Universidade Católica Portuguesa
Escola de Direito do Porto

Os Meios de Obtenção de Prova na Lei do Cibercrime: Pesquisa de Dados Informáticos.

Cláudia Sofia Dias Sequeira
Dissertação de Mestrado em Direito Criminal
sob a orientação do Dr. José Damião da Cunha.

Porto
Outubro 2016

Universidade Católica Portuguesa
Escola de Direito do Porto

Os Meios de Obtenção de Prova na Lei do Cibercrime: Pesquisa de Dados Informáticos.

Cláudia Sofia Dias Sequeira
Dissertação de Mestrado em Direito Criminal
sob a orientação do Dr. José Damião da Cunha.

Outubro de 2016
Porto

Aos meus pais

"Everybody should want to make sure that we have the cyber tools necessary to investigate cyber crimes, and to be prepared to defend against them and to bring people to justice who commit it."[1]

"Digital evidence is becoming a feature of most criminal cases. Everything is moving in this direction"[2]

[1] Janet Reno, disponível em http://www.brainyquote.com/quotes/keywords/cyber.html.
[2] Susan Brenner, disponível em www.quotehd.com.

Agradecimentos

Aos meus pais, meus pilares e exemplos de vida e profissionalismo, o maior dos meus agradecimentos, sem vocês nada disto seria possível, obrigada pelo vosso apoio incondicional e por acreditarem em mim quando eu não acredito.

Ao João, pela compreensão, pelas conversas, por me ouvir e por sempre acreditar em mim.

Aos meus amigos pelos conselhos e pela força que me deram.

O meu especial agradecimento para o Dr. José Damião da Cunha pela disponibilidade e pela verdadeira orientação prestada ao longo da elaboração desta dissertação.

Resumo

O crescimento tecnológico se por um lado contribuiu para o desenvolvimento das sociedades, por outro tornou-se numa arma perigosa, dando origem aos mais diversos tipos de crime. Para combater a crescente criminalidade informática e arranjar soluções para lidar com a prova digital, vários países, entre os quais Portugal, reuniram-se e criaram a Convenção do Cibercrime de 2001. Convenção que teve um papel preponderante no combate à criminalidade informática, ao regular os meios de obtenção de prova no âmbito digital.

Dos meios de obtenção de prova, mereceu-nos destaque a Pesquisa de dados informáticos, que derivando das buscas tradicionais, foi pensada e adaptada à realidade digital. Embora seja notória a aproximação legislativa entre as buscas não domiciliárias e a pesquisa de dados, esta não deixa de ser uma medida inovadora.

A pesquisa de dados pode contudo ser bastante evasiva dos direitos fundamentais dos cidadãos pois, nos dias de hoje há uma grande diversidade de informação armazenada nos sistemas informáticos e, através da pesquisa, as autoridades judiciárias competentes podem aceder a um conjunto de informação muito ampla.

A busca *online*, método oculto de investigação que não se encontra prevista no nosso ordenamento jurídico, permite que se proceda a uma busca *online* a um sistema informático, através doutro sistema, sem que a pessoa tenha conhecimento. Pese embora seja uma medida que põe em causa direitos fundamentais, poderá ser um método bastante efetivo no combate ao terrorismo e à criminalidade altamente violenta e organizada, desde que, legislada com critérios bastante apertados.

Palavras – chave: Cibercrime, Prova Digital, Pesquisa de dados, Buscas Online.

Abstract

The technological growth on the one hand contributes to the development of societies, on the other has become a dangerous weapon, giving rise to various types of crime. To combat the growing crime and come up with solutions to deal with digital evidence, several countries, including Portugal, came together and created the Cybercrime Convention of 2001. Convention which had a leading role in the fight against cybercrime, regulating the means of obtaining evidence under digital.

The means of obtaining evidence, earned us highlight the research of computer data, that deriving from traditional searches, was designed and adapted to the digital reality. Although it is notorious the legislative approximation between non-house searches and research data, this does not cease to be an innovative measure.

The research data can however be quite evasive of fundamental rights of citizens because, nowadays there is a great diversity of information stored in computer systems and, though research, the competent judicial authorities can access a set of very broad information.

The Online search, hidden method of research that is not provided for in our legal system, allows a online search to a computer system through another system, without that person having knowledge. Even though it is a measure that undermines fundamental rights, can be a very effective method in the fight against terrorism and crime highly violent and organized, since, legislated with very tight criteria.

Key words: Cybercrime, Digital Evidence, Searching Data, Online Search

Índice

Advertência

Antes de mais, destacamos algumas observações que facilitaram a leitura da dissertação:

1. Relativamente à bibliografia adotamos o modelo (NP-405-1).

2. Face ao limite de caracteres, não consta das notas de rodapé a edição das obras, a editora das obras, nem o *link* do artigo citado. Remetemos assim o leitor para a Bibliografia da dissertação.

3. As traduções efetuadas ao longo da dissertação foram realizadas por nós, sendo assim da nossa inteira responsabilidade.

Lista de Abreviaturas e Siglas

al. - alínea

art.º/ art.ºs – artigo/artigos

CCiber – Convenção Cibercrime

CDADC – Código do Direito de Autor e dos Direitos Conexos

CP- Código Penal

CPP- Código do Processo Penal

CPP iatliano – Codice di Procedura Penale

CRP – Constituição da Republica Portuguesa

DLG's – Direitos Liberdades e Garantias

EUA – Estados Unidos da América

Idem – O mesmo autor e título da nota anterior.

JIC- Juiz de Instrução Criminal

LC- Lei do Cibercrime

MP- Ministério Publico

n.º - número

Ob. Cit. – obra citada em nota de rodapé anterior

OPC – Orgãos de Policia Criminal

p.- página

pp - páginas

proc. - processo

STJ – Supremo Tribunal de Justiça

TC – Tribunal Constitucional

TJUE – Tribunal de Justiça da União Europeia

TRE – Tribunal da Relação de Évora

TRP – Tribunal da Relação do Porto

v.g. – verbi gratia – por exemplo

Vol. – Volume

Introdução

O desenvolvimento tecnológico e a crescente importância deste na vida das pessoas contribuiu para a criação de uma "sociedade tecnológica" em que tudo se encontra "à distância de um *click*".

Se é verdade que a Internet permite que pessoas um pouco por todo o mundo possam receber todo e qualquer tipo de informação numa questão de segundos, possibilitando de uma forma nunca antes vivenciada, o contacto entre pessoas de diversos países, não é menos verdade que o número de crimes através da Internet tem crescido abruptamente nos últimos anos.

Os sistemas informáticos são uma ferramenta cada vez mais procurada para praticar os mais diversos crimes aliás, nos dias de hoje, basta ligar uma televisão para ver como as redes terroristas conseguem através da Internet passar mensagens e obter apoio de pessoas que nunca tiverem qualquer contacto com aquela realidade. Este fenómeno crescente deve-se à dificuldade de identificar os agentes, que podem estar em diversos países, e obter a designada prova digital.

Como combater a crescente criminalidade através de sistemas informáticos? Como obter a prova digital? Como torna-la válida em tribunal? Como criar condições para que haja uma cooperação internacional nesta matéria?

Todas estas questões, aparentemente sem resposta, levaram a que vários países, entre os quais Portugal, participassem na Convenção sobre a Cibercriminalidade em 2001, de onde resultaram uma série de medidas processuais que ajudam a responder a algumas das questões colocadas.

O nosso estudo visa precisamente analisar os meios de obtenção da prova digital, de que forma são inovadores e, de que forma terão que ser interpretados conjuntamente com o CPP.

Especial destaque será dado à pesquisa de dados informáticos armazenados em sistemas informáticos e à sua conjugação com as buscas tradicionais, bem como à análise desta medida adotada e regulada noutros ordenamentos jurídicos e verificaremos de que forma a pesquisa de dados informáticos armazenados em computador poderão ser evasivos dos direitos fundamentais dos cidadãos.

Faremos ainda um estudo às buscas online, ao seu caráter inovador e à sua (in)admissibilidades no ordenamento jurídico português

1 - Convenção sobre a Cibercriminalidade

1.1 Objetivo e âmbito da convenção

A Internet tornou-se o maior fenómeno dos tempos modernos, convertendo-se em parte integrante da vida dos cidadãos. E se por um lado isso permite que tenhamos acesso a toda e qualquer informação que esteja *online*, por outro lado, a Internet também esconde inúmeros perigos e, prova disso é a crescente criminalidade através de sistemas informáticos.

Surgiu assim a necessidade do direito penal dar resposta à crescente cibercriminalidade, todavia, os ordenamentos jurídicos não estavam pensados, nem preparados, para estes novos tipos de crimes, nem dispunham de legislação que permitisse de forma idónea e célere obter a designada prova digital. O que consequentemente levantou inúmeras questões, nomeadamente: Como travar este tipo de criminalidade? Como obter a prova em ambiente digital? Como conseguir que essa prova seja válida em tribunal?

Ora, foi precisamente a necessidade de dar resposta a estas questões, que levou o Comité dos Ministros do Conselho da Europa a realizar a Convenção sobre a Cibercriminalidade a 8 de Novembro de 2001 em Budapeste.

A CCiber tinha três grandes objetivos: "(1) a harmonização dos elementos relativos a infrações no contexto do direito penal substantivo de âmbito nacional e das disposições conexas na área da cibercriminalidade, (2) a definição, ao abrigo do Código do Processo Penal interno, dos poderes necessários para investigar e intentar ações penais relativamente a tais infracções, assim como a outras infracções cometidas por meio de um sistema informático ou às provas com elas relacionadas e existentes sob a forma eletrónica, (3) a implantação de um regime rápido e eficaz de cooperação internacional".[3]

A CCiber é constituída por quatro capítulos: Capítulo I – Terminologia; Capítulo II – Medidas a tomar ao nível nacional, que contém duas secções, uma referente ao direito material e outra ao direito processual; Capítulo III - Cooperação internacional e Capítulo IV – Cláusulas Finais.

Ao nível do direito processual penal, a CCiber consagra medidas que devem ser implementadas "(…) ao nível nacional, para efeitos de investigação criminal

[3] Relatório Explicativo da CCiber (STE nº185), ponto 16.

relativamente às infracções definidas na Secção 1, a outras infracções penais cometidas por meio de um sistema informático e à recolha de provas sob a forma electrónica, de uma infracção penal."[4]

O combate ao crime praticado através de sistemas informáticos apresenta dificuldades acrescidas, designadamente, a " (…) identificação do infractor, bem como de avaliação da extensão e do impacto dessa mesma infracção. Um outro problema prende-se com a volatilidade dos dados electrónicos, uma vez que estes são passíveis de serem alterados, transferidos ou eliminados apenas em alguns segundos."[5]

Daí que a CCiber tenha, por um lado, adaptado meios tradicionais de obtenção de prova, como é o caso das buscas e apreensões e, por outro lado, criado meios que vieram complementar os meios tradicionais, de forma a torna-los mais eficazes face a "(…) um meio tecnológico que se caracteriza pela volatilidade".[6]

As medidas previstas na CCiber são: a preservação expedita de dados armazenados; a preservação expedita e divulgação parcial de dados de tráfego; a injunção; a busca e apreensão de dados informáticos armazenados; a recolha de dados de tráfego em tempo real e a interceção de dados de conteúdo. Passaremos a analisar cada uma destas medidas, com exceção da busca e apreensão de dados informáticos armazenados que será alvo de uma análise mais extensiva no ponto 3.1.

O art.º 14º CCiber faz referência ao âmbito das disposições processuais. Com este artigo a CCiber pretende aplicar os meios de obtenção de prova "aos crimes que ela define, mas estão previstas duas extensões extremamente significativas: por um lado prevê-se que sejam aplicadas a qualquer outro tipo de crime cometido por via de um sistema de computadores; por outro lado, prevê-se que sejam aplicados à obtenção de prova em forma electrónica, se respeitante a ilícitos criminais"[7] sem prejuízo de reservas por parte dos Estados Partes.

Relativamente ao art.º 15º CCiber refere-se a condições e salvaguardas que os Estados Partes devem observar, tais como, "direitos nacionais e instrumentos internacionais na área dos direitos humanos, bem como a regra da proporcionalidade da medida à natureza e circunstâncias da infracção."[8]

---

[4] Idem, ob. cit., ponto 131
[5] Idem, ob. cit., ponto 133
[6] Idem, ob. cit., ponto 134
[7] VERDELHO, Pedro et al., *Leis do Cibercrime, Vol. I*,p.15
[8] Idem, ob. cit., p.15-16.

