FACULDADE DE DIREITO UNIVERSIDADE NOVA DE LISBOA

CEDIS CENTRO DE I&D SOBRE DIREITO E SOCIEDADE

DIREITO, SEGURANÇA E DEMOCRACIA

A PROVA DIGITAL EM 2017 – REFLEXÕES SOBRE ALGUMAS INSUFICIÊNCIAS PROCESSUAIS E DIFICULDADES DA INVESTIGAÇÃO

The Digital Proof in 2017 - Reflections on Some Procedural Inadequacies and Difficulties of the Investigation

JOÃO GAMA GONÇALVES
Mestrando em Direito e Mercados Financeiros

RESUMO

As tecnologias de informação e comunicação trouxeram novos desafios não apenas no domínio da cibersegurança, cibercrime ou ciberdefesa mas também no respeitante à investigação judiciária e nomeadamente no tocante aos meios de prova, com o aparecimento da prova digital.

Poderosas ferramentas ficaram à disposição da investigação, sendo um dos desafios do legislador arranjar um adequado compromisso entre, por um lado, a segurança dos cidadãos, a realização da justiça e a descoberta da verdade (que podem ser reforçadas com os novos meios à disposição dos órgãos de polícia criminal) e, por outro lado, a

salvaguarda dos direitos, liberdades e garantias e a proteção dos dados pessoais e da privacidade.

Atendendo ao que está em jogo, cumpre identificar algumas áreas onde o poder de atuação dos órgãos de polícia criminal (e sobretudo da Polícia Judiciária) poderá ser agilizado e aumentado quando está em causa a "realidade" do ciberespaço.

PALAVRAS-CHAVE

Tecnologias de informação, prova digital, investigação, cibersegurança, cibercrime

ABSTRACT

Information and communication technologies have brought new challenges not only in the areas of cybersecurity, cybercrime or cyber-defense, but also in relation to judicial investigation and in particular regarding the means of proof, with the appearance of the digital evidence.

Powerful tools have been made available to investigation, and one of the challenges for the legislator is to make an appropriate compromise between, on one hand, citizen security, realization of justice and the discovery of truth (which can be strengthened by new means available to criminal police authorities) and, on the other hand, the rights, freedoms and guarantees and the protection of personal data and privacy.

Given what is at stake, it is necessary to identify some areas where the power of action of criminal police authorities (and especially the Judiciary Police) should be streamlined and increased when the "reality" of cyberspace is involved.

KEYWORDS

Information technologies, digital evidence, investigation, cybersecurity, cybercrime

Introdução: a era digital

Com o surgimento da internet, muitos foram os que previram que a face das comunicações seria alterada de forma indelével. E efetivamente, desde os seus primórdios, com o lançamento do projeto do Ministério da Defesa dos Estados Unidos da América, no final dos anos *sessenta*, que ficou internacionalmente conhecido por "ARPANET" [1] (programa inicialmente designado por "*Resource Sharing Computal Networks*" pela DARPA – Defense Advanced Research Projects Agency), os sistemas de informação não mais abrandaram uma galopante evolução, falando-se numa incontornável "Revolução Digital".

Visionários como Nicholas NEGROPONTE anteciparam a gradual transformação do mundo físico em mundo digital, conseguindo prever com apreciável exatidão o impacto que teria tal mudança nos sistemas de informação e no próprio quotidiano das pessoas[2].

A Era Digital veio promover uma crescente conversão de átomos em *bits*, sendo para tal nuclear o papel da internet (que, no essencial, corresponde ao sistema global de redes de computadores que se encontram conectadas entre si por intermédio de linhas telefónicas comuns, cabos de fibras óticas, satélites e outros serviços de telecomunicações), a qual permitiu uma grande complexificação das redes de informação. E, neste contexto digital, foram diversos os novos desafios que se colocaram, sobretudo ao nível da manutenção da segurança dos mais diversos sistemas informáticos e digitais, sendo ainda de relevar o surgimento de um novo "espaço" não euclidiano, idealizado ou concetualizado à luz da internet: o ciberespaço.

É em 1982 que William GIBSON utiliza pela primeira vez o termo ciberespaço na sua obra de ficção científica *Burning Chrome*[3] ; desde então, tem-se procurado concetualizar

[1] Para mais desenvolvimento sobre o ARPANET, nomeadamente a sua história, os seus objetivos e resultados, vide o relatório da DARPA, *A History of the ARPANET: The First Decade* (Report). Arlington, VA: Bolt, Beranek & Newman Inc. 1 April 1981.

[2] Como referiu o cientista fundador do Media Lab do Massachussetts Institute of Technology (MIT), "Consider a modern newspaper. The text is prepared on a computer; stories are often shipped in by reporters as e-mail. The pictures are digitized and frequently transmitted by wire as well. (…) This is to say that the entire conception and construction of the newspaper is digital, from beginning to end, until the very last step, when ink is squeezed onto dead trees. This is the step where bits becomes atoms. Now imagine that the last step does not happen in a printing plant, but that the bits are delivered to you as bits. You may elect to print them at home for all the conveniences of hard copy (for which reusable paper is recommended, so we all don't need a large pile of blank newsprint). Or you may prefer to download them into your laptop, palmtop, or someday into your perfectly flexible, one-hundredth-of-an-inch-thick, fullcolor, massively high-resolution, large-format, waterproof display". (NEGROPONTE, Nicholas, *Being Digital*, Hodder&Stoughton, 1995, p. 56).

[3] É contudo na obra *Neuromancer* que GIBSON nos faz uma descrição "visual" do que seria o ciberespaço "On the Sony, a twodimensional space war faded behind a forest of mathematically generated ferns, demonstrating the spacial possibilities of logarithmic spirals; cold blue military footage burned through, lab animals wired into test systems, helmets feeding into fire control circuits of tanks and war planes. "Cyberspace". A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphic representation of data abstracted from the banks of every computer in the human system.

este termo, com recurso a metáforas, sendo de realçar a posição de alguns autores, como Clay SHIRKY[4], que questionam se faz tão-pouco sentido falar da existência de um espaço verdadeiramente autónomo do mundo real.

Independentemente da melhor definição a dar[5], a verdade é que a área *aterritorial* do ciberespaço trouxe consigo o ensejo de uma utopia libertária ("information wants to be free"[6]), sendo que, para muitos, este deveria manter-se um espaço de total liberdade sem intervenção dos governos: SHIRKY é, de resto, um defensor do movimento da ciber-utopia[7], a qual não está isenta de críticas (sendo conhecidos alguns ferozes ataques, como os de Malcolm GLADWELL[8] ou de Evgeny MOROZOV[9]).

Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding...". (GIBSON, William, *Neuromancer*, 1984).

[4] "In the developed world, the experience of the average twenty-five-year-old is one of substantial overlap between online and offline friends and colleagues. The overlap is so great, in fact, that both the word and the concept of "cyberspace" have fallen into disuse. The internet augments realworld social life rather than providing an alternative to it. Instead of becoming a separate cyberspace, our electronic networks are becoming deeply embedded in real life". (SHIRKY, Clay, *Here Comes Everybody: The power of organizing without organizations* Penguin Books, 2008, p. 196).

[5] Sublinhe-se a definição de ciberespaço de Lino SANTOS e Armando MARQUES GUEDES: "Tal como noutros termos afins como sejam cibernauta, ciberguerra ou ciberarma, o prefixo "ciber-" apela ao imaginário do virtual e transporta o receptor para o contexto das tecnologias da informação e da comunicação (TIC). Diferentes sectores da sociedade usam o termo ciberespaço para se referirem a coisas tão distintas como a rede planetária de computadores, a possibilidade de realizar actividades através da Internet, ou o armazenamento de informação na cloud, pelo que, numa perspectiva abrangente, podemos definir ciberespaço como o conjunto "[d]as diferentes vivências do espaço associado às tecnologias e à computação" (Strate, 1999, p. 383)". (Breves reflexões sobre Poder e Ciberespaço, *in RDeS – Revista de Direito e Segurança, nº6 (julho/dezembro de 20150),* pp. 190-191).

[6] Steven LEVY explica, num artigo online, a história que esteve na origem desta expressão: a mesma terá nascido de uma conversa entre Stewart Brand e Steve Wosniak na primeira conferência de *hackers* de 1984 – cfr. https://backchannel.com/the-definitive-story-of-information-wants-to-be-free-a8d95427641c.

[7] SHIRSKY defende os benefícios da existência de comunidades online com ampla liberdade: "By lowering transaction costs, social tools provide a platform for communities of practice. (…)Communities of practice are inherently cooperative, and are beautifully supported by social tools, because that is exactly the kind of community whose members can recruit one another or allow themselves to be found by interested searchers. They can thrive and even grow to enormous size without advertising their existence in public (…). [sublinhado nosso]
(...) Every webpage is a latent community. Each page collects the attention of people interested in its contents, and those people might well be interested in conversing with one another, too". (SHIRKY, Clay, *Here* …, cit., pp. 100-102).

[8] Malcolm GLADWELL escreveu um artigo para o New Yorker, em 2010, onde critica frontalmente o modelo ciber-utópico preconizado por Shirky: "Shirky considers this model of activism an upgrade. But it is simply a form of organizing which favors the weak-tie connections that give us access to information over the strong-tie connections that help us persevere in the face of danger. It shifts our energies from organizations that promote strategic and disciplined activity and toward those which promote resilience and adaptability. It makes it easier for activists to express themselves, and harder for that expression to have any impact". (cfr. http://www.newyorker.com/magazine/2010/10/04/small-change-malcolm-gladwell).

[9] Em 2011, Evgeny MOROZOV (um antigo ciber-utopista!), vem criticar duramente a ingenuidade dos ciber-utopistas, lembrando que se, por um lado, a Internet pode ser uma importante ferramenta democrática, por outro lado também poderá servir para que regimes autoritários se tornem ainda mais fortes: "Cyber-utopians ambitiously set out to build a new and improved United Nations, only to end up with a digital Cirque du Soleil. Even if true—and that's a gigantic "if"—their theories proved difficult to adapt to non-Western and particularly nondemocratic contexts". (*The Net Delusion: The Dark Side of Internet Freedom*, PublicAffairs, 2011, Introduction xiii); "Information may, indeed, be the oxygen of the modern age, as Ronald Reagan famously alleged, but it could be that peculiar type of

Com efeito, apesar das vantagens inerentes ao desenvolvimento das tecnologias da informação e da comunicação (TIC) e à instituição da "aldeia global" graças ao poderoso veículo de informação que é o ciberespaço, não se podem ignorar as novas preocupações que resultam deste último: preocupações nacionais ligadas à utilização do ciberespaço para fins de guerra, espionagem ou de ciberterrorismo; preocupações empresariais e/ou profissionais relacionadas com a proteção da confidencialidade dos seus documentos (e com a proteção da propriedade intelectual), e até preocupações sociais (com a proliferação de meios que facilitam a expansão e maior visibilidade de atividades criminosas como a pedofilia ou o recrutamento para grupos terroristas).

Tendo o ciberespaço esta dupla-face, com vantagens e desvantagens, assume particular relevo a questão levantada por Armando MARQUES GUEDES e Lino SANTOS: será que o princípio da neutralidade da rede (segundo o qual a rede Internet deverá estar acessível sem discriminação de conteúdos, salvo exceções devidamente justificadas) é verdadeiramente compatível com uma segurança adequada aos perigos atualmente existentes? A melhor resposta é dada pelos Autores: "Este princípio beneficia os Estados mais desenvolvidos e a actual concentração de poder nas mega.dot.com, dificultando a aplicação de princípios de um Estado de Direito, como o da segurança dos seus cidadãos. O balanço entre este benefício e a crescente dificuldade em proteger as próprias infra-estruturas, deverá justificar uma tendência de "vestfaliarização" do ciberespaço: "Num futuro próximo, os Estados delinearão um acordo formal para por cobro ao actual ingovernável e caótico ciberespaço" do qual resultará um novo mapa com fronteiras e limites. Definidas as fronteiras, serão erigidos muros e criadas leis internas para assegurar o governo da rede e reestabelecer a ordem natural das coisas (Demchak & Dombrowski, 2011, p. 57)", concluindo em seguida "Em suma, sendo claro que o poder absoluto dos indivíduos cresceu, não é líquido afirmar o mesmo relativamente ao seu poder relativo. O ciberespaço e as novas tecnologias trouxeram poder a todos os agentes: indivíduos, empresas e Estados"[10].

