UNIVERSIDADE AUTÓNOMA DE LISBOA

"Luís de camões"

Departamento de direito

Mestrado em Ciências Jurídicas

A PROVA DIGITAL

Orientador: Professor. Dr. Rui Manuel de Freitas Rangel

Candidato: Ivo Filipe de Almeida (20100369)

IvoFilipeAlmeida@Gmail.com

Dissertação para obtenção do Grau de Mestre em Direito

Lisboa, 2014

AGRADECIMENTOS

O espaço limitado desta secção de agradecimentos, seguramente, não me permite agradecer, adequadamente, a todas as pessoas que, ao longo do meu Mestrado em Direito na especialidade de Ciências Jurídicas, me auxiliaram a percorrer este caminho, ultrapassando esta etapa na minha formação académica. Com esta impossibilidade, resta-me deixar umas parcas palavras, poucas, embora de profundo sentido.

Em primeiro lugar à Srª. Coordenadora de Mestrados e Departamento de Direito, e amiga, *Cecília Dias*, pela disponibilidade e apoio incansável nas questões que foram surgindo, e que de forma profissional, foi oferecendo diretrizes no sentido da melhor conclusão possível, deste projecto que agora apresento.

Também com importância, deixar neste espaço, uma palavra de apreço, à tantas vezes banalizada, *biblioteca da Universidade Autónoma de Lisboa*, que me permitiu diversas pesquisas relativamente ao tema, assim como todo o material necessário à conclusão deste trabalho.

Aproveito ainda, para deixar uma palavra de apreço ao *Conselho pedagógico* da Universidade Autónoma de Lisboa, na pessoa do seu Presidente o Exmo. *Prof. João Hipólito*, bem como aos demais ilustres colegas, membros concelheiros do mesmo, pela atenção e auxílio prestado relativamente à metodologia do presente trabalho.

Quero também agradecer de forma especial ao Dr. Ferreira da Costa, assim como à Dra. Raquel Torrão, por toda a compreensão, e disponibilidade logística, pois me auxiliaram na conclusão deste objectivo, nomeadamente em dúvidas que iam surgindo. Um muito obrigado.

Fica desde já, como Vice-Presidente da Associação Académica da Universidade Autónoma de Lisboa, uma palavra de apreço a esta, estendendo-se à nossa secretária Isabel Costa, pela disponibilidade de todos os meios logísticos, e compreensão de muitas ausências em actividades necessárias, manifestando desde sempre todo o apoio e motivação imprescindível.

Agradecer à Universidade Autónoma de Lisboa, pela sempre prontidão e reconhecimentos dos seus alunos.

Ao meu orientador de dissertação de Mestrado, Professor, e amigo, *Dr. Juiz Desembargador Rui Manuel de Freitas Rangel*, agradeço a oportunidade e o privilégio que tive em frequentar este Mestrado sob sua orientação, que em muito contribuiu para o enriquecimento da minha formação académica e científica.

Agradecer ao Presidente da Associação Académica, e amigo, Nuno Nabais, por toda a disponibilização de meios necessários à pesquisa, assim como todo o apoio prestado ao longo do estudo.

Deixar umas poucas palavras de apreço, à amiga Bruna do Amaral, por toda a dedicação, preocupação e companheirismo ao longo dos tempos.

À minha avó, por ser um modelo de coragem, apoio incondicional, incentivo, amizade e paciência demonstrados na total superação de obstáculos ao longo da vida. Uma gratificação especial por ser, um orgulho imenso por estar.

Torna-se igualmente obrigatório deixar umas poucas palavras de agradecimento e admiração à Patrícia Henriques, por todo o apoio, companheirismo e auxílio incondicional nas diversas fases que este estudo obrigou. Obrigado por todos os sorrisos que me dedicou.

Por último, torna-se essencial agradecer aos meus pais, a quem dedico este trabalho. Obrigado pelo amor.

‘No tempo em que os homens rudes imperavam, os bandidos nas cruzes penduravam, hoje que vivemos na época das luzes, no peito dos bandidos penduram cruzes’.

Gilbert Cesbron

INDICE

1. RESUMO

A crescente metamorfose da sociedade actual, causa especial impacto nas áreas de maior proeminência de um país, como é o caso da justiça. Neste sentido, e no que à lei diz respeito, sendo esta criada para as pessoas, devem essas transformações ser acompanhadas por uma lei que se mostre actual, e dê respostas justas aos novos problemas que os tempos modernos impõem.

Significa isto que, com a evolução do mundo, povos, e sociedades, temos hoje novas problemáticas, novos enigmas, que para serem supridos exigem novos instrumentos específicos, como é o caso da *Prova Digital*. Com o avanço da tecnologia, novos conceitos como o *'Cibercrime'* entraram no rol das maiores preocupações do índice de criminalidade de cada vez mais países.

Utilizam-se hoje os avanços na tecnologia de informação, como um poderoso meio de praticar não só crimes comuns, como nasce uma criminalidade que carece de nova tipificação no que diz respeito ao seu meio probatório.

A *Prova Digital*, surge-nos hoje, como uma ferramenta que representa um caminho de soluções que mais que nunca, necessita de ser percorrido. Urge a necessidade de combater a criminalidade informática, adaptando assim o nosso sistema jurídico-penal, a uma realidade que a justiça, a lei e o país, devem saber estar à altura.

Palavras-chave – Prova Digital, Prova, Direito Penal, Crime informático, Cibercrime, Sociedade actual.

2. ABSTRACT

The growing metamorphosis of actual's society, especially impacts on areas of greatest prominence in a country, such as justice. In this sense, and in that respect the law, which is created for people, these changes must be accompanied by a current law that show, and give right answers to new problems that modern times require.

This means that with the changing world, people, and companies, we now have new problems, new puzzles, which require to be supplied specific new instruments, such as the Digital Proof. With the advancement of technology, new concepts such as 'Cybercrime' entered the list of the biggest concerns in crime ever more countries.

They are used today advancements in information technology as a powerful means to practice not only ordinary crimes, such as arises a crime that requires further classification with respect to its evidential means.

The Digital Evidence, appears to us today as a tool that represents a path of solutions that more than ever, need to be traversed. There is an urgent need to combat cybercrime, thus adapting our criminal legal system, a reality that justice, the law and the country must learn to measure up.

Keywords - Digital Prove, Prove, Criminal Law, Informatic Crime, Cybercrime, current Society.

3. LISTA DE ABREVIATURAS

A.	**Autor**
AA.	**Autores**
Ac.	**Acórdão**
Al.	**Alínea**
Art.	**Artigo**
CC	**Código Civil**
CP	**Código Penal**
CPC	**Código Processo Civil**
CPP	**Código de Processo Penal**
CRP	**Constituição da República Portuguesa**
P(p).	**Página (s)**
Cfr.	**Confronte, compare**
Etc. *(et coetera)*	**Etc., e o restante, e outros**
Ex.	**Exemplo**
f., fl., fls., fol.	**Folha (s)**
CPC	**Código de Processo Civil**
CEDH	**Convenção Europeia dos Direitos do Homem**
PIDCP	**Pacto internacional sobre os direitos civis e políticos**
NTIC	**Novas tecnologias da informação e comunicação**
OPC (s)	**Órgão (s) de Polícia Criminal**
PJ	**Polícia Judiciária**
PSP	**Polícia de Segurança Pública**
SEF	**Serviço de Estrangeiros e Fronteiras**
TEP	**Tribunal de Execução de Penas**
TIR	**Tribunal de Instrução Criminal**

4. CONCEITO DE PROVA (A SUA NATUREZA)

Para iniciar esta dissertação, faz todo o sentido que o primeiro ponto recaísse no conceito de prova na sua generalidade aludindo suavemente ao seu factor histórico, assim como à sua natureza.

Essa definição, ou conceito, como tantos outros institutos no direito, tem as suas ligeiras discordâncias doutrinárias, dependendo de autor para autor. No entanto, o seu factor histórico parece-nos assente numa consonância geral da grande maioria dos estudiosos da lei.

A semasiologia, de '*prova*', tem a sua génese no Latim *Probatio*, que por sua vez cresce do verbo '*Probare*'. *Probare*, como verbo, representa dar a conhecer, ou demonstrar algo ou situação, formando em especial um juízo.

"*Entende-se, assim, no sentido jurídico, a demonstração que se faz, pelos meios legais, da existência ou veracidade de um facto material, ou de um acto jurídico, em virtude da qual se conclui por sua existência ou se afirma a certeza a respeito da certeza do facto, ou do acto demonstrado*". (1)

Neste sentido, encontramos uma semelhança dos vários conceitos de «prova», entre autores de sistemas jurídicos completamente diferentes.

- "*Prova é o pressuposto da decisão jurisdicional que consiste na formação através do processo no espirito do julgador da convicção de que certa alegação singular de facto é justificavelmente aceitável como fundamento da mesma decisão*" (2)

Surge-nos então a questão de base, relativamente ao «que é Provar?». Abandonando muitos conceitos técnicos relevantes na doutrina, provar algo em Direito, é com certeza produzir um estado de certeza e convicção no julgador, de forma a que este, aborde determinada avaliação de um facto, como sendo verídico. Auxiliando-se deste modo o julgador, à descoberta da verdade material.

---

(1) DE PLÁCIDO E SILVA. "*Vocabulário Jurídico*". Rio de Janeiro: Ed. Forense, 2ª ed., 1967. Vol. III, pág. 1.253.

(2) CASTRO MENDES, João de – "*Conceito de Prova em Processo Civil*", Lisboa, Edições Atica, 1961; p. 741.

Por sua vez, a prova em si, é edificada em dois sentidos que se complementam.

a) **A prova em sentido Objectivo.**

b) **A prova em sentido Subjectivo.**

O sentido objectivo da prova, trata directamente dos meios que são fornecidos ao tribunal, para a descoberta da veracidade dos factos.

Já no que ao sentido subjectivo da prova diz respeito, ao impacto que as provas irão causar no espirito do julgador, gerando por sua vez a convicção da existência ou inexistência dos factos relevantes e necessários à boa decisão da causa. [3]

Subjacente ao conceito de prova, torna-se essencial frisar os princípios basilares que regulam a Prova enquanto instituto da maior proeminência no sistema jurídico.

4.1.Princípio da auto-responsabilidade das partes.

Segundo este princípio, as partes aquando momento de produção de prova, devem suportar as consequências da sua negligência, apatia, erros ou mesmo actos despropositados.

4.2.Princípio da audiência contraditória

Como se pode verificar no art. 517.º do C.P.C, na sua anterior redacção, referente ao art. 415º do novo CPC, este princípio confere que salvo disposição em contrário, as provas não serão admitidas nem produzidas sem audiência da parte a quem hajam sido opostas.

Significa então este preceito, que todas as provas apresentadas admitem uma contraprova, o que resulta na impossibilidade de se produzir alguma prova, sem o consentimento/conhecimento da parte contrária, relacionando-se assim com o "Principio do contraditório".

---

[3] SAPALO, Arnaldo César Miguel Ribeiro - "*A prova e o ónus da prova nos processos civil e penal*", Sol Nascente: Revista do Centro de Investigação sobre Ética Aplicada. Disponível na internet in: http://www.ispsn.org/sites/default/files/magazine/articles/N1%20art5.pdf

4.3.Princípio da aquisição processual

Na esteira deste princípio, entende-se que a prova que é produzida por uma das partes no processo, não pertence efectivamente a esta. Significa então que, para todos os litigantes, assim como o presado maior interesse da justiça, a prova é então matéria referente ao processo em si.

O tribunal, não obstante à parte que produziu determinada prova, deve apreciá-la, como se entende do art. 515º do CPC, redação antiga.

4.4.Princípio da oralidade

É este o princípio que apresenta consagrado no art. 96º. Do CPP, onde se entende que os actos processuais são em regra de forma oral. Significa isto que, desde o depoimento de testemunhas, interrogatório e mesmo a sentença, realça o cumprimento deste princípio. Na realidade a produção de prova em audiência é sempre elaborada de forma oral. Retira-se do Princípio da oralidade, a prioridade dos depoimentos, afirmações ou debates, tudo oralmente, em detrimento das demais provas possíveis em fase de produção de prova como é o caso da prova documental. Retira-se deste princípio, que a produção de prova de maior relevância, é sem dúvida a apresentada em audiência de forma oral.

Outro dos princípios fundamentais que reveste a Prova, trata-se do *Princípio da Livre Apreciação da Prova*. Contudo, terá este princípio, pela sua relevância, um título específico mais adiante, para considerações mais profundas.

5. FUNÇÃO E FINALIDADE

Numa perspectiva de observar a finalidade e função da prova em Proc. Penal, esta absorve também, a sua matriz à lei civil, e seguindo o nosso CPC vigente, no art. 341.º, no Capitulo II, nas suas disposições gerais, é possível extrair de uma forma simples e directa, que a prova tem como primordial função, a demonstração da verdade, ou realidade dos factos. Como acrescentaria o Dr. Ferreira de Cavaleiro, «*factos juridicamente relevantes*». Quando discorremos pela matéria relativa á função e finalidade da Prova, é importante ressalvar que essa mesma abordagem deve ser observada de vários sentidos.

Dos autores onde se pode retirar com especial clareza as 3 acepções diferenciadas relativamente à caracterização da Prova, no dizer do Dr. Rui Rangel [(4)] explicitou, no seu livro '*O ónus da prova em processo civil*' com nitidez que se subscreve.

5.1. **Prova como actividade probatória**, pode também ser observada como estrutura, na perspectiva do agente, assim como dos efeitos que desta resultam. Enquanto estrutura, abordamos um aglomerados de actos quando num sentido de concepção global, ou até mesmo por actos individuais, apelidando de concepção atomística. Por outro lado, já na perspectiva do agente, poderá ser uma actividade que parte de uma, ou uma pluralidade de pessoas, sendo uma teoria restritiva ou não restritiva. Já no que aos seus resultados e efeitos diz respeito, entende-se como material ou tendencial. Em suma, e sendo que neste sentido, se assume prova como o acto ou conjunto de actos que irão conduzir a entidade decisora a formar a sua convicção;

5.2. **Prova como meio de prova**, assumindo-se neste âmbito, ser o instrumento utilizado para formar a convicção do tribunal; ou seja, a doutrina que entende que a prova não é uma actividade probatória, nem mesmo um resultado, cingem-se a que a prova é um meio, ou um facto que conduzem a investigação a esse resultado. Em suma, compreende-se que o meio é a prova.

5.3. **Prova como resultado**, pois é então o resultado desta, que cria ou não a convicção da entidade decisora acerca da existência ou não de factos jurídico-criminais. Entende-se assim sendo, que a prova não é uma actividade, nem um meio, mas antes um efeito destas duas, ou seja o resultado probatório. [(5)]

---

(4) RANGEL, Rui Manuel de Freitas – "*O Ónus da Prova em Processo Civil"*, Lisboa, 3.ª ed. Almedina, 2006.

(5) EIRAS, Henrique; FORTES, Guilhermina – "*Processo Penal Elementar*", Lisboa, Quid Juris, 2009; p.135.

No que concerne ao objecto da prova, este podem ser todos os factos jurídicos relevantes para a existência ou não de um crime. Determina-se com a prova, a punibilidade ou a não punibilidade do arguido, e mesmo a determinação da pena ou porventura, medida de segurança, tal como consagra o art.º 124.º do CPP.

Segundo Almeida (1927, pp. 112), a prova enquanto função em processo penal, deve ser uma ferramenta de averiguação necessária à causa, e quando em civil, deve corroborar a verdade ou não, das premissas formuladas em juízo pelas partes.

Noutro sentido, a prova não só tem a capacidade de provar determinado facto, como pode inúmeras vezes evidenciar outros tantos, pelo seu indício, ou mesmo presunção.

Como é notório na visão de Carnelutti [(6)], a presunção não consiste de todo numa prova, contudo, ela forma-se, e converte-se por conexão com o facto em especifico que se quer provar, ficando então à última decisão do julgador, a convicção da existência ou não do facto que a parte ou o tribunal tenha levantado.

6. OS MEIOS TRADICIONAIS DE OBTENÇÃO DE PROVA

Abordando o instituto dos *meios de obtenção de prova*, torna-se para mim indispensável diferenciar os infra mencionados, dos meios de prova.

Estes últimos, os *meios de prova*, capitulados especificamente no Titulo II do CPP, estão cuidadosamente plasmados no art.º (s) 128.º e seguintes.

6.1.Prova testemunhal (art.º 128.º, e 129.º do CPP)

A testemunha é inquirida sobre factos de que possua conhecimento directo e que constituam objecto da prova.

Por outro lado, a inquirição poderá recair igualmente sobre factos que a testemunha ouviu dizer, assim seja relativamente a pessoas de impossível inquirição, como por exemplo morte, ou anomalia psíquica.

---

(6) CARNELUTTI, Francesco; "*Sistemas de Derecho Procesual civil"*, Buenos Aires, Vol.II,1944.

6.2.Declarações do arguido (art.º 140.º e 141.º do CPP)

Diz-nos este mesmo disposto, que "*sempre que o arguido prestar declarações, e ainda que se encontre detido ou preso, deve encontrar-se livre na sua pessoa*". No ponto 2) do mesmo art., compreende-se que "*às declarações do arguido é correspondentemente aplicável o disposto nos artigos 128.º e 138.º"* (depoimento das testemunhas), salvo quando a lei dispuser de forma diferente.

6.3. Prova por acareação (art.º 146.º do CPP)

Plasmado no CPP, no Capítulo III, está a prova por acareação. Significa esta que é então possível a acareação entre co-arguidos, entre arguido e assistente, entre testemunhas e entre estas. Ou seja, sempre que existir no entender do julgador contradição entre depoimentos, deve então ser requerida a prova por acareação, de forma a confrontar as partes incidentes da contradição, na justa medida que a diligência se afigure necessária para a descoberta da verdade material.

6.4. Prova por reconhecimento (art.º 147.º do CPP)

A prova por reconhecimento está consagrada no capítulo IV do CPP, onde explica que sempre que existir necessidade de se reconhecer alguma pessoa, solicita-se ao agente que deve então fazer a identificação, para a descrever, com a nomeação dos vários pormenores e características que este se recordar. Após a descrição, é questionada relativamente à altura que viu a pessoa identificada, em que circunstâncias e condições, na tentativa de apurar realmente a veracidade dos factos alegados, correspondendo à fiabilidade da identificação.

6.5. Prova pericial (art.º 151.º do CPP)

A prova pericial, é especialmente necessária quando é urgente a perceção ou apreciação de factos relativos a matérias de conhecimento técnico específico. Por norma é a perícia realizada em estabelecimentos próprios, como laboratórios. Sempre que a perícia recaía sobre matéria que o julgador entenda ser de especial complexidade, pode então haver

lugar a vários peritos, para do relatório destes, se retirar uma maior pluralidade de resultados, e deste modo, decidir ao encontro da verdade material.

6.6.Prova documental (art.º 164.º do CPP)

Em sede de conceito ou definição de *meios de prova*, são estes as formas, do tribunal apurar a veracidade dos factos alegados, comparando-os, e relacionando-os com meios de prova apresentados pela parte contrária.

Por outro lado, quando falamos em *meios de obtenção de prova*, estes relacionam-se directamente com a delimitação e regulamentação de instrumentos necessários à investigação.

6.7.Exames (art.º 171.º do CPP)

Os exames, relacionam-se a pessoas, lugares e das coisas, na tentativa de com a investigação, apurar-se algum vestígio que tenha sido resultado de um crime, assim como os indícios que possam auxiliar na descoberta da verdade. Os exames, tendem a ser céleres, na tentativa de recolher as provas a tempo de que estes não se dissipem, ou modifiquem de forma a tornarem-se inúteis para a investigação. Para tal, e quando a investigação é mais longa, é importante privilegiar o acesso a locais de investigação, na tentativa de proteger o espaço o mais possível.

6.8.Revistas (art.º 175.º do CPP)

Quando existe suspeita de que alguém oculta na sua posse, qualquer objecto que se relacione directa, ou indiretamente com um crime, a investigação deverá prosseguir por meio de revista ao local. Poderá a revista ter de ser ordenada por despacho judicial, caso seja esta em local reservado, e sem acesso ao público.

Antes de se proceder à revista, é entregue ao visado, cópia do despacho que assim a determinou.

6.9.Buscas (art.º 176.º do CPP)

A busca procede-se de igual modo que a revista, com a diferença que no despacho se encontra especificamente o objecto ou objectos para detenção e apreensão. Nos casos em que se trate de buscas domiciliárias, existem pressupostos mais rígidos a cumprir, tendo em vista a dignidade pessoal do visado, e o seu pudor, como por exemplo, horários a ser cumpridos.

6.10. Apreensões (art.º 178.º do CPP)

São susceptíveis de apreensão, os objectos que tiverem sido utilizados, ou estejam como preparatórios de um crime, assim como os seus lucros, preços ou recompensas. São ainda passíveis de apreensão, os objectos deixados pelo agente no local do crime, e ainda quaisquer outros uteis e necessários que sirvam à prova.

Existem do mesmo modo, formalidades específicas nas apreensões, quando ordenadas em locais exclusivos, ou a pessoas determinadas, como é o caso de escritórios de advogados, consultórios médicos, estabelecimentos bancários, ou funcionários que detenham na sua profissão, segredo profissional, ou de estado.

6.11. Escutas telefónicas (art.º 187.º do CPP)

Em última ratio, e sempre que nenhuma outra meio de prova se demonstre eficaz, pode o juiz, ordenar a intercepção e gravação de conversação e comunicação telefónicas. O conjunto de requisitos para que sejam legais as escutas são complicados de obter, como plasma o art. 187º na sua letra.

Conclui-se assim, que os *meios de obtenção de prova*, são instrumentos de que servem as autoridades judiciárias, para investigar e recolher meios de prova. Não sendo por sua vez, instrumentos de demonstração do *Thema Probandi*, são antes instrumentos para recolher no processo, esses mesmos meios. [(7).]

[(7)] DA SILVA, Germano Marques, *"Curso de Processo Penal"*, Vol. II; Lisboa, Verbo, 2002; p. 209.

7. RESTRIÇÕES E LIMITES AOS MEIOS DE OBTENÇÃO DE PROVA

O *Principio da investigação* [8], ou *da verdade material*, incumbe o tribunal de legitimidade e competência para, não obstante às partes, (Cfr. O n.º 3 do art.º 6.º da CEDH, e o n.º 3 do art.º 14.º do PIDCP) proceder à investigação, e deste modo, ordenar todos os meios de prova que considere necessários para a descoberta da verdade material dos factos que foram dirigidos a julgamento. Este princípio não significa que o processo penal abdica da sua estrutura acusatória, mas podemos falar neste contexto de uma estrutura acusatória moderada.