Os artigos 16º e 17º CCiber abordam a Preservação expedita de dados informatizados[9] armazenados e a Preservação expedita e divulgação parcial de dados de tráfego [10], respetivamente. São expeditos em virtude da "velocidade de circulação da informação na internet"[11], todavia, apesar deste elemento comum, as duas normas têm objetos diferentes, a primeira visa a preservação de dados informatizados armazenados, enquanto a segunda visa a preservação e divulgação parcial de dados de tráfego. Como já se referiu a volatilidade dos dados, faz com que a sua preservação expedita, se demonstre essencial para o sucesso de uma investigação criminal. Por isso, se mostra "(…) razoável, neste contexto, quanto aos dados propriamente ditos, apenas impor, como se faz na Convenção, a sua preservação, até ser obtida pelas vias normais a formalidade legalmente exigida para a sua obtenção material ou revelação (ordem judicial ou outra). O mesmo já não vale para os dados de tráfego. De facto, os dados de tráfego permitem reconstruir o percurso de uma determinada comunicação."[12], isto é, nos dados de tráfego pode estar em causa mais do que um servidor de Internet e, através da preservação expedita dos dados e da sua revelação poderá, no âmbito de uma investigação, descobrir-se o outro servidor ou servidores.

Já o art.º 18º CCiber prevê a injunção, que visa atribuir competências às autoridades para ordenarem que cidadãos ou servidores de Internet "(…) forneçam dados armazenados num computador sob a sua responsabilidade ou forneçam dados de subscritores do serviço Internet"[13] respetivamente. É de salientar que a CCiber determina que a injunção se aplique a dados especificados, ou seja, têm que estar determinados quais os dados alvo da injunção.

Por último os artigos 20º e 21º CCiber abordam a Recolha de dados de tráfego em tempo real e da Interceção de dados de conteúdo[14]. O primeiro regula a possibilidade de

---

[9] Os dados informáticos vêm definidos no art.º 2 al.b) da Lei 109/2009 e consistem em "qualquer representação de factos, informações ou conceitos sob uma forma susceptível de processamento num sistema informático, incluindo os programas aptos a fazerem um sistema informático executar uma função".

[10] Os dados de tráfego são uma das categorias dos dados informáticos e, também vêm definidos no art.º 2 al.c) da Lei 109/2009 e correspondem aos "dados informáticos relacionados com uma comunicação efectuada por meio de um sistema informático, gerados por este sistema como elemento de uma cadeia de comunicação, indicando a origem da comunicação, o destino, o trajecto, a hora, a data, o tamanho, a duração ou o tipo do serviço subjacente".

[11] VERDELHO, Pedro et al., ob. cit., p. 16.

[12] Idem, ob. cit., p. 16.

[13] Idem, ob. cit., p. 16.

[14] Tal como os dados de tráfego, também os dados de conteúdo são uma das categorias dos dados informátios, porém não vem definidos na Lei 109/2009. Mas, o Relatório Explicativo da Convenção do Cibercrime, ponto 229, defini-os como o "conteúdo informativo da comunicação, isto é, o significado ou o

as autoridades competentes procederem à "(…) recolha e registo de dados de tráfego em tempo real, para fins de investigações criminais"[15], bem como obriga que um fornecedor de serviços proceda a essa recolha e registo, ou que preste assistência às autoridades competentes. Este meio de obtenção de prova "(…) permite relacionar a hora, a data, a origem e o destino das comunicações efectuadas pelo suspeito com a hora da intrusão no sistema da vítima, possibilitando a identificação de outras vítimas ou revelando ligações com cúmplices."[16] . Ao nível do procedimento o art.º21º segue os mesmos trâmites do art.º20º, registando-se a diferença quanto ao tipo de dados pois, um aplica-se aos dados de tráfego, enquanto o outro, aos dados de conteúdo.

teor da comunicação, ou a mensagem ou informação transmitida. Designa, assim, todos os elementos transmitidos como parte da comunicação mas que não constituam dados de tráfego."

[15] Relatório Explicativo da CCiber (STE nº185), ponto 216.

[16] Idem, ponto 218.

2 - Os Meios de Obtenção de Prova na Lei do Cibercrime

2.1 A Lei do Cibercrime

Apenas em 2009, entrou em vigor a Lei nº 109/2009, designada Lei do Cibercrime, cumprindo assim Portugal as obrigações resultantes da ratificação da CCiber.

Em vez de proceder a alterações legislativas, nomeadamente no CPP, o legislador nacional optou por criar um diploma onde englobasse todas as disposições legais referentes à cibercriminalidade, uma vez que esta opção legislativa vai ao encontro da "(…) tradição portuguesa, onde existem, especificamente na área penal, outros diplomas estruturantes de matérias na especialidade: assim acontece com a criminalidade relacionada com os estupefacientes (…)"[17], outra razão para esta opção legislativa deve-se "(…) a geral inconveniência de ver em diplomas estruturantes do ordenamento penal regras especiais, apenas aplicáveis a uma parcela muito restrita dos tipos de ilícito"[18] e ainda "(…) a conveniência prática, para os operadores judiciários, de ver sistematizados todos os normativos referentes a um sector especifico da criminalidade"[19]

Ora, tal solução não terá sido a mais adequada, na medida em que, e como já tivemos oportunidade de referir anteriormente no, ponto 1.1, o âmbito de aplicação das disposições processuais da LC têm uma aplicação genérica, "(…) aplicam-se aos crimes aí previstos (crimes informáticos *stricto sensu*), aos crimes cometidos por meio de um sistema informático e, ainda, aos crimes em que seja necessário proceder à recolha de prova em suporte digital"[20].

Além disso, e como refere Paulo Dá Mesquita "(…) o capítulo III da Lei do Cibercrime não prevê normas especiais em sentido técnico-jurídico, mas regras de obtenção de prova em suporte electrónico aplicáveis a um elenco de crimes mais amplo"[21], além disso, entende o mesmo autor que também a terceira razão apresentada pela Proposta de Lei não tem razão de ser "(…) já que os normativos processuais em causa não se reportam «a um sector específico de criminalidade», pelo que é da «conveniência prática» dos operadores

[17] Exposição de Motivos Proposta de Lei n.º 289/X/4ª
[18] Idem.
[19] Idem.
[20] CORREIA, João Conde, *Prova Digital: as leis que temos e a lei que devíamos ter*, RMP,2014, p.34
[21] MESQUITA, Paulo Dá, *Processo Penal, Prova e Sistema Judiciário*, 2010, p.99.

judiciários que os mesmos não estejam inseridos em legislação aparentemente dirigida apenas «a um sector específico da criminalidade».”[22]

Apesar de a opção do legislador não ser a mais assertiva, não se pode deixar de mencionar a importância da LC para o ordenamento jurídico português, visto que, foi o primeiro diploma legal a prever meios de obtenção de prova num contexto digital.

2.2 Os Meios de Obtenção de Prova na Lei do Cibercrime

Seguidamente iremos proceder a uma análise sucinta do Capítulo III da LC, referente às disposições processuais (artigos 11º a 19º), para compreendermos de que forma o legislador adaptou a CCiber ao ordenamento jurídico português. O art.º 15º, por ser o nosso principal foco, será, posteriormente, alvo de uma análise mais extensiva.

O art.º 11º refere-se ao âmbito de aplicação das disposições processuais. De acordo com o nº 1 desta norma as disposições processuais do presente diploma legal, à exceção dos art.ºs 18º e 19º, aplicam-se: a) aos crimes previstos na presente lei; b) crimes cometidos por meio de um sistema informático; ou c) em relação aos quais seja necessário proceder à recolha de prova em suporte digital.

Já no nº2 do art.º 11º, o legislador determinou, que as disposições processuais consagradas no presente diploma “não prejudicam o regime da Lei n.º 32/2008”. Esta lei transpôs para a ordem jurídica portuguesa a Diretiva nº 2006/24/CE referente à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações.

A relação entre a LC e a Lei n.º 32/2008 não é de todo pacífica. Paulo Dá Mesquita entende que a primeira veio revogar o art.º 9º da Lei n.º 32/2008, uma vez que a panóplia de dados abrangido pela LC é mais abrangente que os contidos na Lei nº 32/2008, porém o mesmo autor frisa a importância deste diploma “(…) sobretudo, no estabelecimento dos deveres dos fornecedores de serviços de conservação e protecção desses dados, bem como das condições técnicas operativas e destruição desses bens.”[23]

[22] MESQUITA, Paulo Dá, ob. cit., p.99
[23] Idem, ob. cit., p. 123

Já Benjamim Silva Rodrigues e Renato Lopes Militão entendem que os dois diplomas legais se complementam, como aliás resulta expressamente da letra do art.º 11º nº2 da LC.

Pese embora a importância da Lei nº32/2008 não podemos deixar de fazer referência à declaração de invalidade da Diretiva nº2006/24/CE que, como anteriormente mencionado, deu origem à Lei nº32/2008. O TJUE, casos C-293/12 e C-594/12[24], entendeu que o a Diretiva excedia um conjunto de direitos consagrados na Carta dos Direitos Fundamentais Europeus, designadamente, os artigos 7º (Respeito pela vida privada e familiar) e 8º (Protecção de dados pessoais). Trata-se de uma decisão que não tem força obrigatória geral, na medida em que as questões foram suscitadas pelo Supremo Tribunal Irlandês e pelo Tribunal Constitucional Austríaco. Note-se, contudo, que "(…) o legislador português antecipou a generalidade das omissões e insuficiências agora identificadas pelo TJ no texto comunitário e criou um diploma significativamente mais exigente (…)"[25]. Porém e apesar de a Lei n.º 32/2008 já regular alguns dos problemas levantados pelo TJUE, não regulou o principal fundamento para a invalidade da Diretiva, nem podia, visto que tal fundamento prende-se com o escopo da Diretiva, ou seja, "(…) a conservação duradoura e indiscriminada de dados de quase todos os indivíduos que se encontrem, neste caso, em território português".[26]

A preservação expedita de dados encontra-se consagrada no art.º 12 LC, sendo que o legislador português optou por abranger numa única norma a preservação de dados informáticos e dados de tráfego, e regular no art.º 13º LC a revelação expedita de dados de tráfego, diferentemente, do que sucedia na CCiber, que previa na norma 16ª a conservação expedita de dados informáticos armazenados e no art.º 17º a conservação expedita e divulgação parcial dos dados de tráfego.

Nos termos do art.º 12º nº1 LC demonstra-se necessário para a produção de prova, a obtenção de dados informáticos ou de tráfego, em virtude do receio de que tais dados se percam, se alterem ou deixem de estar disponíveis, "a autoridade judiciária competente ordena, a quem tenha disponibilidade ou controle desses dados, designadamente fornecedores de serviço[27]", que os preserve.

---

[24]Consultados a 15/07/2016 em curia.europa.eu.
[25] SANTOS, Manuel Simas, Liber Amicorum, 2016, p.385.
[26] Idem, ob. cit. p. 387.
[27] O art.º 2º al. d) da LC define fornecedor de serviço como "qualquer entidade, pública ou privada, que faculte aos utilizadores dos seus serviços a possibilidade de comunicar por meio de um sistema informático, bem como qualquer outra entidade que trate ou armazene dados informáticos em nome e por conta daquela entidade fornecedora de serviço ou dos respectivos utilizadores".

Pode ainda a preservação ser ordenada por OPC, desde que devidamente autorizada pela autoridade judiciária competente ou em situações de urgência ou de perigo na demora, desde que tal seja imediatamente transmitido à autoridade judiciária competente e, acompanhado de relatório nos termos do art.º 253º CPP (art.º 12º nº 2 LC)

A ordem de preservação terá que indicar: a) a natureza dos dados; b) a sua origem e destino e c) o período de tempo pelo qual deverão ser preservados, até um máximo de três meses, sob pena de nulidade.

Como refere Benjamim da Silva Rodrigues, "Importa notar que o período máximo de três meses não deverá ser ultrapassado, não sendo – a nosso ver - de discutir a possibilidade de renovação, à semelhança do que ocorre com as escutas telefónicas, mas haverá que atentar ao prazo absoluto de conservação dos dados gerados e tratados no âmbito das comunicações electrónicas, disposto no art.º 6º, da Lei n.º 32/2008: um ano". Daí que, e tal como salienta o mesmo autor, o nº 5 do art.º 12º determine expressamente que o período de três meses possa ser renovado "até ao limite máximo de um ano."[28]

Por último, o nº4 deste preceito legal assegura que com a ordem de preservação, quem disponha ou controle os dados, deve "preservar de imediato os dados em causa, protegendo e conservando a sua integridade pelo tempo fixado, isto é, deve "congelar os dados"[29], além de que fica obrigado a assegurar a confidencialidade do processo em curso.

Já o art.º 13º regula a revelação expedita de dados de tráfego, este artigo visa que o fornecedor de serviços a quem tenha sido ordenada a preservação dos dados, identifique os demais fornecedores de serviços através dos quais, aquela comunicação foi efetuada, de forma a que a autoridade competente possa identificar a origem da comunicação, bem como o destino da mesma.

Segue-se a injunção para apresentação ou concessão do acesso a dados, prevista no art.º 14º da LC, que visa que a autoridade judiciária competente ordene, a quem tenha disponibilidade ou controlo sobre determinados dados armazenados num sistema informático: a) que os comunique ao processo ou, b) que permita o acesso aos mesmos, sob pena de punição por crime de desobediência (art.º 14º nº1 LC e art.º 348º CP)

A injunção tem que identificar os dados em causa, aliás como sucede com a ordem de preservação de dados (art.º 14º n.º 2 LC).