A verdade é que, inevitavelmente, o desenvolvimento das TIC suscita algumas apreensões, desde logo pelo papel que o ciberespaço pode ter no desenvolvimento de

oxygen that helps to keep dictators on life support. What reasonable dictator passes up an opportunity to learn more about his current or future enemies? Finding effective strategies to gather such information has always been a priority for authoritarian governments". (*idem,* pp.148-149).

[10] SANTOS, Lino / MARGUES GUEDES, Armando, Breves …, cit., p. 207.

crimes, de conflitos e guerras [11], de terrorismo [12] e de ameaças à segurança de infraestruturas.

Por esse motivo, é, antes de mais, fundamental uma boa estratégia de cibersegurança, alicerçada nos 6 eixos de intervenção definidos na Resolução do Conselho de Ministros n,º 36/2015: estrutura de segurança do ciberespaço; combate ao cibercrime; proteção do ciberespaço e das infraestruturas; educação, sensibilização e prevenção; investigação e desenvolvimento; e a cooperação.

Nunca é demais reforçar a importância deste último pilar, da cooperação entre os mais diversos aliados e parceiros, nacionais ou internacionais. E, não menos importante para a proteção do ciberespaço será a definição de políticas de segurança e de defesa nacionais que assegurem uma atuação eficiente em caso de ciberataques (sendo, em todo o caso, necessária uma adequada coordenação e cooperação entre os diferentes intervenientes).

De resto, o modelo teórico tripartido, preconizado por Lino SANTOS, Rogério BRAVO e Paulo NUNES, assente em três domínios de atuação face a eventuais ciberataques (a saber: proteção simples, prossecução criminal e defesa do Estado[13]),

[11] Autores como Martin C. LIBICKI demonstram que o ciberespaço não é, na sua essência, um espaço de guerra, ainda que, através de uma metáfora utilizada por este autor, se perceba o poder intrínseco e transversal do ciberespaço: "Cyberspace, we are told, pervades the other domains in the sense that warfighters in each of the prior domains would be severely handicapped if their access to cyberspace were successfully challenged. Thus understood, cyberspace has become the new high ground of warfare, the one domain to rule them all and in the ether bind them, which, as this essay will argue, is the wrong way to view cyberspace and what militaries can do by operating "within" it". [sublinhado nosso] (LIBICKI, Martin C., *Cyberspace is Not a Warfighting Domain*, I/S: A Journal of law and policy for the information Society, volume 8, 2012, pp.321-322).
De resto, Lino SANTOS e Armando MARQUES GUEDES expõem cabalmente este duplo-sentido das palavras de LIBICKI: "O objectivo do autor foi o de relevar a transversalidade do ciberespaço relativamente aos restantes domínios "da natureza". No entanto, a alusão à fantasia de Tolkien e a referência ao poder do "anel" como instrumento de controlo de todas as criaturas da "Terra Média" – que encerra em si uma metáfora do poder (destrutivo) da técnica e da industrialização do início do século XX –, permite dar um outro sentido ao jogo de palavras de Libicki: o ciberespaço como domínio para o exercício de poder do Estado sobre os seus cidadãos, empresas e adversários (e aliados)". (*idem,* pp. 202-203).

[12] Sobre a importância de se repensar a legislação relativa a ameaças e ataques ciberterroristas, no sentido de se disciplinar a recolha, o tratamento e a partilha de informação entre os atores intervenientes da prevenção e investigação criminal no âmbito do combate ao ciberterrorismo, vide BRAVO, Rogério, Do espectro de conflitualidade nas redes de informação: por uma reconstrução conceptual do terrorismo no ciberespaço, *in Revista de Investigação Criminal, n.º2,* ASFIC / PJ, Novembro 2011.

[13] Para maior desenvolvimento da protecção do Ciberespaço e da articulação dos três domínios de actuação mencionados (proteção simples, da prossecução criminal e da defesa do Estado), vide SANTOS, Lino / BRAVO, Rogério / NUNES, Paulo Viegas, *Protecção do ciberespaço: Visão analítica*, 2012.

começa a fazer escola, não sendo de espantar que já vá surgindo doutrina oriunda de órgãos de polícia criminal como a GNR a defender a generalização deste modelo[14].

No entanto, as questões suscitadas pela revolução digital não se colocam unicamente nos planos da estratégia nacional de cibersegurança, da ciberdefesa, do ciberterrorismo ou do cibercrime. As TIC encontram-se hoje presentes em praticamente todas as dimensões da sociedade, tanto no domínio empresarial (uma vez que as organizações empresariais se encontram plenamente integradas na sociedade da informação e dependem, também elas, cada vez mais dos sistemas de informação) como no próprio quotidiano dos cidadãos (atendendo à crescente integração de tecnologias "carregadas" de dados pessoais no dia-a-dia da pessoa comum).

Assim, tratando-se de um fenómeno absolutamente transversal, o legislador procurou acompanhar as modificações que os novos meios de informação trouxeram; foi o que aconteceu, por exemplo, ao nível do tratamento e proteção dos dados pessoais dos cidadãos, mas também ao nível da investigação judiciária.

É justamente neste último ponto que nos focaremos: efetivamente, com as TIC (tecnologias de informação e comunicação) surgiram ponderosas ferramentas que poderiam ser utilizadas pela investigação criminal, sendo fundamental delimitar o alcance e os limites desse novo meio de prova: a prova digital.

Importa pois analisar a legislação atualmente em vigor no respeitante à prova digital, procurando descortinar as insuficiências legais ainda existentes e as dificuldades da investigação, e suscitando algumas potenciais soluções para uma melhor investigação no âmbito da descoberta material da verdade.

A prova digital

Definição, natureza e princípios em vigor

No contexto da prova digital, encontramo-nos em pleno *ambiente digital*, conceito que não tem um significado jurídico propriamente dito mas cuja noção tem a utilidade de estabelecer uma fronteira compreensível entre o contexto físico (materializado numa realidade apreensível pelos sentidos) e o contexto digital (imaterial e impercetível aos

[14] Na página 54 de *O Papel da GNR no Contexto da Cibersegurança Nacional* (Instituto de Estudos Superiores Militares, Curso de Estado-Maior Conjunto, 2015), o autor Paulo Daniel Duarte MACHADO defende que, na proteção simples, a GNR atua através do CISRT; na proteção criminal, a GNR atua como órgão de polícia criminal; e na defesa do Estado, a GNR colabora nos termos legais.

sentidos sem a mediação de sinais elétricos). Recorremos à definição de David Silva RAMALHO: "o conceito de *ambiente digital* engloba apenas os dados informáticos que, de algum modo, são criados, processados, armazenados e são identificáveis em sistemas informáticos, de modo a que podem ser acedidos directa ou remotamente. Será, portanto, aquilo que jaz em forma binária e que é virtualmente acessível a um utilizador através da mediação de tecnologias de informação"[15].

Assim, a prova digital "pode definir-se como qualquer tipo de informação, com valor probatório, armazenada [em repositório electrónico-digital de armazenamento] ou transmitida [em sistemas e redes informáticas ou redes de comunicações electrónicas, privadas ou publicamente acessíveis], sob a forma binária ou digital", segundo Benjamin SILVA RODRIGUES[16].

Já na terminologia de Armando DIAS RAMOS, a prova digital pode ser definida como toda e qualquer "informação passível de ser obtida ou extraída de um dispositivo eletrónico (local, virtual ou remoto) ou de uma rede de comunicações», razão pela qual «esta prova digital, para além de ser admissível, deve ser também autêntica, precisa e concreta"[17].

Em todo o caso, David Silva RAMALHO é perentório em afirmar que não se deve confundir prova digital com prova eletrónica, que "abrange, não apenas a prova em formato digital, mas também a prova em formato analógico, como sejam gravações em fita vídeo e áudio ou fotografias em rolo fotográfico, os quais, apesar de digitalizáveis, não têm a sua origem em formato digital"[18].

Acontece que a prova digital constitui uma categoria ainda não totalmente autonomizada, sendo necessário recorrer à analogia ou à interpretação extensiva de normas referentes a outras categorias probatórias, nomeadamente por força do art.º 189.º do Código de Processo Penal (após a alteração pela Lei n.º 47/2007, de 29 de agosto).[19]

---

[15] RAMALHO, David Silva, *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, Almedina, 2017, p. 37.

[16] RODRIGUES, Benjamim Silva, *Direito Penal Parte Especial, Tomo I, Direito Penal Informático-Digital*, Coimbra, 2009, p. 722.

[17] DIAS RAMOS, Armando, *A Prova Digital em Processo Penal*, Chiado Editora, 2014, versão eBook, p. 97.

[18] RAMALHO, David Silva, *Métodos* …, cit., p. 100.

[19] "Artigo 189.º/CPP:
(Extensão)
1 - O disposto nos artigos 187.º e 188.º é correspondentemente aplicável às conversações ou comunicações transmitidas por qualquer meio técnico diferente do telefone, designadamente correio electrónico ou outras formas de transmissão de dados por via telemática, mesmo que se encontrem guardadas em suporte digital, e à intercepção das comunicações entre presentes. 2 - A obtenção e junção aos autos de dados sobre a localização celular ou de registos da realização de conversações ou comunicações só podem ser ordenadas

Apesar de alguma legislação ter conferido à prova digital uma certa regulação "autónoma" _ sobretudo com as regras relativas à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações plasmadas na Lei n.º 32/2008, de 17 de julho, e com as regras processuais constantes na Lei do Cibercrime (Lei n.º 109/2009, de 15 de Setembro) _, a verdade é que não se desenvolveu particular densidade ou sistemática normativa neste âmbito.

Tal dificuldade no enquadramento legal resulta, em grande parte, da complexidade da prova digital, indelevelmente associada à própria complexidade da "*realidade*" cibernética.

Conforme ensina o Professor e Inspetor-chefe da Polícia Judiciária responsável pelo combate à criminalidade informática, Rogério BRAVO, "na realidade, aquilo que de facto se protege no Direito Penal da Criminalidade Informática, é, por um lado, a disponibilidade, a confidencialidade, o não repúdio e a integridade dos dados, que interpretados, constituem informação; por outro lado, protege-se a disponibilidade, a confidencialidade e a integridade do processamento electrónico, nas diferentes fases de integração tecnológica que permite a acumulação, o armazenamento e a transmissão desses dados"[20].

Ora, no contexto da indelével necessidade de preservação da prova, a própria natureza da prova digital dificulta a sua correta regulação: note-se que a prova digital tem uma natureza intrinsecamente efémera, instável e facilmente alterável, sendo que esta mutabilidade dificulta a preservação da integridade da prova bem como o fundamental não repúdio da mesma.

A verdade é que a prova digital, devido a esta fragilidade, tem de ser tratada de forma cuidada, na medida em que um mero descuido poderá efetivamente torná-la inutilizada. De resto, justamente devido à sua complexidade e "delicadeza", DIAS RAMOS considera que, de entre as classificações probatórias tipificadas, se deve incluir a prova digital na prova pericial (por exigir conhecimentos técnicos qualificados de quem a recolhe), sendo que, não obstante a "imaterialidade" da prova digital (que não é suscetível de

ou autorizadas, em qualquer fase do processo, por despacho do juiz, quanto a crimes previstos no n.º 1 do artigo 187.º e em relação às pessoas referidas no n.º 4 do mesmo artigo".

[20] BRAVO, Rogério, *As Tecnologias de Informação e a Compressão dos Direitos, Liberdades e Garantias: os efeitos das regras "10/10" e "1/1"*, 2012, p. 1.

apreensão material[21]), esta também poderá ser classificada enquanto prova documental (na medida em que "possa ser corporizada em escrito ou por outro meio técnico, como, por exemplo, a impressão fotográfica ou audiovisual de uma mensagem de correio eletrónico"[22]). Desta forma, o investigador criminal que apreenda a prova digital tem de saber lidar com este tipo específico de prova (não só na apreensão, transporte e manuseamento mas também na posterior análise da mesma): e foi desta necessidade que resultou a lei da conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas (Lei n.º 32/2008, de 17 de julho).