Contudo, este *Principio da investigação* ou da *Verdade material*, deve ser exercido com especial atenção e prudência à sua mitigação legal. Falamos aqui de um limite a esta investigação lícita por parte do tribunal, que se denomina, como o *Principio da verdade processual*.

Neste sentido, elaboro este meu capítulo relativo às restrições e limites aos meios de obtenção de prova, apontando o *Principio da verdade processual*, como um dos institutos responsáveis por essa limitação.

O *Principio da verdade processual*, funciona a par com os conceitos vertidos no *Principio da verdade material*, levantando a este último, questões de admissibilidade, regrando-o na sua forma, para que se retire da investigação um conteúdo de veracidade, sem zurpar qualquer tipo de direito. Por outras palavras, não permite que se vislumbre ou alcance a verdade absoluta, a todo e qualquer custo.

---

[8] O **princípio da investigação**, respeita à prossecução processual, mas em especial à matéria da prova. É também conhecido pelo princípio do inquisitório, instrutório ou da verdade material. Não utilizamos a terminologia "princípio do inquisitório", porque poderia pensar-se que estávamos a referir-nos ao antigo processo de estrutura inquisitória. E não utilizamos "princípio da instrução"" porque poderia induzir em erro, ligando-se o termo à fase de instrução, crendo-se que se tratava de um princípio que somente se aplicaria nessa fase processual. Quanto à terminologia "verdade material", ela é adequada na medida em que, adoptando-a, procura-se rejeitar uma verdade meramente formal. É precisamente este o sentido que se retira do n.º 1, do art. 340.º do CPP.

Segundo Claus Roxin [(9)], as proibições de prova têm as suas subclasses. Estas são divididas em, *proibições de produção de prova* e *proibições de valoração de prova*. A primeira divisão enunciada, subdivide-se em:

1. **Temas de prova proibidos** – determinados factos não podem ser objecto de prova;
2. **Meios de prova proibidos** – quando determinados meios de prova não podem ser empregues;
3. **Métodos de prova proibidos** - na produção da prova, não podem ser utilizados certos métodos de recolha da mesma;
4. **Proibições de prova relativas** – a ordem ou a obtenção de prova só pode ser levada a cabo por certas pessoas.

A nossa lei fundamental, no âmbito de *Garantias do processo criminal*, consagra também o seu limite relativamente à prova, e à forma com se obtém a mesma. No art.º 32º n.º 8, plasma a CRP, que "*se consideram 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"*.

Esta ingerência, perfeitamente compreensível e necessária da CRP nas Garantias de processo penal, faz especial sentido, e levanta pertinentes questões, especialmente no meio de obtenção de prova do art.º 187.º do CPP; as escutas telefónicas. É precisamente nesta matéria que o nosso CCP é especialmente cauteloso, no sentido de não violar nenhum direito fundamental. Os requisitos e pressupostos necessários para se utilizar como meio de prova as *escutas telefónicas* são bastante musculados, e somente se utiliza este, quando saem frustrados todos os demais meios de obtenção de prova. Cfr. Art.º 187.º 1º) "*A intercepção e a gravação de conversações ou comunicações telefónicas só podem ser autorizadas durante o inquérito, se houver razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter, por despacho fundamentado do juiz de instrução e mediante requerimento do Ministério Público (...)"*, quanto a uma especificidade de crimes plasmados nas alíneas seguintes deste mesmo artigo.

---

(9) LIMA RODRIGUES, Cláudio, "*Derecho Procesal Penal*" (trad. da 25.ª ed. alemã por Gabriela Córdoba e Daniel Pastor), Buenos Aires: Editores del Puerto, 2000, cit., pp. 190, 191 e 194.

É ainda importante ressalvar como nota final deste título, que não valem em julgamento, nomeadamente para o efeito da convicção do tribunal, quaisquer provas que não tiverem sido produzidas ou examinadas em audiência. Contudo, ressalva-se desta situação, as provas contidas em actos processuais, cuja leitura, audição ou visualização em audiência sejam permitidas na lei, como se alcança do art.º 355.º al.) 1.º e 2.º do CPP.

8. PRINCÍPIO DA LIVRE APRECIAÇÃO DE PROVA

A prova enquanto meio para demonstrar a realidade dos factos, como melhor supra disposto, é alicerçada em princípios que são para esta, basilares na sua estrutura e génese.

Entre os inúmeros princípios orientadores da prova, achei especialmente pertinente para este estudo, dissecar um pouco o *Principio da livre apreciação da prova*, elencando-o mais detalhadamente, evidenciando-o dos demais princípios reguladores.

O princípio da livre apreciação da prova, diz-nos no art.º 127 do CPP, que "*salvo quando a lei dispuser diferentemente, a prova é apreciada segundo as regras da experiência e a livre convicção da entidade competente"*. Significa isto que, se a lei for omissa, ou por outro lado, não especificar que valor probatório tem determinada prova, o julgador decide em cada caso, segundo a sua consciência.

"A valoração da prova demonstra uma dinâmica axiológica a cargo do próprio julgador, sem que este esteja vinculado a critérios fixados na lei, de cuja conjugação no sistema da prova legal, resultaria do acerto decisório". [(10)]

Segundo Germano Marques da Silva, "*É geralmente reconhecido que a convicção intima não é por si critério de verdade e também seria erro grosseiro pensar que as regras legais quanto ao valor das provas eram necessariamente arbitrárias. Elas assentavam na experiencia comum representavam a estratificação de conhecimento empírico obtido através dos séculos".*[(11)]

---

(10) NEVES, Rosa Vieira, "*A Livre Apreciação da Prova e a Obrigação de Fundamentação da Convicção*", Coimbra; Coimbra Editora, 2011, p. 57.

(11) DA SILVA, Germano Marques, "*Curso de Processo Penal"*, II Volume, Lisboa, São Paulo, Editorial Verbo, 4ª edição revista e atualizada, 2008, p.148.

Através de Figueiredo Dias, [12] "*A liberdade de apreciação da prova é, no fundo, uma liberdade de acordo com um dever – o dever de perseguir a chamada «verdade material» -, de tal sorte que a apreciação há-de ser, em concreto, recondutível a critérios objetivos e, portanto, em geral susceptível de motivação e de controlo (possa a lei renunciar à motivação e ao controlo efectivos*"

Contudo, o *Principio da livre apreciação da prova* tem os seus limites, pois se assim não fosse, estaríamos à mercê de decisões judiciais simplesmente assentes no livre arbítrio do julgador para a prova em específico, sempre que a esta não corresponda um suporte probatório tipificado.

Muito embora o julgador tenha a liberdade, segundo a sua consciência, e nos casos específicos, valorar a prova segundo a sua consciência, terá sempre de respeitar os métodos proibidos de prova do art.º 126. do CPP, considerando nulas todas as provas que este mesmo artigo estabelece, consagrando-se assim o *Principio da não taxatividade* (Cfr. Maria João Mimoso, Bárbara Magalhães – A disometria da pena, sua determinação "in concreto") dos meios de prova.

Se desse modo o julgador violar este princípio, pode a sentença vir a ser impugnada ao abrigo do disposto no art.º 379 do CPP.

Ainda que seja esta uma matéria de controvérsia tendo em conta a subjectividade que está patente na valoração que o juiz dá a determinada prova, certo é, que é necessária uma convicção absoluta, relativamente à veracidade da prova apresentada, para que o julgador a aprecie, atribuindo-lhe um peso decisório no processo. Quando assim não sucede, deve o julgador saber agilizar estas suas indeterminações, com o *Principio in dubio pro reo*.

---

[12] DIAS, Jorge de Figueiredo, Direito Processual Penal, I volume, Coimbra; Coimbra Editora, 1974, pp. 202-203.

"O juízo crítico e rigoroso sobre a prova e a sua ligação a cada facto a provar, sendo a tarefa mais difícil do julgador, é o momento determinante para termos uma decisão de qualidade. A fundamentação da matéria de facto, (provada ou não provada) e o grau de certeza e de convicção na motivação são os ingredientes indispensáveis de qualquer sentença. O que custa é arrumar os factos e valorar o grau de credibilidade da prova. Se assim agir qualquer juiz cumpre a sua missão, O princípio da livre apreciação da prova não é absoluto, sofre limitações que decorrem do grau de convicção exigido para a decisão, da proibição dos meios de prova, da observância da presunção de inocência e da salvaguarda do «princípio in dubio pro reo".[13]

A livre apreciação da prova, enquanto factor da convicção do julgador, ganha especial complexidade em crimes, cuja prova possível se nuclearia ao depoimento da vítima (Ex. Crime de abuso sexual). Neste sentido, a convicção do julgador tem de ser formada por indícios absolutamente rigorosos, que surjam de critérios objectivos, e forneçam credibilidade ao julgamento da matéria factual.

"*A prova testemunhal assente no depoimento da vítima abusada é legal e admissível. Na ausência de diferentes elementos probatórios, perícias e outros, os indícios da verificação do facto têm de ser fortes e reveladores de uma convicção indubitável de condenação, porque o seu resguardo é apenas a credibilidade do depoimento da vítima violada. Só com a prova testemunhal a credibilidade e os indícios têm de ser fortes*". [14]

---

[13] RANGEL, Rui Manuel de Freitas, Correio da Manhã, 16.09.2010, e ainda, RANGEL, Rui Manuel de Freitas – "*O Onús da Prova em Processo Civil*", Lisboa, 3.ª ed. Almedina, 2006.

[14] RANGEL, Rui Manuel de Freitas, Correio da Manhã, 16.09.2010, e ainda, RANGEL, Rui Manuel de Freitas – "*O Onús da Prova em Processo Civil*", Lisboa, 3.ª ed. Almedina, 2006.

9. SOCIEDADE DE COMUNICAÇÃO/INFORMAÇÃO

Abre o presente título o apetite ao tema central deste estudo, começando com a especificação da *Sociedade de comunicação*.

O Homem, enquanto ser social, tem vindo a alterar substancialmente a forma como se desloca, e pensa, adaptando-se à competitividade a que a sociedade obriga, tornando-se mais competente e especialmente produtivo. As metamorfoses evidentes não surgem apenas através de uma imensa rede de transportes, ou mesmo com a criação de empresas economicamente sustentadas, por sua vez, essa transformação sente-se também ao nível da comunicação.

O economista *Fritz Machlup*, foi, em boa hora, o primeiro estudioso a estabelecer um conceito profundo da Sociedade de informação, como noção absolutamente necessária à caracterização da sociedade actual, abordando desde logo a sua *Globalização*.

Mas começando um pouco antes, a internet [(15)], veio trazer ao Direito, um espaço de liberdade um tanto à margem dos regimes legais existentes. A *Globalização* que acima se frisou, teve na *internet* a sua especial motivação, e assim sendo, gerou-se um impulso criador de novos conceitos, pensamentos e costumes, com a liberdade natural de um sistema que floresce na periferia legal, que não foi devidamente explorado.

Essa Globalização tem as suas vantagens especialmente ao acesso que presentemente qualquer cidadão tem a informações, que outrora, seria extremamente complicado alcançar, ou sequer possível. Esse especial acesso à informação, é o principal responsável das transformações económicas, sociais, culturais e mesmo políticas. Essas transformações, e avanço na tecnologia tem demonstrado ser, o motor da evolução que a sociedade actual tem sentido. (*vide fig.1.1*)

---

(15) **Internet**, teve início em meados de 1969 pelo Departamento de Defesa dos EUA. É a interligação de computadores das mais variadas regiões geográficas numa mesma rede, possibilitando a comunicação em tempo real entre estes. A Internet é agora um conjunto em permanente expansão de redes de computadores, ao nível mundial, formada por servidores ou hots, interligados por uma rede remota e utilizando um protocolo comum de comunicação (TCP/IP – transmission control protocol/Internet protocol) que lhes permite a disponibilização de toda a panóplia de serviços comuns – email, ftp, newsgroups, chat, entre outros. "*Breve introdução da questão da investigação e meios de prova na criminalidade informática"* do Dr. Pedro Dias Venâncio.

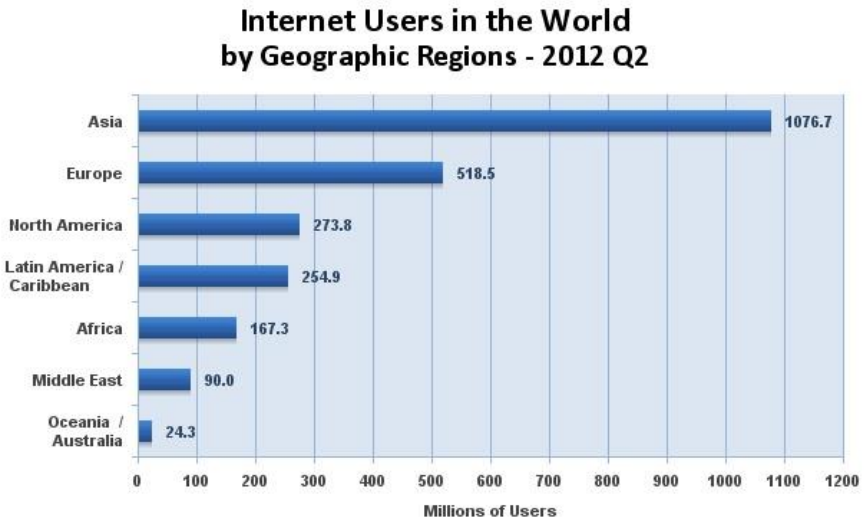

Fig. 1.1 – Crescente número de utilizadores de internet
(Fonte: http://www.internetworldstats.com/)

De facto, pode dizer-se que as *novas tecnologias de informação e/ou da comunicação* (NTIC) determinaram, de forma global, uma nova economia, com a característica onde se introduz a figura dos bens impalpáveis. Sentiu-se igualmente efeitos desta mutação na sociedade, no crescimento do emprego no âmbito dos serviços relacionados com estas tecnologias. A *Globalização*, vem por sua vez, permitir o acesso facilitado a um mercado livre, um mercado à escala mundial.

Os benefícios que as novas tecnologias trouxeram à sociedade são indubitavelmente inegáveis, contudo, também esses benefícios têm uma outra face de uma mesma moeda, que foi a abertura ao Crime informático, tornando-o mais acessível e permeável.

10. CONCEITO E NATUREZA DA PROVA DIGITAL

" [A] *prova electrónico-digital pode definir-se como qualquer tipo de informação, com valor probatório, armazenada* [Em qualquer dispositivo de armazenamento digital]

ou transmitida [em sistemas e redes informáticas ou redes de comunicações electrónicas, privadas ou publicamente acessíveis]*, sob a forma binária ou digital"*. [(16)] Sublinhados meus.

A *Prova Digital*, tal como qualquer outra prova, tem de reter o seu valor probatório, para que este seja susceptível de ser valorado pelo julgador, e crie a sua convicção de veracidade do facto. Por sua vez, a diferença que se encontra entre esta e as demais provas, é a característica do formato digital. Sendo assim, pode esta ser armazenada ou transmitida também no meio digital, seja num computador, ou qualquer dispositivo capaz de conservar com segurança a Prova.

O formato digital desta prova, responde também à necessidade que a sociedade actual vai apresentando, no combate à criminalidade informática. Torna-se então possível a localização, identificação, e delimitação dos infractores, no que diz respeito a crimes que pela sua natureza tecnológica, seria impossível ou muito complicado, extrair uma prova sustentada, capaz de criar convicção, de todo o modo operacional praticado pelos executantes do crime ou ilícito.

A Prova Digital, apesar da sua forma, ainda reveste a capacidade de abraçar um incalculável número útil de conteúdos, permitindo assim, a celeridade, e veracidade da descoberta da verdade material. Com a prova digital, abre-se uma panóplia de possibilidades concretas de conteúdos, todos eles, com a acessibilidade provida pelo formato digital.

Qualquer áudio ou vídeo, e todos os dados de rede, podem ser utilizados como prova, sendo estes extremamente úteis no desenrolar do processo, assim como na descoberta da verdade material.

[(16)] RODRIGUES, Benjamim Silva Rodrigues, Direito Penal. Parte Especial, I, "*Direito Penal Informático-Digital"*, Coimbra, Coimbra Editora, 2009: p. 39.

11. IMPORTÂNCIA OU DISPENSABILIDADE NA BUSCA DA VERDADE MATERIAL

Inegavelmente a *Prova Digital* tem hoje, ou deveria ter, a forçosa importância no panorama criminal nacional e internacional, especialmente em virtude de responder na especificidade a certo tipo de crimes, que com outro tipo de prova, seria complexa e desajustada a sua investigação.

Na realidade, a importância da *Prova Digital* manifesta-se no dia-a-dia da nossa justiça, revelando-a mais débil, e menos producente. Um largo número de processos judiciais são arquivados por insuficiências probatórias, e produzem-se capas de jornais alegando essa mesma lacuna.

Diz-nos a imprensa nacional, que foi especificamente a falta de material probatório que levou a que a grande maioria dos inquéritos investigados no ano de 2012, pelo Ministério Público, em Lisboa, tenham sido arquivados. E que tem levado a que o número de processos arquivados esteja a aumentar de ano para ano, como indicam os relatórios de actividades dos últimos três anos da Procuradoria-Geral Distrital de Lisboa [(17)].

Com a *Prova Digital*, falamos numa criminalidade forma específica, contudo, não somente a criminalidade informática carece de um tipo de prova que responda às suas necessidades. São vários os crimes e ilícitos em que a *Prova Digital* seria uma mais-valia na investigação e continuidade do processo, oferecendo a esta, uma sustentabilidade probatória, capaz de gerar a convicção necessária ao julgador que, entenda-se, de outra forma seria praticamente impossível provar o facto em particular.

Na realidade, é no mínimo desgastante saber que cerca de 20% dos inquéritos em investigação ou investigados nesta área [da criminalidade informática] são concluídos com proposta de arquivamento por inexistência de elementos que permitam prosseguir a investigação [(15)], e neste sentido, em conclusão deste título, denota-se a real indispensabilidade de uma prova que tende a colmatar muitas destas situações, contribuindo para uma justiça melhor.

[(17)] CARVALHO, Paula Torres de, Jornal Público, 20.02.2012.

12. A CRIMINALIDADE INFORMÁTICA

Vários são os conceitos de Criminalidade informática, no entanto, falando num conceito de Criminalidade em sentido amplo, 'englobará toda a panóplia de actividade criminosa que pode ser levada a cabo por meios informáticos, ainda que estes não sejam mais do que um instrumento para a sua prática, mas que não integra o seu tipo legal, pelo que o mesmo crime poderá ser praticado por recurso a outros meios' [(18)]

Com esta definição, torna-se importante congregar a criminalidade informática como um crime tipificado na lei objectiva; como também essa mesma definição, aproveita para qualquer acto que aproveitem dessa tecnologia digital, como meio para cometer o crime, ou mesmo como actos preparatórios deste.

Por sua vez, quando abordando este mesmo conceito, num sentido estrito, diz-nos o mesmo autor que apenas abarcará aqueles crimes em que o elemento digital surge como parte integrador do tipo legal ou mesmo como seu objecto de protecção. [(19)]

Rita Coelho dos Santos, de certa forma, reitera a abordagem defendida por Pedro Dias Venâncio, contudo e segundo esta, é de vital importância a divisão do tema da *Criminalidade informática* em:

12.1. **Crimes tipicamente informáticos** – Sendo os crimes em que o objecto da acção é um computador, ou outro qualquer equipamento derivado da tecnologia. É importante realçar, que nos crimes tipicamente informáticos, a não existir a utilização de um destes equipamentos, entende a autora que dessa forma, não estão preenchidos os elementos do tipo de crime.

12.2. **Crimes essencialmente informáticos** – São os crimes em que se entende que o bem jurídico violado em causa é um equipamento informático, com dignidade suficiente para merecer uma tutela penal.

---

(18) LOPES, José Mouraz, e CABREIRO, Carlos Antão - "*A Emergência da Prova Digital na Investigação da Criminalidade Informática*" in Sub Judice — Justiça e Sociedade, n.º 35, Coimbra, Almedina, 2006.

(19) VENÂNCIO, Pedro Dias – "*Breve introdução dos meios de prova na criminalidade informática*", Verbojuridico, 2006.

12.3. **Crimes acidentalmente informáticos** – Aqueles crimes em que o computador ou o equipamento informático, serviu de meio para o cometer. Deste modo não preenche os elementos tipos do crime.

Na realidade, e tentando explanar estas três divisões de crimes informáticos de uma forma mais simples, encontramos no núcleo uma grande divisão. Os *Crimes informáticos como um meio* para a prática de um crime, ou seja, quando as tecnologias de informação permitem, ser utilizadas para o exercício de crimes tipificados comuns (ex. ameaça, coacção, descriminação, etc.), ou o *Crime informático como elemento integrador do tipo legal*, e isto é, quando o bem jurídico em causa é a liberdade de acesso a tecnologias de informação, ou até a privacidade nas mesmas.

A empresa responsável pela criação e difusão do antivírus *BitDefender*, calculou em Novembro de 2013, que a cada 15 segundos nascia mais uma vítima de fraude de crime informático, com documento furtados, ou informações que desaparecem da rede.

As redes sociais são por excelência um meio, que se relacionam com certo tipo de incursões, fraudes e criminalidade informática, normalmente apelidados de *Phishing*.[(20)] Estas invasões operam em forma de mensagens falsas, ou ligações fraudulentas, e ainda *software* que danifica e permite o acesso a informação privilegiada, pessoal, de vários utilizadores.

Não obstante, as novas tecnologias de informação não se cingem a fraudes de pequeno impacto pessoal, a particulares, podendo ser, como tem sido, utilizadas com impactos superiores, causando prejuízos muito mais avultados e tantas vezes com danos irreparáveis, como aconteceu no caso da operação Israelita "*Orchard*" em 2007, no conflito informático-digital entre a Geórgia e a Federação Russa em 2008, no "*GhostNet"* em 2009, nas recentes de grupos de ativistas como os "Anonymous", ou no recente ataque informático contra a NATO, [Agora reivindicado por piratas informáticos da Ucrânia],

---

[(20)] *Phishing*, vem do inglês "*Fishing*", que significa 'pescar'. *Phishing* é uma forma de fraude eletrónica que opera maioritariamente em redes sociais, no qual existe a intrusão num espaço ou plataforma pessoal de um utilizador, tendo acesso a informação privilegiada que só a este diz respeito. Ex. de *emails*, palavras-chave, mensagens, entre outras matérias.

"CyberBerkout" são exemplos de ataques que vem a tomar a sua predominância no mundo actual. Os E-mails Nigerianos [(21)] (à semelhança das cartas nigerianas), tratou-se da recepção de *e-mail* de alguém que se identifica como alto funcionário da Nigéria, e necessita de ajuda para depositar uma quantia monetária elevada no estrangeiro, para o que solicita o IBAN de uma conta titulada pelo destinatário da mensagem de correio electrónico, com promessa de uma comissão avultada. No desenvolver da correspondência, é solicitado um pequeno adiantamento para se concretizar essa transferência, indicando o remetente uma conta de depósito. Obviamente, que no caso de a vítima aceder, ficará com o prejuízo respectivo no seu património.