---

[28] RODRIGUES, Benjamim Silva, *Da Prova Penal Tomo IV – Da Prova – Electrónico – Digital e da Criminalidade Informático – Digital*, 2011, p.522

[29] Idem, ob. cit., p.522

Este preceito legal aplica-se também aos fornecedores "(…) a quem pode ser ordenado que comuniquem ao processo dados relativos aos seus clientes ou assinantes, neles se incluindo qualquer informação diferente dos dados relativos ao tráfego ou ao conteúdo, contida sob a forma de dados informáticos ou sob qualquer outra forma, detida pelo fornecedor de serviços, e que permita identificar: a) o tipo de serviço de comunicação utilizado, as medidas técnicas tomadas a esse respeito e o período de serviço; b) a identidade, a morada postal ou geográfica e o número de telefone do assistente, e qualquer outro número de acesso, os dados respeitantes à facturação e ao pagamento, disponíveis com base num contrato ou acordo de serviços; ou c) qualquer outra informação sobre a localização do equipamento de comunicação, disponível com base num contrato ou acordo de serviços." (art.º 14º n.º4 LC).

O nº5 do art.º 14º faz uma ressalva, que nos parece da maior importância, a injunção não pode ser dirigida ao arguido ou suspeito. Desta forma o legislador salvaguardou o direito à não autoincriminação por parte do arguido ou suspeito, uma vez que, se a injunção pudesse ser dirigida ao suspeito ou arguido, este poderia ter uma participação ativa na sua incriminação na medida em que seria obrigado a comunicar ao processo os dados objetos da investigação ou teria que permitir o acesso aos mesmos, sob pena de incorrer num crime de desobediência.

A apreensão de dados informáticos vem regulada no art.º 16º da LC, nos termos do nº1 desta norma, a autoridade judiciária competente pode ordenar, mediante despacho, a apreensão de dados ou documentos informáticos, descobertos durante uma pesquisa ou outro acesso legítimo a um sistema informático.

Todavia, existem duas situações, em que os órgãos de polícia criminal podem proceder à apreensão, sem prévia autorização da autoridade judiciária competente, "no decurso de pesquisa informática legitimamente ordenada e executada nos termos do artigo anterior, bem como quando haja urgência ou perigo na demora." (art.º 16º nº2 LC).

O nº 3 do art.º 16º merece especial destaque, uma vez que com este preceito, o legislador pretendeu salvaguardar informação pessoal e que poderia implicar um obstáculo a este meio de obtenção de prova, já que poderia por em causa direitos fundamentais do suspeito ou arguido ou até de terceiro, assim, "Caso sejam apreendidos dados ou documentos informáticos cujo conteúdo seja susceptível de revelar dados pessoais ou íntimos, que possam por em causa a privacidade do respectivo titular ou de terceiro, sob pena de nulidade esses dados ou documentos são apresentados ao juiz, que ponderará a sua junção aos autos tendo em conta os interesses do caso concreto".

De forma a validar as apreensões levadas a cabo por órgão de polícia criminal, estas terão de ser apresentadas à autoridade judiciária competente, num prazo máximo de 72 horas (art.º 16º nº4 LC).

No nº 7 do art.º 16ºLC estão previstas diferentes formas de apreensão que passam pela a) apreensão do suporte onde está instalado o sistema ou apreensão do suporte onde estão armazenados os dados; b) cópia dos dados em suporte autónomo; c) preservação dos dados; d) eliminação não reversível e bloqueio de acesso aos dados.

O art.º 17º LC regula a apreensão de correio eletrónico e registo de natureza semelhante, que prevê a possibilidade de o juiz poder autorizar ou ordenar, a apreensão de mensagens de correio eletrónico ou registo de natureza semelhante, aplicando-se o regime de apreensão de correspondência previsto no art.º 179º CPP.

É de salientar que não se aplicará neste contexto a al. b) do nº1 do art.º 179º CPP, ou seja, quando estejam em causa crimes puníveis com pena de prisão, no seu máximo, superior a três anos. Isto porque, o art.º 11º da LC especifica que o art.º 17º LC aplica-se a crimes previstos na LC, a crimes cometidos por meio de um sistema informático e aos crimes em que seja necessário proceder à recolha de prova em suporte electrónico.

Uma questão que tem levantado alguma divergência doutrinal é que tutela dar ao correio eletrónico já lido. Antes de avançarmos para a divergência em si mesma, convém primeiramente definir correio eletrónico e, se à partida tal se afiguraria tarefa fácil, a verdade é que não existe no nosso ordenamento jurídico nenhuma legislação que defina correio eletrónico.

A Diretiva 2002/58/CE no seu art.º 2º al. h) define correio eletrónico como "qualquer mensagem textual, vocal, sonora ou gráfica enviada através de uma rede pública de comunicações que pode ser armazenada na rede ou no equipamento terminal do destinatário até o destinatário a recolher.", não obstante, o legislador nacional ao transpor a Diretiva para o direito nacional, que deu origem à Lei nº 41/2004, olvidou a definição de correio eletrónico.

Retomando a divergência, Manuel da Costa Andrade entende 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."[30]

Paulo Dá Mesquita refere que o art.º 179º CPP faz alusão à comunicação que está em curso e não à comunicação já lida e guardada pelo seu destinatário, pelo que o legislador ao remeter do art.º 17º LC para o art.º 179º CPP, parece querer reconduzir "(…) o intérprete à teleologia do regime processual sobre a apreensão de correspondência, pelo que não são objecto da sua tutela especial, nomeadamente, mensagens de correio eletrónico já acedida pelo destinatário."[31], para este autor esta foi uma questão que o legislador negligenciou.

Rita Castanheira Neves entende que, embora o legislador não tenha sido elucidativo, o facto de o art.º 17º LC mencionar expressamente que a mensagem de correio eletrónico ou os registos de natureza semelhante se encontrem "armazenados"[32], indica que a mensagem já foi lida pelo seu destinatário que optou por a guardar. Pelo que o legislador optou por dar um tratamento diferente à mensagem de correio eletrónica lida pelo seu destinatário face ao correio tradicional.

João Conde Correia entende que uma vez que o legislador não determinou "qualquer distinção legal"[33], não poderá o interprete fazê-lo, pelo que não se deverá dar um tratamento diferente ao correio eletrónico aberto e lido. Vai mais longe porém o autor ao afirmar que, na sua ótica não faz sentido o tratamento diferenciado, uma vez que o sigilo de comunicações deve terminar quando a mensagem chega à esfera do seu destinatário, pelo que uma mensagem de correio eletrónico já lida, poderia ser apreendida pela simples intervenção do MP, sendo posteriormente sujeita a controlo judicial, como sucede no art.º 16º nº 3 LC.

Armando Dias Ramos[34] entende que não se pode equiparar o correio tradicional ao correio eletrónico, na medida em que, não se pode tratar de igual forma duas coisas que são distintas.

Analisaremos agora a interceção[35] de comunicações regulada no art.º 18º LC, esta norma aplica-se a crimes previstos na LC, bem como a crimes cometidos por meio de um

---

[30] ANDRADE, Manuel da Costa, *"Bruscamente no Verão Passado", a reforma do Código do Processo Penal*, 2009, p.159.
[31] MESQUITA, Paulo Dá, ob. cit., p. 118
[32] 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, 2011, p.276
[33] CORREIA, João Conde, ob. cit., pp. 40-41
[34] RAMOS, Armando, Dias, *A Prova Digital Em Processo Penal: O Correio Eletrónico*,2014.
[35] O art.º 2º al.e) LC contém a definição de intercepção "acto que se destina a captar informações contidas num sistema informático, através de dispositivos eletromagnéticos, acústicos, mecânicos ou outros."

sistema informático ou em relação aos quais seja necessário proceder à recolha de prova em suporte digital, quando tais crimes estejam previstos no art.º 187º CPP.

A interceção é autorizada por despacho do JIC, mediante requerimento do MP, apenas durante a fase de inquérito, desde que: a) haja razões para crer que a diligência é indispensável à descoberta da verdade ou, b) que de outra forma a prova seria muito difícil, ou até impossível, de obter (art.º 18º nº2 LC).

Salienta o nº3 do preceito em análise, que o despacho do JIC deve especificar o âmbito da interceção, atendendo às necessidades da investigação.

Por último o art.º 18 LC remete, em tudo o que não seja contrario, para os art.ºs 187º, 188º e 190º CPP. Assim, chama-mos à atenção para o facto de esta medida apenas poder ser utilizada contra: a) suspeito ou arguido; b) pessoa que sirva de intermediário, desde que haja fundados motivos para crer que recebe ou transmite mensagens destinadas ou provenientes do arguido ou suspeito; c) vitima do crime, desde que com o seu consentimento.

Além disso, as interceções de comunicação são autorizadas pelo prazo máximo de três meses, renováveis por períodos sujeitos ao mesmo limite.

Rita Castanheira Neves destaca o facto de o art.º 18º LC não remeter para o art.º 189º CPP, pelo facto, de a LC substituir quase por completo aquele artigo "no âmbito, claro está, da criminalidade definida no seu n.º1."[36].

Assim, quando estejam em causa interceções referentes a crimes cometidos no âmbito da LC, bem como do art.º 187º do CP, quando sejam cometidos por meio de um sistema informático ou em relação aos quais seja necessário proceder à recolha em suporte eletrónico, aplica-se o regime do art.º 18º LC, verificando-se apenas a realização de algum dos crimes previsto no art.º 187º CPP então o regime aplicável já será o do art.º 188º CPP.

Por último temos o art.º 19º LC que (estranhamente, até porque não há qualquer referência ao mesmo na CCiber) faz referência às ações encobertas. De acordo com o nº1 deste preceito legal, as ações encobertas podem ser aplicadas, no decurso do inquérito, relativamente a: a) crimes previstos na LC; b) crimes cometidos por meio de um sistema informático quando lhes corresponda, em abstrato, pena de prisão de máximo superior a cinco anos; c) ainda que a pena seja inferior, e sendo dolosos, os crimes contra a liberdade e autodeterminação sexual nos casos em que os ofendidos sejam incapazes ou menores, burla qualificada, burla informática e nas comunicações, discriminação racial, religiosa

[36] NEVES, Rita Castanheira, ob. cit., p.280.

ou sexual, infracções económico-financeiras; e ainda d) crimes consagrados no título IV do CDADC.

Enquanto no nº2 refere-se que, na eventualidade de se ter que recorrer a meios e dispositivos informáticos, observa-se o regime previsto na interceção de comunicações.

Atendendo que as ações encobertas são um dos meios de obtenção de prova mais lesivos, devendo apenas ser utilizado para a criminalidade altamente organizada, não se compreende a razão de o legislador aumentar o seu campo de aplicação.

Após a análise sucinta dos meios de obtenção de prova na LC, podemos concluir que, de uma forma geral, o legislador português respeitou o que era pretendido pela CCiber, com algumas inovações à mistura.

3 - Pesquisa de Dados Informáticos

3.1 O art.º 19º da CCiber – Busca e Apreensão de dados informatizados

Esta norma refere-se à busca e apreensão de dados informatizados armazenados, e visa, que as legislações nacionais procedam à modernização e harmonização em matéria de buscas e apreensões. Apesar dos ordenamentos jurídicos preverem regimes de buscas e apreensões como meios de obtenção de prova, esses regimes estão pensados apenas para objetos tangíveis, não abrangendo assim os dados informáticos, que são intangíveis, o que consequentemente leva a que os mesmos não possam ser obtidos no âmbito de investigações criminais e ações penais nos mesmos moldes que os objetos tangíveis.

Assim, ao nível de buscas de dados informáticos armazenados seria necessário a criação de disposições que complementassem as normas processuais já existentes, de forma a garantir que os dados informáticos armazenados seriam obtidos, no âmbito de uma investigação criminal, com a mesma admissibilidade e eficácia que são obtidos os objetos tangíveis.

O primeiro parágrafo deste artigo prevê que os Estados Partes devem adotar medidas legislativas de forma a capacitar as autoridades competentes para proceder a uma busca ou ter acesso: a) a um sistema informático ou a uma parte do mesmo, bem como a dados informáticos que nele se encontrem armazenados e; b) a um suporte que permita armazenar dados informáticos.

O parágrafo segundo deste preceito prevê uma possibilidade de extensão da busca. Assim, as autoridades competentes pela investigação poderão ampliar as buscas a um outro sistema informático, quando existam razões que os façam crer que os dados procurados se encontram armazenados nesse outro sistema informático, isto é, por vezes o sistema informático que está a ser alvo de buscas não contém os dados procurados, mas através desse sistema ou dispositivo consegue estender-se a busca de forma expedita a outro sistema. Estas circunstâncias ocorrem nomeadamente devido a redes de área alargada ou da Internet.