Independentemente da categorização que seja feita deste tipo de prova, ser-lhe-ão sempre aplicáveis os princípios gerais que impõem restrições e limites a todos os meios de obtenção de prova. Neste âmbito, por exemplo, o princípio da investigação (ou da verdade material) concede ao tribunal a competência para ordenar todos os meios de prova necessários para a descoberta da verdade material dos factos, ainda que exista um limite à investigação por parte do tribunal: o princípio da verdade processual (suscitando questões de admissibilidade, para que não existam excessos na procura da verdade material). Igualmente importante é o princípio da livre apreciação de prova (o art.º 127.ºCPP estabelece que "salvo quando a lei dispuser diferentemente, a prova é apreciada segundo as regras da experiência e a livre convicção da entidade competente"[23]).

Importa ainda relevar que, na esteira da doutrina de SILVA RODRIGUES[24], são aplicáveis, à obtenção da prova digital, além dos princípios relativos à prova contidos no processo penal, os princípios específicos contidos na *International Hi-Tech Crime and Forensics Conference de Outubro de 1999.*[25]

---

[21] "Efectivamente, como diz Breno Lessa (2009), um "documento eletrónico [textos, sons, imagens, etc.] nada mais é do que uma sequência de números binários (isto é, zero ou um) que, reconhecidos e traduzidos pelo computador, representam uma informação»; tem a «sua forma original em bits, ou seja, não é impresso ou assinado em papel: sua circulação e verificação de autenticidade se dão em sua forma original, eletrônica". (BRENO LESSA, *apud* MILITÃO, Renato Lopes, *A Propósito da Prova Digital no Processo Penal,* Faculdade de Direito e de Ciências Sociais e Humanas da Universidade de Lisboa).

[22] DIAS RAMOS, *A Prova* …, cit., p. 97.

[23] Para mais desenvolvimento, vide ALMEIDA, Ivo Filipe de, *A Prova Digital*, Universidade Autónoma de Lisboa, 2014, pp. 20-24.

[24] RODRIGUES, *Direito Penal*…, cit., pp. 726 e segs.

[25] "These principles were presented and approved at the International Hi-Tech Crime and Forensics Conference in October 1999. They are as follow:

- Upon seizing digital evidence, actions taken should not change that evidence.
- When it is necessary for a person to access original digital evidence, that person must be forensically competent.
- All activity relating to the seizure, access, storage, or transfer of digital evidence must be fully documented, preserved, and available for review.

Destacamos aqui princípios como o princípio de não alteração da prova no ato de recolha, o princípio da qualificação do investigador forense digital, o princípio de preservação em todas as fases processuais da prova digital (recolha, acesso, armazenamento e transferência da mesma), o princípio de responsabilidade pessoal (aplicável a todos os profissionais da investigação forense digital enquanto tenham em sua posse a prova digital), e a responsabilização dos vários intervenientes na produção da prova digital (que se encontram adstritos ao cumprimento destes princípios).

Parece-nos, por fim, relevante elencar aqui alguns princípios de tratamento de dados pessoais, constantes na Lei de Proteção de Dados Pessoais (Lei n.º 67/98, de 26 de outubro).

Antes de mais, nos termos da Lei de Proteção de Dados Pessoais (Lei n.º 67/98, de 26 de outubro), no artigo 3.º, são dados pessoais "qualquer informação de qualquer natureza e independentemente do respectivo suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável», sendo que «é considerada identificável a pessoa que possa ser identificada directa ou indiretamente, designadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social". Como tal, desde logo se percebe que a identidade tem sempre como referência uma pessoa singular identificada ou identificável (ou seja, uma pessoa física) _ o que suscitará algumas questões ao nível da identidade digital (conforme será abordado no **ponto 3.6**).

A verdade é que este diploma legal visa, por um lado, consagrar direitos dos titulares de dados pessoais, como o direito ao esquecimento (segundo o qual apenas se pode conservar os dados pessoais durante o período estritamente necessário – cfr. art.º 5.º/1/ alínea e) da Lei n.º 67/98, de 26 de outubro), o direito à curiosidade (todos os cidadãos podem perguntar a qualquer entidade se esta detém dados pessoais acerca da sua pessoa

- An individual is responsible for all actions taken with respect to digital evidence while the digital evidence is in their possession.
- Any agency that is responsible for seizing, accessing, storing, or transferring digital evidence is responsible for compliance with these principles.

Other items recommended by IOCE for further debate and/or facilitation included:

- Forensic competency and the need to generate agreement on international accreditation and the validation of tools, techniques, and training;
- Issues relating to practices and procedures for the examination of digital evidence; and
- The sharing of information relating to hi-tech crime and forensic computing, such as events, tools, and techniques". (retirado do site *online* do FBI: https://archives.fbi.gov/archives/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm , consultado no dia 21/05/2017.

– cfr. art.º 11.º n.º 1, *alínea a)*, 1ª parte), o direito de informação (art.º 10.º), o direito de acesso aos dados pessoais (art.º 11.º), ou o direito de oposição (segundo o qual o titular dos dados poderá opor-se ao tratamento dos seus dados pessoais, desde que tenha razões legítimas para tal – cfr. art.º 12.º), entre outros[26].

Por outro lado, são particularmente importantes os princípios que têm de ser tidos em consideração no tratamento de dados pessoais: o princípio da finalidade (os dados não podem ser tratados posteriormente com um fim incompatível com essas finalidades – cfr. art.º 5.º n.º 1 *alínea b)*), o princípio da transparência do art.º 2.º (que pressupõe que o responsável pelo tratamento de dados esteja devidamente identificado, e que é efetivado também pelo direito de informação do art.º 10.º e pelo direito de acesso do art.º 11.º), o princípio da qualidade dos dados do art.º 5.º n.º 1 (sendo que os dados devem ser tratados de forma lícita (*alínea a)*) e ser adequados, pertinentes e não excessivos relativamente às finalidades para que são recolhidos e posteriormente tratados (*alínea c)*), entre outros[27].

Finalmente, saliente-se o princípio da confidencialidade ou inviolabilidade das comunicações eletrónicas vertido no art.º 4.º da Lei nº 41/2004, de 18 de agosto (relativa à proteção de dados pessoais e privacidade nas telecomunicações), que impõe, no n.º 2, a proibição de escuta, a instalação de dispositivos de escuta, o armazenamento ou outros meios de interceção ou vigilância de comunicações e dos respetivos dados de tráfico sem o consentimento expresso dos utilizadores (salvo as exceções previstas na lei).

Concluída esta breve resenha acerca da proliferação de princípios aplicáveis à prova digital, cumpre agora atentar nas normas processuais especificamente direcionadas para obtenção de prova digital.

Normas basilares do regime processual em vigor no âmbito da prova digital

Parece-nos pacífico que a prova digital tem atualmente relevância tanto enquanto prova (ou seja como forma de o tribunal apurar a verdade material dos factos) como

[26] Para mais desenvolvimento, vide CASTRO, Catarina Sarmento e, Protecção de Dados Pessoais na Internet, *in Sub Judice n.º 35*, Almedina, Abril – Junho 2006

[27] Para mais desenvolvimento, vide CASTRO, *idem*.

enquanto meio de prova (ou seja, como modo de delimitar os instrumentos que se afiguram essenciais para a investigação criminal).

Uma das questões fundamentais relativas à prova digital foi cabalmente colocada por Jorge MOURAZ LOPES e por Carlos Antão CABREIRO: "A questão fulcral assenta na construção de uma base formal e legal sobre a admissibilidade da prova digital, seja ela proveniente da actividade da investigação (por exemplo, buscas e apreensões), seja resultante dos registos que uma comunicação possa ter deixado nos denominados operadores de comunicações (por exemplo, dados de tráfego), que permita que o sistema judicial conte com uma prova autêntica, precisa, completa e em conformidade com o princípio de legalidade"[28].

Importa, assim, discorrer sobre o regime legal atualmente em vigor (ainda que não esteja sistematizado num único diploma), para depois refletir sobre algumas lacunas ou insuficiências existentes na prática e/ou na lei.

As principais normas aplicáveis encontram-se previstas em três diplomas distintos (Código de Processo Penal, Lei do Cibercrime e Lei da Conservação de Dados ou Tratados no Contexto da Oferta de Serviços de Comunicações Eletrónicas), diplomas esses que não têm uma "coexistência" harmoniosa, havendo diversos autores que apontam o dedo à falta de articulação entre os mesmos[29].

Desde logo, a prova digital encontra-se regulada nos artigos 187.º e 188.º do CPP, por remissão dos artigos 189.º e 190.º (cfr. **nota de rodapé 19**): a lei processual penal confere os mesmos pressupostos de admissibilidade e formalidades às conversações ou comunicações transmitidas por correio eletrónico ou outras formas de transmissão de dados por via telemática que atribui às interceções das escutas telefónicos.

Por outro lado, a Lei n.º 109/2009, de 15/09, transpôs para a ordem jurídica portuguesa a Decisão-Quadro n.º2005/222/JAI, do Conselho, de 24 de fevereiro, e adaptou ao direito português a Convenção sobre o Cibercrime, do Conselho da Europa, estabelecendo nomeadamente disposições penais materiais e processuais que acabam por constituir como que um regime processual penal específico da prova digital.

[28] LOPES, José Mouraz / CABREIRO, Carlos Antão, A Emergência da Prova Digital na Investigação da Criminalidade Informática, *in Sub Judice n.º 35*, Almedina, Abril – Junho 2006.

[29] Para um maior desenvolvimento dos problemas de articulação entre os três diplomas legais principais relativos à prova digital, vide CORREIA, João Conde, Prova digital: as leis que temos e a lei que devíamos ter, *in Revista do Ministério Público nº 139*, Julho – Setembro 2014.

Relativamente às medidas processuais gerais, esta Lei do Cibercrime veio regular sobretudo: a preservação expedita de dados (art.º 12.º); a revelação expedita de dados de tráfego (art.º 13.º); a injunção para apresentação ou concessão do acesso a dados (art.º 14.º); a pesquisa de dados informáticos (art.º 15.º); a apreensão de dados informáticos (art.º 16.º); a apreensão de correio eletrónico e registos de comunicações de natureza semelhante (art.º 17.º); e a interceção de comunicações (art.º 18.º).

São ainda de salientar as medidas de cooperação internacional fixadas nesta Lei n.º 109/2009: a preservação e revelação expeditas de dados informáticos em cooperação internacional (art.º 22.º); a pesquisa, apreensão e divulgação de dados informáticos em cooperação internacional (art.º 24.º); o acesso das autoridades estrangeiras competentes, sem necessidade de pedido prévio às autoridades portuguesas, a dados informáticos armazenados em sistema informático localizado em Portugal, quando publicamente disponíveis (art.º 25.º, *al. a)*); a receção ou acesso das autoridades estrangeiras competentes, sem necessidade de pedido prévio às autoridades portuguesas, através de sistema informático localizado no seu território, a dados informáticos armazenados em Portugal, mediante consentimento legal e voluntário de pessoa legalmente autorizada a divulgá-los (art. 25.º, *al. b)*).

Ora, importa sublinhar que a Lei n.º 109/2009 é cumulativa com a Lei n.º 32/2008, de 17 de julho, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações (conforme expressamente previsto no art.º 11 n.º 2: "As disposições processuais previstas no presente capítulo não prejudicam o regime da Lei n.º 32/2008, de 17 de Julho"). De resto, autores como Paulo DÁ MESQUITA debruçam-se sobre os problemas que advêm da cumulação entre estes dois diplomas legais[30].