A criminalidade informática, torna-se especialmente complexa no que diz respeito à identificação do ou dos infractores. Com este tipo de criminalidade, permite-se facilmente o encobrimento da identidade, em primeira instância porque possibilita que o infractor esteja muitas vezes distante do local do crime, e ainda mais, afinal possibilita ainda, tomar uma identidade virtual, ou mesmo de terceiros, o que dificulta bastantes vezes a investigação.

A este propósito, é relevante o catálogo dos ciberdelinquentes apresentado por Vladimir Aras [(22)], segundo o qual:

12.4. **Os Hackers** «são, em geral, simples invasores de sistemas, que atuam por espírito de emulação, desafiando seus próprios conhecimentos técnicos e a segurança de sistemas informatizados de grandes companhias e organizações governamentais;

12.5. **Os Crackers**, por sua vez, são os "*Hackers aéticos*". Invadem sistemas para adulterar programas e dados, furtar informações e valores, e prejudicar pessoas. Praticam fraudes eletrônicas e derrubam redes informatizadas, causando prejuízos a vários usuários e à coletividade;

---

(21) MAGRIÇO, Manuel Aires, '*A criminalidade informática'*, 2011, p.3

(22) ARAS, Vladimir, disponível em http://pt.wikipedia.org/, e do Artigo, '*A propósito da prova Digital'*, LOPES Militão, Renato, p. 14.

12.6. **Os Phreakers** são especialistas em fraudar sistemas de telecomunicação, principalmente linhas telefônicas convencionais e telemóveis, fazendo uso desses meios gratuitamente ou às custas de terceiros;

12.7. Os **Cyberpunks** e os **Cyberterrorists**, que desenvolvem vírus de computadores perigosos, como os "*Trojan horses"* (cavalos de Troia) e as *Logic bombs*, com a finalidade de sabotar redes de computadores, e em alguns casos propiciar a chamada DoS — Denial of Service, com a queda dos sistemas de grandes provedores, por exemplo, impossibilitando o acesso de utilizadores e causando graves prejuízos económicos.

13. AS DIFICULDADES COLOCADAS PELA PROVA DIGITAL

A par da sua decorrente utilidade, a *Prova digital* é acompanhada de inúmeras dificuldades na sua utilização. Devo iniciar este tema abordando em primeiro lugar as dificuldades colocadas pela *Prova Digital* no que diz respeito à sua busca, apreensão, análise, e mesmo tratamento desta.

Onde, como e quando?

A busca da Prova digital, não incide desde logo, na identificação do local onde é cometido o crime, pois atendendo que esta criminalidade pode ser operada, sendo bastante um computador ligado à internet, o mesmo que pode acontecer em qualquer parte do mundo, e mesmo em locais públicos como *cibercafés*, ou pontos de acesso a redes públicas. Pode ainda tornar-se mais complicada a identificação do local, quando verificamos que, se é apenas necessário um computador com acesso à internet, também é certo, que muitos telemóveis são actualmente capazes de o fazer, o que torna o infractor imprevisível no que diz respeito à volatilidade da movimentação, assim como no momento em que o faz.

Ou seja, A *Prova digital* pode estar armazenada em dispositivos de armazenamento, desde o computador, ao telemóvel, discos, etc. É certo que na grande maioria dos casos, esta prova raramente se encontra exactamente no local do crime, mas antes em posse de terceiros. Em várias situações em que se torna imprescindível a *Prova Digital*, não existe

sequer contacto entre o infractor, e o objecto do crime. Este é cometido a uma distância difícil de determinar.

Outra das problemáticas relacionadas com as buscas ou apreensão da *Prova digital*, recai na facilidade de ser apagado qualquer tipo de indício probatório, que foi em determinado local, ou de determinado dispositivo. Muitas vezes limpando o histórico de navegação, ou carregando somente numa tecla, consegue-se destruir uma prova digital, que porventura seria a única capaz de relacionar o crime à acção do agente que o cometeu.

Para agravar esta dificuldade de estabelecer a acção a determinado sujeito e local, ainda existe a complicação de determinar o momento. Isto porque, em toda e qualquer acção, é passível, independentemente do dispositivo, de se alterar as horas, embaraçando deste modo as investigações [(23)]

No que concerne à problemática levantada pela *Prova digital*, é de essencial importância abordar as competências técnicas distintas, e necessárias à boa operação da prova. Se por um lado, para um informático a apreensão e tratamento de dados de uma prova digital é idêntica a qualquer outro conjunto de bytes, para um jurista, as dificuldades são inúmeras, começando desde logo pela necessidade de tratamento diferenciado das restantes provas, ou ainda, as questões que se levantam no sentido da competência jurisdicional. As questões de competência jurisdicional são pertinentes, especialmente no que diz respeito ao *Cloud computing* [(24)].

[(23)] ARAS, Vladimir, disponível no Artigo, '*A propósito da prova Digital*', LOPES Militão, Renato, p. 14.

[(24)] **Cloud computing**, (disponível em *http://pt.wikipedia.org/*) este conceito em Português, computação em nuvem) alude à utilização da memória e capacidade de armazenamento *online*, de computadores e especialmente servidores compartilhados e interligados por meio da *Internet*. O armazenamento de dados é feito em serviços que podem ser acedidos a partir de qualquer lugar do mundo, a qualquer hora, não havendo necessidade de instalação de *software* ou de armazenar dados. O acesso a programas, serviços e arquivos é remoto, através da *Internet* - daí a alusão à nuvem. O uso desse modelo (ambiente) é mais viável do que o uso de unidades físicas. Num sistema operacional disponível na Internet, a partir de qualquer computador e em qualquer lugar, podemos ter acesso a informações, arquivos e programas num sistema único, independente de plataforma. O requisito mínimo é um computador compatível com os recursos disponíveis na *Internet*. O computador torna-se apenas um chip ligado à Internet — a "*grande nuvem*" de computadores.

Com este conceito, todo e qualquer dispositivo, independentemente do local onde se encontra, pode aceder a uma rede, pública ou privada, e desde aí, operar na mais vasta panóplia de acções, como consulta, acesso a dados, copia destes, alteração, em suma, tem acesso a pacotes de dados de terceiros, podendo tantas vezes, usar estes como próprios, e/ou beneficiando-se ou prejudicando outrem, com esse acesso privilegiado.

Surgirá sempre a questão da competência jurisdicional, colocando a dúvida se, esta é legítima do local onde o ou os dispositivos acederam à rede, ou por sua vez, o local onde está hospedada a rede que se acedeu.

14. A SUA FRAGILIDADE E FIABILIDADE

Existem várias situações onde é incontroverso dizer-se que a *Prova Digital* é, ainda, uma prova frágil, onde a fiabilidade é pertinentemente colocada em causa.

Especialmente no que diz respeito à identificação do agente que acede à rede e pode porventura provocar o crime, torna-se difícil, senão muitas vezes impossível determinar a pessoa que utilizou da tecnologia de informação, (Computador, Telemóvel, Ipad, etc.) pois na realidade, esta identidade não pode ser confirmada visualmente. Todo e qualquer número, ou código identificador do agente, em qualquer rede pública, tem a sua valoração mitigada em razão de ser possível a alteração desses dados. A confirmação plena de que foi o cidadão x a realizar determinado acto, na determinada hora, no determinado dispositivo eletrónico, é no mínimo complicada.

Normalmente, a identificação do dispositivo é possível, tendo em conta o IP [Internet Protocol] [(25)]. Com este IP, não se obtém uma identificação do utilizador do computador, mas somente um reconhecimento e informação do computador, e da localização do mesmo.

[(25)] **Internet protocol**, (disponível em *http://pt.wikipedia.org/*), é uma identificação de um dispositivo (computador, impressora, etc.) numa rede local ou pública. Cada computador na internet possui um IP (Internet Protocol) único, sendo este o meio em que as máquinas usam para comunicarem entre si na Internet.

Por sua vez, a única forma em que através da internet se pode identificar um agente, é quando este utiliza uma assinatura electrónica. A assinatura electrónica controla a veracidade do documento, ou da qualquer mensagem enviado por este. Presume-se deste modo, quem é o autor de uma determinada mensagem. Esta não deixa de ser uma ideia de presunção, e nunca passa para uma certeza. Torna-se complicada essa certeza, na medida em que a utilização de uma assinatura digital, assim como um *login* [(26)], é uma credenciação privilegiada, e uma área reservada, necessitando de uma palavra-chave para aceder à credenciação ou área pessoal. Não se pode confirmar se é somente uma pessoa a ter acesso a essa palavra-chave, ou à credenciação. Esta é sem dúvida uma fragilidade da *Prova Digital*, na medida em que no direito penal as suposições e hipóteses, não são bastantes para responsabilizar um arguido. Para não falar na possibilidade da assinatura digital ou credenciação, ser utilizada no equipamento relativo à qual faz parte, porém por pessoa diferente do proprietário deste.

Com este panorama, muitos são os autores, como Breno Lessa [(27)], que revelam com convicção, ser impossível confirmar com absoluta certeza a autoria de uma mensagem electrónica, ou alteração de dados de uma rede pública ou particular.

15. REGIME JURÍDICO DA PROVA DIGITAL E DIPLOMAS RELEVANTES

A *Prova digital*, no que diz respeito ao regime jurídico no território português, é entendida nos art(s).º 189.º e 190.º do CPP. Por sua vez, não encontramos nestes art(s). um regime legal especifico relativo à *Prova Digital*, mas antes uma remissão para os art(s). 187.º e 188.º do mesmo diploma. Acontece que a lei penal portuguesa, atribuí, em sede de *meios de prova*, a qualquer conversação ou comunicação transmitida por meio electrónico diferenciado dos já consagrados na lei (ex. telefone), a mesma admissibilidade, requisitos e pressupostos das intercepções das escutas telefónicas.

---

(26) **Login** (disponível em http://pt.wikipedia.org/) Em termos informáticos, login, sendo por vezes também utilizada a alternativa *log on* e de forma menos comum: *sign in*) define o processo através do qual o acesso a um sistema informático é controlado através da identificação e autenticação do utilizador através de credenciais fornecidas por esse mesmo utilizador. Essas credenciais são normalmente constituídas por um nome de utilizador ou apenas utilizador (do inglês username) e uma palavra-passe ou senha (do inglês password) - ocasionalmente, dependendo de sistemas menos complexos, apenas pedida a senha.

(27) LESSA, Breno Lessa, "*A invalidade das provas digitais no processo judiciário*", 2009, disponível na Internet, in http://jus.uol.com.br/revista

O art.º 189º do CPP,

1 – *"O disposto nos artigos 187.º e 188.º é correspondentemente aplicável às conversações ou comunicações transmitidas por qualquer meio técnico diferente do telefone, designadamente correio electrónico ou outras formas de transmissão de dados por via telemática, mesmo que se encontrem guardadas em suporte digital, e à intercepção das comunicações entre presentes."*

2 – *"A obtenção e junção aos autos de dados sobre a localização celular ou de registos da realização de conversações ou comunicações só podem ser ordenadas ou autorizadas, em qualquer fase do processo, por despacho do juiz, quanto a crimes previstos no n.º 1 do artigo 187.º e em relação às pessoas referidas no n.º 4 do mesmo artigo".* [(28)]

Para além da harmonização destes regimes ser susceptível de ocasionar dificuldades a nível da tutela do segredo profissional, [(29)] significa isto que, e para o tema em apreço, relativamente à Prova Digital, esta utiliza o regime jurídico das escutas telefónicas, o que a meu ver, pode levantar especiais problemas no que diz respeito à sua admissibilidade. Os problemas levantados na necessidade de uma intercepção de uma Prova Digital, são muitas vezes, diferenciados das exigências das escutas telefónicas, não podendo ter como regime de admissibilidade, os pressupostos que encontramos nas escutas telefónicas, como será melhor aprofundado adiante, em título competente.

No que à Prova Digital diz respeito, e no enquadramento legal português, é igualmente importante comentar, desde logo, sobre a vigente lei da criminalidade informática, ou 'lei do cibercrime'. [(30)] Com este normativo, transpõe-se para a ordem jurídica interna a **Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro**, relativa a ataques contra sistemas de informação, e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa, [mais adiante abordado]. É da maior importância esta lei, pois muito embora seja referente à Lei da criminalidade informática, aporta também ela, no art.º 1.º, refere especificamente a recolha da prova em suporte eletrónico.

---

(28) Código de processo penal, e legislação complementar, 6.ª edição, revista e actualizada / 2012, Almedina, art.º 189.º

(29) Cf. Ac. TRC, n.º 135/09.4JAAVR-A.C1 de 9-12-2009, Jorge Jacob

(30) Lei n.º 109/2009, de 15 de Setembro, consultada no sítio da Procuradoria-Geral da República.

"(…) *A presente lei estabelece as disposições penais materiais e processuais, bem como as disposições relativas à cooperação internacional em matéria penal, relativas ao domínio do cibercrime e da recolha de prova em suporte electrónico*".

Este normativo que transpõe a decisão do JAI, ao mesmo tempo, adapta o direito interno às decisões alcançadas no Conselho da Europa, estabelecendo vários conceitos necessários à criminalidade informática, tipificando os seus crimes.

Contudo, no seu art.º 12.º da **Lei n.º 109/2009, de 15 de Setembro**, debruça-se especialmente na matéria da preservação da *Prova Digital*, definindo que se desse modo se tornar necessário, compete à autoridade judiciária ordenar que os dados em apreço possam ser guardados, armazenados de forma a garantir uma posterior consulta ou análise. *"Se no decurso do processo for necessário à produção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos armazenados num sistema informático, incluindo dados de tráfego, em relação aos quais haja receio de que possam perder-se, alterar-se ou deixar de estar disponíveis, a autoridade judiciária competente ordena a quem tenha disponibilidade ou controlo desses dados, designadamente a fornecedor de serviço, que preserve os dados em causa".*

A competência da autoridade judiciária para ordenar a preservação dos danos, contudo, são também competentes os 'OPC's', quando perante um caso de perigo, demorado, tratando de informar a autoridade judiciária logo que possível, transmitindo-lhe o relatório previsto no art.º 253.º do CPP.

São definitivamente musculadas, as formalidades das medidas exigidas para que seja possível a preservação da Prova Digital. A **Lei n.º 109/2009, de 15 de Setembro**, atenta também, ainda sede de preservação dos dados, a sua ordem, o intransigente sigilo, e os prazos, ao que, não sendo estes requisitos cumpridos, considerar-se-ão nulas todas elas. (art.º 12º al. 3º da **Lei n.º 109/2009, de 15 de Setembro**). Significa isto que, mesmo sendo os *OPC's* a proceder à sua preservação, são estes obrigados a respeitar a ordem de armazenamento, sigilo, e prazos, para que possam ser obtidos e posteriormente utilizados pelas autoridades judiciárias, no estrito cumprimento da lei.

É ainda importante salientar que a Lei nº 109/2009 confere um *regime processual penal geral* no que diz respeito à obtenção de *prova digital*, potencialmente dirigido a *todos* os tipos de crime. Com esta realidade, tal como supra mencionei, impunha-se a inclusão das suas regras no C.P.P., especificamente no Título III, sob epígrafe «*Meios de obtenção de prova*» do Livro II «Da prova».

O **Decreto-lei 32/2008 de 17 de Junho**, no seu art. 4º, plasma que a conservação e preservação dos dados, deve existir durante um ano.

A competência das autoridades judiciárias, dos OPC's quanto à preservação dos dados informáticos, estende-se de igual modo quanto à pesquisa destes, e mesmo à sua apreensão.

Explica-nos o mesmo diploma que as entidades competentes tem o dever de cooperação com a entidades competentes estrangeiras quando do mesmo modo, se tratar de crimes em que envolva a pesquisa, análise, apreensão, preservação de dados informáticos e especialmente recolha de prova. Todas estas manobras de investigação, seja de investigação no âmbito interno, ou de cooperação com entidades estrangeiras, devem, e estão ao abrigo da lei, respeitando por sua vez o acordo com as normas sobre transferência de dados pessoais. [(31)] Normas essas, que debruçam especial atenção, ao tratamento de dados pessoais, salvaguardado que este processo se deve realizar de forma transparente e no estrito respeito pela reserva da vida privada.

Por exemplo, a **Comissão Nacional de Protecção de Dados**, estabelece no seu art.º 7.º que existem certo tipo de dados que são considerados *"sensíveis"*.

São deste modo sensíveis, todos os dados que incidem de alguma forma em direitos fundamentais, como as *"convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem racial ou étnica"*, no fundo, direitos esses inalienáveis e constitucionalmente protegidos, como se pode verificar no art.º 13.º da CRP [(32)]. Nesses casos, são necessárias condições especiais para que seja então permitido o tratamento desses dados.

---

(31) Lei n.º 67/98, de 26 de Outubro, pesquisada e analisada no sítio oficial da Comissão Nacional da Protecção de dados. *'http://www.cnpd.pt/'*.

(32) Art.º 13.º da Constituição da República Portuguesa – 'Principio da igualdade'.- *Ser necessário para proteger interesses vitais do titular dos dados ou de uma outra pessoa e o titular dos dados estiver física ou legalmente incapaz de dar o seu consentimento; - Ser efectuado, com o consentimento do titular, por fundação, associação ou organismo sem fins lucrativos de carácter político, filosófico, religioso ou sindical, no âmbito das suas actividades legítimas, sob condição de o tratamento respeitar apenas aos membros desse organismo ou às pessoas que com ele mantenham contactos periódicos ligados às suas finalidades, e de os dados não serem comunicados a terceiros sem consentimento dos seus titulares; - Dizer respeito a dados manifestamente tornados públicos pelo seu titular, desde que se possa legitimamente deduzir das suas declarações o consentimento para o tratamento dos mesmos; - Ser necessário à declaração, exercício ou defesa de um direito em processo judicial e for efectuado exclusivamente com essa finalidade.*

Para além da '*lei do Cibercrime*', é também vital abordar a '**Directiva do Parlamento Europeu e do Conselho, de 12 de Julho de 2002**' [(33)], relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas. Esta Directiva, foi concebida com o objectivo claro de, em primeira instância, vigorar um regime de garantias no que diz respeito à privacidade [art.º 5º. – Confidencialidade nas comunicações] e o livre tráfego de dados pessoais, onde também, *"visa assegurar o respeito dos direitos fundamentais e a observância dos princípios reconhecidos, em especial, pela Carta dos Direitos Fundamentais da União Europeia".*

Foi do mesmo modo criada a presente directiva, com vários intuitos mais específicos, como o de *"proporcionar um nível idêntico de protecção dos dados pessoais e da privacidade aos utilizadores de serviços de comunicações publicamente disponíveis, independentemente das tecnologias utilizadas, a nível Europeu"* [(34)] para que todos os estados-membros, dispusessem de um regime em condições de paridade. Instaurar um princípio de cooperação entra as instâncias comunitárias competentes, possibilitando os Estados-Membros de interceptarem legalmente comunicações electrónicas ou tomarem outras medidas, se necessário, para quaisquer desses objectivos e em conformidade com a Convenção Europeia para a Protecção dos Direitos Humanos e das Liberdades Fundamentais, segundo a interpretação da mesma na jurisprudência do Tribunal Europeu dos Direitos do Homem. Procurou-se então, com esta Directiva, um regime musculado no sentido de blindar o acesso a informação privilegiada ou não autorizada, a fim de proteger a confidencialidade do seu conteúdo e de quaisquer dados com elas relacionados, procurando-se ir ao encontro com a já existente legislação nacional de alguns Estados-Membros, que apenas proibia o acesso intencional não autorizado às comunicações. Estabeleceu de igual modo, um regime de proibição de armazenamento das comunicações e dos dados de tráfego armazenados por terceiros, que não os utilizadores, ou sem o seu consentimento.

---

(33) 2002/58/CE, consultada no '*Official website of the European Union', www.europa.eu*.

(34) Art.º 1.º da Directiva do Parlamento Europeu e do Conselho, de 12 de Julho de 2002 – "*A presente directiva harmoniza as disposições dos Estados-Membros necessárias para garantir um nível equivalente de protecção dos direitos e liberdades fundamentais, nomeadamente o direito à privacidade, no que respeita ao tratamento de dados pessoais no sector das comunicações electrónicas, e para garantir a livre circulação desses dados e de equipamentos e serviços de comunicações electrónicas na Comunidade".*

16. A CONVENÇÃO DO CIBERCRIME DO CONSELHO DA EUROPA

A convenção do Cibercrime, ou também intitulada de '**Convenção de Budapeste**', é um acordo assinado entre vários Estados-membros pertencentes à união europeia, e não só, que surgiu com o intuito de controlar, e regular, os vários crimes cometidos através de dados electrónicos.

A convenção foi adoptada pelo Comité de Ministros do Conselho da Europa na Sessão n.º 109 de 08 de Novembro de 2001. Só posteriormente, em 23 de Novembro do mesmo ano, Foi aberta à assinatura em Budapeste, tendo entrado em vigor, em 01 de julho de 2004.

Esta convenção teve por objectivo principal, a harmonização entre os vários países signatários, dos elementos relativos às infracções, do direito penal, respeitantes a crimes realizados através de meios electrónicos, ou seja, a *Cibercriminalidade*. Por outro lado, consagra a implementação de um sistema de cooperação internacional, para que as infracções cometidas por meio de sistema informático, tenha o acompanhamento, auxílio, e apoio dos demais Estados-Membros.

Pode ler-se na minuta do relatório explicativo da convenção de Budapeste, que a mesma surgiu com o sentido de fazer acompanhar o processo penal, a esta nova criminalidade informática, visto que as novas tecnologias começaram a demonstrar-se um novo desafio, face aos conceitos jurídicos existentes.

17. INEXISTÊNCIA DE UM REGIME JURÍDICO SOBRE A PROVA DIGITAL

Quando se fala na inexistência de um regime jurídico relativo à Prova Digital, é no sentido especificado. Ou seja, quando o julgador necessita de meio probatório colhido em ambiente digital, para a descoberta ou aclaramento da verdade material, este aplica as normas constantes no C.P.P, onde tipifica inúmeras formas de obtenção de prova como por exemplo nas estações de correios e de telecomunicações, nas cartas, encomendas, valores, telegramas ou qualquer outra correspondência, porém, não especificamente referindo-se à Prova Digital.

Uma dessas crassas situações, apresenta-se no art. 179º do C.P.P, em sede de apreensões, onde "*o juiz pode autorizar ou ordenar, por despacho, a apreensão, mesmo nas estações de correios e de telecomunicações, de cartas, encomendas, valores, telegramas ou qualquer outra correspondência*", onde não se compreende o porquê, desta mesma disposição não se aplicar igualmente à correspondência electrónica. Fica no vazio jurídico, susceptível de uma interpretação extensa ou não, a terminologia "qualquer outra correspondência".