Não obstante, a CCiber não elucida em que termos se deverá proceder a essa extensão, contudo, no Relatório Explicativo da mesma mencionam-se algumas possibilidades: a) capacitar/instruir a entidade competente, para autorizar a busca a um sistema informático, dos poderes para autorizar a extensão da busca a outro sistema informático que esteja

conectado com aquele (o sistema informático alvo de buscas), desde que hajam indícios que levem a crer que o sistema informático conectado contém os dados objeto da busca; b) delegar nas autoridades competentes pela investigação, o poder de poderem estender as bucas a um sistema conectado com o sistema alvo das buscas, desde que se verifique os tais indícios de que os dados objeto da busca se encontram nesse sistema conectado, ou c) as autoridades competentes pela investigação possam exercer os poderes de busca aos sistemas conectados de forma rápida e coordenada.

Já o terceiro parágrafo refere-se à apreensão e determina que os Estados Partes deverão legislar no sentido de habilitar as autoridades competentes para apreender ou guardar dados informáticos armazenados que previamente foram alvo de buscas nos termos dos dois parágrafos anteriores. As medidas devem ter como base guardar os dados, isto é, "(…) "preservar a integridade dos dados", ou manter a "cadeia de posse" dos dados, o que significa que os dados copiados ou removidos são conservados no estado em que foram encontrados aquando da apreensão, mantendo-se inalterados no período durante o qual é intentada a acção penal".[37] Com a remoção dos dados, estes não são destruídos, ficando apenas temporariamente inacessíveis ao suspeito, que poderá ter novamente acesso a eles uma vez finda a investigação.

Enquanto a busca de dados tem por escopo aceder a um determinado sistema e obter certos dados armazenados nesse mesmo sistema, a apreensão de dados visa essencialmente reunir provas, mediante a cópia de dados ou através da remoção dos dados que anteriormente foram alvo de busca, efetuando cópias destes, e consequentemente tornando inacessível a versão original dos dados. Tendo sempre em conta que, a apreensão de dados não significa a eliminação definitiva dos mesmos. Assim, a busca é um meio para chegar aos dados e a apreensão um meio de os recolher.

O parágrafo quarto visa introduzir "(…) uma medida coerciva cujo objectivo é o de facilitar a busca e apreensão de dados informatizados."[38]. Assim, cada Estado Parte deverá adotar medidas, para que as autoridades competentes possam ordenar que qualquer pessoa, que possua conhecimentos acerca do funcionamento do sistema informático ou conheça as medidas utilizadas para proteger os dados informáticos neles armazenados, faculte na medida do admissível as informações razoavelmente necessárias para se proceder às buscas.

[37] Relatório Explicativo da CCiber (STE nº185), ponto 197.
[38] Idem, ob. cit. ponto 200.

A quantidade exacerbada de dados suscetíveis de processamento e armazenamento, bem como o progresso das medidas de segurança, dificulta o acesso aos dados investigados e a sua consequente identificação como elemento de prova. Pelo que se pode mostrar necessário recorrer a um administrador de sistema, de forma a delinear a melhor forma de conduzir a investigação ao nível da modalidade técnica, "(…) a presente disposição autoriza as entidades competentes a obrigar um administrador de sistema a prestar o seu contributo, da forma que se afigure razoável, no quadro da operação de busca e apreensão".[39]

As informações razoavelmente necessárias para se proceder às buscas pode variar consoante as circunstâncias do caso concreto. Em determinados casos essa informação razoável pode ser a solicitação de uma *password*, mas haverá casos em que pedir a divulgação desta se pode mostrar "(…) uma ameaça à privacidade de outros utilizadores ou ao carácter confidencial de outros dados para os quais não exista uma autorização de busca".[40]

Por último, o parágrafo quinto faz uma remissão para os artigos 14º e 15º da CCiber, que se referem às disposições gerais processuais desta Convenção.

No contexto deste último parágrafo do art.º19º CCiber, levantou-se a questão de saber se os sujeitos alvos de uma busca devem, ou não, ser notificados da execução da busca. Os redatores da CCiber entenderam, que seria mais adequado deixar ao critério dos Estados Parte essa questão uma vez que, em alguns ordenamentos jurídicos não está prevista a notificação para as designadas buscas clássicas, pelo que, se a CCiber impusesse a notificação para as buscas de dados armazenados, provocaria uma disparidade legislativa em alguns Estados Parte. Entendeu-se ainda que alguns Estados Partes podem considerar a notificação essencial para distinguir a busca de dados armazenados da interceção de dados em curso de transmissão (art.ºs 20º e 21º CCiber), sendo a primeira uma medida que não se pressupõe ser "sub-reptícia"[41], diferentemente da segunda que é "sub-reptícia"[42]. Todavia, a CCiber alerta que "Caso as Partes ponderem a adopção de um sistema de notificação obrigatória das pessoas visadas, deverá ser tido em consideração o facto de que tal notificação é susceptível de prejudicar a investigação.

[39] Idem, ob. cit., ponto 200.
[40] Idem, ob. cit., ponto 202.
[41] Idem, ob. cit., ponto.202
[42] Idem, ob. cit. ponto. 202

Uma vez cientes da existência de tal risco, as Partes deverão considerar a possibilidade de adiamento da emissão da notificação".[43]

Após uma análise ao âmbito de aplicação do art.º19º CCiber, verifica-se que os meios tradicionais de busca previstos no CPP não são eficazes face à prova eletrónica e que o legislador nacional teria que introduzir alterações de forma a poder tornar operacionais as buscas no âmbito digital.

3.2 O art.º 15.º da LC – Pesquisa de dados informáticos

Se durante uma investigação se revelar essencial para a descoberta da verdade obter determinados dados informáticos armazenados num sistema informático, a autoridade judiciária competente autoriza ou ordena, mediante despacho, a pesquisa de tais dados no sistema informático (art.º 15º n.º 1 LC)

3.2.1 – Autoridade Judiciária Competente

A LC determina que quando se mostrar necessário para efeitos de prova proceder a uma pesquisa num sistema informático, a entidade competente para autorizar ou ordenar tal diligência é a autoridade judiciária competente. Devendo esta, sempre que possível, presidir à diligência.

Para Benjamim Silva Rodrigues, deve-se fazer uma interpretação restrita desta norma "(…) no sentido de se apagar a aparente abertura para que esta operação ocorra sem que à mesma presidia a autoridade judiciária competente que a ordenou ou autorizou". [44] Sendo que para este autor será da competência do juiz presidir a tal diligência. Discordamos com esta posição. A lei é clara quando refere que a pesquisa deverá ser presidida, sempre que tal se mostra possível, pelo que não nos parece que seja necessário fazer uma interpretação restritiva da norma, além disso, a lei também refere que quem deverá presidir à operação é o MP e não o JIC. Podemos é outrossim questionar se, atendendo ao núcleo de informação armazenado num sistema informático, não deveria ser o JIC a ordenar e autorizar a pesquisa? Uma pesquisa de dados num sistema

[43] Idem, ob. cit., ponto 204.
[44] RODRIGUES, Benjamim da Silva, ob. cit. p.525

informático pode revelar-se uma medida de obtenção de prova bastante lesiva de certos direitos fundamentais, pelo que, entendemos que se justificaria que recaísse sobre o JIC a competência de ordenar ou autorizar uma pesquisa, como forma de garantia dos direitos do suspeito ou arguido e de controlo sobre a legalidade da pesquisa.

O n.º 2 do art.º 15.º da LC especifica que o despacho que autoriza ou ordena a pesquisa tem uma validade de 30 dias, sob pena de nulidade.

3.2.2 – Pesquisa sem autorização prévia

Existem situações especiais em que é possível ao OPC proceder à pesquisa de dados sem prévia autorização do MP, são elas:

a) o consentimento de quem tiver a disponibilidade ou controlo dos dados, desde que fique devidamente documentado (art.º 15.º n.º 3 al.a);

b) em casos de terrorismo, criminalidade violenta ou altamente organizada desde que haja indícios fundados de prática de crime iminente que coloque em perigo a vida ou a integridade física de qualquer cidadão (art.º 15.º n.º 3 al.b).

É de salientar que enquanto a LC se refere a "quem tiver a disponibilidade ou controlo sobre esses dados", o CPP, no art.º 174.º n.º 5 al.c), faz referência ao consentimento do visado.

João Conde Correia[45] entende que a terminologia da LC vem facilitar o trabalho dos OPC, mas desvaloriza o direito à intimidade da vida privada da pessoa alvo da pesquisa, pois admite que um terceiro possa autorizar a pesquisa, bastando para tal que tenha disponibilidade sobre tais dados. Defende ainda o autor que "Só o portador concreto daquele bem jurídico (reserva da intimidade da vida privada) poderá, validamente, prescindir dele."[46]

Concordamos com a posição do autor, não obstante a dificuldade que existe a nível de investigação envolvendo a prova digital, isso não pode resultar numa desvalorização do direito à intimidade da pessoa visada pela diligência, sendo sobre ela que recai o bem jurídico só ela deveria ter poder para o afastar.

O nº 4 vem complementar o nº 3 ao regular que após a pesquisa os OPC têm que elaborar um relatório e remete-lo ao MP e ainda, no caso previsto na al.b) do nº 3, têm

[45] Neste sentido João Conde Correia, ob. cit. p. 51.
[46] Idem, ob. cit. p. 51

que, imediatamente, dar conhecimento da mesma ao MP para que este valide, ou não, a pesquisa.

3.2.3 – Ampliação da pesquisa a outro sistema informático.

O nº5 do art.º 15 da LC traz uma inovação para o ordenamento jurídico português, se no decurso de uma pesquisa, surgirem razões para crer que os dados alvo de busca se encontram noutra parte do sistema ou até noutro sistema informático, e que é possível aceder-lhes através do sistema inicial, pode ampliar-se a pesquisa desde que tal seja autorizado ou ordenado, de acordo com o nº 1 e 2 do art.º 15º. Esta extensão da pesquisa estava prevista no segundo parágrafo da CCiber, deixando ao critério dos Estados Parte determinar de que forma se realizaria essa extensão. Parece-nos que a decisão tomada pelo legislador nacional - necessidade de autorização para proceder a essa extensão de pesquisa - foi a solução mais adequada ao nosso ordenamento jurídico, uma vez que a pesquisa está sujeita a autorização, excecionados determinados casos identificados na lei, não faria sentido que uma medida que amplia a pesquisa pudesse ser feita pela iniciativa dos OPC sem qualquer supervisão, sendo esta a solução que mais protege o direito à privacidade do arguido ou suspeito.

3.2.4 – Omissões legislativas

Se de uma forma geral o legislador nacional teve em consideração os diversos parágrafos do art.º 19º CCiber, parece-nos que o parágrafo quarto, que tivemos oportunidade de mencionar no ponto 3.1, foi negligenciado pelo legislador nacional.

Não ficou assim regulado de que forma as pessoas que conhecem o sistema informático e a forma como está protegido devem colaborar com as autoridades judiciárias e, mais importante, não legislou "(…) a informação cujo fornecimento é passível de ser solicitado"[47].

Existiu preocupação por parte da CCiber em esclarecer os Estados Parte de que há situações em que exigir a divulgação, de *v.g.* uma *password,* poderá ser admissível, porém noutras, nomeadamente quando se solicita o acesso a dados que não fazem parte do objeto da pesquisa, demonstrar-se-á uma ameaça à privacidade. Parece-nos assim que quando se

[47] Relatório Explicativo da CCiber (STE nº185), ponto 202.

mostrar necessário na investigação de pesquisa de dados, recorrer *v.g* ao fornecedor de serviços ou ao administrador de rede, para lhe solicitar informação não disponibilizada pelo arguido, ou quando a complexidade dos dados em causa leve os OPC a necessitar de colaboração, esta terá que ser ordenada pelo MP e não poderá extravasar os dados objeto da pesquisa.

Embora a nossa análise à relação entre as buscas tradicionais e a pesquisa de dados, por força da remissão do art.º 15º n.º6, se vá fazer no ponto 3.5, não podemos desde já deixar de mencionar que esta remissão demonstra a necessidade de conjugar diferentes diplomas para se proceder à obtenção da prova digital. Ora, diversos diplomas com o mesmo fim poderão criar dificuldades de articulação na prática, o que levará a uma acentuada dificuldade de obter uma prova, que já de si levanta dificuldades. Somos da opinião que teria sido mais vantajoso que o legislador nacional tivesse procedido a uma atualização do Livro III (Da Prova) do CPP, de forma a que os meios previstos na LC estivessem regulados no CPP.

3.2.5 – Questões práticas

No entanto, antes de avançar chamamos atenção para uma questão prática que nos pareceu bastante pertinente e que foi levantada por Armando Dias Ramos. O autor alerta para cuidados a ter no momento em que se vai proceder à pesquisa para que não se percam dados, e consequentemente se coloque em perigo a investigação. A questão prende-se essencialmente em saber o que devem fazer os OPC quando o dispositivo alvo de pesquisa se encontra desligado ou em funcionamento. Quando o dispositivo se encontra desligado "(…) nada mais haverá a fazer se não recolher os mesmos e proceder ao respetivo auto de apreensão, com indicação de todos os elementos que o identifiquem inequivocamente (…)".[48] Problemas maiores colocam-se no caso dos dispositivos estarem ligados ou em modo de hibernação, nesses casos o autor refere que o mais seguro será "(…) mover o rato, sem efetuar nenhum *click*, ou carregar na barra de espaços do teclado".[49] Defende o autor que ao fazer-se um *click* no rato ou a tocar-se aleatoriamente no teclado poderá ativar algum programa que apague todo o conteúdo do disco rígido.

