ACESSO TRANSFRONTEIRIÇO A DADOS E FLUXOS DE DADOS JUNTO DO COMITÉ DA CONVENÇÃO SOBRE O CIBERCRIME, *Draft Decision Preparation by the T-CY of a draft Additional Protocol to the Convention on Cybercrime (ETS 185) regarding transborder access to data*, T-CY(2013)18, disponível em: http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/T-CY(2013)18_TB_prot_mandate_v5.pdf.

[35] Cf. SUB-GRUPO AD-HOC SOBRE JURISDIÇÃO E ACESSO TRANSFRONTEIRIÇO A DADOS E FLUXOS DE DADOS JUNTO DO COMITÉ DA CONVENÇÃO SOBRE O CIBERCRIME, *Report of the Transborder Group for 2013*, T-CY (2013)30, p. 6, disponível em: http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/T-CY%282013%2930_Final_transb_rep_V5.pdf e T-CY, Abridged meeting report, T-CY (2013)28E rev, disponível em: http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/T-CY(2013)28_Plen10AbrRep_V3.pdf.

[36] Na ilustrativa expressão de Jan Kerkhofs, na Bélgica prevaleceria a *teoria do aquário*, o que significa que o investigador se comportaria como se estivesse a olhar para o interior de um aquário através do vidro, sem possibilidade de tocar no seu conteúdo, mas com o poder de fotografar a imagem que perante si se apresenta.

5, da Lei do Cibercrime, recolher a informação independentemente da sua localização. Como refere Pedro Verdelho «[e]sta norma é bastante aberta, deixando por regular muitos dos seus detalhes de aplicação ao caso concreto. Desde logo, por exemplo, não limita o acesso a computadores em território nacional. Isto é, legitima o acesso *virtual* a todo e qualquer computador, independentemente da sua localização física que, assim, pode ser em qualquer parte do mundo»[37]. A solução portuguesa aparenta admitir essa pesquisa num cenário de busca, e, portanto, a título excepcional – embora não seja evidente que essa pesquisa não possa ocorrer directamente por via do artigo 15.º, n.º 1, da Lei do Cibercrime, quando as credenciais de acesso estejam na posse do investigador –, sem prever especiais normas de apreensão para o efeito. Parece, contudo, que uma solução de compatibilização possível entre os interesses em causa pressuporia que a única modalidade de apreensão a realizar nestes casos seria a *cópia* e não qualquer das outras previstas no artigo 16.º, n.º 7, da Lei do Cibercrime.

Solução semelhante foi adoptada recentemente pelo legislador espanhol, que previu expressamente no artigo 588 *sexies* a possibilidade de serem realizadas pesquisas informáticas a sistemas de armazenamento massivo de informação, designadamente por via de extensão da pesquisa, sem que da norma conste qualquer limitação territorial em relação ao local onde se encontre armazenada a informação.

Embora pareça difícil que venha a formar-se um costume internacional sobre o tema do acesso transfronteiriço, em grande medida por questões de princípio dos Estados que não querem abdicar de qualquer parcela da sua soberania, tudo indica que o debate continuará a decorrer numa plataforma essencialmente académica ou no plano da discussão legislativa supranacional[38], enquanto uma parte cada vez maior dos operadores judiciários tenderá a ignorar o problema, por ignorância ou por despreocupação – eventualmente fundada – em relação a eventuais consequências no foro diplomático ou probatório daí decorrentes.

Afigura-se, contudo, da maior importância que o debate seja alargado e que se procure explorar uma solução adequada à realidade digital, se necessário repensando conceitos tradicionais que neste foro são de difícil aplicabilidade e procurando uma compatibilização de interesses adaptada às especificidades deste ambiente.

[37] PEDRO VERDELHO, *A obtenção de prova online*, em AA.VV. *Cibercrimen – Aspectos de Derecho penal y procesal penal. Cooperación internacional. Recolección de evidencia digital. Responsabilidad de los provedores de servicios de Internet* (org. Daniela Dupuy / Mariana Kiefer), Montevideo Buenos Aires: BdeF, 2016, p. 445.
[38] Sem prejuízo, naturalmente, de se continuarem a procurar soluções que tornem mais expeditos os mecanismos de auxílio mútuo, como é o caso da proposta de Regulamento do Parlamento Europeu e do Conselho sobre a Ordem de Produção e Preservação Europeia de prova digital em matéria criminal, publicada no dia 17 de Abril de 2018.

CENTRO
DE ESTUDOS
JUDICIÁRIOS