Já em sede de obtenção do meio de prova, como infra mencionado no presente trabalho, não encontramos nos art.(s) um regime legal especifico relativo à *Prova Digital*, mas antes uma remissão para os art(s). 187.º e 188.º do mesmo diploma, aplicando-se então os requisitos necessários às 'escutas telefónicas'.

18. VANTAGEM DO REGIME JURÍDICO REFERENTE À PROVA DIGITAL

Sendo inúmeras as vantagens da inserção de um regime jurídico específico, relativo à Prova Digital, é até na própria Convenção do Cibercrime, que nos artigos 14º a 25º da mesma, que se preveem cinco medidas essenciais que os Estados subscritores adoptem, com vista a agilizar a investigação e punição da criminalidade informática a nível internacional.

Nestes artigos iniciais, mais especificamente no art. 15.º do primeiro título da convenção, explica que cada estado membro que a subscreveu, deve adoptar medidas do foro legislativo, *e outras que sejam então necessárias*, de forma a determinar os procedimentos mais eficazes nas investigações criminais.

É ainda notório no normativo da convenção, o sentido de tornar esses mesmos poderes e implementações, sempre sujeitos às circunstâncias e garantias previstas nos dispostos da legislação interna de cada estado. Para o efeito, faria então todo o sentido na legislação nacional um regime específico, de forma a agilizar, facilitando, e indo de encontro às necessidades que a cibercriminalidade vem obrigando, assim como, a própria convenção do Cibercrime, assim previu.

De certa forma, requereu-se que a convenção fosse criar uma cooperação, uniformizando os vários estados membros no sentido de contribuir para uma diminuição de um tipo de criminalidade que cada vez mais se alastra pelo mundo. Desse modo, essa convenção veio traçar normativos fundamentais, com a finalidade de se relacionarem, facilitando e oferecendo uma maior clareza e eficácia, à legislação interna de cada estado membro.

É claro, e a meu ver, que não pode um estado membro aproveitar no seu todo dessa convenção, não existindo em si [internamente], uma legislação própria, de forma a coadunar-se com a internacional, para assim, atingir-se os objectivos da convenção, que seriam, a uniformização, e auxílio no controlo, e regulamentação, dos vários crimes cometidos através de dados electrónicos.

É também clara, a necessidade de inserção de um regime específico da Prova Digital, no sentido do que infra mencionado foi, no presente título 12º, que a Prova Digital, utiliza, ao abrigo do art. 189º 1) do C.P.P, o regime correspondente ao das escutas telefónicas, plasmado no art. 187º do mesmo diploma. Ora, os problemas levantados na necessidade de uma intercepção de uma Prova Digital, - chamados de 'Dados de conteúdo', são muitas vezes, diferenciados das exigências das escutas telefónicas, não podendo ter como regime de admissibilidade, os pressupostos que encontramos nas escutas telefónicas.

O Art. 187.º aborda relativamente à Admissibilidade das Escutas telefónicas.

1 – "A intercepção e a gravação de conversações ou comunicações telefónicas só podem ser autorizadas durante o inquérito, se houver razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma,

impossível ou muito difícil de obter, por despacho fundamentado do juiz de instrução e mediante requerimento do Ministério Público, quanto a crimes:

a) Puníveis com pena de prisão superior, no seu máximo, a 3 anos;

b) Relativos ao tráfico de estupefacientes;

c) De detenção de arma proibida e de tráfico de armas;

d) De contrabando;

e) De injúria, de ameaça, de coacção, de devassa da vida privada e perturbação da paz e do sossego, quando cometidos através de telefone;

f) De ameaça com prática de crime ou de abuso e simulação de sinais de perigo; ou

g) De evasão, quando o arguido haja sido condenado por algum dos crimes previstos nas alíneas anteriores.

2 - A autorização a que alude o número anterior pode ser solicitada ao juiz dos lugares onde eventualmente se puder efectivar a conversação ou comunicação telefónica ou da sede da entidade competente para a investigação criminal, tratando-se dos seguintes crimes:

a) Terrorismo, criminalidade violenta ou altamente organizada;

b) Sequestro, rapto e tomada de reféns;

c) Contra a identidade cultural e integridade pessoal, previstos no título iii do livro ii do Código Penal e previstos na Lei Penal Relativa às Violações do Direito Internacional Humanitário;

d) Contra a segurança do Estado previstos no capítulo i do título v do livro ii do Código Penal;

e) Falsificação de moeda ou títulos equiparados a moeda prevista nos artigos 262.º, 264.º, na parte em que remete para o artigo 262.º, e 267.º, na parte em que remete para os artigos 262.º e 264.º, do Código Penal;

f) Abrangidos por convenção sobre segurança da navegação aérea ou marítima".

3 – "Nos casos previstos no número anterior, a autorização é levada, no prazo máximo de setenta e duas horas, ao conhecimento do juiz do processo, a quem cabe praticar os actos jurisdicionais subsequentes".

4 – "A intercepção e a gravação previstas nos números anteriores só podem ser autorizadas, independentemente da titularidade do meio de comunicação utilizado, contra:

a) Suspeito ou arguido;

b) Pessoa que sirva de intermediário, relativamente à qual haja fundadas razões para crer que recebe ou transmite mensagens destinadas ou provenientes de suspeito ou arguido; ou

c) Vítima de crime, mediante o respectivo consentimento, efectivo ou presumido.

5 - É proibida a intercepção e a gravação de conversações ou comunicações entre o arguido e o seu defensor, salvo se o juiz tiver fundadas razões para crer que elas constituem objecto ou elemento de crime.

6 - A intercepção e a gravação de conversações ou comunicações são autorizadas pelo prazo máximo de três meses, renovável por períodos sujeitos ao mesmo limite, desde que se verifiquem os respectivos requisitos de admissibilidade.

7 - Sem prejuízo do disposto no artigo 248.º, a gravação de conversações ou comunicações só pode ser utilizada em outro processo, em curso ou a instaurar, se tiver resultado de intercepção de meio de comunicação utilizado por pessoa referida no n.º 4 e na medida em que for indispensável à prova de crime previsto no n.º 1.

8 - Nos casos previstos no número anterior, os suportes técnicos das conversações ou comunicações e os despachos que fundamentaram as respectivas intercepções são juntos, mediante despacho do juiz, ao processo em que devam ser usados como meio de prova, sendo extraídas, se necessário, cópias para o efeito".

A título exemplificativo, imagine-se um panorama criminoso em que, o arguido é indiciado pelo crime onde ameaçou outrem, atentando à sua vida / coagiu / perturbou a paz ou sossego, e deste modo cometeu o crime através da internet, para o exemplo numa rede social.

Segue a acusação, e em fase de produção de prova requer a parte, ou oficiosamente, a junção aos autos das ameaças / coacção / perturbação da paz e sossego. Estamos deste modo, em âmbito que se enquadra na *Prova Digital*, e para tal, vejamos então o que a legislação em vigor nos consagra.

Por força do art. 189º 1) do C.P.P, somos remetidos para o art. 187º relativo à admissibilidade das escutas telefónicas, pois afinal, aplica-se o regime correspondente a estas sempre que se trate de "*conversações ou comunicações transmitidas por qualquer meio técnico diferente do telefone, designadamente correio electrónico ou outras formas de transmissão de dados por via telemática, mesmo que se encontrem guardadas em suporte digital".*

Chegando então ao art. 187º [*Admissibilidade das escutas telefónicas*], diz-nos então a alínea a) do ponto 1, que;

"A intercepção e a gravação de conversações ou comunicações telefónicas só podem ser autorizadas durante o inquérito, se houver razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter, por despacho fundamentado do juiz de instrução e mediante requerimento do Ministério Público, quanto a crimes:

Puníveis com pena de prisão superior no seu máximo, a 3 anos".

Neste sentido, deparamo-nos de imediato com o problema da moldura penal. Os Crimes de ameaça, coacção e devassa da vida privada, nenhum deles ultrapassa os 3 anos de prisão no seu limite máximo, pelo que, em primeira instância, não seria então possível ao tribunal/parte a intercepção da conversa, que seria prova fundamental, impossível de se obter de outro modo.

É então mister salientar a importância da alínea e) do mesmo art. [187º]. É colocada uma exepção à moldura penal de máximo 3 anos, em certo tipo de crimes. São eles, Injúria, Ameaça, Coacção, devassa da vida privada, e perturbação da paz e sossego. Porém, é uma exepção mitigada, quando na mesma alínea se compreende que é novamente impossibilitado o julgador de requerer a intercepção da conversação, sempre que esta [e para os crimes em apreço – art. 187.º 1/e] não for cometido através do telefone.

*"De injúria, de ameaça, de coacção, de devassa da vida privada e perturbação da paz e sossego, **quando cometidos através de telefone"**.*

Não sendo o crime balizado em nenhuma das alíneas do ponto 2 do mesmo art. [Terrorismo, criminalidade violenta Etc.], estaríamos então numa situação de fragilidade para o julgador, dificultando em muito, a produção de prova em audiência.

Nesta observação, acrescenta-se desde já, que deveria ser copulado ao regime relativo aos *meios de obtenção de prova*, a especificação do *meio de obtenção da Prova Digital*.

Responsavelmente, certo é que sem o cuidado devido este tipo de regime poderia entrar em colisão com demais normativos, inclusive com a nossa lei fundamental, pelo que, sem prejuízo, deveria o mesmo ser elaborado com algumas adaptações, especificando o tipo de prova, e certas particularidades.

A recolha de *dados ou circunstâncias da comunicação,* também referenciados como *dados de tráfego,* deveriam ser munidas de um regime próprio, à vista da importância e constante crescimento que esta criminalidade moderna tem vindo a instalar-se.

Só com a inserção desse regime específico, ficará harmonizado o meio de obtenção da *Prova Digital*, com os demais regimes concernentes aos meios de obtenção de provas.

Segundo Mesquita (2010), os meios de obtenção da *Prova Digital*, sem prejuízo com os ajustes prementes, conduzem-nos aos tradicionais meios de obtenção da prova. Trata-se, portanto de exames, revistas, buscas, apreensões e intercepções de comunicações. (35)

19. PROVA DIGITAL COMO PROVA OU COMO MEIO DE PROVA?

A questão colocada neste título é se a *Prova Digital*, poderá ser uma forma do tribunal apurar a veracidade dos factos alegados pelas partes, poderá compará-los, e mesmo relacioná-los com as provas apresentadas pela parte contrária, ou se, por sua vez, a *Prova Digital*, é especialmente útil no que diz respeito à delimitação e regulamentação dos instrumentos necessários à investigação.

Esta questão não pode ser colocada sob forma de falso dilema, quando a resposta que me apraz apresentar é no sentido de salientar a importância da *Prova Digital,* tanto como prova capaz de apurar a veracidade de factos, como, e especialmente, no caminho da investigação de um crime, ou indício.

(35) MESQUITA, Paulo Dá, "*Processo Penal Prova e Sistema Judiciário*", Coimbra, Coimbra Editora, 2010.

É válida e necessária a *Prova Digital*, em momento que se torne imperativo consubstanciar ou apurar a veracidade de uma alegação de parte em audiência, não existindo outro meio, serve então esta, para comprovar declarações, acções e porventura decifrar intenções que se denotam fundamentais para a convicção do julgador no que diz respeito ao dolo.

Na justa medida, não será a *Prova Digital*, um meio de prova que dê resposta a todas as dúvidas colocadas em audiência, no entanto, demonstrar-se-á inúmeras vezes, que para certo tipo de criminalidade, ser o único meio de prova susceptível de criar convicção de veracidade no julgador.

Do mesmo modo, em sede de investigação, como meio de obtenção de prova, não vem substituir de forma alguma, nenhum meio de obtenção de prova já existentes no CPP, porém, em certo tipo de investigação [não somente as relacionadas directamente com o cibercrime], pode vir a ser uma ferramenta fundamental, tendo por característica a sua especial celeridade, imediata, contrapondo-se à investigação de um crime dito de 'tradicional'. Consegue deste modo, a entidade competente, na sua investigação, inspecionar os vestígios electrónicos deixados pelo crime em fase de preparação, no momento da execução, e mesmo daqueles já consumados.

20. A SUA IMPORTÂNCIA NO COMBATE À CRIMINALIDADE INFORMÁTICA

A importância no que concerne ao combate da criminalidade informática, é absoluta, e especialmente sustentada, quando ultimamente se tem produzido, uma transferência criminosa para a Internet, resultando em que cada vez mais utilizadores observam a internet como meio para as suas práticas criminosas, ou mesmo a arriscar-se na consumação de crimes, o que por outros meios não praticariam, ou pelo menos com a mesma certeza de que se torna complicada a identificação do agente, e do local. Mas neste título, abordamos especialmente a criminalidade informática.

Torna-se então necessário passar pelos crimes mais frequentes, para posteriormente gerar-se uma consciência relevante do quando é imprescindível, necessária, a Prova Digital, na resolução deste tipo de criminalidade.

No que respeita aos crimes informáticos, a **devassa da vida privada** (art. 193º CP) através da internet. Na nossa lei fundamental, plasma o art. 35º n.º 3 que a protecção da reserva da vida privada, contra possíveis actos de discriminação provenientes de meios informáticos.

Violação de correspondência ou de telecomunicações, onde este crime é directamente ligado à forma como actualmente empresas comunicam entre si, ou seja, por correio electrónico, vulgo 'Email'. Desta forma, permite-se correspondência entre emissor e destinatário, de forma fechada, onde só os dois ou mais intervenientes, podem controlar quem tem acesso ao conteúdo do que é transmitido.

Quando aqui se aborda uma violação de correspondência ou de telecomunicações, caímos não só em sede de violação de privacidade, mas também num contexto de dano na confiança da sociedade em geral.

Relativamente à tipificação legal destes crimes, é importante estabelecer a sua base legal. Segundo Pedro Venâncio, e assente na Lei 109/91, que veio a ser revogada pela Lei 109/2009 de 15 de Setembro, tratar-se-á de um crime de interceptação ilegítima, sempre que a mensagem seja difundida pelo emissor, e esta seja interceptada antes de chegar ao destinatário.

O C.P. Português, no seu art. 194º sob a epígrafe «Violação de correspondência ou de telecomunicações», consagra que, "*Quem, sem consentimento, abrir encomenda, carta ou qualquer outro escrito que se encontre fechado e lhe não seja dirigido, ou tomar conhecimento, por processos técnicos, do seu conteúdo, ou impedir, por qualquer modo, que seja recebido pelo destinatário, é punido com pena de prisão até 1 ano ou com pena de multa até 240 dias".*

2 – *"Na mesma pena incorre quem, sem consentimento, se intrometer no conteúdo de telecomunicação ou dele tomar conhecimento."*

3 – *"Quem, sem consentimento, divulgar o conteúdo de cartas, encomendas, escritos fechados, ou telecomunicações a que se referem os números anteriores, é punido com pena de prisão até 1 ano ou com pena de multa até 240 dias".*

Neste crime, **Violação de correspondência ou telecomunicações**, é necessária, e praticamente exclusiva a utilização da Prova Digital, no sentido em que o ilícito é praticado em ambiente electrónico, e quer em fase de investigação, ou de produção de prova, a prova a recolher, é também esta apreendida de algum dispositivo electrónico, seja computador, servidor, telemóvel ou equivalente. Certo é que com os demais meios de prova tradicional, não seria então possível dar resposta à necessidade de demonstrar probatoriamente a existência ou não da conduta criminosa.

Outro crime sob o qual a Prova Digital se demonstra como essencial para a investigação e produção de prova, passa pela **burla informática e nas telecomunicações.** Consagrado no art. 221 do C.P. Português, que é, de certa forma uma continuação da **burla**, do art. 217º do mesmo diploma, onde se compreende que com «*intenção de obter para si ou para terceiro enriquecimento ilegítimo e o requisito de causar a terceiro prejuízo patrimonial*», mas por sua vez direccionado para ambiente digital. Isto é, se esse enriquecimento ilícito, prejudicando terceiro, se manifestar interferindo com *"o tratamento de dados, mediante estruturação incorrecta de programa informático, utilização incorrecta de dados, utilização de dados sem autorização ou intervenção por qualquer outro modo não autorizado"*, preenche-se então o elemento tipo do crime de burla informática, e nas telecomunicações.

Sendo que, este tipo de crime prevê a utilização de dados informáticos, manipulando-os, editando os seus conteúdos e resultados, torna-se complicado a acção probatória desta conduta, sem recorrer à Prova Digital

O crime de **Falsidade Informática**, plasmado no art. 3º da Lei 109/2009 de 15 de Setembro, diz-nos que «*Quem, com intenção de provocar engano nas relações jurídicas, introduzir, modificar, apagar ou suprimir dados ou programas informáticos ou, por qualquer outra forma, interferir num tratamento informático de dados, quando esses dados ou programas sejam susceptíveis de servirem como meio de prova, de tal modo que a sua visualização produza os mesmos efeitos de um documento falsificado, ou, bem assim, os utilize para os fins descritos, será punido com pena de prisão até cinco anos ou multa de 120 a 600 dias*».

Acrescenta ainda o ponto 2) do mesmo art. que, «*Nas mesmas penas incorre quem use documento produzido a partir de dados ou programas informatizados que foram*

objecto dos actos referidos no número anterior, actuando com intenção de causar prejuízo a outrem ou de obter um benefício ilegítimo, para si ou para terceiros».

Deste modo, permanece clara a necessidade e importância da Prova Digital para evidenciar e descortinar a existência ou não deste tipo de criminalidade [(36)]

No caso da **Sabotagem informática**, que conta com base legal o art. 5.º da lei 109/2009 de 15 de Setembro, entende-se que «*quem introduzir, alterar, apagar ou suprimir dados ou programas informáticos ou, por qualquer outra forma, interferir em sistema informático, actuando com intenção de entravar ou perturbar o funcionamento de um sistema informático ou de comunicação de dados à distância, será punido com pena de prisão até 5 anos ou com pena de multa até 600 dias*», e é este também um tipo legal, sobre o qual a Prova Digital manifesta directamente a sua importância, afinal sem ela, tornar-se-ia extremamente complexa a prova que não pertença a ambiente digital.

É igualmente merecedor de referência no presente trabalho, a figura do '**Acesso ilegítimo'**, presente igualmente no art.6º da lei 109/2009 de 15 de Setembro, onde se compreende que «*Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, de qualquer modo aceder a um sistema informático, é punido com pena de prisão até 1 ano ou com pena de multa até 120 dias*».

Por outro lado, e no mesmo art., encontra-se consagrado que a mesma pena é aplicável a quem por sua vez utilize a permissão ilegal para vender, distribuir ou difundir os conteúdos alcançados.

---

(36) Relativamente a matéria descrita em sede de falsidade informática, vd ., v.g. , acórdão da Relação do Porto, de 24/04/2013, Processo n.º 585/11.6PAOVR.P1, pela relator Exma. Drª Juiza Fátima Furtado, disponível na Internet, no sítio da DGSI, em http://www.dgsi.pt/jtrp.nsf/c3fb530030ea1c61802568d9005cd5bb/872f3063233d8de480257b78003e60f3?OpenDocument

Significa então que ao preencher-se os elementos do tipo "Acesso ilegítimo', tem o agente de infringir desde logo, a segurança do sistema digital, violando o património do lesado.

Contudo, mais uma vez se torna complexa a formação probatória deste tipo de conduta ilegal, sendo que somente em registo e formado digital, se poderá verificar a existência ou não do crime. Seja porque um IP de terceiro acedeu a determinada plataforma de acesso privilegiado, ou mesmo porque a difusão do conteúdo pode ser efectuada através de armazenamento (servidor, disco, pen, etc.), e desse modo, somente a Prova Digital, poderá esclarecer com clareza, e auxiliar a justiça na busca da verdade material.

Como previamente feito no presente título, carece de aprofundar a **Intercepção ilegítima**.

A intercepção ilegítima, plasmada no art. 7º da lei 109/2009 de 15 de Setembro, tem em paridade o interesse maior de proteger o direito à privacidade na comunicação dos dados.

Sempre que exista transferência de dados electrónicos de ligação particulares, seja por telemóveis, redes sociais, correio electrónico entre outras, torna-se deste modo susceptível desta precisa informação privilegiada ser interceptada por terceiros de forma ilícita.

A protecção dos dados pessoais, têm também a sua garantia constitucional no ponto 4) do art. 35º da CRP.

«*Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua rectificação e actualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei.*

2. A lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua protecção, designadamente através de entidade administrativa independente.

3. A informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis.

4. ***É proibido o acesso a dados pessoais de terceiros, salvo em casos excepcionais previstos na lei.***

5. É proibida a atribuição de um número nacional único aos cidadãos.

6. A todos é garantido livre acesso às redes informáticas de uso público, definindo a lei o regime aplicável aos fluxos de dados transfronteiras e as formas adequadas de protecção de dados pessoais e de outros cuja salvaguarda se justifique por razões de interesse nacional.

7. Os dados pessoais constantes de ficheiros manuais gozam de protecção idêntica à prevista nos números anteriores, nos termos da lei».

21. A SUA FRACA APLICAÇÃO NUM MUNDO AINDA DESCONHECIDO.

De facto, se o cibercrime está em constante crescimento, e os dados de trafego, revelam-se uma preciosa ajuda no que respeita à investigação criminal, onde permanece a questão – *Porquê da uma fraca aplicação de uma 'ferramenta', que é, notoriamente a resposta de certas investigações, impossíveis de se alcançar de outro modo?* -

Deveria deste modo, tornar-se bastante apelativo às entidades investigadoras, contudo, este rasto que é deixado nos sistemas de informação, sendo por sua vez, susceptíveis de ser preservados e utilizados como prova, vão ao encontro de um facilitismo, até quando na verdade, e no seu conjunto, os dados discriminados pela comunicação alvo, e pelo sistema de relação de conversa, se revelam, bastantes vezes, mais consideráveis que o próprio conteúdo da comunicação em si, revelando tudo o mais que se procurou na amostra dos dados de trafego.

É por sua vez também mais fácil e cómodo, conseguir as provas através de conteúdo de dados, do que recorrendo aos meios habituais de obtenção de prova.
Esta realidade é também susceptível de gerar um crescimento na amplitude da valoração da *Prova indiciária* [37] e especialmente uma simplificação da prova dos factos alegados em sede de julgamento.