[48] RAMOS, Armando Dias, ob. cit., p.92.
[49] Idem, ob. cit., p. 92.

3.3 Direito Comparado

Achamos que seria enriquecedor para o nosso estudo compreender de que forma outros Estados Parte da CCiber, transpuseram para os seus ordenamentos jurídicos a busca de dados informáticos armazenados.

3.3.1 Itália

As buscas estão previstas no Livro XIII do Codice di Procedura Penale, mais precisamente, entres os art.ºs 247º a 252º.

Com a Lei nº 48 de 18 de março de 2008, entrou em vigor no ordenamento jurídico as medidas reguladas na CCiber de combate ao cibercrime. Contrariamente ao que sucedeu no ordenamento jurídico português, o legislador italiano não criou uma lei nova, antes reformulou o CPP italiano de forma a adequa-lo à prova digital.

Ao nível das buscas regulada no art.º 247º do CPP italiano, referente à causa e forma da busca, o legislador acrescentou que "Quando houver fundados motivos para acreditar que dados, informações, programas informáticos e qualquer vestígio ainda relevantes da infração estão num sistema informático ou telemático, mesmo que protegidos por medidas de segurança, é admitida a pesquisa, adotando medidas técnicas adequadas a assegurar a conservação de dados originais e a impedir a alteração."[50]

O órgão competente pela busca será o MP que poderá contudo delegar nos OPC, nos termos do art.º 247º CPP italiano.

Ao art.º 352º CPP italiano, que regula as buscas por iniciativa dos OPC em situações de flagrante delito ou de fuga do suspeito, foi introduzido que "Em relação aos dados, à informação e programas informáticos ou sistemas informáticos ou telemáticos, o oficial da policia judiciária adota igualmente medidas técnicas ou fornece os requisitos necessários a assegurar a conservação e para impedir a alteração e o acesso, e assegurar, sempre que possível, a imediata duplicação num suporte adequado, mediante um

[50] Art.º 247º 1 comma bis Codice di Procedura Penale "Quando vi è fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informático o telemático, anorché protetto da misure di sicurezza, ne è disposta la perquisizione, adotando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad imperdine l'alterazione".

procedimento que assegure a conformidade da cópia com o original e a sua imodificabilidade."[51]

Neste caso e uma vez terminada a busca é necessário a sua validação pela autoridade judiciária competente.

Embora seja de louvar que o legislador italiano tenha procedido a uma reforma no CPP italiano de forma a adequar os meios de obtenção de prova nele contido, em vez de criar uma lei avulsa, não se pode deixar de evidenciar que tal reforma ficou aquém do que era pretendido pela CCiber, referimo-nos *v.g.* à extensão das buscas prevista no parágrafo segundo do art.º 19º CCiber e, que não foi tido em consideração pelo legislador italiano, contrariamente ao que sucedeu em Portugal, tendo o legislador nacional previsto no n.º5 do art.º 15.º LC.

Salientamos porém que o legislador italiano quando no art.º 247 refere - mesmo que protegido por medidas de segurança - está a consagrar a medida coerciva estabelecida no parágrafo quarto da CCiber e que tem como escopo facilitar a investigação. Com o desenvolvimento das medidas de segurança em determinados casos será necessário ordenar aos administradores de rede ou aos fornecedores de serviço que colaborem com os OPC, entendemos que o legislador italiano ao fazer esta ressalva, está a garantir que em caso de necessidade a autoridade judiciária competente pode ordenar a colaboração para a pesquisa dos dados informáticos. Salientamos que esta medida ficou omissa por parte do legislador nacional, não estando a mesma regulada LC, como tivemos oportunidade de mencionar no ponto 3.2.4.

Assim podemos concluir que, de uma forma geral o legislador italiano prosseguiu as orientações da CCiber, tendo, todavia negligenciado questões que poderão dificultar, desnecessariamente, a investigação.

[51] Art.º 354 2 comma Codice di Procedura Penale "In relazione ai dati, alle informazioni e ai programmi informatici o ai sistemi informatici o telematici, gli ufficiali della polizia giudiziaria adottano, altresì, le misure tecniche o impartiscono le prescrizioni necessarie ad assicurarne la conservazione e ad impedirne l'alterazione e l'accesso e provvedono, ove possibile, alla loro immediata duplicazione su adeguati supporti, mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità".

3.3.2 Estados Unidos da América

Nos EUA existe a IV Emenda à Constituição que tem por escopo a proteção dos cidadãos contra buscas e apreensões arbitrárias, isto é, visa garantir a privacidade dos indivíduos. "A IV Emenda consagra o direito dos cidadãos à inviolabilidade das suas pessoas, casas, papéis e efeitos, não deverá ser violado por buscas e apreensões irrazoáveis e nenhum mandado deverá ser emitido sem causa provável, apoiado por juramento ou afirmação e descrevendo particularmente o local onde deverá decorrer a busca e as pessoas e as coisas a apreender."[52]

Perante uma busca num computador, a questão que se colocou face à IV Emenda, era se um individuo teria uma razoável expectativa de privacidade em relação aos dados informáticos armazenados em computadores ou outros dipositivos. Quando os tribunais americanos foram confrontados com esta questão fizeram uma analogia entre o computador e uma mala ou uma pasta, defendendo que existia uma expectativa razoável por parte do individuo em relação à informação que armazena nos vários dispositivos. Em regra, as autoridades quando tenham que proceder a uma busca de dados informáticos terão que obter um mandado que terá que determinar a causa provável bem como o local em que deve decorrer a busca e as coisas a apreender, ou no âmbito digital, descrever os ficheiros sobre os quais a busca deve recair. Não será uma tarefa fácil identificar os ficheiros na medida em que nem sempre os OPC saberão toda a informação contida num sistema informático, nem que informação pode ter sido trocada entre sistemas informáticos, ou onde estarão armazenados os dados alvos de busca.

Existem contudo situações em que não é necessário mandato para se proceder uma busca, nomeadamente, o consentimento; circunstâncias exigentes; doutrina da "Primeira Vista" (Plain View).

Destacamos o consentimento, por ser também uma das situações no nosso ordenamento jurídico em que os OPC podem atuar sem prévia autorização. Nos EUA o consentimento pode ser dado pelo proprietário, por um terceiro que seja co-proprietário ou por uma pessoa que os OPC tenham motivos para acreditar que tem autoridade para

[52] "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.".

consentir. Assim, presumimos que tal como acontece em Portugal, também nos EUA o consentimento é atribuído por quem tiver a disponibilidade ou controlo sobre os dados.

Durante a nossa pesquisa não conseguimos saber exatamente de que forma os EUA transpuseram para o seu direito interno a CCiber, mas conseguimos perceber um conjunto de medidas que eles adaptaram, algumas delas semelhantes à do nosso ordenamento jurídico.

3.4 Pesquisa de Dados e Direitos Fundamentais

Os meios de obtenção de prova na LC levantam questões também ao nível da proteção dos DLG's. Não restam dúvidas que estes meios são mais evasivos que os meios tradicionais, sendo consequentemente mais agressivos para os direitos constitucionalmente consagrados.

Nos termos do art.º 18º n.º2 da CRP "A lei só pode restringir os direitos, liberdades e garantias nos casos expressamente previstos na Constituição, devendo as restrições limitar-se ao necessário para salvaguardar outros direitos ou interesses constitucionalmente protegidos". Acrescentado o nº 3 do mesmo preceito, que as leis que restrinjam direitos, liberdades e garantias não podem "(…) diminuir a extensão e o alcance do conteúdo essencial dos preceitos constitucionais".

A questão da restrição dos DLG's está relacionada com situações de colisão ou conflito entre direitos, "Haverá colisão ou conflito sempre que se deve entender que a Constituição protege simultaneamente dois valores ou bens em contradição numa determinada situação concreta (real ou hipotética)."[53]

Vejamos no nosso caso, a pesquisa de dados afeta o direito a inviolabilidade de domicílio e das comunicações, consagrado no art.º 34º CRP, mas afeta ainda outros direitos, nomeadamente, o direito à imagem, à palavra e à reserva da intimidade da vida privada, previstos no art.º 26º da CRP.

Como referem Gomes Canotilho e Vital Moreira "O direito à **inviolabilidade de domicílio** é ainda um direito à liberdade da pessoa pois está relacionado, tal como o direito à inviolabilidade de correspondência, com o *direito à inviolabilidade pessoal*

[53] ANDRADE, José Carlos Vieira de Andrade, *Os Direitos Fundamentais na Constituição Portuguesa de 1976*, p.301.

(esfera privada espacial, prevista no art.º 26º), considerando-se o domicílio como projeção espacial da pessoa e a correspondência como exteriorização da própria pessoa". [54]

Considerando que nos dias de hoje se partilha os mais variados tipos de informação na Internet, facilmente se conclui que também o sistema informático poderá funcionar como uma esfera intima do individuo, sendo utilizada para atividades normais do quotidiano mas também para armazenar informação intima e até sigilosa. Uma pesquisa de dados poderá facultar a quem investiga um conjunto de informação muito mais abrangente sobre o suspeito, comparativamente a uma busca tradicional.

Do outro lado temos o "(…) *interesse objectivo* na *eficácia da investigação criminal* e, portanto, na obtenção de *prova digital*, sem dúvida um interesse constitucionalmente tutelado, decorrente, desde logo, do principio do Estado de Direito (art.º 2.º CRP) (…)"[55]

Devendo assim o legislador ponderar no quão danosa pode ser a medida para o suspeito, ou até para um terceiro – casos em que o sistema informático alvo de buscas pertence a um terceiro – e na importância deste método de obtenção de prova, especialmente atendendo que estamos a tratar da prova digital, sendo esta altamente volátil e de fácil eliminação, não sendo os meios tradicionais de obtenção de prova idóneos a levar esta prova de forma válida a tribunal.

Porém outra questão nos parece pertinente abordar, até porque julgamos que poderá contribuir para a salvaguarda dos DLG's, é a autorização judicial da pesquisa de dados.

Quanto mais minucioso for o mandato de buscas mais salvaguardados estarão os direitos do suspeito ou arguido pois, ao saberem quais os fins pretendidos com a diligência será mais fácil evitar abusos por parte dos OPC, além de que o suspeito ou arguido pode colaborar indicando onde podem os OPC encontrar os dados alvo de busca. Contudo de acordo com a Juiz de Direito, Teresa Maria da Silva Bravo, "A prática dos Tribunais, tem sido a de autorizar a realização de buscas e apreensões, fazendo-se menção no respectivo despacho (para além da identificação do visado, do local, do prazo de validade do mandado etc) dos tipos incriminadores em causa. No entanto, e por regra, nos despachos que autorizam a realização de buscas e apreensões, não constam, quaisquer factos, nem referências aos fins visados com a diligência."[56]

---

[54] CANOTILHO, Gomes e MOREIRA, Vital, *Constituição da Republica Portuguesa Anotada*, Volume I, 2007, p..

[55] MILITÃO, Renato Lopes, *A Propósito da Prova Digital no Processo Penal*, p.270.

[56] BRAVO, Teresa Maria da Silva, *Revistas e Buscas: O Processo Penal na Era da Globalização* in III Congresso de Processo Penal, Coordenação de Manuel Monteiro Guedes Valente, Almedina, 2010, p. 156.

Tal situação parece-nos inaceitável. Como se poderá salvaguardar os direitos de quem é alvo de uma busca ou de uma pesquisa, se o mandato não menciona qual o fim pretendido com a diligência?

É compreensível que as investigações tenham "(…) sempre um grau de incerteza, de indeterminação e de imprevisibilidade (…)"[57] e que o MP e os OPC não possam determinar com elevado grau de certeza o que irá resultar da pesquisa de dados, mas "(…) pelo menos sabem seguramente (ou deverão saber) o que pretendem obter com a realização daquela diligência."[58]

Um despacho de autorização de uma pesquisa de dados – bem como de uma busca tradicional- deverá sempre conter um certo grau de determinação, nem que seja a razão de ser da pesquisa e o que se pretende com a mesma. Enquanto nas buscas tradicionais há um espaço determinado onde ocorrem as buscas seja um domicílio, um carro ou um escritório, o mesmo não sucede quando falamos em dados informáticos, estes podem encontrar-se nos mais variados locais como o computador, CD-ROM, *pen*, cartões de memória, telemóveis, entre outros. Obviamente que determinar o local da pesquisa não é minimamente aconselhável, contudo fica evidenciado as dificuldades com que se podem deparar os OPC. O despacho deverá mencionar que dados estão a ser pesquisados, embora se reconheça que na prática nem sempre seja fácil determina-los com exatidão.