A título de exemplo dessa sobreposição nem sempre clara, a Lei n.º 32/2008, de 17 de julho, viu o regime processual nela constante (nomeadamente, o artigo 3.º n.º 1 e 2, e o artigo 9.º) revogado e substituído pelo regime processual contido na Lei n.º 109/2009 para todos os dados que não estejam especificamente previstos no artigo 4.º n.º1 daquela lei: o

[30] DÁ MESQUITA, Paulo, *Processo Penal, Prova e Sistema Judiciário*, Coimbra Editora, 2010, pp. 110-111.

douto acórdão do Tribunal da Relação de Évora de 06.01.2015, no âmbito do processo 6793/11.2TDLSB-A.E1, relator João Gomes de Sousa, veio reforçar este entendimento[31].

No entanto, algumas regras importantes estão contidas nesta Lei n.º 32/2008: por exemplo, a conservação e a transmissão dos dados necessitam forçosamente de ter por finalidade exclusiva a investigação, deteção e repressão de crimes graves (art.º 3.º), devendo a transmissão dos dados ser ordenada ou autorizada por despacho do juiz (art.º 3.º/2, que remete para o art.º 9.º); neste diploma, são identificadas as categorias de dados que devem ser conservadas pelos fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou de uma rede pública de comunicações (art.º 4.º), estabelecendo-se que a CNPD deve manter um registo eletrónico atualizado das pessoas especialmente autorizadas a aceder aos dados (art.º 8.º), havendo ainda regras quanto à proteção e segurança dos dados (7.º) e quanto à destruição dos mesmos (art.º 11.º).

Note-se, por fim que o art.º 9.º nº 4 refere especificamente que a decisão judicial de transmitir os dados deve respeitar os princípios da adequação, necessidade e proporcionalidade.

Algumas dificuldades da investigação no âmbito do ciberespaço (e inerentes insuficiências processuais)

Por um lado, se o ciberespaço trouxe consigo novas "realidades" e inerentemente novos crimes, específicos, que só existem neste espaço (por exemplo, todos os crimes contra os sistemas informáticos) e se ainda facilitou mais o desenvolvimento de outros tantos crimes subsumíveis a tipos legais que já eram preexistentes ao ciberespaço (como a extorsão, a devassa da vida privada, etc. _ não havendo, neste caso, necessidade de alterações legislativas quanto ao código penal), a verdade é que, por outro lado, trouxe uma indesmentível necessidade de se legislar no âmbito da investigação (tanto para aproveitamento das autoridades policiais dos novos poderosos meios de obtenção de prova, como para limitar o acesso e utilização dos mesmos de modo a não ferir nucleares direitos liberdades e garantias).

[31] O acórdão do Tribunal da Relação de Évora de 06.01.2015, no âmbito do processo 6793/11.2TDLSB-A.E1, relator João Gomes de Sousa, determinou que "não deixamos de afirmar a conclusão de que o regime da Lei 32/2008 – designadamente o artigo 3º, nº 1 e 2 e o artigo 9º, nº 3 – se mostram revogados e substituídos pelo regime processual contido na Lei nº 109/2009". (acórdão disponível em: http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/847dae6b85353cb880257de10056ff4c?OpenDocument).

A legislação atualmente em vigor suscita algumas questões no respeitante às complexas particularidades da investigação relacionada com prova digital, admitindo-se que, nalguns aspetos, poderá ser profícua a adoção de um enquadramento legal mais adaptado e eficiente e de procedimentos mais agilizados e apropriados à realidade cibernética. É pois sobre algumas dificuldades que subsistem na prática e/ou insuficiências do regime legal em vigor que irão incidir as seguintes reflexões.

Na recolha de prova – os problemas relativos aos métodos ocultos de investigação criminal em ambiente digital (as restrições de direitos, liberdades e garantias)

A prova digital tem uma complexidade acentuada derivada das suas especificidades técnicas, conforme já foi anteriormente explanado (no **ponto 2.1**); contudo, no plano legislativo, apenas se tem efetuado uma analogia com os regimes de outros meios de prova.

O facto é que a prova digital se encontra atualmente disseminada em praticamente todas as vertentes do nosso quotidiano: telemóveis, *tablets*, computadores, máquinas fotográficas, sistemas de videovigilância, gravadores de áudio, e até em automóveis e em eletrodomésticos a podemos encontrar, para mencionar alguns exemplos.

Todos estes aparelhos contêm fontes diferentes de prova, cada qual exigindo um processo diferente de recolha de prova, de acordo com a própria ENISA (European Union Agency for Network and Information Security)[32].

A recolha da prova digital é por isso complexa, devendo obedecer aos cinco princípios estabelecidos pela ENISA: o princípio da integridade dos dados ("No action taken […] should change data which may subsequently be relied upon in court"[33]), o princípio da cadeia de custódia da prova (que se traduz no processo de preservação da integridade da prova digital)[34], o princípio do apoio especializado ("Specialist support needs to be

[32] Refere a ENISA: "There are numerous sources of digital evidence and each requires a different process for gathering that evidence as well as different tools and methods for capturing it. It is not just the personal computer, laptop, mobile phone or Internet that provide sources of digital evidence, any piece of digital technology that processes or stores digital data could be used to commit a crime. The device and information it contains may store relevant digital evidence for proving or disproving a suspected offence*".* (ENISA, *Electronic evidence – a basic guide for First Responders (Good practice material for CERT first responders,* 2014, p.4).

[33] *Idem*, p. 6.
[34] *Idem*, p. 7.

requested as soon as possible when evidence gathering raises some specific (technical issues) and the first responders in charge of the evidence collection is not familiar with the issue or its implications. As there exist so many different systems and technical situations, it is almost impossible for a digital forensics expert to have the specific know-how on how to deal with all these sorts of electronic evidence. This is why it is so crucial to call in the right specialist"[35]), o princípio do treino apropriado ("Appropriate and constant training should be provided to all first responders dealing with digital forensic"[36]), e o princípio da legalidade ("The person in charge of the investigation has overall responsibility for ensuring that the law and these principles [the principles of digital evidence] are adhered to"[37]).

Existem preocupações que vão desde o momento da chegada ao local do crime à avaliação e apresentação da prova[38], e que se alastram ao risco de erro por força de influências externas (ou as *evidence dynamics*, na terminologia de Eoghan CASEY) promovidas pelos agentes do crime, pelas próprias vítimas ou ainda pelos investigadores que recolhem a prova[39].

A verdade, porém, é que o legislador nacional não estabeleceu um modelo de recolha, preservação e apresentação da prova digital, pelo que a ciência forense digital portuguesa se pode basear, *grosso modo*, no modelo proposto pelo NIST (National Institute

[35] *Idem*, p. 7.

[36] *Idem*, p. 8.

[37] *Idem*, p. 8.

[38] Para maior desenvolvimento, vide ENISA, *Electronic*…, cit.

[39] CASEY explica o conceito de *evidence dynamics* recorrendo a alguns exemplos: *"*Offenders, victims, first responders, digital evidence examiners, and anyone who had access to digital evidence prior to its preservation can cause evidence dynamics. Some examples of evidence dynamics encountered in past cases:

- A system administrator attempted to recover deleted files from a hard drive by installing software on an evidential computer, saving recovered files onto the same drive. This process overwrote unallocated space, rendering potentially useful data unrecoverable.
- Consultants installed a pirated version of a forensic tool on the compromised server. In addition to breaking the law by using an unlicensed version of digital forensic software, the installation altered and overwrote data on the evidential computer.
- Responding to a computer intrusion, a system administrator intentionally deleted an account that the intruder had created and attempted to preserve digital evidence using the standard backup facility on the system. This backup facility was outdated and had a flaw that caused it to change the times of the files on the disk before copying them. Thus, the date-time stamps of all files on the disk before copying them. Thus, the date-time stamps of all files on the disk were changed to the current time, making it nearly impossible to reconstruct the crime (…)". (CASEY, Eoghan, *Digital Evidence and Computer Crime – Forensic science, computers and the internet,* Academic Press, 2011, p. 27.

for Standards and Technology), baseado em quatro etapas: a recolha (*collection*), o exame (*examination*), a análise (*analysis*) e o relatório (*reporting*)[40].

Ora, as peculiaridades da recolha de prova digital também são acompanhadas de alguns problemas jurídicos que se prendem com a utilização de métodos ocultos pela investigação criminal.

Manuel da COSTA ANDRADE define-os do seguinte modo: "os métodos ocultos de investigação representam uma intromissão nos processos de acção, interação e comunicação das pessoas concretamente visadas, sem que estas tenham conhecimento do facto nem dele se aperceba"[41]).

A verdade é que não é possível não reconhecer a esta ocultação de métodos uma relevância assinalável no que tange à procura da verdade e ao combate à criminalidade. Tem contudo um "custo" não negligenciável: o sacrifício de alguns direitos fundamentais.

Por esse mesmo motivo se estabeleceram limites à descoberta da verdade; desde logo, a Constituição da República Portuguesa estabeleceu, no seu art.º 32.º n.º 8, que "são nulas todas as provas obtidas mediante tortura, coação, ofensa da integridade física ou moral da pessoa, abusiva intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações".

Por sua vez, o art.º 126.º do CPP desenvolve este artigo da CRP, prevendo os métodos proibidos de prova[42].

---

[40] Para uma explicação detalhada de cada uma destas quarto etapas, vide RAMALHO, *Métodos*…, cit., pp. 117-130.

[41] COSTA ANDRADE, Manuel da, *"Bruscamente no Verão Passado", a reforma do Código do Processo Penal – Observações Críticas sobre uma lei que podia e devia ter sido diferente*, Coimbra Editora, 2009, p.105.

[42] "Artigo 126.º do CPP
(Métodos proibidos de prova)
1 - São nulas, não podendo ser utilizadas, as provas obtidas mediante tortura, coacção ou, em geral, ofensa da integridade física ou moral das pessoas.
2 - São ofensivas da integridade física ou moral das pessoas as provas obtidas, mesmo que com consentimento delas, mediante:
a) Perturbação da liberdade de vontade ou de decisão através de maus tratos, ofensas corporais, administração de meios de qualquer natureza, hipnose ou utilização de meios cruéis ou enganosos;
b) Perturbação, por qualquer meio, da capacidade de memória ou de avaliação;
c) Utilização da força, fora dos casos e dos limites permitidos pela lei;
d) Ameaça com medida legalmente inadmissível e, bem assim, com denegação ou condicionamento da obtenção de benefício legalmente previsto;
e) Promessa de vantagem legalmente inadmissível.
3 - Ressalvados os casos previstos na lei, são igualmente nulas, não podendo ser utilizadas, as provas obtidas mediante intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações sem o consentimento do respectivo titular.
4 - Se o uso dos métodos de obtenção de provas previstos neste artigo constituir crime, podem aquelas ser utilizadas com o fim exclusivo de proceder contra os agentes do mesmo".

Ora as proibições de prova tanto se referem às proibições de produção de prova (proibições de temas de prova; proibições de meios de prova; proibições de métodos de prova) como às proibições de valoração de prova (proibição de se utilizar certos meios de prova como fundamento para determinada decisão desfavorável ao arguido)[43].

E é sobretudo ao nível da proibição de valoração de prova que têm ocorrido as maiores dificuldades em encontrar um equilíbrio entre a descoberta da verdade (e a realização da justiça) e a tutela dos direitos fundamentais (como o direito à privacidade dos cidadãos).

Somente casuisticamente, e com fundamento na gravidade do crime, se poderá aferir se se pode justificar a valoração de uma prova *a priori* proibida: por exemplo, no caso da valoração de diários íntimos, díspares têm sido os entendimentos, em diversos tribunais e em diversos países; sendo que, nalgumas situações, atendendo à gravidade do crime em causa, se pode justificar a valoração do diário íntimo. Conforme argumentou o douto acórdão do Supremo Tribunal de Justiça de 03.03.2010, numa situação em que o arguido era um *serial killer*:

"A Constituição não exclui que, neste domínio específico, uma ponderação possa conduzir a que, em concreto, o interesse público geral na investigação dos ilícitos penais imputados ao arguido e na prossecução da verdade material e a subsequente realização da justiça se sobreponham, acauteladas as devidas reservas, às necessidades de tutela da sua esfera de privacidade. Porém, quando o juízo sobre a existência, ou não, de uma afronta à dignidade do homem tem implícita a forma como o imputado equaciona a sua relação com a dignidade dos outros, colocando em causa valores fundamentais (como o direito à vida) aquele núcleo essencial deve ser avaliado num juízo de ponderação em que pesam a gravidade do crime e os valores jurídicos tutelado pela lei penal. O respeito pela dignidade e intimidade de cada cidadão acaba quando o mesmo desrespeita a dignidade dos outros cidadãos e os valores fundamentais prosseguidos pelo Estado como é o caso da funcionalidade da justiça penal.