Umas das razões da sua fraca aplicabilidade, vem no sentido de várias reivindicações com o fundamento de que existe uma facilitismo e ampliação relativamente ao regime da *Prova Digital* no regime processual penal. Por outro lado, as operadoras de telecomunicações, mostram-se reservadas quanto à preservação e apresentação desta prova, no sentido de que a simplificação da cooperação internacional neste registo, têm demonstrado um elevado índice de eficácia, levando a condenações sem realmente a necessidade de demonstração dos factos imputados aos arguidos, recorrendo-se à apreensão de conteúdo de dados. Entende-se aqui o argumento de que, a investigação elaborada segundo os trâmites de cooperação internacional, são bastantes para a descoberta dos factos relevantes. Apela-se desta forma, a utilização de provas consideradas mais seguras, e que por sua vez se reflecte numa investigação criminal com riscos diminutos para os respectivos agentes competentes da investigação.

---

[37] É clássica a distinção entre *prova directa* e *prova indiciária*. A prova directa, refere-se aos factos probandos, ao tema da prova, enquanto a prova indirecta, ou indiciária, se refere a factos diversos do tema da prova, mas que permitem, com o auxílio de regras da experiência, uma ilação quanto ao tema da prova. Na prova indiciária, mais do que em qualquer outra, intervêm a inteligência e a lógica do juiz. A prova indiciária pressupõe um facto, demonstrado através de uma prova directa, ao qual se associa uma regra da ciência, uma máxima da experiência ou uma regra de sentido comum. Este facto indiciante permite a elaboração de um facto que revela uma consequência em virtude de uma ligação racional e lógica. Aliás, é importante que se refira que a prova indiciária, ou o funcionamento da lógica e das presunções, bem como das máximas da experiência, é transversal a toda a teoria da prova, começando pela averiguação do elemento subjectivo de crime, que só deste modo pode ser alcançado, até à própria creditação da prova directa constante do testemunho. *(Intervenção no Centro de Formação Jurídica e Judiciária de Macau em 30 de Novembro de 2011)*
- Sobre o conceito de prova indiciária e o alcance que lhe tem sido conferido, vd ., v.g. , *Acórdão da Relação do Porto*, de 30/01/2008, Processo n.º 0744740, disponível na Internet, no sítio da DGSI.

São então estas matérias que usualmente tendem a ser descoradas, quando se encara a problemática relativa à Prova Digital, e o porquê desta, se tão útil, ainda mostre uma tão musculada resistência na sua aplicação no campo jurídico-penal. [38]

22. OS SEUS LIMITES E AGRESSIVIDADE PARA COM OS DIREITOS LIBERDADES E GARANTIAS

É absolutamente vital frisar a *Prova digital*, relativamente à sua agressividade para com os DLG's. Quando na tentativa de utilizar a prova digital como ferramenta, ou meio essencial para apurar a verdade material, incidimos do risco imenso de ofender direitos constitucionalmente salvaguardados. Senão, observemos: O direito à palavra, o Direito à imagem, (Art. 26º da CRP) o Direito à autodeterminação informacional e da comunicação, o Direito à inviolabilidade do domicílio informático (Art. 34.º da CRP), o direito à reserva da intimidade da vida privada e familiar, e muitos outros que em resultado da utilização da prova digital, são ofendidos [39] e [40]

No art. 26º da CRP, sob a epígrafe, "***Outros Direitos Pessoais***", consagra que "*a todos são reconhecidos os direitos à identidade pessoal, ao desenvolvimento da personalidade, à capacidade civil, à cidadania, ao bom nome e reputação, à imagem, à palavra, à reserva da intimidade da vida privada e familiar e à protecção legal contra quaisquer formas de discriminação*".

Continuando assim no ponto 2) do mesmo diploma, que *"a lei estabelecerá garantias efectivas contra a obtenção e utilização abusivas, ou contrárias à dignidade humana, de informações relativas às pessoas e famílias".*

---

(38) LOPES Militão, Renato, Artigo, "*A propósito da prova Digital no processo penal"*, p. 20.

(39) RODRIGUES, BENJAMIM SILVA RODRIGUES, *Da Prova Penal, IV, Da Prova- Electrónico-Digital e da Criminalidade Informático-Digital*, Lisboa, Rei dos Livros, 2011.

(40) Relativamente a matéria descrita em sede de proibição dos meios de prova, vd ., v.g. , acórdão da Relação de Guimarães, de 29/03/2004, Processo n.º 1680/03-2, pela relator Exma. Drª Juiza Maria Augusta, disponível na Internet, no sítio da DGSI, em http://www.dgsi.pt/jtrg.nsf/86c25a698e4e7cb7802579ec004d3832/926f6fea6511bf6e80256ee0003afd32?OpenDocument

A nossa lei fundamental, conserva em si, inúmeras formas de garantir a defesa dos DLG's, consagrando essas garantias, impondo limites imperativos à validade dos meios de prova, assim como, para o título em apreço, aos meios de obtenção de prova.

Se por um lado, a lei processual penal, (CPP), no seu art. 126º, relativo à epígrafe **"*Métodos proibidos de prova*",** "*Ressalvados os casos previstos na lei, são igualmente nulas as provas obtidas mediante intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações, sem o consentimento do respectivo titular*", o que se traduz numa garantia processual.

Contudo, garantia processual essa, que não nos devemos suster na sua interpretação autónoma e superficial, aprofundando o espirito do legislador quando por sua vez, a nossa CRP, no seu art. 26º oferece o Direito à imagem e à reserva da intimidade da vida privada, conservando este primeiro (Direito à imagem), implicitamente, o direito de cada um não ser fotografado, ou que as suas fotos, não diferenciado formatos (papel, digital, ou outro), sejam então partilhadas ou alcançadas [(41)].

Encontramos ainda, no art. 18.º da nossa CRP, com a epígrafe "Força Jurídica", no ponto 2) um absoluto limite na salvaguarda dos DLG's, postulando que "*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*".

Ainda no ponto 3) do art. 18.º, consagra que, "*as leis restritivas de Direitos Liberdades e Garantias têm de revestir carácter geral e abstracto e não podem ter efeito retroactivo nem diminuir a extensão e o alcance do conteúdo essencial dos preceitos constitucionais"*.

É então deste modo, possível constatar inúmeros limites e salvaguardas constitucionalmente calculados, a qualquer processo ou ferramenta, susceptível de lesar ou violar os Direitos Fundamentais e os Direitos liberdades e garantias. [(42)]

---

(41) Art. 26.º da Constituição da República Portuguesa, «*Outros direitos pessoais*».
(42) Art. 18.º da Constituição da República Portuguesa, «*Força Jurídica*».

23. RESTRIÇÕES DOS DIREITOS FUNDAMENTAIS

Após a supramencionada abordagem relativa à agressividade da Prova Digital, para com os DLG's, assim como os seus limites, faz absoluto sentido no que diz respeito à estrutura desta dissertação, que se verse umas palavras relativamente às restrições dos Direitos Fundamentais.

Em forma de conceito, é importante frisar que um Direito Fundamental, não obstante a demais conceitos semelhantes, é uma posição jurídica positiva que salvaguarda o individuo e a sociedade, em relação ao estado. Um D.F. permite que o individuo, enquanto cidadão, detenha uma garantia em última ratio, de que certa proposta, medida ou acção, não poderá de todo ser materializável, pois afinal, coloca em causa um ou vários Direitos Fundamentais. Deste modo, só é realmente possível coabitar num estado de democracia, existindo e respeitando-se os Direitos Fundamentais.

No entanto, e não menos importante que a sua existência, não são os Direitos Fundamentais completamente absolutos, nem mesmo ilimitados. Ao invés disso, têm estes uma limitação interna. Entende-se um limite interno, quando este serve de garante para uma igualdade a todos os cidadãos, de modo a que, todos tenham o mesmo acesso e ver protegido os seus direitos, tendo como baluarte principal, o Principio da dignidade da pessoa humana [(43)].

[(43)] ***Art. 1.º da Constituição da República Portuguesa***, *"Portugal é uma República soberana, baseada na dignidade da pessoa humana e na vontade popular e empenhada na construção de uma sociedade livre, justa e solidária".*

Não seria de todo possível a vida colectiva e em sociedade, caso não fossem previstos mecanismos de limitação material dos direitos fundamentais genericamente proclamados, com o propósito originário de garantir a própria permanência da respectiva tipologia no seu conjunto [(44)].

É contudo importante de frisar, que a possível restrição de Direitos Fundamentais, não deverá nunca colocar em causa o Principio da dignidade da pessoa humana, afinal, se tal suceder, é relacionalmente colocado também em causa todos os demais direitos fundamentais. A ocorrer, estar-se-ia a demolir um dos alicerces basilares da República Portuguesa.

Torna-se neste ponto, importante distinguir as restrições dos direitos fundamentais, das delimitações, ou mesmo da harmonização.

1. Entende-se por delimitar um Direito Fundamental, quando se torna necessário salientar os contornos, estabelecendo os limites do conteúdo de cada direito, de forma a contornar, evitando interpretações extensiva que colidam com o espirito do legislador quando estabeleceu os Direitos Fundamentais, separando por sua vez, situações que são tao somente manifestas colisões de direitos.

2. Já no que à harmonização diz respeito, sucede quando dois ou mais Direitos Fundamentais colidem, e existe por sua vez, uma inversão do poder judicial, de forma a dirimir oposições entre o Direitos Fundamentais de dois ou mais agentes, ou até conflitos directos entre Direitos Fundamentais, ou interesses legalmente preservados. Quando assim se trata, normalmente a harmonização passa por retirar paritariamente de forma flexível, o que gera conflitos entre os Direitos Fundamentais, tomando como garantia, a manutenção do núcleo de cada um.

---

(44) BACELAR Gouveia, Jorge – "*Manual de Direito Constitucional"*, vol. II, Almedina

Por sua vez, para a restrição de Direitos Fundamentais, requer-se competência específica para a operar. No que aos DLG's, diz respeito, diz-nos o art. 165º 1) b) da CRP, sob a epígrafe "*Reserva relativa da competência legislativa*", que é da exclusiva competência da Assembleia da República legislar, salvo autorização do governo, em matéria de Direitos, Liberdades e Garantias. Já no que concerne aos Direitos Económicos, sociais e culturais, estamos em sede de legitimidade concorrencial da Assembleia da República e do Governo.

24. O PERIGO DA SUA UTILIZAÇÃO SEM REGRAS E SEM CONTROLO

Não obstante a que a Prova Digital, possa, como supra mencionado ser fundamental para certo tipo de crimes, sendo uma ferramenta insubstituível, é também coerente frisar que a mesma poderá demonstrar-se um perigo, quando utilizada sem regras ou controlo.

Quer pela própria natureza da prova quer pelo seu formato, no que diz respeito à sua apreensão, é muito provável que esta se proceda em ambientes privados, de utilizadores privados, aos quais a lei protege, e bem, a sua privacidade.

A título exemplificativo, o raciocínio é bastante simples, se imaginarmos que a *Prova Digital*, na sua ampla maioria, deverá ser conseguida através de sistemas informáticos, pertencentes a terceiros, que por sua vez são controlados por operadores de telecomunicações. Se reflectirmos, ao obter a prova digital a estes sistemas, certo é que, se ofende igualmente alguns dos direitos destas, violando as obrigações contractuais, legalmente consagradas, das operadoras, como é o caso do dever sigiloso, que protege então, distintos valores públicos.

Deste modo, este processo de apreensão da Prova para investigação, faz com que inúmeras pessoas tenham acesso a informação privilegiada, e que por sua vez, essa violação, é Constitucionalmente salvaguardada. Produz-se assim, um risco acrescido de inúmeras das informações, virem a ser utilizadas para fins dissemelhantes daqueles a que a apreensão assim determinara inicialmente.

25. QUEM CONTROLA, USA, E VALIDA A PROVA DIGITAL

O controlo e o uso da prova digital, assim como a sua validação, é um tema da maior importância, na medida em que é um prelúdio processual, que sem ele, a Prova Digital não será de forma alguma útil nem para a investigação, nem mesmo em tribunal para a descoberta da verdade material.

Iniciando o tema pela investigação forense necessária, a validação dos suportes digitais, é decisiva. É então fulcral, em primeira instância, que se possa garantir a capacidade da prova retirada, assim como a exacta utilização dos programas necessários e adequados a esse mesmo meio de obtenção, promovendo principalmente, a não contaminação da prova. Significa isto que, uma simples acção, poderá por sua vez, modificar uma data, um registo, ou mesmo inutilizar a prova para a sua leitura [(45)].

Contudo, não só em fase de investigação nos deveremos preocupar, em quem, e de que forma se valida e aprecia a Prova Digital.

Em sede de audiência de julgamento, especialmente em fase de produção de prova, a questão subentendida no presente título, é a quem fica a legitimidade e competência de validar a Prova Digital.

Recorrendo ao regime de proibições de prova no âmbito do processo penal, encontra-se essencialmente regulado pelo preceituado nos arts.° 125.° e 126.°, do Código Processo Penal, que são admitidas todas as provas que não forem por sua vez, proibidas por lei, e ainda consagra, todos os métodos de prova processualmente proibidos. Normativos estes, que devem ser integrados com as garantias constitucionais de defesa, consagradas no art. 32.°, da Constituição da Republica Portuguesa, como seja a nulidade da prova imposta pelo seu n.°8, assim como com as disposições específicas que controlam a obtenção do meio de prova.

[(45)] PENHA LEITÃO DA COSTA MARQUES, Pedro – "*Informática Forense: Recolha e preservação da Prova Digital"*. Porto: Universidade Católica Portuguesa: Faculdade de Engenharia, 2013 pp. 43.

Em sede de prova proibida, a mesma deve ser oficiosamente conhecida e declarada em qualquer fase do processo, surgindo como autênticas nulidades insanáveis, a par daquelas que expressamente integram o catálogo do art° 119 com epígrafe de 'Nulidades Insanáveis' do CP.P [46]

«Constituem nulidades insanáveis, que devem ser oficiosamente declaradas em qualquer fase do procedimento, além das que como tal forem cominadas em outras disposições legais:

a) A falta do número de juízes ou de jurados que devam constituir o tribunal, ou a violação das regras legais relativas ao modo de determinar a respectiva composição;

b) A falta de promoção do processo pelo Ministério Público, nos termos do artigo 48.º, bem como a sua ausência a actos relativamente aos quais a lei exigir a respectiva comparência;

c) A ausência do arguido ou do seu defensor, nos casos em que a lei exigir a respectiva comparência;

d) A falta de inquérito ou de instrução, nos casos em que a lei determinar a sua obrigatoriedade;

e) A violação das regras de competência do tribunal, sem prejuízo do disposto no n.º 2 do artigo 32.º;

f) O emprego de forma de processo especial fora dos casos previstos na lei».

Em consequência desse normativo, encontramos como primeira entidade responsável pela validade e controlo, a própria lei, quer processual Penal, como constitucional.

Contudo, não se pode esgotar este controlo e validação da Prova Digital em sede de julgamento, exclusivamente ao normativo legal, muito por força do '*Principio da Livre apreciação da prova'*, consagrado no art. 127º do C.P.P.

---

[46] Relativamente a matéria descrita em sede de proibição dos meios de prova, vd., v.g., acórdão do Tribunal da Relação do Porto, de 23/11/2011, Processo n.º 1373/08.2PSPRT.P1, pelo Relator Exmo. Sr. Dr. Juiz Mouraz Lopes, disponível na Internet, no sítio da DGSI, em http://www.dgsi.pt/jtrp.nsf/d1d5ce625d24df5380257583004ee7d7/1fce85582debcec280257967003fc659?OpenDocument.

Com esta norma [art. 127º do CPP], não podemos ignorar que também o julgador, tem um papel fundamental na validação e controlo da Prova Digital, pois ainda que o princípio da livre apreciação da prova não seja absoluto, sofrendo limitações que decorrem do grau de convicção exigido para a decisão, há-de ser sempre uma convicção pessoal – até porque nela desempenham um papel de relevo não só a actividade puramente cognitiva mas também elementos racionalmente não explicáveis, e mesmo puramente emocionais [47].

Neste sentido, o controlo e uso da Prova Digital, numa primeira instância, em fase de investigação, é assegurado pelos órgãos de polícia criminal, com vista a recolhe-las de forma legal, sem violar algum dos dispositivos legais existentes.

Por sua vez, num segundo plano, em audiência de julgamento, recaí sobre o normativo legal supramencionado, assim como no julgador que à semelhança de qualquer outro tipo de prova, tem o dever de a apreciar, utilizando para tal, a lei, e a sua convicção.

26. UMA LEI SECURITARISTA

Com toda a emergente susceptibilidade de com a utilização da Prova Digital, se violar normativos, princípios, e preceitos constitucionais, certo é que a lei n.º 109/2009, de 15 de Setembro, que transpôs para a ordem jurídica interna a supramencionada Decisão-Quadro nº 2005/222/JAI, do Conselho da E.U., e que adequou ao direito português a aludida Convenção sobre o Cibercrime, do Conselho da Europa, emergiu uma lei que visa a primordialmente a segurança, garantindo a total legalidade da sua intervenção.

---

[47] (v. g. "*A credibilidade que se concede a um certo meio de prova"*) – Prof. Figueiredo Dias. Direito Processual Penal. vol. I. ed.1974. pp. 204.

Torna-se no presente capítulo, essencial discorrer um pouco pelo diploma de principal abordagem à Prova Digital. Em linhas gerais, a Lei n.º 109/2009 de 15 de Setembro, introduziu e ampliou inúmeros conceitos jurídicos, relacionando-os com a informática, como é exemplo de 'Dados de Tráfego', 'Sistema informático', 'Dados informáticos', entre muitos outros, como se alcança do art.º 2º do mesmo diploma, sob epígrafe de 'Definições'.

«Art. 2º»
Para efeitos da presente lei, considera-se:

*a) «**Sistema informático**», qualquer dispositivo ou conjunto de dispositivos interligados ou associados, em que um ou mais de entre eles desenvolve, em execução de um programa, o tratamento automatizado de dados informáticos, bem como a rede que suporta a comunicação entre eles e o conjunto de dados informáticos armazenados, tratados, recuperados ou transmitidos por aquele ou aqueles dispositivos, tendo em vista o seu funcionamento, utilização, protecção e manutenção;*

*b) «**Dados informáticos**», 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;*

*c) **«Dados de tráfego»,** os 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;*

*d) **«Fornecedor de serviço»**, 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;*

*e) **«Intercepção»**, o acto destinado a captar informações contidas num sistema informático, através de dispositivos electromagnéticos, acústicos, mecânicos ou outros;*

*f) «**Topografia**», uma série de imagens ligadas entre si, independentemente do modo como são fixadas ou codificadas, que representam a configuração tridimensional das camadas que compõem um produto semicondutor e na qual cada imagem reproduz o desenho, ou parte dele, de uma superfície do produto semicondutor, independentemente da fase do respectivo fabrico;*

*g) «**Produto semicondutor**», a forma final ou intermédia de qualquer produto, composto por um substrato que inclua uma camada de material semicondutor e constituído por uma ou várias camadas de matérias condutoras, isolantes ou semicondutoras, segundo uma disposição conforme a uma configuração tridimensional e destinada a cumprir, exclusivamente ou não, uma função electrónica.* [(48)]

A presente lei, veio ainda vincular o "*Principio da competência universal*" , consagrou inúmeras medidas no que se relaciona com a obtenção da prova, especificamente no que concerne ao cibercrime. Por sua vez, ampliou também, os tipos de crime que se encontravam tipificados na Lei n.º 109/91 de 17 de Agosto.

Regulamentou ainda, a obrigação a várias operadoras de comunicação, preservarem, e apresentar sempre que necessário, a Prova Digital no seu art. 12º do presente normativo, sob epígrafe de "*Preservação expedita de dados*".

Ainda como ponto de referência, a Lei 109/2009 de 15 de Setembro, define várias medidas que visam a cooperação internacional, no que se relaciona com a obtenção da Prova Digital, assim como no próprio combate à criminalidade informática, como se entende no Capítulo IV – Cooperação internacional – no seu art. 20º sob epígrafe de **«Âmbito da cooperação internacional».**

(48) Art. 2º, da Lei n.º 109/2009, de 15 de Setembro, consultada no sítio da Procuradoria-Geral da República

«As autoridades nacionais competentes cooperam com as autoridades estrangeiras competentes para efeitos de investigações ou procedimentos respeitantes a crimes relacionados com sistemas ou dados informáticos, bem como para efeitos de recolha de prova, em suporte electrónico, de um crime, de acordo com as normas sobre transferência de dados pessoais previstos na Lei n.º 67/98, de 26 de Outubro».

Foi ainda criado, no art. 21º do presente diploma, o 'Ponto de contacto permanente' para cooperação internacional, onde ficou disponível o contacto 24 horas por dia, todos os dias.

«Art. 21º - Ponto de contacto permanente para cooperação internacional»

1 - *Para fins de cooperação internacional, tendo em vista a prestação de assistência imediata para os efeitos referidos no artigo anterior, a Polícia Judiciária assegura a manutenção de uma estrutura que garante um ponto de contacto disponível em permanência, vinte e quatro horas por dia, sete dias por semana.*

2 - *Este ponto de contacto pode ser contactado por outros pontos de contacto, nos termos de acordos, tratados ou convenções a que Portugal se encontre vinculado, ou em cumprimento de protocolos de cooperação internacional com organismos judiciários ou policiais.*

3 - *A assistência imediata prestada por este ponto de contacto permanente inclui:*

a) A prestação de aconselhamento técnico a outros pontos de contacto;

b) A preservação expedita de dados nos casos de urgência ou perigo na demora, em conformidade com o disposto no artigo seguinte;

c) A recolha de prova para a qual seja competente nos casos de urgência ou perigo na demora;

d) A localização de suspeitos e a prestação de informações de carácter jurídico, nos casos de urgência ou perigo na demora;

e) A transmissão imediata ao Ministério Público de pedidos relativos às medidas referidas nas alíneas b) a d), fora dos casos aí previstos, tendo em vista a sua rápida execução.

***4** - Sempre que actue ao abrigo das alíneas b) a d) do número anterior, a Polícia Judiciária dá notícia imediata do facto ao Ministério Público e remete-lhe o relatório previsto no artigo 253.º do Código de Processo Penal».*

No que diz respeito aos meios de obtenção de prova, a Lei 109/2009 de 15 de Setembro, consagra especificamente normas que vieram dotar terceiros de mecanismos necessários para a apreensão da Prova.

Com este diploma, passaram a constar medidas processuais de extrema relevância, que deslizam no sentido de salvaguardar a hipótese de se obter provas, através de sistemas informáticos. Desde logo, no art. 12º da presente lei, a - preservação expedita dos dados -. Significa assim, que caso seja necessário à produção de prova, obter dados informáticos específicos, e receando que estes se possam perder, dissipar, ou deixarem de estar disponíveis, a autoridade judiciária, solicita para que o fornecedor dos dados (operadoras) preservem os mesmos.