3.5 Conjugação entre a Pesquisa de Dados e as Buscas Tradicionais

Como anteriormente tivemos oportunidade de referir, o art.º 15º n.º6 da LC faz remissão para as buscas reguladas no CPP e no Estatuto do Jornalista.

De acordo com o art.º 174.º n.º 2 do CPP "Quando houver indícios de que os objectos referidos no número anterior, ou o arguido ou outra pessoa que deva ser detida, se encontram em lugar reservado ou não livremente acessível ao público, é ordenada a busca". A busca é um meio de obtenção de prova "(…) que visa a recolha de informação relativa à pratica de um crime (…)"[59], recolha essa realizada mediante a "(…)intromissão num espaço alheio(…)".[60]

[57] Idem, ob. cit. p. 156.
[58] Idem, ob. cit. p. 156.
[59] PINTO, Ana Luísa, Aspectos Problemáticos do Regime das Buscas Domiciliárias, RPCC, 2005, Ano 15, nº3, p.415.
[60] PINTO, Ana Luísa, As buscas não domiciliárias no direito processual penal português, RMP, 2007, Ano 28, n.º 109, p.24.

Benjamim da Silva Rodrigues na sua análise ao regime das buscas face à prova digital adapta o conceito de buscas à realidade digital "A "busca informática" é ordenada sempre que houver indícios de que alguém oculta no seu computador, vestígios de crime informático-digital que cometeu ou facilitou o cometimento (art.º 174º n.º2 CPP)"[61]

O CPP regula as buscas domiciliárias e as buscas não domiciliárias que têm tramitação diferente, e ainda buscas sujeitas a um regime diferente. As buscas domiciliárias, como o próprio nome indica, são buscas que ocorrem no domicílio e como tal colocam em causa a intimidade da vida privada e são autorizadas ou ordenadas pelo JIC. As buscas não domiciliárias ocorrem em locais que não sejam considerados domicílio, tais como automóveis e jardins, e são ordenadas e autorizadas pelo MP, não obstante, também as buscas domiciliárias podem colocar em causa direitos fundamentais como o direito à intimidade da vida privada, ao sigilo da correspondência e de outros meios de comunicação.

3.5.1 – Semelhança de Pressupostos

O art.º 174º CPP refere-se aos pressupostos da busca, sendo que muitos desses pressupostos foram utilizados no art.º 15.º da LC, vejamos:

- Tanto as buscas como a pesquisa são ordenadas ou autorizadas por autoridade judiciária competente, devendo a mesma, sempre que possível, presidir à diligência (art.º 174º n.º 3 CPP e art.º 15.º n.º1 LC);
- O despacho tem um prazo de validade de 30 dias, sob pena de nulidade (art.º 174.º n.º 4 CPP e art.º 15.º n.º 2 LC);
- Estão previstas circunstâncias em que os OPC podem atuar sem prévia autorização, tendo posteriormente que dar conhecimento, de forma a mesma ser validada (art.º 174.º n.º 5 e 6 e art.º 15.º n.º 3 e 4 LC).

Há assim uma clara aproximação do regime da pesquisa de dados ao regime das buscas não domiciliárias.

[61] RODRIGUES, Benjamim Silva, ob. cit. p.504.

3.5.2 – Demais formalidades

Quanto às formalidades das buscas consagradas no art.º 176º CPP podemos perceber que há uma aproximação da terminologia da LC à terminologia do CPP, na medida em que, quem recebe o despacho é quem tem a disponibilidade do lugar. O nº2 do art.º 176º CPP refere que se a pessoa que tiver a disponibilidade do lugar não estiver presente pode ser substituída por outra pessoa, ou seja, caso a pessoa que tenha disponibilidade sobre os dados não esteja presente, a cópia do despacho será entregue a outra pessoa. Enquanto o nº3 do mesmo preceito refere que a pessoa que esteja presente na altura da pesquisa pode ser alvo de uma revista, parece-nos que tal só fará sentido caso haja por parte dos OPC motivos para acreditar que a pessoa poderá estar a esconder uma pen ou um cartão de memória, ou seja, algo de pequenas dimensões, fácil de ocultar e onde podem estar armazenados os dados.

Caso seja necessário entrar no domicílio para proceder à pesquisa, terá que ser seguir as regras do art.º 177º CPP referente às buscas domiciliárias, terá que ser autorizada pelo JIC e terá que ocorrer no período compreendido entre as 7 e as 21 horas. Excecionalmente, a busca pode ter lugar entre as 21 e as 7 horas em caso de terrorismo ou criminalidade altamente organizada, consentimento do visado e flagrante delito desde que pela prática de crime punível com pena de prisão, no seu máximo, superior a três anos. Nos termos do nº3 do art.º 177º também o MP pode ordenar ou podem os OPC realizar buscas, no período compreendido entre as 7 e as 21 horas, em caso de terrorismo e criminalidade altamente organizada, flagrante delito pela prática de crime que corresponda pena de prisão e consentimento do visado. Já entre as 21h e as 7h, nos casos em que haja consentimento do visado ou em flagrante delito. Ora, no que diz respeito à pesquisa de dados só se aplicará à situação do consentimento de quem disponha dos dados informáticos e que já analisamos.

3.5.3 – Buscas e Pesquisas em escritório de advogados, consultório médico e redação de jornalismo.

Regime especial existe para as buscas em escritório de advogados ou em consultório médico e, em estabelecimento oficial de saúde, regulados no art.177º n.ºs 5 e 6 CPP, respetivamente.

Nestas buscas o juiz terá que presidir, sob pena de nulidade, tendo tal medida que ser dada a conhecer ao presidente do conselho local da Ordem dos Advogados ou da Ordem dos Médicos, para que este ou um delegado possa estar presente. Caso seja um estabelecimento de saúde então terá que se avisar o presidente do conselho diretivo ou de gestão do estabelecimento, ou alguém que o substitua.

Também o Estatuto dos Jornalistas, no seu art.º 11º - referente ao sigilo profissional – contém regras especiais no âmbito das buscas e apreensões. Refere o n.º 6 desta norma que "A busca em órgãos de comunicação social só pode ser ordenada ou autorizada pelo juiz, o qual preside pessoalmente à diligência, avisando previamente o presidente da organização sindical dos jornalistas com maior representatividade para que o mesmo, ou um seu delegado, possa estar presente, sob reserva de confidencialidade". Acrescentando o n.º 7 que "O material utilizado pelos jornalistas no exercício da sua profissão só pode ser apreendido no decurso das buscas em órgãos de comunicação social previstas no número anterior ou efectuadas nas mesmas condições noutros lugares mediante mandato de juiz, nos casos em que seja legalmente admissível a quebra do sigilo profissional". Estas regras aplicam-se também no decorrer de uma pesquisa de dados.

3.5.4 – Buscas e Pesquisa sem autorização prévia

Existem questões, no âmbito da busca realizadas pelos OPC sem autorização prévia, que merecem o nosso destaque, nomeadamente a questão do consentimento que tem soluções diferente no CPP e na LC e a situação de flagrante delito que ficou de fora da LC.

No que concerne ao consentimento, o art.º 174º n.º5 al.b) permite que os OPC procedam à busca desde que haja o consentimento do visado, enquanto a LC no art.º 15º n.º3 al.a) exige o consentimento de quem tenha disponibilidade ou controlo sobre os dados informáticos - não nos iremos alargar sobre a questão do termo mais adequado,

uma vez que já o fizemos no ponto 3.2 – sendo também o consentimento um requisito do art.º 34.º n.º 3 da CRP.

O consentimento do visado, tem uma papel preponderante na "(…) resolução do conflito de interesses em jogo – a busca da verdade material, para realização da justiça criminal, e a preservação da reserva da intimidade do visado"[62]. Posto isto, a questão que se coloca é quem pode dar o consentimento exigido pelo CPP e pela CRP?

Parte considerável da jurisprudência tem entendido que o consentimento tem de partir "(…) da pessoa afectada ou seja daquela que tenha a livre disponibilidade, quanto ao local onde a diligência é efectuada e que possa ser por ela afectado (…)"[63] , assim, não tem que coincidir com o proprietário do local onde se realiza a diligência, mas sim com a pessoa cuja intimidade e privacidade poderá ser devassada pela diligência, isto é, o visado.

Existem contudo situações mais complexas com que o TC se viu confrontado, falamos de situações em que o domicílio é partilhado por diversas pessoas. Em 2013, o TC decidiu que o consentimento para uma busca não pode ser dado por pessoa diferente do arguido, "(…) mesmo que tal pessoa seja um co-domiciliado com disponibilidade da habitação em causa."[64]

No que concerne à LC, foi outra a opção do legislador nacional ao determinar, no art.º 15.º n.º 3, que o consentimento deve ser dado por "(…) quem tiver a disponibilidade ou controlo desses dados (…)". Assim, embora haja uma clara semelhança de pressupostos entre as buscas não domiciliárias e a pesquisa de dados, ao nível do consentimento o legislador optou por uma maior abertura às pessoas que podem dar o consentimento na LC, o que pode desencadear numa violação da privacidade da pessoa que verdadeiramente terá a sua intimidade lesada pela diligência.

Vejamos algumas hipóteses práticas. Se apenas o suspeito ou arguido tiverem a disponibilidade ou controle dos dados não se levantam problemas, sendo apenas este que poderá dar o seu consentimento.

---

[62] PINTO, Ana Luísa, ob. cit., p.438.

[63] Ac. TRE de 17-09-2009, proc. n.º549/08.7PBBJA-A.E1, disponível em www.dgsi.pt. No mesmo sentido ac. do STJ de de 08-05-1995, proc. n.º47.084, disponível em http://jusnet.wolterskluwer.pt. Neste último ac., o consentimento foi prestado pelo filho da arguida que não era o visado pela diligência, além de que nem sequer residia no local, entendendo o tribunal, e bem, que nem sequer tinha a disponibilidade sobre o mesmo.

[64] Ac. do TC n.º 126/2013, de 27-02-2013, disponível em www.dgsi.pt (consultado em 29-08-2016). Em causa estava a realização de umas buscas domiciliárias em que o consentimento foi dado pela cônjuge do arguido.

E o cônjuge do arguido poderá dar o seu consentimento? Julgamos que nesta situação teremos que analisar algumas hipóteses, a primeira é se o dispositivo eletrónico alvo de pesquisa é utilizado apenas pelo suspeito ou arguido, ou se é utilizado por ambos.

No caso de ser utilizado apenas pelo suspeito ou arguido então julgamos que a situação se aproxima com a do ac. do TC - que tivemos oportunidade de mencionar – e assim apenas o suspeito poderá dar o seu consentimento, uma vez que é este que tem disponibilidade e controlo sobre os dados. Fazendo uma analogia com os fundamentos apresentados pelo TC, quando os OPC pretendam proceder a uma pesquisa de dados num determinado dispositivo, é a intimidade da pessoa que utiliza esse dispositivo que está a ser posta em causa e não a intimidade do casal, pelo que achamos que seria inadequado os OPC procederem à pesquisa apenas com o consentimento do cônjuge.

No caso de o dispositivo ser utilizado por ambos então as circunstâncias alteram-se pois, ambos têm disponibilidade sobre os dados, pelo que o consentimento de qualquer um é suficiente para que os OPC procedam à pesquisa de dados. Porém, pode suceder que apesar de o dispositivo ser utilizado em conjunto, estes tenham contas diferentes no dispositivo, porque aí mais uma vez parece-nos que cada um terá apenas disponibilidade sobre os dados referentes à sua conta, logo, também apenas o suspeito/arguido poderá dar consentimento – o que foi exposto aplica-se sempre que o dispositivo seja utilizado por mais do que uma pessoa.

Parece-nos relevante questionar se o fornecedor de serviços poderá dar o seu consentimento? Aparentemente sim, afinal ele tem controlo sobre tais dados.

Parece que existe um número elevado de pessoas que podem dar o seu consentimento para uma pesquisa de dados, sem que ao fim ao cabo, sejam essas pessoas que terão a sua privacidade exposta.

Nos casos em que o dispositivo esteja em locais de acesso público – *v.g* cibercafés – o proprietário do espaço será a pessoa idónea a dar o consentimento pois, nesses casos é ele quem tem a disponibilidade sobre tais dados.

No atinente à al.c) do nº 5 do art. 174º do CPP, está prevista a possibilidade de uma busca sem autorização prévia para casos de flagrante delito, não existindo igual previsão na LC. Será possível proceder a uma pesquisa de dados em flagrante delito? O Art.º 256º CPP prevê três situações em que há flagrante delito: a) quando o crime está a ser cometido; b) quando o crime acabou de ser cometido e; c) quando logo após o crime o agente é perseguido ou encontrado com objetos ou sinais que mostrem claramente que realizou ou participou no crime. Face à dificuldade de investigação no âmbito digital, será

extremamente difícil apanhar em flagrante delito o agente que acabou de cometer um crime por meio de um sistema informático. Pelo que, concordamos com o legislador ao deixar de fora do nº3 do art.º 15.º da LC esta hipótese. O TRP[65] recentemente viu-se confrontado com uma situação de flagrante delito de tráfico de droga, em que se mostrava necessário aceder ao computador de um dos arguidos, foi realizada uma busca à casa do arguido tendo sido apreendido o computador, posteriormente o MP mediante despacho autorizou que fosse realizada a pesquisa de dados informatizados ao computador apreendido. Esta é uma situação que não estando diretamente relacionada com o nosso estudo, nos permite compreender de que forma se pode processar uma busca seguida de uma pesquisa de dados.