É, quanto a nós, incontornável o pressuposto de que dificilmente se pode afirmar um núcleo inviolável de dignidade a respeitar quando o que está em causa é a perseguição penal do agente que coloca em causa direitos fundamentais como é a vida dos seus

[43] Para maior desenvolvimento, vide RAMALHO, *Métodos*…, cit., pp. 189-191.

concidadãos (por exemplo a leitura do diário íntimo do serial killer revelando a sua psicopatia, ou a situação da desresponsabilização do injustamente condenado).

Assumida uma defesa do princípio da ponderação nesta área de prova proibida e protecção do direito á intimidade é evidente que a invocação do recorrente não tem o mínimo de fundamento. A ponderação investigatória, e probatória, da agenda do telemóvel como factor de determinação da sua propriedade, e da relação sequente com o crime praticado, não colide com nenhum núcleo fundamental da dignidade do mesmo recorrente e está perfeitamente justificada pela ponderação do interesse em perseguir criminalmente quem comete um crime de homicídio voluntário, sob a forma tentada, face à mera determinação dos contactos telefónicos existente na agenda do telemóvel que foi abandonado"[44].

Deve ser pois de forma casuística que é feita a avaliação do grau de restrição de DLG's aceitável (atendendo ao que estiver em jogo em cada situação).

Por outro lado, importa sublinhar que, no âmbito da prova digital, sempre que houver uma restrição dos DLG's, sempre se terá de respeitar o princípio constitucional da proibição do excesso (na terminologia de Jorge Reis NOVAIS), vertido no art.º 18.º n.º 2 da CRP, e nomeadamente os seus subprincípios da idoneidade/ adequação (segundo a qual as medidas têm de ser aptas a realizar o fim visado com a restrição), da necessidade (devendo-se escolher, entre os meios à disposição, aquele que produza efeitos menos restritivos) e da proporcionalidade em sentido estrito (devendo-se respeitar a *justa medida*, ou seja, ponderar a relação entre o sacrifício imposto pela restrição e os benefícios que a mesma proporciona). Assim, na aplicação de um meio de prova lesivo de algum direito de um cidadão, terá de passar pelo crivo do princípio da proibição do excesso, verificando-se se o mesmo não será excessivo, desproporcionado ou desrazoável[45].

No mesmo sentido, Gomes CANOTILHO e Vital MOREIRA defendem que, além de "precisarem de autorização constitucional, as restrições de direitos fundamentais carecem também de justificação, não podendo legitimar-se senão pela necessidade de salvaguardar

[44] Acórdão do Supremo Tribunal de Justiça, de 03.03.2010, no âmbito do processo 886/07.8PSLSB.L1.S1, relator Santos Cabral, disponível em: http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/25061d49157a048c8025770a002ed7d7?OpenDocument.

[45] Para maior desenvolvimento sobre o princípio da proibição do excesso, vide NOVAIS, Jorge Reis, *Os Princípios Constitucionais Estruturantes da República Portuguesa,* Coimbra Editora, 2004, pp. 161-193.

outros direitos ou interesses constitucionalmente protegidos e não podendo ultrapassar a medida necessária para o efeito"[46].

Justamente, no âmbito da investigação criminal e da prova digital, inúmeros intervenientes têm acesso a informação privilegiada de um número alargado de cidadãos, havendo o risco dessa informação ser indevidamente utilizada para outros propósitos que não os da investigação em curso. Por isso, o controlo da legalidade e dos excessos não devem nunca ser descorados.

Por exemplo, o douto acórdão do Tribunal da Relação de Lisboa, de 22.06.2016[47], determinou que é obviamente proibido solicitar a operadoras de telemóveis a disponibilização de todos os dados de tráfego dos cartões SIM que tiverem operado num determinado período de tempo em 19 antenas sem que haja a concretização de alvos determináveis: com efeito tal medida iria atingir um universo ilimitado e indiferenciado de cidadãos que necessariamente não se integrariam no conceito jurídico-penal de "suspeitos".

Não é por isso de ânimo leve que se restringem direitos fundamentais, carecendo a obtenção de prova digital de uma devida fundamentação por parte dos investigadores e de procedimentos operacionais que não violem o princípio da proibição do excesso.

Nas buscas online

Este método oculto de investigação permite hoje, "mediante várias técnicas informáticas à distância, via internet, aceder aos dados contidos num computador, observá-los, monitoriza-os, copiá-los sem o conhecimento ou consentimento do visado. Tal como um hacker, também o Estado pode intrometer-se num computador alheio e verificar o que lá está" (na terminologia de João Conde CORREIA)[48].

Independentemente de a terminologia "buscas *online*" ser ou não a mais adequada (sendo preferível, para alguma doutrina, a terminologia "pesquisa de dados *online"*), a verdade é que, apesar da sua larga disseminação, este método de investigação

[46] CANOTILHO,J. J. Gomes, e MOREIRA,Vital, *Fundamentos da Constituição*, 2.ª ed., Coimbra Editora, 1991, pp. 133-134.

[47] Acórdão do Tribunal da Relação de lisboa de 22.06.2016, no âmbito do processo 48/16.3PBCSC-A.L1-9, relator Sérgio Calheiros da Gama, disponível em: http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/916a3f11e71847c780257fdf004f7f74?OpenDocument.

[48] CORREIA, Prova …, cit., p. 42.

ainda não foi regulado na lei portuguesa, não sendo por isso um meio de prova admitido em Portugal.

Ora, atendendo ao facto de a *internet* se ter tornado, ao longo do tempo, um território fértil em criminalidade organizada e um centro de recrutamento para grupos terroristas, é inegável que a busca *online* poderia ser extremamente útil no combate a este tipo de criminalidade.

O problema, uma vez mais, prende-se com a restrição não negligenciável dos DLG's dos cidadãos que este método implica, uma vez que, nos termos de Andrade COSTA ANDRADE, "para um número exponencialmente crescente de pessoas, quase tudo passa pelo computador: desde os dados aparentemente mais anódinos (compras, vendas, planificação de negócios, contabilidade, trabalhos feitos, movimentos bancários, músicas, etc), aos mais sensíveis (saúde, religião, correspondência, fotografias, etc.)"[49]. Como tal, um controlo da vida privada de um cidadão desta magnitude pode significar, para alguns Autores, uma ingerência inaceitável[50], e a restrição de direitos fundamentais (como o da inviolabilidade do domicílio, da correspondência e das telecomunicações, previsto no art.º 34.º da CRP).

No entanto, Autores como João Conde CORREIA defendem que este tipo de método de obtenção de prova, apesar de não se encontrar consagrado na lei, deve ser utilizado.

E é esse o nosso ponto de vista; a investigação deve poder utilizar esta poderosa ferramenta, utilização essa que já tem sido abordada pela jurisprudência alemã, que tem aceitado o método (apesar de também nesse país não existir legislação sobre o mesmo).

Por exemplo, o Tribunal Constitucional Federal Alemão, numa decisão de 27 de Fevereiro de 2008, considerou que o acesso oculto ao sistema informático permitia uma recolha de informações que não seria possível de outra forma[51].

[49] COSTA ANDRADE, *"Bruscamente* …, cit., p. 167.

[50] Rita Castanheira NEVES defende que "a referência à presença da autoridade judiciária na diligência de pesquisa de dados informáticos no n.º1 do artigo 15.º, bem como o elenco das apreensões dos dados informáticos nas alíneas a) a d) do n.º 7 do art.º 16.º da Lei do Cibercrime, deixam de fora a possibilidade de as instâncias formais de controlo poderem levar a cabo buscas sem que o visado seja directamente confrontado com a diligência". (NEVES, Rita Castanheira, *As Ingerências nas Comunicações Electrónicas em Processo Penal - Natureza e Respectivo Regime Jurídico do Correio Electrónico Enquanto Meio de Obtenção de Prova*, Coimbra Editora, 2011, p. 284).

[51] Numa versão inglesa desta decisão, lê-se o seguinte:

Ora, João Conde CORREIA defende que as buscas *online* acabaram por ficar consagradas na Lei do Cibercrime no art.º 15.º n.º 5[52], tratando-se de uma mera "extensão online de uma pesquisa de dados informáticos em curso. Não se trata, pois, de uma diligência complementarmente oculta, realizada à revelia do visado. O acesso ao primeiro sistema informático compromete o secretismo da diligência, permitindo ao visado o controlo da sua legalidade"[53].

Apesar deste método ter um forte grau de intrusão da privacidade, e de ser a priori inadmissível quando a sua realização é secreta, a verdade é que, mesmo assim, "**parece haver alguma margem de constitucional para a implementação processual destas medidas**. Segundo o BVerfG, a infiltração secreta em sistemas informáticos alheios, para efeitos de monitorização ou de leitura de dados, será constitucionalmente admissível, mediante prévia autorização judicial, em casos de perigo concreto para bens jurídicos individuais como a vida, o corpo ou a liberdade ou para interesses coletivos, cuja ameaça afete os fundamentos ou a sobrevivência do Estado de direito ou da própria existência humana"[54] [destaque nosso].

"The secret reconnaissance of the Internet encroaches on the secrecy of telecommunication if the constitution protection authority monitors secured communication contents by using access keys which it collected without the authorisation or against the will of those involved in the communications. Such a grievous encroachment on fundamental rights is, in principle at least, also conditional on the provision of a qualified substantive encroachment threshold. This is not the case here. The provision permits intelligence service measures to a considerable degree in the run-up to concrete endangerment without regard to the grievousness of the potential violation of legal interests, and even towards third parties. What is more, the provision does not contain any precautions to protect the core area of private life. If, by contrast, the state obtains knowledge of communication contents which are publicly accessible on the Internet, or if it participates in publicly accessible communication processes, in principle it does not encroach on fundamental rights.(…)
Encroachments on the fundamental right to the guarantee of the confidentiality and integrity of information technology systems may be justified both for preventive purposes, and for criminal prosecution. They must however be based on a statutory foundation that is constitutional". (decisão disponível em:
http://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2008/bvg08-022.html)

[52] "Artigo 15.º
Pesquisa de dados informáticos:
(…) 5) Quando, no decurso de pesquisa, surgirem razões para crer que os dados procurados se encontram noutro sistema informático, ou numa parte diferente do sistema pesquisado, mas que tais dados são legitimamente acessíveis a partir do sistema inicial, a pesquisa pode ser estendida mediante autorização ou ordem da autoridade competente, nos termos dos n.os 1 e 2".

[53] CORREIA, Prova…, cit., p. 42.
[54] *Idem*, p. 44.

No âmbito dos dados de tráfego e de localização

O ciberespaço continua a desenvolver-se (e, consigo, o cibercrime), sendo que asTIC e os dados de tráfego poderiam dar um apoio inestimável à investigação: contudo, esta continua a ser uma ferramenta ainda por explorar convenientemente.

Com efeito, nos termos de Benjamim Silva RODRIGUES, "contrariamente ao que se defende noutros quadrantes normativos, o ordenamento português não admite o recurso aos dados de tráfego ou elementos externos das comunicações electrónicas com vista a abrir novas linhas de investigação», sendo que «o recurso aos dados de tráfego ocorre para corroborar as hipóteses de investigação que se encontram em curso e nas quais se analisa a possibilidade de imputação de um determinado crime, com uma gravidade suficiente para admitir a medida de ingerência nas comunicações electrónicas, a uma ou mais pessoas devidamente identificadas"[55].