Ficam então obrigados, sempre com a finalidade de auxilio na descoberta da verdade material, e/ou Princípio da investigação, independentemente do número de fornecedores, a informar a polícia judiciária, ou qualquer OPC's, dos serviços que prestaram a comunicação que está a ser investigada ou obtida, como se compreende ao abrigo do art. 13º e 14º da presente lei.

Tem deste modo tem a Polícia competência, para proceder do mesmo modo, sempre que sejam necessária a pesquisa de dados informáticos (art. 15º), apreensão, e apreensão de correio electrónicos e registos de natureza semelhante, como explicita o art. 17º.

Todas as normas acima mencionadas, tendem, segundo autores como é o caso de Benjamin Silva Rodrigues, a alimentar um fim menos perseguido pelo legislador. A monotorização, apreensão, preservação e leitura, podem porventura, resultar numa forma menos proveitosa para a descoberta da verdade material, oferecendo uma via à intromissão desrespeitosa da vida privada de cada utilizador de telecomunicações, e/ou equipamento digital [(49)].

[(49)] RODRIGUES, Benjamim Silva Rodrigues, Da Prova Penal, IV, "*Da Prova-Electrónico-Digital e da Criminalidade Informático-Digital"*, Lisboa, Rei dos Livros, 2011. Pp. 36.

27. COOPERAÇÃO INTERNACIONAL

Têm surgido diversas organizações internacionais, que ao longo dos tempos, têm vindo a publicar documentos e artigos concernentes à recolha e preservação da Prova Digital.

Em meados de Março de 1998, a IOCE foi competente para delimitar os princípios a ser respeitados no que diz respeito à forma de proceder no contacto com a Prova Digital, quer no que trata da sua apreensão, ou preservação desta. Esses princípios, tornaram-se necessários, especialmente como uma forma de garantir uma concertação das práticas e costumes reiterados nos mais diversos países, para o efeito. A partir deste normativo, garantia-se a hipótese legal da se aproveitar da Prova Digital colhida num determinado país, ou noutro, assim que sejam cumpridas e respeitadas essas regras.

Mais tarde, na conferência "*International hight-Tech crimes and forensics*", que se realizou em Londres, por 1999, emergiram destas, uma serie de recomendações, que se adoptaram pelos estados membros que nela participaram.

Em primeira instância, cada estado membro foi estimulado a seguir os princípios recomendados, e definir os seus comportamentos para a recolha, preservação e manipulação de Prova Digital, adaptando-os, por sua vez, às respetivas disposições jurídicas, e organizações nacionais internas, devendo no entanto, e como primordial objecto, estar organizados para oferecer resposta às diferentes imposições de cada país na sua especificidade criminosa e digital, mostrando-se adequado o meio.

Deste mesma conferência, acordou-se ainda alguns dos princípios basilares de cooperação internacional, definindo-se que quando se trata com uma Prova Digital:

Devem ser aplicados todos os procedimentos necessários, equiparando-os às demais provas, nos seus tipos.

Nenhuma acção, especialmente na fase de investigação, deve promover a alguma alteração da Prova, no que diz respeito a datas, conteúdos e formas.

A Prova Digital deverá ser obtida, utilizada ou interpretada, sempre e somente por quem especializado esteja habilitado a fazer. Desta forma não correndo o risco de violar, ainda que involuntariamente o disposto mencionado no supracitado ponto 2.

Todas as acções e actividades que envolvam a apreensão, acesso, leitura e mesmo o transporte da Prova Digital, deverá ser especificamente documentada, para se necessário, ser futuramente consultada e verificada.

Com o elevado risco de degradação, alteração ou perca da Prova Digital, cada agente que procede a sua recolha, leitura ou transporte, deverá ser igualmente responsável por qualquer tipo de alteração, omissão ou dano desta.

Algumas, e relevantes, são as várias organizações a nível internacional que se debruçam com especial crédito, no que trata de recolher e preservar, a Prova Digital, criando deste modo uma maior unificação no que diz respeito a práticas e procedimentos que os estados devem aplicar no seu âmbito interno, de forma a conseguir um melhor resultado a nível da investigação, e utilização da Prova, enquanto meio de confirmar o indício ou não de um crime.

O G8 [(50)], assim como a IOCE9, estiverem, por Março de 1998, encarregues de delimitar e definir os preceitos que passariam a definir a nível comunitário, as normas reguladoras dos procedimentos a efectuar com as Provas Digitais**.**

Deste assentimento, emergiu a possibilidade prática de se recolher uma determinada Prova Digital num determinado país estrangeiro, desde que se demonstrassem respeitados os preceitos legais então acordados.

A Forensic Computing Group, oriunda do Reino Unido, é uma das instituições de cooperação internacional mais antiga no que se relaciona com os procedimentos a efectuar com a Prova Digital.

A Forensic Computing Group, (FCG) é constituída por diversas agências de investigação criminal, como a Association of Chief Police Officers (ACPO), e a Computer Crime Working Group. (CCWG).

[(50)] *O Grupo dos Sete é um grupo internacional que reúne os sete países mais industrializados e desenvolvidos economicamente do mundo. Todos os países fundadores são nações democráticas: Estados Unidos, Alemanha, Canadá, França, Itália, Japão, Reino Unido. Recentemente foi excluída do grupo (G8) a Rússia, que agora passa a ser G7 novamente.*

A agência de investigação criminal Computer Crime Working Group, foi a primeira a instituir um manual de boas práticas a executar no que diz respeito à recolha, preservação, busca e exame da Prova Digital. Foi o primeiro documento que consagrou diversos procedimentos necessários e vantajosos a utilizarem-se de forma a permitir uma investigação mais célere, e respeitosa de normativos internos de cada estado. Contudo, este manual de boas práticas, foi em primeira instância adoptado especialmente pelo país que o originou, através da National High Tech Crime Unit. O mesmo, foi progredindo ao longo dos tempos, expandindo-se na sua aplicação, aos exames forenses.

Outro grupo de trabalho com a sua relevância na cooperação internacional, passa *pela European Network of Forensic Science Institutes - Forensic Information Technology Working Group (FIT-WG).*

O "*Forensic Information Technology Working Group*" foi criado em 1998, e inicialmente este grupo debruçava-se em aprofundar as técnicas forenses, trocando informações entre si, porém, posteriormente, em meados de 2001, em estruturação com a IOCEO debruçou-se na elaboração de um manual que abordou mais que questões técnicas e boas práticas, também versou relativamente a formação específica para quem agentes que necessitam de lidar e trabalhar com a Prova Digital.

O Instituto Nacional de Justiça dos EUA, também produz legislação com normas referentes a práticas que devem ser levadas a cabo por diversos países, com as suas normais e constantes adaptações ao processo penal interno de cada um, de forma a corrigir erros que possam gerar violações de normativos.

O Scientific Working Group on Digital Evidence (SWGDE), é um grupo de trabalho, também responsável pelo a cooperação internacional no que diz respeito à gestão e procedimentos a utilizar com a Prova Digital. Este grupo foi criado inicialmente por membros de agências Norte Americanas como o FBI e os Serviços Secretos, contudo actualmente, elenca vários membros dos mais diversos países, que em cooperação, se debatem por um objectivo único de gestão e boa prática de procedimento no que diz respeito à Prova Digital.

Não seria então possível ficar completo este título, sem abordar a mais importante lei relativa à Prova Digital, provinda da Convenção do Cibercrime do Conselho da Europa de 23 de Novembro de 2001.

As disposições específicas, plasmadas na 2ºa secção da presente Convenção, tendem a criar uma forma de auxílio e mecanismos internacionais, de forma a tornar mais eficaz, toda e qualquer situação que envolva uma investigação crucial por meio digital.
A subsecção primeira, sob a epígrafe de Disposições específicas, divide-se por sua vez em três títulos, sendo que o primeiro, abrange os artsº 29º relativo à conservação expedita de dados informáticos armazenados, e 30º, que diz respeito à divulgação expedida dos dados conservados, sendo estes normativos, semelhantes na sua génese com os artsº 16º e 17º da Lei n.º 109/2009, de 15 de Setembro, que vigora no plano nacional. (Portugal)

Mais especificamente, explica-nos o artº 29º da Convenção, que são dotadas as partes de legitimidade e competência jurídica, capaz de adquirir, sob formalidade de requerimento, a *'preservação expedita'* dos dados informáticos, que estejam em posse, e armazenados em dispositivos ou redes da parte requerida. Deste modo, protege-se assim a Prova Digital, tentando assegurar que a mesma não seja apagada, modificada ou sofra qualquer alteração que impossibilite a sua total utilidade na investigação.

Já no que ao artº 30 diz respeito, este elucida-nos que ao executar por requerimento, o pedido do art. 29º, relativo a conservação expedita de dados relativos a um trafego de determinada pessoa ou empresa, e se evidenciar na investigação, que a parte requerida teve a participação de um fornecedor de dados participando dessa comunicação à qual se requer, esta, informa desde logo a quantidade de dados necessários e suficientes para identificar o fornecedor de serviços, e ainda a forma como essa comunicação foi efectuada, de forma a cooperar com a investigação.

Compreendem-se neste mesmo normativo duas exepções, caso seja informação envolta de matéria política, ou se a parte requerida, para fazer cumprir o disposto do artº 30º, atentar contra a sua segurança, soberania, ordem pública ou qualquer outro interesse social. (51)

(51) Art. 29º e 30º da "*Convenção do Cibercrime do Conselho da Europa de 23 de Novembro de 2001"*

Encontramos no art. 23º da presente convenção, que a cooperação internacional, se compreende entre todas as transgressões penais efectuadas por meio informático ou digital, assim como no que concerne à recolha de Provas Digitais.

"*As partes cooperarão entre si, em conformidade com as disposições do presente capítulo, em aplicação dos instrumentos internacionais pertinentes sobre a cooperação internacional em matéria penal, de acordos celebrados com base nas legislações uniformes e recíprocas, e do seu direito nacional, na medida mais ampla possível, para efeitos de investigações ou de procedimentos relativos a infracções penais relacionados com sistemas de dados informáticos, ou para recolher provas sob forma electrónica de uma infracção penal"* (52)

Compreende-se nesta medida, que o art. 23º, determina que a cooperação internacional, deverá ser utilizada sempre que possível, e de forma a abranger o maior número de países, e de forma a agilizar todos os auxílios necessários à obtenção da Prova recolhida em ambiente digital ou informatizado, resultando deste modo numa colaboração entre estados, à descoberta da verdade material.

(52) Art. 23º da "*Convenção do Cibercrime do Conselho da Europa de 23 de Novembro de 2001"*

28. CONCLUSÃO

Com este estudo, atendendo especialmente à célere metamorfose que a sociedade actual tem vindo a sofrer, procurei demonstrar que essas alterações se manifestam também, e especialmente ao nível da criminalidade. Certo é então que, a lei, ao ser criada para as pessoas, deve a estas responder, explorando sempre novas formas de corroborar com a justiça, sendo actual e especialmente eficiente.

1. É deste modo, e no meu entender necessário com este trabalho, fazer denotar não só uma componente descritiva relativamente ao tema, como sobretudo uma componente crítica.
2. Actualmente, em Portugal, em sede de Prova Digital, a sua aplicação não se encontra particularmente especificada, no sentido em que se enquadra no seguimento dos art(s). 189.º e 188.º do C.P.P. Estes, remete a sua aplicabilidade, e requisitos para os pressupostos e admissibilidade das intercepções das escutas telefónicas.
3. Deste modo, parece-me claro que os requisitos necessários à legalidade das escutas telefónicas em muito diverge do que seria por sua vez necessária e adequada, a uma prova digital.
4. Assim não sendo, prejudica gravemente qualquer facto que embora em formato digital, ou proveniente deste, possa constituir objecto de prova, determinando a existência ou inexistência de um crime, a punibilidade ou não, assim como a determinação da própria pena ou medida de segurança, e não possa ser utilizado como tal, em virtude de não corresponder aos requisitos do art. 187º do CPP, e deste modo descartado.
5. Torna-se urgente, segundo o meu ponto de vista, legislar no sentido de agregar um instituto autónomo referente à Prova Digital, para que desse modo, e a título de exemplo uma Intervenção e tratamento médico-cirúrgico arbitrário (art. 156º do CP) em que a sua prova (confissão ou gravação de imagens) esteja em formato e suporte digital, ou um crime de Participação em rixa (art. 151º do CP), que a prova desta seja captada por um telemóvel, possa por ser vez valer como prova, caminhando-se assim para um julgamento mais justo, e descoberta da verdade material.

REFERÊNCIAS

BACELAR Gouveia, Jorge – *Manual de Direito Constitucional*, vol. II, Almedina

CARNELUTTI, Francesco; *Sistemas de Derecho Procesual civil*, Buenos Aires, Vol.II,1944.

CARVALHO, Paula Torres de, Jornal Público, 20.02.2012.

CASTRO MENDES, João de – "*Conceito de Prova em Processo Civil*", Lisboa, Edições Atica, 1961; p. 741.

DA SILVA, Germano Marques, *Curso de Processo Penal*, Vol. II; Lisboa, Verbo, 2002; p. 209.

DA SILVA, Germano Marques, *Curso de Processo Penal*, II Volume, Lisboa, São Paulo, Editorial Verbo, 4ª edição revista e atualizada, 2008, p.148.

DE PLÁCIDO E SILVA. "*Vocabulário Jurídico*". Rio de Janeiro: Ed. Forense, 2ª ed., 1967. Vol.III, pág. 1.253.

DIAS, Jorge de Figueiredo, Direito Processual Penal, I volume, Coimbra; Coimbra Editora, 1974, pp. 202-203.

EIRAS, Henrique; FORTES, Guilhermina – "Processo Penal Elementar", Lisboa, Quid Juris, 2009; p.135.

LIMA RODRIGUES, Cláudio. Derecho Procesal Penal (trad. da 25.ª ed. alemã por Gabriela Córdoba e Daniel Pastor), Buenos Aires: Editores del Puerto, 2000, cit., pp. 190,191 e 194.

LOPES, José Mouraz, e CABREIRO, Carlos Antão - "*A Emergência da Prova Digital na Investigação da Criminalidade Informática*" in Sub Judice — Justiça e Sociedade, n.º 35, Coimbra, Almedina, 2006.

LOPES Militão, Renato, Artigo, "*A propósito da prova Digital no processo penal*", p. 20.

MAGRIÇO, Manuel Aires, 2011*, "A criminalidade informática",* p.3

MESQUITA, Paulo Dá, "*Processo Penal Prova e Sistema Judiciário*", Coimbra, Coimbra Editora, 2010.

NEVES, Rosa Vieira, *"A Livre Apreciação da Prova e a Obrigação de Fundamentação da Convicção",* Coimbra; Coimbra Editora, 2011, p. 57.

PENHA LEITÃO DA COSTA MARQUES, Pedro – *"Informática Forense: Recolha e preservação da Prova Digital"*. Porto: Universidade Católica Portuguesa: Faculdade de Engenharia, 2013 pp. 43.

RANGEL, Rui, Correio da Manhã, 16.09.2010.

RANGEL, Rui Manuel de Freitas – O Ónus da Prova em Processo Civil, Lisboa, 3.ª ed. Almedina, 2006.

RODRIGUES, Benjamim Silva Rodrigues, Direito Penal. Parte Especial, I, Direito Penal Informático-Digital, Coimbra, Coimbra Editora, 2009: p. 39.

RODRIGUES, Benjamim Silva Rodrigues, Da Prova Penal, IV, Da Prova-Electrónico-Digital e da Criminalidade Informático-Digital, Lisboa, Rei dos Livros, 2011

VENÂNCIO, Pedro Dias – "*Breve introdução dos meios de prova na criminalidade informática"*, Verbojuridico, 2006.

Web grafia

2002/58/CE, consultada no *"Official website of the European Union"*, www.europa.eu.

ARAS, Vladimir, disponível em *http://pt.wikipedia.org/*, e do Artigo, "*A propósito da prova Digital*", LOPES Militão, Renato, p. 14.

Intervenção no Centro de Formação Jurídica e Judiciária de Macau em 30 de Novembro de 2011.
http://www.stj.pt/ficheiros/estudos/provaindiciarianovasformascriminalidade.pdf

LESSA, Breno Lessa, "A invalidade das provas digitais no processo judiciário", 2009, disponível na Internet, in http://jus.uol.com.br/revista

SAPALO, Arnaldo César Miguel Ribeiro – "*A prova e o ónus da prova nos processos civil e penal*", Sol Nascente: Revista do Centro de Investigação sobre Ética Aplicada. Disponível na internet in:
http://www.ispsn.org/sites/default/files/magazine/articles/N1%20art5.pdf

Bibliografia

ANDRADE, Manuel da Costa, - "*Sobre Proibições de prova em processo penal*", Coimbra Editora, 1992.

ASCENÇÃO, José de Oliveira, -"*Estudos sobre Direito da Internet e da Sociedade da Informação*", Livraria Almedina, Abril, 2001.

CASTRO, Catarina Sarmento - "*Direito da Informática, Privacidade e Dados Pessoais*", Almedina, Lisboa, 2005.

COSTA; José F. de faria, - "*Direito Penal da Comunicação*", Coimbra Editora, Coimbra, 1998.

FARINHO, Domingos Miguel Soares, - "*Intimidade da Vida Privada e Media no Ciberespaço*", Almedina, Lisboa, 2006

MARTINS, A. G. Lourenço, *"Criminalidade Informática*", artigo publicado em Direito da Sociedade da Informação, Volume IV, APDI, Coimbra Editora, 2003.

MENDES, Paulo de Sousa, "*A responsabilidade das pessoas colectivas no âmbito da criminalidade informática em Portugal*", artigo publicado em Direito da Sociedade da Informação, Volume IV, APDI, Coimbra Editora, 2003.

PEREIRA, Joel Timóteo Ramos, "*Compêndio Jurídico da Sociedade da Informação*",Quid Júris, Lisboa, 2004.

PEREIRA, Joel Timóteo Ramos; - "*Direito da Internet e Comércio Electrónico, Quid Júris"*, Lisboa, 2001.

RANGEL, Rui Manuel de Freitas – "*O Ónus da Prova em Processo Civil"*, Lisboa, 3.ª ed. Almedina, 2006.

SANTOS, Cristina Máximo dos, - "*As novas tecnologias da informação e o sigilo das telecomunicações*", Revista do Ministério Público, Ano 25, n.º 99, Julho/Setembro 2004.

SANTOS, Liane, - "*Bárbara Borges é perseguida por perfil falso no Twitter*", http://ego.globo.com/Gente/Noticias/0,,MUL1638305-9798,00-BARBARA+BORGES+E+PERSEGUIDA+POR+PERFIL+FALSO+NO+TWITTER.html, acesso dia 24 de Setembro de 2014

SOUSA, Miguel Teixeira de, - "*O valor probatório dos documentos electrónicos*", in Direito da Sociedade da Informação – Volume II, FDUL / APDI, Coimbra Editora, 2001.

VEIGA, Frederico, PIRES, Nafica, BOTELHO, Susana & TAVEIRA, Zenaide, - "*A Prova Digital*", Faculdade de Direito, Universidade Nova de Lisboa, 2011.

VENÂNCIO, Pedro Dias, - *"Investigação e meios de prova na criminalidade informática",* Compilação doutrinais: Verbo Jurídico, 2006.

VERDELHO, Pedro, BRAVO, Rogério, e LOPES ROCHA, Manuel, *"Leis do Cibercrime – volume 1*", Centro Atlântico, 2003.

VERDELHO, Pedro, "*Cibercrime*", artigo publicado em Direito da Sociedade da Informação, Volume IV, APDI, Coimbra Editora, 2003.

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

VERÍSSIMO, Joana; MACIAS, Maria & RODRIGUES, Sofia – "*Implicações Jurídicas das redes sociais na internet: um novo conceito de privacidade*?", Lisboa, Faculdade de Direito da Universidade Nova de Lisboa, 2012.

Legislação

Art.º 1.º da Directiva do Parlamento Europeu e do Conselho, de 12 de Julho de 2002

Art. 1.º da Constituição da República Portuguesa, "Portugal é uma República soberana, baseada na dignidade da pessoa humana e na vontade popular e empenhada na construção de uma sociedade livre, justa e solidária".

Art. 2º, da Lei n.º 109/2009, de 15 de Setembro, consultada no sítio da Procuradoria-Geral da República

Art.º 13.º da Constituição da República Portuguesa – 'Principio da igualdade'.

Art. 29º e 30º da Convenção do Cibercrime do Conselho da Europa de 23 de Novembro de 2001

Art. 23º da Convenção do Cibercrime do Conselho da Europa de 23 de Novembro de 2001

Código de processo penal, e legislação complementar, 6.ª edição, revista e actualizada / 2012, Almedina, art.º 189.º

Cf. Ac. TRC, n.º 135/09.4JAAVR-A.C1 de 9-12-2009, Jorge Jacob

Lei n.º 109/2009, de 15 de Setembro, consultada no sítio da Procuradoria-Geral da República.

Lei n.º 67/98, de 26 de Outubro, pesquisada e analisada no sítio oficial da Comissão Nacional da Protecção de dados. 'http://www.cnpd.pt/'.

Acórdão da Relação do Porto, de 24/04/2013, Processo n.º 585/11.6PAOVR.P1, pela relator Exma. Drª Juiza Fátima Furtado, disponível na Internet, no sítio da DGSI, em http://www.dgsi.pt/jtrp.nsf/c3fb530030ea1c61802568d9005cd5bb/872f3063233d8de480257b78003e60f3?OpenDocument

Acórdão da Relação do Porto, de 30/01/2008, Processo n.º 0744740, disponível na Internet, no sítio da DGSI.

Acórdão da Relação de Guimarães, de 29/03/2004, Processo n.º 1680/03-2, pela relator Exma. Drª Juiza Maria Augusta, disponível na Internet, no sítio da DGSI, em http://www.dgsi.pt/jtrg.nsf/86c25a698e4e7cb7802579ec004d3832/926f6fea6511bf6e80256ee0003afd32?OpenDocument

Acórdão do Tribunal da Relação do Porto, de 23/11/2011, Processo n.º 1373/08.2PSPRT.P1, pelo Relator Exmo. Sr. Dr. Juiz Mouraz Lopes, disponível na Internet, no sítio da DGSI, em http://www.dgsi.pt/jtrp.nsf/d1d5ce625d24df5380257583004ee7d7/1fce85582debcec280257967003fc659?OpenDocument

'A credibilidade que se concede a um certo meio de prova') – Prof. Figueiredo Dias. Direito Processual Penal. vol. I. ed.1974. pp. 204.

Anexos

Lei do Cibercrime (109/2009 de 15 de Setembro)

Objecto e definições

Artigo 1.º

Objecto

A presente lei estabelece as disposições penais materiais e processuais, bem como as disposições relativas à cooperação internacional em matéria penal, relativas ao domínio do cibercrime e da recolha de prova em suporte electrónico, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação, e adaptando o direito interno à Convenção sobre Cibercrime do Conselho da Europa.