Por último, é de salientar que quando os OPC atuam sem autorização prévia, têm que comunicar imediatamente a busca ou pesquisa para que a mesma seja validada. No que concerne à busca, caberá ao JIC apreciar a diligência, nos casos de terrorismo e criminalidade organizada, já na pesquisa de dados caberá à autoridade judiciária competente validar a diligência. Não concordamos com este tratamento diferenciado pois, entendemos que uma pesquisa de dados, em virtude da invasão da intimidade que pode representar para os cidadãos, além de ser uma medida que poderá vir a ter grande aplicação em casos de terrorismo e criminalidade organizada, deveria ser validade pelo JIC tal como sucede nas buscas sem autorização prévia.

3.5.5 – Não cumprimento das formalidades

Uma vez analisadas as formalidades das buscas tradicionais e a sua adaptação à realidade da pesquisa de dados, passaremos a analisar de forma sucinta as consequências do não cumprimento de tais formalidades.

No título V do Livro II do CPP regula-se as nulidades, determinando o art.º 118º - sob a epígrafe Principio da Legalidade – no seu n.º 3 que "As disposições do presente título não prejudicam as normas deste Código relativas a proibições de prova".

O art.º 32 n.º 8 da CRP determina que "São nulas todas as provas obtidas mediante tortura, coacção, ofensa da integridade física ou moral da pessoa, abusiva intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações". No mesmo

[65] Ac.TRP de 07-07-2016, proc.º n.º2039/14.0JAPRT.P1, disponível em www.dgsi.pt (consultado em 16-09-2016).

sentido, o CPP regula no art.º 126º os métodos proibidos de prova, sendo que nos n.ºs 1 e 2 desta norma "(…) vigora uma proibição absoluta de obtenção de prova através dos meios ali indicados, ainda que sejam a coberto do consentimento do titular dos direitos em causa"[66] . Já o n.º 3 do mesmo preceito faz uma ressalva "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".

No entendimento de Paulo Sousa Mendes o legislador consagrou o mesmo tipo de nulidades no art.º 126º n.º 1, 2 e 3, a diferença reside na admissibilidade de restrição do n.º 3 às situações previstas na lei. Assim, para este autor "(…) são nulidades de conhecimento oficioso a todo o tempo e podem ser atacadas excepcionalmente depois do trânsito em julgado da decisão final, caso só sejam descobertos depois disso".[67]

No mesmo sentido, a Juiz de Direito, Teresa Bravo, refere que "(..) a lei processual penal, ao elencar os requisitos dos quais depende, por exemplo, a validade (…) de uma busca (…) fê-lo com um duplo objectivo: garantir a transparência do procedimento; validar do ponto de vista constitucional a sua legalidade"[68]. Para a Juiz de Direito, o não cumprimento de tais formalidades "(…) consubstancia uma prova nula, nulidade essa que é do conhecimento oficioso, e apenas sanável com o trânsito em julgado da decisão"[69].

[66] MENDES, Paulo Sousa, Lições de Direito Processual Penal, 2014, p.180.
[67] Idem, ob. cit., p.190.
[68] BRAVO, Teresa Maria da Silva, ob. cit., p.138
[69] Idem, ob. cit., p. 138.

4 - A (In)Admissibilidade da Busca Online

4.1 Um método oculto de investigação

Fraseando Manuel da Costa Andrade " (…) 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 apercebam".[70]

Embora se reconheça o cariz invasivo que estes métodos têm sobre bens jurídicos essenciais como a direito à privacidade, à inviolabilidade do domicilio, ao sigilo das telecomunicações, entre outros; também se reconhece que estes têm, nos dias de hoje, um papel preponderante no combate à criminalidade altamente organizada.

Estes métodos contém desde logo uma questão preocupante, a pessoa que está a ser investigada não tem conhecimento disso, e por regra, quando tem conhecimento, os indícios que levaram à realização da medida, já serão factos de que o individuo poderá vir a ser acusado.

Os métodos ocultos estão sujeitos a um conjunto de regras e princípios que têm que ser observados. O primeiro é o da reserva da lei, isto quer dizer que "(…) só a lei pode autorizar e legitimar as medidas".[71] Deve especificar-se qual o bem jurídico lesado e de que forma vai ser lesado pois, só desta forma os Tribunais poderão determinar a sua valoração.

Acresce ainda que, deve elaborar-se um catálogo de crimes que justifica a aplicação destes métodos, designadamente, situações de terrorismo e criminalidade altamente organizada. Mostra-se assim importante que haja critérios de proporcionalidade entre o crime cometido e os métodos utilizados durante a investigação.

Além destes, os métodos ocultos estarão ainda sujeitos ao princípio da subsidiariedade, quer a nível intrínseco, quer a nível extrínseco, pelo que se dois métodos garantirem o mesmo resultado, deve dar-se sempre prioridade ao método menos gravoso, ou seja, ao que menos lesar os direitos fundamentais do visado.

---

[70] ANDRADE, Manuel da Costa, ob. cit., p.105.
[71] Idem, ob. cit., p.112.

Face aos danos que estes métodos provocam, a entidade competente para autorizar ou ordenar os mesmos é o Juiz ou o JIC pois, só desta forma se pode garantir a tutela dos direitos fundamentais e evitar abusos de poder.

4.2 A busca *online*

Não se confunda busca *online* com pesquisa de dados armazenados, pois são meios de obtenção de prova totalmente distintos, sendo a primeira um método oculto de investigação que consiste na "(…) infiltração online pela polícia num sistema informático, por exemplo através dos chamados cavalos de Tróia, de modo a que a polícia possa em tempo real conhecer a informação à medida que ela é introduzida no sistema informático". [72] Podendo ocorrer "(…) sob a forma de intromissão instantânea e descontínua ("espelho") ou de forma contínua, permitindo o registo das alterações ocorridas nos computadores-alvos (monitoring)."[73].

Resulta daqui que estamos perante métodos completamente distintos, pois, enquanto na pesquisa de dados – e buscas tradicionais- há uma deslocação dos OPC ao local onde se encontra o sistema informático, na busca *online* a diligência realiza-se "(…) a partir de outro terminal informático(…)" [74], o que consequentemente leva a que na primeira o visado tenha conhecimento de que está a ser alvo de uma investigação, tendo através do despacho conhecimento do que se pretende com tal diligência, ao contrário do que sucede com a busca *online* em que o visado não sabe que o seu computador está a ser observado, monitorizado e até copiado, desconhecendo também a razão de ser da diligência, o que limita também o poder do visado, uma vez que não lhe é "(…) dada qualquer hipótese de controlar os limites legais da diligência ou reclamar conteúdos sigilosos".[75]

Armando Dias Ramos não concorda com a terminologia de buscas *online,* considerando outrossim, que o que está verdadeiramente em causa é uma "pesquisa de dados *online" [76],* que é no fundo "(…) uma intervenção encoberta em sistemas informáticos(…)"[77]. Concordamos que o termo buscas *online,* poderá não ser o mais adequado, em virtude de não existir conhecimento por parte do visado que o seu

[72] ALBUQUERQUE, Paulo Pinto de, *Crime Informático*, artigo de opinião.
[73] ANDRADE, Manuel da Costa, ob. cit., p.153.
[74] NEVES, Rita Castanheira, ob. cit. p.195.
[75] Idem, ob. cit. p. 198.
[76] RAMOS, Armando Dias, ob. cit. p.90.
[77] Idem, ob. cit., pp 90-91.

computador está a ser "vigiado", algo que difere bastante das buscas e da pesquisa, em que há conhecimento da diligência bem como do que se pretende com a mesma.

A Internet tornou-se uma aliada da criminalidade organizada, especialmente do terrorismo, pois através dela grupos terroristas transmitem as suas ideologias e crenças e conseguem recrutar pessoas de todo o mundo para se juntarem a eles, além de ser um meio para organizar atentados. A busca *online*, em virtude da sua característica oculta, poderia ser um método bastante eficaz na luta contra a criminalidade organizada. Nestes casos, as autoridades competentes poderiam ter acesso a informação que lhes permitiria prever o crime e atuar antes da sua realização.[78]

Em contrapartida também tem que se ter em consideração que a busca *online* provoca danos em alguns dos direitos fundamentais dos indivíduos, até porque "(…) 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.)."[79]. Daí que se saliente o quão lesivo é este método, especialmente, se tivermos em consideração que tal medida é oculta, pelo que o suspeito não tem conhecimento que o seu computador está a ser observado.

O legislador nacional omitiu na LC qualquer referência à busca *online*, pelo que esta não é admitida no nosso ordenamento jurídico por falta de disposição legal. Como tivemos oportunidade de referir anteriormente, os métodos ocultos estão sujeitos à reserva da lei, não havendo norma legal que preveja a busca *online* não pode fazer-se uso desta no âmbito de uma investigação.

Rita Castanheira Neves entende 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".[80]

Já João Conde Correia, não considera os fundamentos apresentados determinantes. Quanto ao fundamento de a diligência ter que ser presidida, o autor refere que "A presidência do magistrado tanto pode ser para in locu dirigir a diligência como para o fazer online. Ele não tem que estar presente no local onde está o computador, mas no

[78] Também neste sentido ANDRADE, Manuel da Costa, ob. cit. p.166
[79] Idem, ob. cit., p. 167.
[80] NEVES, Rita Castanheira, ob. cit. p. 284.

local onde se acede".[81] Já quanto à forma de apreensão dos dados informáticos, o procurador entende "(…) que tanto pode ser concretizado no local, como à distância, mediante cópia em suporte autónomo".[82]

Concordamos com João Conde Correia, não obstante a não consagração das buscas *online* no ordenamento jurídico português, os fundamentos apresentados não são determinantes, o que nos parece determinante outrossim é que no Relatório Explicativo do CCiber é expressamente mencionado que as buscas – na formulação da LC, pesquisa de dados – não devem ser encaradas como uma medida "sub-reptícia"[83].

No ordenamento jurídico alemão, as buscas *online* têm sido já alvo de uma análise jurisprudencial, e, apesar de também na Alemanha tal método de obtenção de prova não estar legislado, tal análise tem contribuído para compreender melhor este método.

Vejamos, o Tribunal Constitucional Federal Alemão, num arresto de 27 de Fevereiro de 2008[84], determinou que o acesso oculto a sistemas informáticos permitiria obter um conjunto de informações sobre determinada pessoa, que de outra forma não seria possível, além de permitir traçar o perfil de determinada pessoa, uma vez que com os avanços dos novos meios tecnológicos cada vez mais estes são um meio de armazenamento a que as pessoas recorrem quotidianamente.

Julgou ainda o Tribunal que os art.ºs 10º e 13º da Lei Fundamental (*Grundgesetz*) – sigilo das telecomunicações e inviolabilidade do domicílio, respetivamente – não contém a necessária proteção que exige o desenvolvimento das tecnologias de informação, o que leva a que os cidadãos não estejam totalmente protegidos, por isso, o Tribunal sugeriu a criação de um novo direito fundamental, o direito à "integridade e confidencialidade dos sistemas informáticos".[85]

---

[81] CORREIA, João Conde, ob. cit. p. 42, nota de rodapé 29

[82] Idem, ob. cit. p. 42, nota de rodapé 29

[83] Relatório Explicativo da Convenção sobre a Cibercriminalidade (STE nº185), Ponto 204.

[84] Estava em causa uma norma contida na Constituição de North Rhine-Westphalia que autorizava o acesso oculto a sistemas informáticos, a versão inglesa da decisão encontra-se disponível em http://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2008/bvg08-022.html (consultado em 22/08/2016)

[85] Nesse sentido Manuel da Costa Andrade " (…) o Tribunal Constitucional Federal sugeriu a decantação e institucionalização de um novo direito fundamental, sob o já referido nome de *integridade e confidencialidade dos sistemas informáticos*.Enquanto isto,propõem outros que a expansão teleológica e a protecção se orientem noutras direcções. E falam, por exemplo, de uma "esfera privada electrónica" ou "digital) (Böckenförde)" ob. cit. p. 168. João Conde Correia "Em causa estará, quando muito, a «integridade e condifencialidade do sistema informático»", ob. cit p. 43. E ainda Cesare Maioli e Elisa Sanguedolce "*Sul punto la Corte ne amplia il contenuto, creando, di fatto, un "nuovo" diritto alla riservatezza e integrità del sistema informatico o telematico, ai quali viene offerta una "prosecuzione della tutela" proprio perché attraverso gli stessi l'individuo moderno traspone ed esplica parte della propria personalità e in forza di ciò deve essere tutelato contro l'accesso segreto.*".