Saliente-se que os dados de tráfego correspondem a dados informáticos ou técnicos que estão relacionados com uma comunicação efetuada por intermédio de TIC's, indicando a origem da comunicação, o destino, os trajetos, a hora, a data, o tamanho, a duração e/ou o tipo do serviço subjacente[56].

Por sua vez, os dados de tráfego estão na base dos dados de localização (que indicam a posição geográfica do equipamento terminal de um utilizador de um serviço de comunicações eletrónicas publicamente disponível), dos dados de base (relativos à conexão à rede de comunicações) e dos dados de conteúdo (relativos ao conteúdo da comunicação ou de uma mensagem)[57].

No quadro de uma investigação criminal eficiente, os dados de tráfego e de localização devem pois poder ser solicitados por autoridades judiciárias ou por autoridades de polícia criminal aos operadores, devendo estes últimos disponibilizar a informação requerida (sob pena do crime de desobediência).

E, neste contexto dos dados de localização, importa falar da localização de viaturas de suspeitos com recurso à tecnologia GPS (Global Positioning System). Ainda não existe consagração legal para a possibilidade de os órgãos de polícia criminal

[55] RODRIGUES, Benjamim Silva, *Das Escutas Telefónicas à obtenção da prova [em ambiente] digital, tomo II "A monitorização dos Fluxos informacionais e comunicacionais"*, Coimbra, 2009.
[56] LOPES, A Emergência…, cit., p. 74.
[57] *Idem,* p. 74.

colocarem aparelhos GPS nas viaturas sem o consentimento dos suspeitos; no entanto, e apesar de alguns Autores como Paulo Pinto de ALBUQUERQUE recusarem a admissibilidade desta prova[58], alguma jurisprudência já começa a aceitar a utilização destes localizadores na investigação criminal, considerando não estar em causa um método proibido de prova[59].

Na recolha de prova penal em sistemas de computação em nuvem

Quando está em causa o conceito de computação em nuvem pretende-se "caracterizar um serviço de disponibilização de recursos informáticos em rede destinados ao armazenamento de dados e/ou à utilização ou desenvolvimento de software a partir de servidores, com recurso às capacidades de memória e de processamento destes.

O acesso a estas funcionalidades assenta frequentemente num método de virtualização que permite ao utilizador aceder aos serviços como se estivesse a ver uma pasta ou a executar um programa no seu computador, tablet ou smartphone, apesar de, na realidade, poder estar a aceder a informação armazenada em vários servidores em diferentes países"[60 e 61].

[58] "No direito português, a colocação de um receptor de GPS no veículo do suspeito ou do arguido não é admissível como meio atípico de obtenção de prova, uma vez que semelhante meio de obtenção de prova deve ser previsto por uma lei expressa, dado o seu elevado grau de intrusão na privacidade do sujeito". (ALBUQUERQUE, Paulo Pinto de, *Comentário do Código de Processo Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem*, 4ª ed., Universidade Católica Editora, 2011, p. 545, comentário ao art.º 189.º do CPP).

[59] Neste sentido, temos, a título de exemplo, o sumário do douto acórdão do Tribunal da Relação de Évora de 07.10.2008, no âmbito do processo 2005/08-1, relator Martinho Cardoso: "Não carece de prévia autorização judicial o uso pelos órgãos de polícia criminal de localizadores de GPS colocados em veículos utilizados por pessoas investigadas em inquérito (e pelo tempo tido por necessário pelo órgão de polícia criminal encarregue do mesmo)". (acórdão disponível em: http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/590ec3fbf20ce49980257de100574d24?OpenDocument)
Já o acórdão do Tribunal da Relação do Porto, de 21 de março de 2013, no âmbito do processo 246/12.9TAOAZ-A.P1, relator Joaquim Gomes, prolatou que "A localização através da tecnologia GPS (Global Positioning System) está sujeita a autorização judicial, aplicando-se, por interpretação analógica, o disposto no artigo 187.° do Código de Processo Penal". (acórdão disponível em: http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/b0fa2aa7d8fa4ce780257b4900518387?OpenDocument)

[60] RAMALHO, David Silva, A recolha de prova em sistemas de computação em nuvem, *in Revista de direito intelectual*, *Nº 2*, Almedina, 2014, p. 126.

[61] O NIST (National Institute of Standards and Technology) define a computação em nuvem da seguinte forma: "Cloud computing is a model for enabling ubiquitous, conveniente, on-demand network access to a shared pool of configurable computing resources (e.g., networks, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction". LEE BADGER et al., *Cloud computing Synopsis and recommendations,* NIST Special Publication 800-146 (Maio de 2012), p.2-1, apud RAMALHO, *idem,* p. 126.

Desde logo, estando em causa informação comummente armazenada em servidores de vários países (tratando-se assim de um ato plurilocalizado), coloca-se a questão de saber se é admissível uma extensão da aplicação espacial da lei processual penal portuguesa aos dados informáticos que estejam localizados (isto é, armazenados) no estrangeiro.

Neste caso, a Convenção sobre o Cibercrime (Convenção de Budapeste, de 23.11.2001 _ aprovada em Portugal pela Resolução da Assembleia da República n.º 88/2009) estabeleceu um regime para os Estados membros que passa pela possibilidade de acesso a dados informáticos armazenados seja qual for a sua localização geográfica desde que estejam acessíveis ao público ou a dados informáticos armazenados no território de outro Estado membro desde que se obtivesse o consentimento legal e voluntário da pessoa legalmente autorizada a divulgar esses dados (conforme art.º 32.º da Convenção).

Ora, a opção legislativa nacional foi a de dar a seguinte redação ao artigo 15.º n.º 5 da Lei do Cibercrime: "Quando, no decurso de pesquisa, surgirem razões para crer que os dados procurados se encontram noutro sistema informático, ou numa parte diferente do sistema pesquisado, mas que tais dados são legitimamente acessíveis a partir do sistema inicial, a pesquisa pode ser estendida mediante autorização ou ordem da autoridade competente, nos termos dos n.os 1 e 2".

É possível interpretar esta norma de um modo restritivo (segundo o qual esta norma só tem aplicação no território português, sendo necessário recorrer aos mecanismos de cooperação internacional em caso de situação plurilocalizada) ou de um modo literal e teleológico (segundo o qual a apreensão de dados informáticos, por parte de autoridades portuguesas, a sistemas informáticos acessíveis através de outro sistema que se encontre em Portugal não tem qualquer limitação territorial, desde que o acesso a esse sistema informático seja lícito). É justamente esta segunda hipótese que colhe a preferência de David Silva RAMALHO[62], bem como a nossa.

Com efeito, note-se que, no contexto da computação em nuvem, podem os dados armazenados ser continuadamente transferidos de servidor em servidor (ou de país em país) tornando-se ainda mais difícil o seu rastreio (sendo famoso o caso *Gorshkov-*

[62] RAMALHO, *idem,* p. 143.

Ivanov, que ilustra bem as dificuldades de recolha de prova armazenada no estrangeiro sem recorrer a mecanismos de cooperação internacional[63]).

Como tal, e atendendo às dificuldades inerentes à constante deslocalização dos dados (a qual é cada vez mais facilitada pela cada vez maior acessibilidade dos serviços de computação em *cloud*) e à volatilidade da prova digital na nuvem, corroboramos a posição de Rogério BRAVO quando afirma que "**Não há, neste espaço da "cloud", forma de desmotivar para a prática do crime**, até porque, falta a muitos a consciência de que se pratica um crime e os que os praticam, contam com a impossibilidade técnica e legislativa de serem detectados ou sequer, responsabilizados. **A única forma de contrariar esta tendência anonimizante do uso das TIPC parece ser a de se legislar sobre a conservação e a obtenção de perfis e de dados de tráfego das comunicações electrónicas**, **revendo em baixa o seu actual regime do segredo das telecomunicações**, até porque não há, neste espaço, protecção estadual para os utilizadores seus titulares, nem lugar por estes, à auto-defesa e sedimenta-se a ideia de que é possível a prática de crimes sem a correspondente sanção"[64] [destaque nosso].

Na não equiparação do correio eletrónico ao conceito tradicional de correspondência

O art.º 17.º da lei do cibercrime vem regular a apreensão do correio eletrónico, onde se prevê que o juiz possa autorizar ou ordenar a apreensão dos mails que possam ser importantes para a descoberta da verdade.

Tem-se entendido _ ainda que não seja de todo uma posição pacífica _ , que a melhor interpretação a dar é a de corresponder a interceção de comunicações por correio eletrónico com a interceção de correspondência por correio normal: tal solução revela-se, contudo, inoperante na prática. Efetivamente, por exemplo, a interceção de correspondência pressupõe que o juiz valide em tempo reduzido a apreensão das cartas que cumpram especificamente os rigorosos critérios do art.º 179.º/1 do CPP; ora, a verdade

[63] Para maior desenvolvimento do caso *Gorshkov-Ivanov*, ver RAMALHO, *idem,* pp. 148-153.

[64] BRAVO, *As Tecnologias*…, cit., p. 7. O Autor refere ainda que, "pelas características já enunciadas do espaço "cloud" e sendo, tanto este, como o espaço das TIPC baseado, desencadeado e proporcionado por comunicações electrónicas, é então compreensível que os Estados tendam a aumentar a possibilidade de tutela e de supervisão, comprimindo os direitos, as liberdades e as garantias (DLG's) individuais, proporcionando novas formas de controlo legal das comunicações electrónicas e dos seus conteúdos".

é que tal procedimento é manifestamente desadequado à apreensão de correspondência eletrónica atendendo ao figurino desta realidade (onde é normal a receção de dezenas, centenas, por vezes milhares de mails eletrónicos, em pouco tempo). Não é, de resto, adequado (nem tão-pouco eficiente ou viável) que a triagem da correspondência eletrónica a apreender passe sempre pelo crivo de um juiz.

Note-se, porém, que o art.º 179.º n.º 1 alínea b) do CPP (relativo ao pressuposto de dever estar em causa crime punível com pena de prisão superior, no seu máximo, a 3 anos) não é aplicável aos crimes perpetrados por correio eletrónico, por se tratar de crimes cometidos por meio de um sistema informático ou em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico (nos termos do art.º 11.º).

Voltando ao problema central, a doutrina tem-se debruçado sobre a equiparação do correio eletrónico ao conceito tradicional de correspondência, havendo profundas divergências quanto à equiparação a ser feita.

Pedro VERDELHO, antes da revisão do CPP de 2007 defendia esta equiparação, argumentando que "não existem normas específicas que regulamentem a obtenção e utilização, como meio de prova, das mensagens de correio eletrónico"[65], remetendo então para a norma da integração de lacunas (art.º 4.º do CPP), para defender que a expressão contida no art.º 179.º n.º 4 ("qualquer outra correspondência") não se quedaria apenas pelo correio tradicional.

Contudo, Armando DIAS RAMOS refuta este argumentário: "Não será de aceitar este argumento porquanto, no pensamento teleológico do legislador quando procedeu à redação deste artigo, estava apenas em mente a correspondência em papel"[66].

Rogério BRAVO vai ainda mais longe, ao afirmar que "a vingar esta corrente de pensamento [no sentido de o correio eletrónico dever ser tratado como correspondência tradicional], não restarão dúvidas de que em consequência, também terão de cair sob a mesma categoria de "correspondência" as mensagens de e para telemóveis, ou qualquer outro tipo de mensagens escritas com destino a terminais de comunicações, nomeadamente, os chamados SMS's e MMS's"[67].

[65] VERDELHO, Pedro, A obtenção da prova no ambiente digital, *in Revista do Ministério Público n.º 99*, Ano 25, Julho-Setembro 2004, p. 122.

[66] DIAS RAMOS, *A Prova*…, cit., p. 55.

[67] BRAVO, Rogério, Da não equiparação do correio-electrónico ao conceito tradicional de correspondência por carta, *in Revista Polícia e Justiça, Janeiro – Junho 2008 – III Série, N.º 7,* Coimbra Editora, 2008, p.2.