Artigo 2.º

Definições

Para efeitos da presente lei, considera-se:

a) «Sistema informático», qualquer dispositivo ou conjunto de dispositivos interligados ou associados, em que um ou mais de entre eles desenvolve, em execução de um programa, o tratamento automatizado de dados informáticos, bem como a rede que suporta a comunicação entre eles e o conjunto de dados informáticos armazenados, tratados, recuperados ou transmitidos por aquele ou aqueles dispositivos, tendo em vista o seu funcionamento, utilização, protecção e manutenção;

b) «Dados informáticos», 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;

c) «Dados de tráfego», os 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;

d) «Fornecedor de serviço», 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;

e) «Intercepção», o acto destinado a captar informações contidas num sistema informático, através de dispositivos electromagnéticos, acústicos, mecânicos ou outros;

f) «Topografia», uma série de imagens ligadas entre si, independentemente do modo como são fixadas ou codificadas, que representam a configuração tridimensional das camadas que compõem um produto semicondutor e na qual cada imagem reproduz o desenho, ou parte dele, de uma superfície do produto semicondutor, independentemente da fase do respectivo fabrico;

g) «Produto semicondutor», a forma final ou intermédia de qualquer produto, composto por um substrato que inclua uma camada de material semicondutor e constituído por uma ou várias camadas de matérias condutoras, isolantes ou semicondutoras, segundo uma disposição conforme a uma configuração tridimensional e destinada a cumprir, exclusivamente ou não, uma função electrónica.

Artigo 3.º
Falsidade informática

1 - Quem, com intenção de provocar engano nas relações jurídicas, introduzir, modificar, apagar ou suprimir dados informáticos ou por qualquer outra forma interferir num tratamento informático de dados, produzindo dados ou documentos não genuínos, com a intenção de que estes sejam considerados ou utilizados para finalidades juridicamente relevantes como se o fossem, é punido com pena de prisão até 5 anos ou multa de 120 a 600 dias.

2 - Quando as acções descritas no número anterior incidirem sobre os dados registados ou incorporados em cartão bancário de pagamento ou em qualquer outro dispositivo que permita o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado, a pena é de 1 a 5 anos de prisão.

3 - Quem, actuando com intenção de causar prejuízo a outrem ou de obter um benefício ilegítimo, para si ou para terceiro, usar documento produzido a partir de dados informáticos que foram objecto dos actos referidos no n.º 1 ou cartão ou outro

dispositivo no qual se encontrem registados ou incorporados os dados objecto dos actos referidos no número anterior, é punido com as penas previstas num e noutro número, respectivamente.

4 - Quem importar, distribuir, vender ou detiver para fins comerciais qualquer dispositivo que permita o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado, sobre o qual tenha sido praticada qualquer das acções prevista no n.º 2, é punido com pena de prisão de 1 a 5 anos.

5 - Se os factos referidos nos números anteriores forem praticados por funcionário no exercício das suas funções, a pena é de prisão de 2 a 5 anos.

Artigo 4.º

Dano relativo a programas ou outros dados informáticos

1 - Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, apagar, alterar, destruir, no todo ou em parte, danificar, suprimir ou tornar não utilizáveis ou não acessíveis programas ou outros dados informáticos alheios ou por qualquer forma lhes afectar a capacidade de uso, é punido com pena de prisão até 3 anos ou pena de multa.

2 - A tentativa é punível.

3 - Incorre na mesma pena do n.º 1 quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos destinados a produzir as acções não autorizadas descritas nesse número.

4 - Se o dano causado for de valor elevado, a pena é de prisão até 5 anos ou de multa até 600 dias.

5 - Se o dano causado for de valor consideravelmente elevado, a pena é de prisão de 1 a 10 anos.

6 - Nos casos previstos nos n.os 1, 2 e 4 o procedimento penal depende de queixa.

Artigo 5.º

Sabotagem informática

1 - Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, entravar, impedir, interromper ou perturbar gravemente o funcionamento de um sistema informático, através da introdução, transmissão, deterioração, danificação, alteração, apagamento, impedimento do acesso ou supressão de programas ou outros dados informáticos ou de qualquer outra forma de interferência em sistema informático, é punido com pena de prisão até 5 anos ou com pena de multa até 600 dias.

2 - Na mesma pena incorre quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos destinados a produzir as acções não autorizadas descritas no número anterior.

3 - Nos casos previstos no número anterior, a tentativa não é punível.

4 - A pena é de prisão de 1 a 5 anos se o dano emergente da perturbação for de valor elevado.

5 - A pena é de prisão de 1 a 10 anos se:

a) O dano emergente da perturbação for de valor consideravelmente elevado;

b) A perturbação causada atingir de forma grave ou duradoura um sistema informático que apoie uma actividade destinada a assegurar funções sociais críticas, nomeadamente as cadeias de abastecimento, a saúde, a segurança e o bem-estar económico das pessoas, ou o funcionamento regular dos serviços públicos.

Artigo 6.º

Acesso ilegítimo

1 - Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, de qualquer modo aceder a um sistema informático, é punido com pena de prisão até 1 ano ou com pena de multa até 120 dias.

2 - Na mesma pena incorre quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos

dispositivos, programas, um conjunto executável de instruções, um código ou outros dados informáticos destinados a produzir as acções não autorizadas descritas no número anterior.

3 - A pena é de prisão até 3 anos ou multa se o acesso for conseguido através de violação de regras de segurança.

4 - A pena é de prisão de 1 a 5 anos quando:

a) Através do acesso, o agente tiver tomado conhecimento de segredo comercial ou industrial ou de dados confidenciais, protegidos por lei; ou

c) O benefício ou vantagem patrimonial obtidos forem de valor consideravelmente elevado.

5 - A tentativa é punível, salvo nos casos previstos no n.º 2.

6 - Nos casos previstos no n.º, 3 e 5 o procedimento penal depende de queixa.

Artigo 7.º

Intercepção ilegítima

1 - Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, e através de meios técnicos, interceptar transmissões de dados informáticos que se processam no interior de um sistema informático, a ele destinadas ou dele provenientes, é punido com pena de prisão até 3 anos ou com pena de multa.

2 - A tentativa é punível.

3 - Incorre na mesma pena prevista no n.º 1 quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos destinados a produzir as acções não autorizadas descritas no mesmo número.

Artigo 8.º

Reprodução ilegítima de programa protegido

1 - Quem ilegitimamente reproduzir, divulgar ou comunicar ao público um programa informático protegido por lei é punido com pena de prisão até 3 anos ou com pena de multa.

2 - Na mesma pena incorre quem ilegitimamente reproduzir topografia de um produto semicondutor ou a explorar comercialmente ou importar, para estes fins, uma topografia ou um produto semicondutor fabricado a partir dessa topografia.

3 - A tentativa é punível.

Artigo 9.º

Responsabilidade penal das pessoas colectivas e entidades equiparadas

As pessoas colectivas e entidades equiparadas são penalmente responsáveis pelos crimes previstos na presente lei nos termos e limites do regime de responsabilização previsto no Código Penal.

Artigo 10.º

Perda de bens

1 - O tribunal pode decretar a perda a favor do Estado dos objectos, materiais, equipamentos ou dispositivos que tiverem servido para a prática dos crimes previstos na presente lei e pertencerem a pessoa que tenha sido condenada pela sua prática.

2 - À avaliação, utilização, alienação e indemnização de bens apreendidos pelos órgãos de polícia criminal que sejam susceptíveis de vir a ser declarados perdidos a favor do Estado é aplicável o disposto no Decreto-Lei n.º 11/2007, de 19 de Janeiro.

Artigo 11.º

Âmbito de aplicação das disposições processuais

1 - Com excepção do disposto nos artigos 18.º e 19.º, as disposições processuais previstas no presente capítulo aplicam-se a processos relativos a crimes:

a) Previstos na presente lei;

b) Cometidos por meio de um sistema informático; ou

c) Em relação aos quais seja necessário proceder à recolha de prova em suporte electrónico.

2 - As disposições processuais previstas no presente capítulo não prejudicam o regime da Lei n.º 32/2008, de 17 de Julho.

Artigo 12.º

Preservação expedita de dados

1 - Se no decurso do processo for necessário à produção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos armazenados num sistema informático, incluindo dados de tráfego, em relação aos quais haja receio de que possam perder-se, alterar-se ou deixar de estar disponíveis, a autoridade judiciária competente ordena a quem tenha disponibilidade ou controlo desses dados, designadamente a fornecedor de serviço, que preserve os dados em causa.

2 - A preservação pode também ser ordenada pelo órgão de polícia criminal mediante autorização da autoridade judiciária competente ou quando haja urgência ou perigo na demora, devendo aquele, neste último caso, dar notícia imediata do facto à autoridade judiciária e transmitir-lhe o relatório previsto no artigo 253.º do Código de Processo Penal.

3 - A ordem de preservação discrimina, sob pena de nulidade:

a) A natureza dos dados;

b) A sua origem e destino, se forem conhecidos; e

c) O período de tempo pelo qual deverão ser preservados, até um máximo de três meses.

4 - Em cumprimento de ordem de preservação que lhe seja dirigida, quem tenha disponibilidade ou controlo sobre esses dados, designadamente o fornecedor de serviço,

preserva de imediato os dados em causa, protegendo e conservando a sua integridade pelo tempo fixado, de modo a permitir à autoridade judiciária competente a sua obtenção, e fica obrigado a assegurar a confidencialidade da aplicação da medida processual.

5 - A autoridade judiciária competente pode ordenar a renovação da medida por períodos sujeitos ao limite previsto na alínea c) do n.º 3, desde que se verifiquem os respectivos requisitos de admissibilidade, até ao limite máximo de um ano.

Artigo 13.º

Revelação expedita de dados de tráfego

Tendo em vista assegurar a preservação dos dados de tráfego relativos a uma determinada comunicação, independentemente do número de fornecedores de serviço que nela participaram, o fornecedor de serviço a quem essa preservação tenha sido ordenada nos termos do artigo anterior indica à autoridade judiciária ou ao órgão de polícia criminal, logo que o souber, outros fornecedores de serviço através dos quais aquela comunicação tenha sido efectuada, tendo em vista permitir identificar todos os fornecedores de serviço e a via através da qual aquela comunicação foi efectuada.

Artigo 14.º

Injunção para apresentação ou concessão do acesso a dados

1 - Se no decurso do processo se tornar necessário à produção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos e determinados, armazenados num determinado sistema informático, a autoridade judiciária competente ordena a quem tenha disponibilidade ou controlo desses dados que os comunique ao processo ou que permita o acesso aos mesmos, sob pena de punição por desobediência.

2 - A ordem referida no número anterior identifica os dados em causa.

3 - Em cumprimento da ordem descrita nos n.os 1 e 2, quem tenha disponibilidade ou controlo desses dados comunica esses dados à autoridade judiciária competente ou

permite, sob pena de punição por desobediência, o acesso ao sistema informático onde os mesmos estão armazenados.

4 - O disposto no presente artigo é aplicável a fornecedores de serviço, 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 determinar:

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 assinante, 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.

5 - A injunção prevista no presente artigo não pode ser dirigida a suspeito ou arguido nesse processo.

6 - Não pode igualmente fazer-se uso da injunção prevista neste artigo quanto a sistemas informáticos utilizados para o exercício da advocacia, das actividades médica e bancária e da profissão de jornalista.

7 - O regime de segredo profissional ou de funcionário e de segredo de Estado previsto no artigo 182.º do Código de Processo Penal é aplicável com as necessárias adaptações.

Artigo 15.º

Pesquisa de dados informáticos

1 - Quando no decurso do processo se tornar necessário à produção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos e determinados, armazenados num determinado sistema informático, a autoridade judiciária competente autoriza ou ordena por despacho que se proceda a uma pesquisa nesse sistema informático, devendo, sempre que possível, presidir à diligência.

2 - O despacho previsto no número anterior tem um prazo de validade máximo de 30 dias, sob pena de nulidade.

3 - O órgão de polícia criminal pode proceder à pesquisa, sem prévia autorização da autoridade judiciária, quando:

a) A mesma for voluntariamente consentida por quem tiver a disponibilidade ou controlo desses dados, desde que o consentimento prestado fique, por qualquer forma, documentado;

b) Nos casos de terrorismo, criminalidade violenta ou altamente organizada, quando haja fundados indícios da prática iminente de crime que ponha em grave risco a vida ou a integridade de qualquer pessoa.

4 - Quando o órgão de polícia criminal proceder à pesquisa nos termos do número anterior:

a) No caso previsto na alínea b), a realização da diligência é, sob pena de nulidade, imediatamente comunicada à autoridade judiciária competente e por esta apreciada em ordem à sua validação;

b) Em qualquer caso, é elaborado e remetido à autoridade judiciária competente o relatório previsto no artigo 253.º do Código de Processo Penal.

5 - Quando, no decurso de pesquisa, surgirem razões para crer que os dados procurados se encontram noutro sistema informático, ou numa parte diferente do sistema pesquisado, mas que tais dados são legitimamente acessíveis a partir do sistema inicial, a pesquisa pode ser estendida mediante autorização ou ordem da autoridade competente, nos termos dos n.os 1 e 2.

6 - À pesquisa a que se refere este artigo são aplicáveis, com as necessárias adaptações, as regras de execução das buscas previstas no Código de Processo Penal e no Estatuto do Jornalista.

Artigo 16.º

Apreensão de dados informáticos

1 - Quando, no decurso de uma pesquisa informática ou de outro acesso legítimo a um sistema informático, forem encontrados dados ou documentos informáticos necessários à produção de prova, tendo em vista a descoberta da verdade, a autoridade judiciária competente autoriza ou ordena por despacho a apreensão dos mesmos.

2 - O órgão de polícia criminal pode efectuar apreensões, sem prévia autorização da autoridade judiciária, no decurso de pesquisa informática legitimamente ordenada e executada nos termos do artigo anterior, bem como quando haja urgência ou perigo na demora.

3 - Caso sejam apreendidos dados ou documentos informáticos cujo conteúdo seja susceptível de revelar dados pessoais ou íntimos, que possam pôr 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.

4 - As apreensões efectuadas por órgão de polícia criminal são sempre sujeitas a validação pela autoridade judiciária, no prazo máximo de 72 horas.

5 - As apreensões relativas a sistemas informáticos utilizados para o exercício da advocacia e das actividades médica e bancária estão sujeitas, com as necessárias adaptações, às regras e formalidades previstas no Código de Processo Penal e as relativas a sistemas informáticos utilizados para o exercício da profissão de jornalista estão sujeitas, com as necessárias adaptações, às regras e formalidades previstas no Estatuto do Jornalista.

6 - O regime de segredo profissional ou de funcionário e de segredo de Estado previsto no artigo 182.º do Código de Processo Penal é aplicável com as necessárias adaptações.

7 - A apreensão de dados informáticos, consoante seja mais adequado e proporcional, tendo em conta os interesses do caso concreto, pode, nomeadamente, revestir as formas seguintes:

a) Apreensão do suporte onde está instalado o sistema ou apreensão do suporte onde estão armazenados os dados informáticos, bem como dos dispositivos necessários à respectiva leitura;

b) Realização de uma cópia dos dados, em suporte autónomo, que será junto ao processo;

c) Preservação, por meios tecnológicos, da integridade dos dados, sem realização de cópia nem remoção dos mesmos; ou

d) Eliminação não reversível ou bloqueio do acesso aos dados.

8 - No caso da apreensão efectuada nos termos da alínea b) do número anterior, a cópia é efectuada em duplicado, sendo uma das cópias selada e confiada ao secretário judicial dos serviços onde o processo correr os seus termos e, se tal for tecnicamente possível, os dados apreendidos são certificados por meio de assinatura digital.

Artigo 17.º

Apreensão de correio electrónico e registos de comunicações de natureza semelhante

Quando, no decurso de uma pesquisa informática ou outro acesso legítimo a um sistema informático, forem encontrados, armazenados nesse sistema informático ou noutro a que seja permitido o acesso legítimo a partir do primeiro, mensagens de correio electrónico ou registos de comunicações de natureza semelhante, o juiz pode autorizar ou ordenar, por despacho, a apreensão daqueles que se afigurem ser de grande interesse para a descoberta da verdade ou para a prova, aplicando-se correspondentemente o regime da apreensão de correspondência previsto no Código de Processo Penal.

Artigo 18.º

Intercepção de comunicações

1 - É admissível o recurso à intercepção de comunicações em processos relativos a crimes:

a) Previstos na presente lei; ou

b) Cometidos por meio de um sistema informático ou em relação aos quais seja necessário proceder à recolha de prova em suporte electrónico, quando tais crimes se encontrem previstos no artigo 187.º do Código de Processo Penal.

2 - A intercepção e o registo de transmissões de dados informáticos só podem ser autorizados durante o inquérito, se houver razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma,

impossível ou muito difícil de obter, por despacho fundamentado do juiz de instrução e mediante requerimento do Ministério Público.

3 - A intercepção pode destinar-se ao registo de dados relativos ao conteúdo das comunicações ou visar apenas a recolha e registo de dados de tráfego, devendo o despacho referido no número anterior especificar o respectivo âmbito, de acordo com as necessidades concretas da investigação.

4 - Em tudo o que não for contrariado pelo presente artigo, à intercepção e registo de transmissões de dados informáticos é aplicável o regime da intercepção e gravação de conversações ou comunicações telefónicas constante dos artigos 187.º, 188.º e 190.º do Código de Processo Penal.

Artigo 19.º

Acções encobertas

1 - É admissível o recurso às acções encobertas previstas na Lei n.º 101/2001, de 25 de Agosto, nos termos aí previstos, no decurso de inquérito relativo aos seguintes crimes:

a) Os previstos na presente lei;

b) Os cometidos por meio de um sistema informático, quando lhes corresponda, em abstracto, pena de prisão de máximo superior a 5 anos ou, ainda que a pena seja inferior, e sendo dolosos, os crimes contra a liberdade e autodeterminação sexual nos casos em que os ofendidos sejam menores ou incapazes, a burla qualificada, a burla informática e nas comunicações, a discriminação racial, religiosa ou sexual, as infracções económico-financeiras, bem como os crimes consagrados no título iv do Código do Direito de Autor e dos Direitos Conexos.

2 - Sendo necessário o recurso a meios e dispositivos informáticos observam-se, naquilo que for aplicável, as regras previstas para a intercepção de comunicações.

Artigo 20.º

Âmbito da cooperação internacional

As autoridades nacionais competentes cooperam com as autoridades estrangeiras competentes para efeitos de investigações ou procedimentos respeitantes a crimes relacionados com sistemas ou dados informáticos, bem como para efeitos de recolha de prova, em suporte electrónico, de um crime, de acordo com as normas sobre transferência de dados pessoais previstas na Lei n.º 67/98, de 26 de Outubro.

Artigo 21.º

Ponto de contacto permanente para a cooperação internacional

1 - Para fins de cooperação internacional, tendo em vista a prestação de assistência imediata para os efeitos referidos no artigo anterior, a Polícia Judiciária assegura a manutenção de uma estrutura que garante um ponto de contacto disponível em permanência, vinte e quatro horas por dia, sete dias por semana.

2 - Este ponto de contacto pode ser contactado por outros pontos de contacto, nos termos de acordos, tratados ou convenções a que Portugal se encontre vinculado, ou em cumprimento de protocolos de cooperação internacional com organismos judiciários ou policiais.

3 - A assistência imediata prestada por este ponto de contacto permanente inclui:

a) A prestação de aconselhamento técnico a outros pontos de contacto;

b) A preservação expedita de dados nos casos de urgência ou perigo na demora, em conformidade com o disposto no artigo seguinte;

c) A recolha de prova para a qual seja competente nos casos de urgência ou perigo na demora;

d) A localização de suspeitos e a prestação de informações de carácter jurídico, nos casos de urgência ou perigo na demora;

e) A transmissão imediata ao Ministério Público de pedidos relativos às medidas referidas nas alíneas b) a d), fora dos casos aí previstos, tendo em vista a sua rápida execução.

4 - Sempre que actue ao abrigo das alíneas b) a d) do número anterior, a Polícia Judiciária dá notícia imediata do facto ao Ministério Público e remete-lhe o relatório previsto no artigo 253.º do Código de Processo Penal.

Artigo 22.º

Preservação e revelação expeditas de dados informáticos em cooperação internacional

1 - Pode ser solicitada a Portugal a preservação expedita de dados informáticos armazenados em sistema informático aqui localizado, relativos a crimes previstos no artigo 11.º, com vista à apresentação de um pedido de auxílio judiciário para fins de pesquisa, apreensão e divulgação dos mesmos.

2 - A solicitação especifica:

a) A autoridade que pede a preservação;

b) A infracção que é objecto de investigação ou procedimento criminal, bem como uma breve exposição dos factos relacionados;

c) Os dados informáticos a conservar e a sua relação com a infracção;

d) Todas as informações disponíveis que permitam identificar o responsável pelos dados informáticos ou a localização do sistema informático;

e) A necessidade da medida de preservação; e

f) A intenção de apresentação de um pedido de auxílio judiciário para fins de pesquisa, apreensão e divulgação dos dados.

3 - Em execução de solicitação de autoridade estrangeira competente nos termos dos números anteriores, a autoridade judiciária competente ordena a quem tenha disponibilidade ou controlo desses dados, designadamente a fornecedor de serviço, que os preserve.

4 - A preservação pode também ser ordenada pela Polícia Judiciária mediante autorização da autoridade judiciária competente ou quando haja urgência ou perigo na demora, sendo aplicável, neste último caso, o disposto no n.º 4 do artigo anterior.

5 - A ordem de preservação especifica, sob pena de nulidade:

a) A natureza dos dados;

b) Se forem conhecidos, a origem e o destino dos mesmos; e

c) O período de tempo pelo qual os dados devem ser preservados, até um máximo de três meses.

6 - Em cumprimento de ordem de preservação que lhe seja dirigida, quem tem disponibilidade ou controlo desses dados, designadamente o fornecedor de serviço, preserva de imediato os dados em causa pelo período de tempo especificado, protegendo e conservando a sua integridade.

7 - A autoridade judiciária competente, ou a Polícia Judiciária mediante autorização daquela autoridade, podem ordenar a renovação da medida por períodos sujeitos ao limite previsto na alínea c) do n.º 5, desde que se verifiquem os respectivos requisitos de admissibilidade, até ao limite máximo de um ano.

8 - Quando seja apresentado o pedido de auxílio referido no n.º 1, a autoridade judiciária competente para dele decidir determina a preservação dos dados até à adopção de uma decisão final sobre o pedido.