Mas porquê a criação de um novo direito fundamental se é pacifico que "(…) os direitos fundamentais são, em si e de per si, dinâmicos e abertos ao futuro, não dependendo a sua revelação e expansão de prévia e necessária intervenção do legislador."[86]?

Tendo como ponto de partida o ordenamento jurídico português - e à semelhança do que sucede no ordenamento jurídico alemão- as buscas *online* provocam dano no direito à inviolabilidade do domicílio e das telecomunicações, art.º 34º CRP. O sigilo das telecomunicações visa a proteção da comunicação em si, mas não do sistema, assim, apesar de a busca *online* ser "(…) um ato de telecomunicação, as buscas online não são uma intromissão nas telecomunicações"[87]. Daí que o que verdadeiramente é atingido pela busca *online* não é a telecomunicação em si mesma, mas o sistema. Já quando as autoridades judiciárias tiverem que realizar uma busca *online*, elas não estão verdadeiramente a proceder a uma busca domiciliária, mas mais importante o visado não sabe que o seu sistema informático está a ser alvo de uma busca, estando limitado no seu campo de atuação, *v.g* o visado não pode colaborar entregando a autoridade judiciária competente o que ela procura, nem pode controlar a duração da busca ou se estão a ser cometidos excessos face ao despacho que autoriza ou ordena a busca. Foi tendo em consideração estas questões que o Tribunal Constitucional Federal alemão levantou a possibilidade de criação deste direito fundamental que teria como escopo a "integridade e confidencialidade do sistema informático".[88]

Contudo, entendeu o Tribunal Constitucional Federal alemão que as buscas *online* poderiam ser constitucionalmente admitidas, desde que, se verificassem indícios concretos de um perigo eminente para um bem jurídico predominantemente fundamental, tais como a vida, a integridade física, interesses coletivos, e ainda ameaças aos Estado de Direito e à existência humana.

E é precisamente sobre esta possibilidade de constitucionalização das buscas *online* que nos debruçaremos agora.

Torna-se evidente que perante um método bastante invasivo, teríamos que ter critérios bastante restritos para a sua utilização pelas autoridades judiciárias competentes. Um dos pressupostos das buscas online teria que ser a existência de "(…) um perigo concreto- e

---

[86] ANDRADE, Manuel da Costa, ob. cit. p. 150.
[87] CORREIA, João Conde, ob. cit. p. 43.
[88] Entre nós, no mesmo sentido, ANDRADE, Manuel da Costa, ob. cit. pag. 168 e, CORREIA, João Conde, ob. cit. p. 43.

um perigo cuja ameaça assente em circunstâncias de facto(…)"[89].Acresce que, e como foi oportunamente esclarecido pelo Tribunal Constitucional Federal alemão, têm que estar em causa bens jurídicos de predominante importância.

A vulnerabilidade a que fica exposto o sujeito alvo das buscas *online* é tal, que permitir a sua realização num vasto catálogo de crimes seria desadequado, assim as buscas online deveriam apenas ser utilizadas em casos de terrorismo, pornografia infantil e criminalidade altamente organizada. Julgamos que nos dias de hoje, e com a crescente criminalidade através de sistemas informáticos - não obstante alguns crimes não serem praticados com recurso a um sistema informático, mas sim os atos preparatórios, como é o caso do terrorismo *v.g*., as buscas *online* poderiam dar um enorme contributo às autoridades judiciais tanto ao nível da investigação como ao nível da prevenção.

Por último, a autorização judiciária no âmbito de uma busca *online* teria que ser sempre da competência do Juiz ou do JIC, dependendo do momento processual. Tendo a autorização que identificar o perigo e os bens jurídicos em risco. Na prática, colocar-se-ão alguns problemas, nomeadamente, o hiato temporal que medeia o risco do crime e a concretização do mesmo, nem sempre será suficiente para que as autoridades judiciárias competentes procedam ao pedido de autorização. Nesses casos não se poderá recorrer às buscas *online*, com ressalva para o terrorismo, onde há casos em que as autoridades judiciárias competentes quando têm conhecimento de um possível atentado, este já é iminente. Nesses casos julgamos que estando em causa várias vidas, seria de admitir a possibilidade de, mesmo sem autorização prévia, as autoridades competentes procederem à busca pois, num conflito de direitos fundamentais entre o direito à vida e o direito à inviolabilidade do domicílio e das telecomunicações, prevalece claramente o primeiro.

[89] ANDRADE, Manuel da Costa, ob. cit. p. 168.

Conclusão

A CCiber é o primeiro grande diploma no combate à criminalidade informática. O art.º 19.º da CCiber, referente às buscas e apreensões, foi transposto para o ordenamento jurídico português através da LC sob a epígrafe "Pesquisa de dados informáticos". Não se pode deixar de criticar a opção legisladtiva do legislador nacional, na medida em que veio dificultar o trabalho das autoridades competentes pela investigação que terá que recorrer a vários diplomas legais para obter a prova digital, teria sido mais simples ter procedido a uma alteração do CPP.

É de salientar que o legislador nacional ao elaborar a LC teve em consideração tanto a CCiber, como o seu Relatório Explicativo, contudo, ficou por legislar de que forma as pessoas que conhecem o sistema informático e a forma como este se encontra protegido, podem colaborar com as autoridades competentes, nem que informação lhes pode ser solicitada.

Apesar de a pesquisa de dados derivar das buscas tradicionais, não podemos deixar de mencionar o seu caráter inovador, permitindo inclusive uma extensão da pesquisa a outros sistemas informáticos, o que não se verifica nas buscas tradicionais, art.º 15.º n.º 4 LC. Também o consentimento para uma pesquisa de dados, pelos OPC sem autorização prévia do MP, merece a nossa atenção, pelo variadíssimo número de pessoas que podem consentir, isto pela escolha do legislador de atribuir o consentimento a quem tiver a "disponibilidade ou controle sobre tais dados". Escolha essa com a qual concordamos, até porque a prova digital é, por si só, muito mais fácil de dissipar que a prova física.

No que concerne às consequências do incumprimento das formalidades da pesquisa de dados, não tivemos oportunidade de tratar o assunto como gostaríamos, todavia, somos da opinião que o não cumprimento das formalidades previstas na lei leva à nulidade da pesquisa o que consequentemente implica a invalidade da prova em tribunal.

As buscas *online* também mereceram especial atenção da nossa parte, seja por uma certa conexão entre este método oculto e a pesquisa de dados, seja também pela controvérsia que rodeia esta medida.

Sendo um método oculto de investigação, as buscas *online* distinguem-se da pesquisa de dados uma vez que, ao contrário desta, o visado não sabe que o seu computador está a ser "vigiado", além de que a intromissão no sistema informático é realizado à distância, ou seja, através de um outro sistema informático.

Este método oculto não está previsto no nosso ordenamento jurídico, porém somos da opinião que esta medida deveria ser legislada, com requisitos bastante exigentes pois, estamos perante uma medida altamente lesiva de direitos fundamentais.

Bibliografia

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

ANDRADE, Manuel da Costa, «Bruscamente no Verão Passado» a Reforma do Código do Processo Penal - Observações críticas sobre uma Lei que podia e devia ter sido diferente, s.l., Coimbra Editora, 2009.

ANTUNES, Maria João, Direito Processual Penal, s.l., Almedina, 2016.

BRAVO, Rogério; ROCHA, Manuel Lopes; VERDELHO, Pedro, Leis do Cibercrime, Vol.I, s.l., Centro Altântico, 2003, consultado em: 16-05-2016, disponível em: centroatlantico.pt

BRAVO, Teresa Maria da Silva, Revistas e Buscas: O Processo Penal na Era da Globalização, III Congresso de Processo Penal Coordenação de Manuel Monteiro Valente, s.l., Almedina, 2010.

BAILIE, Michael W.; HAGEN, Ed; JARRET, H. Marshall, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, s.n, s.l, 2009, consultado em: 04-05-2016, disponível em https://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf.

CANOTILHO, J.J. Gomes; MOREIRA, Vital Martins, Constituição da República Portuguesa Anotada, Vol. I, 4ª Edição Revista, Coimbra Editora, 2007.

CERQUA, Frederico di, Ancora Dubbi e Incertezze Sull'Acquisizione della Corrispondenza Elettronica, Direito Penale Contemporaneo, 2015, consultado em : 03-08-2016, disponível em: http://www.penalecontemporaneo.it/upload/1437560206CERQUA_F._2015a.pdf.

CORREIA, João Conde, Prova Digital: as leis que temos e a lei que deviamos ter, Revista do Ministério Público nº 139, Ano 35, Junho- Setembro 2014.

FARMER JR., John J. - Computer Evidence Search & Seizure Manual, Department of Law & Public Safety Division of Criminal Justice, New Jersey, 2000, consultado em: 05-08-2016 ,disponível em www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf.

FLIPSE, Rachel - An Unbalanced Standard: Search and Seizure of Electronic Data Under the Border Search Doctrine, Journal of Constitutional Law, 2010,consultado em : 04-05-2016, disponível em scholarship.law.upenn.edu.

HOPKINS, Shannon L., Cybercrime Convention: A Positive Beginning to a Long Road Ahead, Journal of High Technology Law, Vol. II, n.º1, 2000, consultado em :03-05-2016, disponível em https://www.suffolk.edu/documents/jhtl.../SHOPKINSV2N1N.pdf.

JESUS, Francisco Marcolino de, Os Meios de Obtenção de Prova em Processo Penal, 2ª Edição, Almedina.

LUPÁRIA, Luca, Computer Crimes e Procedimento Penale in Modelli Differenziati Di Accertaento, Vol. 7, Tomo I, Trattato Utet, 2011, consultado em 04-05-2016, disponível em: http://www.dmi.unict.it/~battiato/CF1011/Lup%C3%A0ria%20-%20Computer%20crimes%20e%20procedimento%20penale%20-%20Trattato%20Utet%202011.pdf.

MARION, Nancy E., The Council of Europe's Cyber Crime Treaty: An exercise in symbolic Legislation, in International Journal of Cyber Criminology Vol 4 Issue 1&2 January - July 2010 / July - December 2010, consultado em: 03-05-2016, disponível em www.cybercrimejournal.com/marion2010ijcc.pdf.

MENDES, Paulo Sousa, Lições de Direito Processual Penal, s.l., Almedina, 2014-Reimpressão, 177 – 198.

MESQUITA, Paulo Dá, Processo Penal, Prova e Sistema Judiciário, s.l., Coimbra Editora, 2010.

MILITÃO, Renato Lopes, A Propósito da Prova Digital no Processo Penal, s.l., s.n., consultado em: 10-05-2016 disponível em: https://www.oa.pt/upl/%7B53f46e96-536f-47bc-919d-525a494e9618%7D.pdf.

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, s.l., Coimbra Editora, 2011.

PINTO, Ana Luísa, Aspectos Problemáticos do Regime das Buscas Domiciliárias, Revista Portuguesa de Ciência Criminal, Ano 15, n.º 3, 2005.

PINTO, Ana Luísa, As buscas não dominiciliárias no direito processual penal português, Revista do Ministério Público, Ano28, n.º 109, Janeiro- Março 2007.

RODRIGUES, Benjamim Silva, Da Prova Penal – Tomo IV, Da Prova- Electrónico-Digital e da Criminalidade Informático-Digital, 1ª Edição, s.l., Rei dos Livros, 2011.

SANTOS, Manuel Simas, LIBER AMICORUM, s.l., Rei dos Livros, 2016.

VENÂNCIO, Pedro Dias, Lei do Cibercrime Anotada e Comentada, 1ª Edição, s.l., Coimbra Editora, 2011.

VENÂNCIO, Pedro Dias, As Medidas de Prova Digital da Lei do Cibercrime- regra ou exceção, Boletim da Ordem dos Advogados, nº 123,Fevereiro,2015, pp 40-41.

VERDELHO, Pedro, A obtenção de prova no ambiente digital, Revista do Ministério Público, Ano 25, n.º 99, 2004.

VERDELHO, Pedro, A Nova Lei do Cibercrime, Boletim da Ordem dos Advogados, nº 65, Abril, 2010, pp 34-35.

Outras Fontes

ALBUQUERQUE, Paulo Pinto de, Crime Informático, artigo de opinião disponível em www.dn.pt, consultado a 10/08/2016

MAIOLI, Cesare e SANGUEDOLCE, Elisa, artigo de opinião, consultado em 22/08/2016 disponível em http://www.altalex.com/documents/news/2012/05/03/i-nuovi-mezzi-di-ricerca-della-prova-fra-informatica-forense-e-l-48-2008

Minuta Relatório Explicativo da Convenção do Cibercrime em Português, consultado em 19-04-2016, disponível em http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/Convention%20and%20protocol/ETS_185_Portugese-ExpRep.pdf.

Proposta de Lei n.º 289/X/4ª https://www.parlamento.pt/ActividadeParlamentar/Paginas/DetalheIniciativa.aspx?BID=34566