Por outro lado, o Autor aprofunda as dificuldades em sujeitar a apreensão do correio eletrónico às regras da correspondência, questionando até que ponto é viável a apresentação, por parte da polícia, do computador ao Ministério Público, rematando em seguida: "pese embora por princípio os DLG's não deverem ceder perante custos económicos e/ou operacionais, imaginem-se as consequências práticas desta opção aquando da realização de uma busca a uma PME; no caso, não seriam meros custos mas uma impossibilidade material para os JIC's lidarem com o número de equipamentos apreendidos"[68].

Rogério BRAVO apresenta ainda o problema do correio eletrónico que é visualizado em "sites de WebMail", não sendo possível recuperá-lo de outra forma que não em laboratório, em ambiente técnico-policial (o que, por sua vez, acarretaria um ato processualmente nulo)[69].

Outra questão que tem suscitado uma querela doutrinária é a da tutela a dar ao correio eletrónico já lido. As diversas posições doutrinárias revelam, só por si, a falta de clareza da solução legal em vigor.

João Conde CORREIA defende que "numa perspetiva literal, não tendo ele [o legislador] estabelecido qualquer distinção legal, também o intérprete não deverá separar, beneficiando o correio aberto e lido do regime previsto para todo o restante. Em ambos os casos só a autorização judicial legitima a sua apreensão"[70].

Por outro lado, Manuel da COSTA ANDRADE considera que "depois de recebido, lido e guardado no computador do destinatário, um e-mail deixa de pertencer à área de tutela das telecomunicações, passando a valer como um normal escrito. E, como tal, sujeito ao mesmo regime em que se encontra um qualquer ficheiro produzido pelo utilizador do computador e nele arquivado. Podendo, como tal, figurar como objecto idóneo da busca, em sentido tradicional"[71].

Uma vez mais, sobressai a posição de Rogério BRAVO, que rebate uma diferenciação entre correio não lido (ou fechado) e correio lido (ou aberto) de uma forma

---

[68] *Idem*, p. 3.

[69] Remetemos para a ob. citada, para maior desenvolvimento (nomeadamente de três outros argumentos em defesa da não equiparação do correio eletrónico ao correio tradicional).

[70] CORREIA, Prova…, cit., p. 40.

[71] COSTA ANDRADE, *"Bruscamente*…, cit., p.159.

bastante incisiva: "Esta ideia de que a mensagem já foi (ou não) lida conforme apresente (ou não) aquela sinalética, é tudo menos fiável como indicador de leitura (e ainda menos de inviolabilidade após a emissão) uma vez que a maior parte dos programas deixa ao alcance do utilizador a possibilidade de remarcar sem limite de vezes as mensagens já lidas, como estando ainda «por ler»"[72].

Conclui-se este ponto, reforçando-se que a posição do Autor quanto à não equiparação entre correio eletrónico e correio tradicional é clara e inequívoca, sugerindo-se assim uma autonomização do correio eletrónico (o qual deverá ser caracterizado como "«dados armazenados em memória de massa» de um sistema informático nas fases da emissão e da receção, consistindo em dados de conteúdo aquando da sua transmissão eletrónica", e o qual deverá estar acessível à investigação criminal).

Na identidade digital

A identidade digital "traduz a atribuição de propriedades a uma pessoa, as quais são imediata e operacionalmente acessíveis através de meios técnicos», sendo que «engloba todos os dados relacionados com a pessoa, e que podem ser armazenados e automaticamente interligados por uma aplicação informática", nos termos da Associação para a Promoção e Desenvolvimento da Sociedade de Informação[73]. É justamente neste contexto que se enquadra, por exemplo, o documento nacional eletrónico de identidade (o qual acredita a identidade pessoal do titular e lhe permite inclusivamente assinar documentos eletronicamente, dispensando-se a presença física do signatário).

O problema levantado pela identidade no ambiente digital prende-se justamente com essa dicotomia entre realidade física (em que a identidade se reporta a uma pessoa física) e a realidade virtual do ciberespaço: não é, de todo, claro que, por exemplo, um correio eletrónico sem qualquer identificação do seu titular ou, outro exemplo, um *nickname* possam ser considerados dados pessoais (passíveis de serem objeto de proteção).

Mais, a lei portuguesa atualmente não prevê a autonomização de identidades alternativas (as quais aparecem, por exemplo, no caso de *alter-egos* criados sob

[72] *Idem,* p. 8.

[73] ADPSI (Associação para a Promoção e Desenvolvimento da Sociedade de Informação), *Identidade Digital*, Coordenador Paulo Esteves Veríssimo, Março de 2007, p. 19.

pseudónimos através de *nicknames*), imputando a lei portuguesa os direitos e obrigações apenas e só à pessoa física que se encontra por detrás dessa identidade alternativa.

Ora, neste contexto, a Associação para a Promoção e Desenvolvimento da Sociedade de Informação sustenta que "a existência e legitimação de pseudónimos digitais com direitos (ex. privacidade) e obrigações (ex. responsabilidade) jurídicas pode vir a ser instrumental para o sucesso de uma forma de ID equilibrada entre direitos e obrigações dos cidadãos"[74].

Por outro lado, a esfera digital potencia outras formas de fraude, de furto de identidade ou de violação da privacidade (pelo acesso não autorizado aos dados associados à identificação digital).

A APDSI emite na ob. citada, por um lado, recomendações relativas a mecanismos de combate a esta nova criminalidade potencial mas também recomenda, por outro lado, outras medidas que merecem atenção: a promoção de leis relacionadas com a identidade e identificação e a criação de meios de natureza tecnológica que possam garantir a eficácia das polícias e dos tribunais na esfera digital[75].

O que nos parece pacífico é que a implementação destes métodos apenas poderá ser realizada por especialistas que dominem a *realidade* em causa: tanto na conceção como na execução, não poderão ser outros agentes que não informáticos qualificados a fazer essa ponte com as autoridades policiais e com os tribunais.

A prova digital: possível noutras áreas jurídicas que não a penal?

Atualmente, apenas no contexto do Código de Processo Penal (e no âmbito da investigação criminal) se permite o acesso ao tráfico de dados, estando tal possibilidade vedada aos demais tribunais não criminais.

Coloca-se a questão de saber até que ponto não se poderia alargar o âmbito de aplicação a outros tribunais, como forma de o julgador ter, também noutras áreas, preciosos auxílios para a descoberta material da verdade dos factos.

[74] *Idem,* p. 41.

[75] *Idem,* pp. 73-74.

Até que ponto, por exemplo, num processo de divórcio, não terá um dos cônjuges o direito a valer-se de conversas que o outro cônjuge teve na internet para constituir prova da sua infidelidade? Até que ponto o direito à não devassa da vida privada de uma pessoa se deve sempre sobrepor ao direito do seu cônjuge em ver justiça a ser feita? E, efetivamente, pode-se ponderar a aplicação de um regime da prova digital que permita ao Tribunal de Família valorar a prova constituída pelas conversas cibernéticas privadas que o cônjuge infiel teve (desde que a recolha da prova seja feita com o mesmo rigor a que se assiste na investigação criminal, e no respeito dos mesmos princípios).

Note-se, de resto, que noutras áreas, como no direito bancário, a privacidade dos cidadãos se vai cada vez mais colocando em causa: até na questão tão delicada do sigilo bancário (o qual é inequivocamente basilar na privacidade dos cidadãos) se vão avançando propostas legislativas que vão no sentido de uma maior facilidade em permitir o levantamento do sigilo, em nome de superiores interesses (como o combate à fraude fiscal)[76].

Ora, o ponto relevante é justamente esse: se até por razões tributárias se permite uma invasão da privacidade dos cidadãos, outros motivos indelevelmente relevantes (como a prossecução da descoberta da verdade em tribunais não criminais) poderão e deverão ser ponderados numa utilização mais generalizada da prova digital. Com uma maior importância da prova digital, é verdade que poderiam surgir novas possibilidades de restrição de alguns Direitos, Liberdades e Garantias; no entanto, tal aconteceria apenas e só na estrita medida em que essa restrição fosse o contraponto necessário da salvaguarda de outros direitos (que, no caso concreto, denotassem ter mais relevância do que os direitos restringidos).

Conclusões

1) As insuficiências do regime legal relativo à prova digital são reais e manifestam-se desde logo em artigos como o art.º 179.º do CPP [apreensão de correspondência], que simbolicamente representa as omissões que ainda persistem relativamente às TIC na lei

[76] O XXI Governo Constitucional de Portugal acabou por recuar no diploma nacional sobre o levantamento do sigilo bancário (para contas bancárias com um saldo superior a 100.000€), mas continuou a aplicar as regras referente à cooperação europeia em matéria de fraude fiscal, conforme amplamente noticiado na imprensa portuguesa. A título de exemplo: http://www.tsf.pt/economia/interior/governo-deixa-cair-lei-do-levantamento-do-sigilo-bancario-5427544.html ou http://www.dn.pt/dinheiro/interior/saldos-de-conta-acima-de-219-mil-euros-reportados-ao-fisco-5164314.html).

portuguesa. Estabelece o n.º 1 deste artigo que "sob pena de nulidade, o juiz pode autorizar ou ordenar, por despacho, a apreensão, mesmo nas estações de correios e de telecomunicações, de cartas, encomendas, valores, telegramas ou qualquer outra correspondência (…)". Ora, atendendo à disseminação da utilização de correspondência eletrónica, afigura-se incompreensível a persistente omissão relativamente à mesma e a necessidade de ainda se ter de recorrer, quanto muito, a uma interpretação extensiva da parte final do trecho citado (a qual é totalmente desadequada pelo facto de a correspondência eletrónica não ser de forma alguma equiparável à correspondência tradicional, como vimos **no ponto 3.5**): esta omissão simboliza a forma como o legislador não tem desenvolvido os melhores esforços por acompanhar as tendências da era digital.

De resto, novo exemplo representativo das gritantes insuficiências legais se pode encontrar na cláusula de extensão prevista no art.º 189.º do CPP, através da qual crimes informáticos (ou ainda de injúria, ameaça, coação e/ou devassa da vida privada _ desde que cometidos por via informática) ficam sujeitos às regras das interceções telefónicas, não tendo assim um regime autónomo. Não será demais vincar as palavras usadas pelo Procurador da República João Conde CORREIA neste contexto: "o legislador esqueceu, assim, as situações em que, paradoxalmente, a intromissão é mais necessária e legítima, tornando quase impossível investigar estes crimes com sucesso"[77].

2) As três leis principais que contêm normas processuais relativas à prova digital (CPP, Lei do Cibercrime e Lei n.º 32/2008) não se encontram perfeitamente delimitadas, sendo por vezes complexa a perceção do regime a aplicar (conforme demonstrado no citado acórdão do Tribunal da Relação de Évora de 06.01.2015, que remete as situações relacionadas com os dados especificamente previstos no art.º 4.º da Lei 32/2008 para o regime processual deste diploma, e todos os outros dados que aí não estejam previstos para o regime contido na Lei n.º 109/2009), podendo-se possivelmente pensar numa solução legislativa mais simples e clara (que poderia passar por uma recodificação processual, introduzindo a prova digital no seio do CPP e já não em legislação avulsa).

3) Quanto aos métodos ocultos de investigação criminal em ambiente digital, a utilização dos mesmos tem como inevitável consequência a restrição de direitos fundamentais: por esse mesmo motivo, nunca são retirados da equação os métodos

[77] CORREIA, Prova…, cit., p. 32.

proibidos de prova nem tão-pouco os princípios a respeitar sempre que está em causa a restrição de DLG's (como o princípio da proibição do excesso).

Em todo caso, é importante que se encontre o melhor equilíbrio possível entre o potencial de descoberta da verdade que representa a prova digital e a salvaguarda dos DLG's (que em caso algum podem ser restringidos sem um fundamento fortemente atendível).

4) Por exemplo, as buscas *online* (que correspondem a um método oculto de investigação criminal) são poderosas ferramentas de investigação que não devem ser negligenciadas pelo legislador: apesar de terem ínsita uma compressão dos DLG's não negligenciável, o potencial de investigação é demasiado importante para ser ignorado e não se procurar chegar a uma nova solução legislativa.

5) No domínio dos dados de tráfego e dos dados de localização (como é o caso da tecnologia GPS), deveria o legislador fazer uma clarificação, de modo a que não haja espaço para a subsistência de posições doutrinárias que recusem a admissibilidade desta prova digital devido à falta de tipicidade destes meios de obtenção de prova.

6) Relativamente aos sistemas de computação em nuvem, são por demais evidentes as lacunas legais ainda existentes, na medida em que a redação do artigo 15.º n.º 5 da Lei do Cibercrime é manifestamente insuficiente para se perceber de um modo claro qual a interpretação a dar no caso de uma situação plurilocalizada (sendo que a solução deveria ir no sentido de uma maior flexibilização e cooperação internacional, atendendo à fácil deslocalização dos dados na computação em *cloud*).

7) Reforce-se agora uma ideia já aflorada na primeira conclusão: atendendo às especificidades do correio eletrónico, corroboramos a posição doutrinária que vai no sentido da sua não equiparação ao correio tradicional. É sim necessária uma nova solução normativa, que passe pela autonomização do correio eletrónico. Sufragamos integralmente a conclusão de Rogério Bravo quando defende que "atendendo à seriedade da questão, é preferível para o bem geral e certeza jurídica que o legislador se apresse a dar corpo ao princípio da legalidade e da tipicidade, clarificando o tema definitivamente e evitando assim que se arraste a indesejável indefinição em sucessivos recursos"[78].

8) Na identidade digital, importa saber até que ponto podem ser autonomizáveis identidades alternativas (como, por exemplo, os *alter-egos* criados sob pseudónimos

[78] BRAVO, Da não equiparação…, cit., p. 8.

através de *nicknames*) de modo a implementar-se uma cultura de maior responsabilização dos atos criminosos que são praticados escudados numa falsa identidade.

9) Coloca-se, por fim, a questão de saber até que ponto a prova digital deverá ficar circunscrita apenas e só ao direito criminal. A verdade é que se trata de uma ferramenta poderosa na descoberta material da verdade, a qual poderia ser fundamental para que se ajudasse a fazer justiça noutros tribunais que não os criminais (desde que o rigor estivesse presente em todas as fases da recolha da prova digital, tal como sucede na investigação criminal).

10) Em jeito de nota final, não se poderia terminar este conjunto de reflexões jurídicas relacionadas com a "*realidade*" do ciberespaço sem fazer uma alusão à transposição de uma diretiva que poderá alterar o panorama do ambiente digital em Portugal (e na Europa em geral), podendo vir a produzir alguns efeitos também ao nível da prova digital.

A designada Diretiva NIS [Diretiva (EU) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União] poderá e deverá ter, acima de tudo, um papel determinante no reforço dos poderes da CERT (serviço integrante do Conselho Nacional de Cibersegurança português encarregue de coordenar a resposta a incidentes de cibersegurança envolvendo o ciberespaço nacional).

Esta diretiva NIS traz consigo a esperança de que, como resultado da sua transposição, o Conselho Nacional de Cibersegurança possa ter um maior *empowerment* e que as suas competências possam ser alargadas.

Por um lado, pode e deve o CNC ver aumentados os seus poderes de articulação entre as CSIRT nacionais ou internacionais, devendo haver igualmente uma consolidação e um reforço das suas funções de coordenação operacional e de autoridade nacional em matéria de cibersegurança relativamente às entidades públicas e às infraestruturas críticas nacionais (conforme resulta do ponto 2 do Eixo 1 [Estrutura de segurança do ciberespaço] do Anexo da Resolução do Conselho de Ministros n.º 36/2015).

Por outro lado, talvez seja igualmente a ocasião de permitir o alargamento dos poderes de acesso a tráfico de dados, por parte do CNC, no âmbito da cibersegurança e do ciberterrorismo (como forma de agilizar um procedimento, que, de outra forma, poderá

pecar nalgumas situações por excessivamente moroso e ineficiente) _ o que, a acontecer, produzirá inevitavelmente alguns efeitos ao nível da prova digital.

Bibliografia

ALBUQUERQUE, Paulo Pinto de, *Comentário do Código de Processo Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem*, 4ª ed., Universidade Católica Editora, 2011

ALMEIDA, Ivo Filipe de, *A Prova Digital*, Universidade Autónoma de Lisboa, 2014

ADPSI (Associação para a Promoção e Desenvolvimento da Sociedade de Informação), *Identidade Digital*, Coordenador Paulo Esteves Veríssimo, Março de 2007

BOLT, BERANEK & NEWMAN, INC, *A History of the ARPANET: The First Decade* (Report). Arlington, VA. 1 April 1981.

BRAVO, Rogério, *As Tecnologias de Informação e a Compressão dos Direitos, Liberdades e Garantias: os efeitos das regras "10/10" e "1/1"*, 2012

BRAVO, Rogério, Da não equiparação do correio-electrónico ao conceito tradicional de correspondência por carta, *in Revista Polícia e Justiça, Janeiro – Junho 2008 – III Série, N.º 7,* Coimbra Editora, 2008

BRAVO, Rogério, Do espectro de conflitualidade nas redes de informação: por uma reconstrução conceptual do terrorismo no ciberespaço, *in Revista de Investigação Criminal, n.º2,* ASFIC / PJ, Novembro 2011

CANOTILHO, J. J. Gomes / MOREIRA,Vital, *Fundamentos da Constituição*, 2.ª ed., Coimbra Editora, 1991

CASEY, Eoghan, *Digital Evidence and Computer Crime – Forensic science, computers and the internet,* Academic Press, 2011

CASTRO, Catarina Sarmento e, Protecção de Dados Pessoais na Internet, *in Sub Judice n.º 35*, Almedina, Abril – Junho 2006

CORREIA, João Conde, Prova digital: as leis que temos e a lei que devíamos ter, *in Revista do Ministério Público nº 139*, Julho – Setembro 2014

COSTA ANDRADE, Manuel da, *"Bruscamente no Verão Passado", a reforma do Código do Processo Penal – Observações Críticas sobre uma lei que podia e devia ter sido diferente*, Coimbra Editora, 2009

DÁ MESQUITA, Paulo, *Processo Penal, Prova e Sistema Judiciário*, Coimbra Editora, 2010

DARPA, *A History of the ARPANET: The First Decade* (Report). Arlington, VA: Bolt, Beranek & Newman Inc. 1 April 1981

DIAS RAMOS, Armando, *A Prova Digital em Processo Penal*, Chiado Editora, 2014, versão eBook

ENISA, *Electronic evidence – a basic guide for First Responders (Good practice material for CERT first responders,* 2014

GIBSON, William, *Neuromancer*, 1984

LIBICKI, Martin C., *Cyberspace is Not a Warfighting Domain*, I/S: A Journal of law and policy for the information Society, volume 8, 2012, pp.321-336

LOPES, José Mouraz / CABREIRO, Carlos Antão, A Emergência da Prova Digital na Investigação da Criminalidade Informática, *in Sub Judice n.º 35*, Almedina, Abril – Junho 2006

MACHADO, Paulo, *O Papel da GNR no Contexto da Cibersegurança Nacional*, Instituto de Estudos Superiores Militares, Curso de Estado-Maior Conjunto, 2015

MILITÃO, Renato Lopes, *A Propósito da Prova Digital no Processo Penal,* Faculdade de Direito e de Ciências Sociais e Humanas da Universidade de Lisboa

MOROZOV, Evgeny, *The Net Delusion: The Dark Side of Internet Freedom*, PublicAffairs, 2011

NEGROPONTE, Nicholas, *Being Digital*, Hodder&Stoughton, 1995

NOVAIS, Jorge Reis, *Os Princípios Constitucionais Estruturantes da República Portuguesa,* Coimbra Editora, 2004

RAMALHO, David Silva, A recolha de prova em sistemas de computação em nuvem, *in Revista de direito intelectual*, *Nº 2*, Almedina, 2014, pp. 123-162

RAMALHO, David Silva, *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, Almedina, 2017

RODRIGUES, Benjamim Silva, *Direito Penal Parte Especial, Tomo I, Direito Penal Informático-Digital*, Coimbra, 2009

RODRIGUES, Benjamim Silva Rodrigues, *Das Escutas Telefónicas à obtenção da prova [em ambiente] digital, tomo II "A monitorização dos Fluxos informacionais e comunicacionais"*, Coimbra, 2009

SANTOS, Lino / MARGUES GUEDES, Armando, Breves reflexões sobre Poder e Ciberespaço, *in RDeS – Revista de Direito e Segurança, nº6 (julho/dezembro de 20150),* pp. 189-209

SANTOS, Lino, Contributos para uma Melhor Governação da Cibersegurança em Portugal*, in* GOUVEIA, Jorge Bacelar / PEREIRA, Rui, *Estudos Avançados de Direito e Segurança (Vol. II, pp. 217-305),* Almedina, 2012

SANTOS, Lino / BRAVO, Rogério / NUNES, Paulo Viegas, *Protecção do ciberespaço: Visão analítica*, 2012

SHIRKY, Clay, *Here Comes Everybody: The power of organizing without organizations,* Penguin Books, 2008

VERDELHO, Pedro, A obtenção da prova no ambiente digital*, in Revista do Ministério Público n.º 99*, Ano 25, Julho-Setembro 2004

Jurisprudência

Acórdão do Tribunal da Relação de Évora de 07.10.2008, no âmbito do processo 2005/08-1, relator Martinho Cardoso, disponível em:
http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/590ec3fbf20ce49980257de100574d24?OpenDocument.

Acórdão do Supremo Tribunal de Justiça, de 03.03.2010, no âmbito do processo 886/07.8PSLSB.L1.S1, relator Santos Cabral, disponível em:
http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/25061d49157a048c8025770a002ed7d7?OpenDocument (consultado em 22/05/2017)

Acórdão do Tribunal da Relação do Porto, de 21 de março de 2013, no âmbito do processo 246/12.9TAOAZ-A.P1, relator Joaquim Gomes, disponível em:

http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/b0fa2aa7d8fa4ce780257b4900518387?OpenDocument (consultado em 26/05/2017)

Acórdão do Tribunal da Relação de Évora de 06.01.2015, no âmbito do processo 6793/11.2TDLSB-A.E1, relator João Gomes de Sousa, disponível em:

http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/847dae6b85353cb880257de10056ff4c?OpenDocument (consultado em 22/05/2017)

Acórdão do Tribunal da Relação de lisboa de 22.06.2016, no âmbito do processo 48/16.3PBCSC-A.L1-9, relator Sérgio Calheiros da Gama, disponível em: http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/916a3f11e71847c780257fdf004f7f74?OpenDocument (consultado em 22/05/2017)

Decisão do Tribunal Constitucional Federal Alemão, de 27 de Fevereiro de 2008, disponível em: http://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2008/bvg08-022.html (consultado em 26/05/2017).

Informações Online

Artigo de Malcolm GLADWELL para o New Yorker onde critica o modelo ciberutópico, disponível em: http://www.newyorker.com/magazine/2010/10/04/small-change-malcolm-gladwell (consultado em 11/05/2017)

Artigo de Steven LEVY sobre a origem ta expressão «*information wants to be free*», disponível em: https://backchannel.com/the-definitive-story-of-information-wants-to-be-free-a8d95427641c (consultado em 11/05/2017).

Site online do FBI – princípios da *International Hi-Tech Crime and Forensics Conference* em outubro de 1999, disponível em https://archives.fbi.gov/archives/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm (consultado em 21/05/2017)

Notícias sobre levantamento de sigilo bancário: http://www.tsf.pt/economia/interior/governo-deixa-cair-lei-do-levantamento-do-sigilo-bancario-5427544.html e

http://www.dn.pt/dinheiro/interior/saldos-de-conta-acima-de-219-mil-euros-reportados-ao-fisco-5164314.html (consulta em 26/05/2017)

FACULDADE DE DIREITO UNIVERSIDADE NOVA DE LISBOA

CEDIS CENTRO DE I&D SOBRE DIREITO E SOCIEDADE

DIREITO, SEGURANÇA E DEMOCRACRIA

Nº 57

CEDIS WORKING PAPERS OUTUBRO 2017