9 - Os dados preservados ao abrigo do presente artigo apenas podem ser fornecidos:

a) À autoridade judiciária competente, em execução do pedido de auxílio referido no n.º 1, nos mesmos termos em que poderiam sê-lo, em caso nacional semelhante, ao abrigo dos artigos 13.º a 17.º;

b) À autoridade nacional que emitiu a ordem de preservação, nos mesmos termos em que poderiam sê-lo, em caso nacional semelhante, ao abrigo do artigo 13.º

10 - A autoridade nacional à qual, nos termos do número anterior, sejam comunicados dados de tráfego identificadores de fornecedor de serviço e da via através dos quais a comunicação foi efectuada, comunica-os rapidamente à autoridade requerente, por forma a permitir a essa autoridade a apresentação de nova solicitação de preservação expedita de dados informáticos.

11 - O disposto nos n.(s) 1 e 2 aplica-se, com as devidas adaptações, aos pedidos formulados pelas autoridades portuguesas.

Artigo 23.º

Motivos de recusa

1 - A solicitação de preservação ou revelação expeditas de dados informáticos é recusada quando:

a) Os dados informáticos em causa respeitarem a infracção de natureza política ou infracção conexa segundo as concepções do direito português;

b) Atentar contra a soberania, segurança, ordem pública ou outros interesses da República Portuguesa, constitucionalmente definidos;

c) O Estado terceiro requisitante não oferecer garantias adequadas de protecção dos dados pessoais.

2 - A solicitação de preservação expedita de dados informáticos pode ainda ser recusada quando houver fundadas razões para crer que a execução de pedido de auxílio judiciário subsequente para fins de pesquisa, apreensão e divulgação de tais dados será recusado por ausência de verificação do requisito da dupla incriminação.

Artigo 24.º

Acesso a dados informáticos em cooperação internacional

1 - Em execução de pedido de autoridade estrangeira competente, a autoridade judiciária competente pode proceder à pesquisa, apreensão e divulgação de dados informáticos armazenados em sistema informático localizado em Portugal, relativos a crimes previstos no artigo 11.º, quando se trata de situação em que a pesquisa e apreensão são admissíveis em caso nacional semelhante.

2 - A autoridade judiciária competente procede com a maior rapidez possível quando existam razões para crer que os dados informáticos em causa são especialmente vulneráveis à perda ou modificação ou quando a cooperação rápida se encontre prevista em instrumento internacional aplicável.

3 - O disposto no n.º 1 aplica-se, com as devidas adaptações, aos pedidos formulados pelas autoridades judiciárias portuguesas.

Artigo 25.º

Acesso transfronteiriço a dados informáticos armazenados quando publicamente disponíveis ou com consentimento

As autoridades estrangeiras competentes, sem necessidade de pedido prévio às autoridades portuguesas, de acordo com as normas sobre transferência de dados pessoais previstas na Lei n.º 67/98, de 26 de Outubro, podem:

a) Aceder a dados informáticos armazenados em sistema informático localizado em Portugal, quando publicamente disponíveis;

b) Receber ou aceder, através de sistema informático localizado no seu território, a dados informáticos armazenados em Portugal, mediante consentimento legal e voluntário de pessoa legalmente autorizada a divulgá-los.

Artigo 26.º

Intercepção de comunicações em cooperação internacional

1 - Em execução de pedido da autoridade estrangeira competente, pode ser autorizada pelo juiz a intercepção de transmissões de dados informáticos realizadas por via de um sistema informático localizado em Portugal, desde que tal esteja previsto em acordo, tratado ou convenção internacional e se trate de situação em que tal intercepção seja admissível, nos termos do artigo 18.º, em caso nacional semelhante.

2 - É competente para a recepção dos pedidos de intercepção a Polícia Judiciária, que os apresentará ao Ministério Público, para que os apresente ao juiz de instrução criminal da comarca de Lisboa para autorização.

3 - O despacho de autorização referido no artigo anterior permite também a transmissão imediata da comunicação para o Estado requerente, se tal procedimento estiver previsto no acordo, tratado ou convenção internacional com base no qual é feito o pedido.

4 - O disposto no n.º 1 aplica-se, com as devidas adaptações, aos pedidos formulados pelas autoridades judiciárias portuguesas.

Artigo 27.º

Aplicação no espaço da lei penal portuguesa e competência dos tribunais portugueses

1 - Para além do disposto no Código Penal em matéria de aplicação no espaço da lei penal portuguesa, e salvo tratado ou convenção internacional em contrário, para efeitos da presente lei, a lei penal portuguesa é ainda aplicável a factos:

a) Praticados por Portugueses, se aos mesmos não for aplicável a lei penal de nenhum outro Estado;

b) Cometidos em benefício de pessoas colectivas com sede em território português;

c) Fisicamente praticados em território português, ainda que visem sistemas informáticos localizados fora desse território; ou

d) Que visem sistemas informáticos localizados em território português, independentemente do local onde esses factos forem fisicamente praticados.

2 - Se, em função da aplicabilidade da lei penal portuguesa, forem simultaneamente competentes para conhecer de um dos crimes previstos na presente lei os tribunais portugueses e os tribunais de outro Estado membro da União Europeia, podendo em qualquer um deles ser validamente instaurado ou prosseguido o procedimento penal com base nos mesmos factos, a autoridade judiciária competente recorre aos órgãos e mecanismos instituídos no seio da União Europeia para facilitar a cooperação entre as autoridades judiciárias dos Estados membros e a coordenação das respectivas acções, por forma a decidir qual dos dois Estados instaura ou prossegue o procedimento contra os agentes da infracção, tendo em vista centralizá-lo num só deles.

3 - A decisão de aceitação ou transmissão do procedimento é tomada pela autoridade judiciária competente, tendo em conta, sucessivamente, os seguintes elementos:

a) O local onde foi praticada a infracção;

b) A nacionalidade do autor dos factos; e

c) O local onde o autor dos factos foi encontrado.

4 - São aplicáveis aos crimes previstos na presente lei as regras gerais de competência dos tribunais previstas no Código de Processo Penal.

5 - Em caso de dúvida quanto ao tribunal territorialmente competente, designadamente por não coincidirem o local onde fisicamente o agente actuou e o local onde está fisicamente instalado o sistema informático visado com a sua actuação, a competência cabe ao tribunal onde primeiro tiver havido notícia dos factos.

Artigo 28.º

Regime geral aplicável

Em tudo o que não contrarie o disposto na presente lei, aplicam-se aos crimes, às medidas processuais e à cooperação internacional em matéria penal nela previstos, respectivamente, as disposições do Código Penal, do Código de Processo Penal e da Lei n.º 144/99, de 31 de Agosto.

Artigo 29.º

Competência da Polícia Judiciária para a cooperação internacional

A competência atribuída pela presente lei à Polícia Judiciária para efeitos de cooperação internacional é desempenhada pela unidade orgânica a quem se encontra cometida a investigação dos crimes previstos na presente lei.

Artigo 30.º

Protecção de dados pessoais

O tratamento de dados pessoais ao abrigo da presente lei efectua-se de acordo com o disposto na Lei n.º 67/98, de 26 de Outubro, sendo aplicável, em caso de violação, o disposto no respectivo capítulo vi.

Artigo 31.º

Norma revogatória

É revogada a Lei n.º 109/91, de 17 de Agosto.

Artigo 32.º

Entrada em vigor

A presente lei entra em vigor 30 dias após a sua publicação.

Aprovada em 23 de Julho de 2009.

O Presidente da Assembleia da República, Jaime Gama.

Promulgada em 29 de Agosto de 2009.

Publique-se.

O Presidente da República, Aníbal Cavaco Silva.

Referendada em 31 de Agosto de 2009.

O Primeiro-Ministro, José Sócrates Carvalho Pinto de Sousa

Lei n.º 32/2008, de 17 de Julho

Transpõe para a ordem jurídica interna a Directiva n.º 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de Março, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações.

Artigo 1.º
Objecto

1 - A presente lei regula a conservação e a transmissão dos dados de tráfego e de localização relativos a pessoas singulares e a pessoas colectivas, bem como dos dados conexos necessários para identificar o assinante ou o utilizador registado, para fins de investigação, detecção e repressão de crimes graves por parte das autoridades competentes, transpondo para a ordem jurídica interna a Directiva n.º 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de Março, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Directiva n.º 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de Junho, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas.

2 - A conservação de dados que revelem o conteúdo das comunicações é proibida, sem prejuízo do disposto na Lei n.º 41/2004, de 18 de Agosto, e na legislação processual penal relativamente à intercepção e gravação de comunicações.

Artigo 2.º

Definições

1 - Para efeitos da presente lei, entende-se por:

a) «Dados», os dados de tráfego e os dados de localização, bem como os dados conexos necessários para identificar o assinante ou o utilizador;

b) «Serviço telefónico», qualquer dos seguintes serviços:

i) Os serviços de chamada, incluindo as chamadas vocais, o correio vocal, a teleconferência ou a transmissão de dados;

ii) Os serviços suplementares, incluindo o reencaminhamento e a transferência de chamadas; e

iii) Os serviços de mensagens e multimédia, incluindo os serviços de mensagens curtas (SMS), os serviços de mensagens melhoradas (EMS) e os serviços multimédia (MMS);

c) «Código de identificação do utilizador» («user ID»), um código único atribuído às pessoas, quando estas se tornam assinantes ou se inscrevem num serviço de acesso à Internet, ou num serviço de comunicação pela Internet;

d) «Identificador de célula» («cell ID»), a identificação da célula de origem e de destino de uma chamada telefónica numa rede móvel;

e) «Chamada telefónica falhada», uma comunicação em que a ligação telefónica foi estabelecida, mas que não obteve resposta, ou em que houve uma intervenção do gestor da rede;

f) «Autoridades competentes», as autoridades judiciárias e as autoridades de polícia criminal das seguintes entidades:

i) A Polícia Judiciária;

ii) A Guarda Nacional Republicana;

iii) A Polícia de Segurança Pública;

iv) A Polícia Judiciária Militar;

v) O Serviço de Estrangeiros e Fronteiras;

vi) A Polícia Marítima;

g) «Crime grave», crimes de terrorismo, criminalidade violenta, criminalidade altamente organizada, sequestro, rapto e tomada de reféns, crimes contra a identidade cultural e integridade pessoal, contra a segurança do Estado, falsificação de moeda ou títulos equiparados a moeda e crimes abrangidos por convenção sobre segurança da navegação aérea ou marítima.

2 - Para efeitos da presente lei, são aplicáveis, sem prejuízo do disposto no número anterior, as definições constantes das Leis n.os 67/98, de 26 de Outubro, e 41/2004, de 18 de Agosto.

Artigo 3.º

Finalidade do tratamento

1 - A conservação e a transmissão dos dados têm por finalidade exclusiva a investigação, detecção e repressão de crimes graves por parte das autoridades competentes.

2 - A transmissão dos dados às autoridades competentes só pode ser ordenada ou autorizada por despacho fundamentado do juiz, nos termos do artigo 9.º

3 - Os ficheiros destinados à conservação de dados no âmbito da presente lei têm que, obrigatoriamente, estar separados de quaisquer outros ficheiros para outros fins.

4 - O titular dos dados não pode opor-se à respectiva conservação e transmissão.

Artigo 4.º

Categorias de dados a conservar

1 - Os fornecedores de serviços de comunicações electrónicas publicamente disponíveis ou de uma rede pública de comunicações devem conservar as seguintes categorias de dados:

a) Dados necessários para encontrar e identificar a fonte de uma comunicação;

b) Dados necessários para encontrar e identificar o destino de uma comunicação;

c) Dados necessários para identificar a data, a hora e a duração de uma comunicação;

d) Dados necessários para identificar o tipo de comunicação;

e) Dados necessários para identificar o equipamento de telecomunicações dos utilizadores, ou o que se considera ser o seu equipamento;

f) Dados necessários para identificar a localização do equipamento de comunicação móvel.

2 - Para os efeitos do disposto na alínea a) do número anterior, os dados necessários para encontrar e identificar a fonte de uma comunicação são os seguintes:

a) No que diz respeito às comunicações telefónicas nas redes fixa e móvel:

i) O número de telefone de origem;

ii) O nome e endereço do assinante ou do utilizador registado;

b) No que diz respeito ao acesso à Internet, ao correio electrónico através da Internet e às comunicações telefónicas através da Internet:

i) Os códigos de identificação atribuídos ao utilizador;

ii) O código de identificação do utilizador e o número de telefone atribuídos a qualquer comunicação que entre na rede telefónica pública;

iii) O nome e o endereço do assinante ou do utilizador registado, a quem o endereço do protocolo IP, o código de identificação de utilizador ou o número de telefone estavam atribuídos no momento da comunicação.

3 - Para os efeitos do disposto na alínea b) do n.º 1, os dados necessários para encontrar e identificar o destino de uma comunicação são os seguintes:

a) No que diz respeito às comunicações telefónicas nas redes fixa e móvel:

i) Os números marcados e, em casos que envolvam serviços suplementares, como o reencaminhamento ou a transferência de chamadas, o número ou números para onde a chamada foi reencaminhada;

ii) O nome e o endereço do assinante, ou do utilizador registado;

b) No que diz respeito ao correio electrónico através da Internet e às comunicações telefónicas através da Internet:

i) O código de identificação do utilizador ou o número de telefone do destinatário pretendido, ou de uma comunicação telefónica através da Internet;

ii) Os nomes e os endereços dos subscritores, ou dos utilizadores registados, e o código de identificação de utilizador do destinatário pretendido da comunicação.

4 - Para os efeitos do disposto na alínea c) do n.º 1, os dados necessários para identificar a data, a hora e a duração de uma comunicação são os seguintes:

a) No que diz respeito às comunicações telefónicas nas redes fixa e móvel, a data e a hora do início e do fim da comunicação;

b) No que diz respeito ao acesso à Internet, ao correio electrónico através da Internet e às comunicações telefónicas através da Internet:

i) A data e a hora do início (**log in**) e do fim (**log off**) da ligação ao serviço de acesso à Internet com base em determinado fuso horário, juntamente com o endereço do protocolo IP, dinâmico ou estático, atribuído pelo fornecedor do serviço de acesso à Internet a uma comunicação, bem como o código de identificação de utilizador do subscritor ou do utilizador registado;

ii) A data e a hora do início e do fim da ligação ao serviço de correio electrónico através da Internet ou de comunicações através da Internet, com base em determinado fuso horário.

5 - Para os efeitos do disposto na alínea d) do n.º 1, os dados necessários para identificar o tipo de comunicação são os seguintes:

a) No que diz respeito às comunicações telefónicas nas redes fixa e móvel, o serviço telefónico utilizado;

b) No que diz respeito ao correio electrónico através da Internet e às comunicações telefónicas através da Internet, o serviço de Internet utilizado.

6 - Para os efeitos do disposto na alínea e) do n.º 1, os dados necessários para identificar o equipamento de telecomunicações dos utilizadores, ou o que se considera ser o seu equipamento, são os seguintes:

a) No que diz respeito às comunicações telefónicas na rede fixa, os números de telefone de origem e de destino;

b) No que diz respeito às comunicações telefónicas na rede móvel:

i) Os números de telefone de origem e de destino;

ii) A Identidade Internacional de Assinante Móvel (**International Mobile Subscriber Identity**, ou IMSI) de quem telefona;

iii) A Identidade Internacional do Equipamento Móvel (**International Mobile Equipment Identity**, ou IMEI) de quem telefona;

iv) A IMSI do destinatário do telefonema;

v) A IMEI do destinatário do telefonema;

vi) No caso dos serviços pré-pagos de carácter anónimo, a data e a hora da activação inicial do serviço e o identificador da célula a partir da qual o serviço foi activado;

c) No que diz respeito ao acesso à Internet, ao correio electrónico através da Internet e às comunicações telefónicas através da Internet:

i) O número de telefone que solicita o acesso por linha telefónica;

ii) A linha de assinante digital (**digital subscriber line**, ou DSL), ou qualquer outro identificador terminal do autor da comunicação.

7 - Para os efeitos do disposto na alínea f) do n.º 1, os dados necessários para identificar a localização do equipamento de comunicação móvel são os seguintes:

a) O identificador da célula no início da comunicação;

b) Os dados que identifiquem a situação geográfica das células, tomando como referência os respectivos identificadores de célula durante o período em que se procede à conservação de dados.

Artigo 5.º

Âmbito da obrigação de conservação dos dados

1 - Os dados telefónicos e da Internet relativos a chamadas telefónicas falhadas devem ser conservados quando sejam gerados ou tratados e armazenados pelas entidades referidas no n.º 1 do artigo 4.º, no contexto da oferta de serviços de comunicação.

2 - Os dados relativos a chamadas não estabelecidas não são conservados.

Artigo 6.º

Período de conservação

As entidades referidas no n.º 1 do artigo 4.º devem conservar os dados previstos no mesmo artigo pelo período de um ano a contar da data da conclusão da comunicação.

Artigo 7.º

Protecção e segurança dos dados

1 - As entidades referidas no n.º 1 do artigo 4.º devem:

a) Conservar os dados referentes às categorias previstas no artigo 4.º por forma a que possam ser transmitidos imediatamente, mediante despacho fundamentado do juiz, às autoridades competentes;

b) Garantir que os dados conservados sejam da mesma qualidade e estejam sujeitos à mesma protecção e segurança que os dados na rede;

c) Tomar as medidas técnicas e organizativas adequadas à protecção dos dados previstos no artigo 4.º contra a destruição acidental ou ilícita, a perda ou a alteração acidental e o armazenamento, tratamento, acesso ou divulgação não autorizado ou ilícito;

d) Tomar as medidas técnicas e organizativas adequadas para garantir que apenas pessoas especialmente autorizadas tenham acesso aos dados referentes às categorias previstas no artigo 4.º;

e) Destruir os dados no final do período de conservação, excepto os dados que tenham sido preservados por ordem do juiz;

f) Destruir os dados que tenham sido preservados, quando tal lhe seja determinado por ordem do juiz.

2 - Os dados referentes às categorias previstas no artigo 4.º, com excepção dos dados relativos ao nome e endereço dos assinantes, devem permanecer bloqueados desde o início da sua conservação, só sendo alvo de desbloqueio para efeitos de transmissão, nos termos da presente lei, às autoridades competentes.

3 - A transmissão dos dados referentes às categorias previstas no artigo 4.º processa-se mediante comunicação electrónica, nos termos das condições técnicas e de segurança fixadas em portaria conjunta dos membros do Governo responsáveis pelas áreas da administração interna, da justiça e das comunicações, que devem observar um grau de codificação e protecção o mais elevado possível, de acordo com o estado da técnica ao momento da transmissão, incluindo métodos de codificação, encriptação ou outros adequados.

4 - O disposto nos números anteriores não prejudica a observação dos princípios nem o cumprimento das regras relativos à qualidade e à salvaguarda da confidencialidade e da segurança dos dados, previstos nas Leis n.os 67/98, de 26 de Outubro, e 41/2004, de 18 de Agosto.

5 - A autoridade pública competente para o controlo da aplicação do disposto no presente artigo é a Comissão Nacional de Protecção de Dados (CNPD).

Artigo 8.º

Registo de pessoas especialmente autorizadas

1 - A CNPD deve manter um registo electrónico permanentemente actualizado das pessoas especialmente autorizadas a aceder aos dados, nos termos da alínea d) do n.º 1 do artigo anterior.

2 - Para os efeitos previstos no número anterior, os fornecedores de serviços de comunicações electrónicas ou de uma rede pública de comunicações devem remeter à CNPD, por via exclusivamente electrónica, os dados necessários à identificação das pessoas especialmente autorizadas a aceder aos dados.

Artigo 9.º

Transmissão dos dados

1 - A transmissão dos dados referentes às categorias previstas no artigo 4.º só pode ser autorizada, por despacho fundamentado do juiz de instrução, se houver razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter no âmbito da investigação, detecção e repressão de crimes graves.

2 - A autorização prevista no número anterior só pode ser requerida pelo Ministério Público ou pela autoridade de polícia criminal competente.

3 - Só pode ser autorizada a transmissão de dados relativos:

a) Ao suspeito ou arguido;

b) A pessoa que sirva de intermediário, relativamente à qual haja fundadas razões para crer que recebe ou transmite mensagens destinadas ou provenientes de suspeito ou arguido; ou

c) A vítima de crime, mediante o respectivo consentimento, efectivo ou presumido.

4 - A decisão judicial de transmitir os dados deve respeitar os princípios da adequação, necessidade e proporcionalidade, designadamente no que se refere à definição das categorias de dados a transmitir e das autoridades competentes com acesso aos dados e à protecção do segredo profissional, nos termos legalmente previstos.

5 - O disposto nos números anteriores não prejudica a obtenção de dados sobre a localização celular necessários para afastar perigo para a vida ou de ofensa à integridade física grave, nos termos do artigo 252.º-A do Código de Processo Penal.

6 - As entidades referidas no n.º 1 do artigo 4.º devem elaborar registos da extracção dos dados transmitidos às autoridades competentes e enviá-los trimestralmente à CNPD.

Artigo 10.º

Condições técnicas da transmissão dos dados

A transmissão dos dados referentes às categorias previstas no artigo 4.º processa-se mediante comunicação electrónica, nos termos das condições técnicas e de segurança previstas no n.º 3 do artigo 7.º.

Artigo 11.º

Destruição dos dados

1 - O juiz determina, oficiosamente ou a requerimento de qualquer interessado, a destruição dos dados na posse das autoridades competentes, bem como dos dados preservados pelas entidades referidas no n.º 1 do artigo 4.º, logo que os mesmos deixem de ser estritamente necessários para os fins a que se destinam.

2 - Considera-se que os dados deixam de ser estritamente necessários para o fim a que se destinam logo que ocorra uma das seguintes circunstâncias:

a) Arquivamento definitivo do processo penal;

b) Absolvição, transitada em julgado;

c) Condenação, transitada em julgado;

d) Prescrição do procedimento penal;

e) Amnistia.

Artigo 12.º

Contra-ordenações

1 - Sem prejuízo da responsabilidade criminal a que haja lugar nos termos da lei, constitui contra-ordenação:

a) A não conservação das categorias dos dados previstas no artigo 4.º;

b) O incumprimento do prazo de conservação previsto no artigo 6.º;

c) A não transmissão dos dados às autoridades competentes, quando autorizada nos termos do disposto no artigo 9.º;

d) O não envio dos dados necessários à identificação das pessoas especialmente autorizadas, nos termos do n.º 2 do artigo 8.º

2 - As contra-ordenações previstas no número anterior são puníveis com coimas de (euro) 1500 a (euro) 50 000 ou de (euro) 5000 a (euro) 10 000 000 consoante o agente seja uma pessoa singular ou colectiva.

3 - A tentativa e a negligência são puníveis.

Artigo 13.º

Crimes

1 - Constituem crime, punido com pena de prisão até dois anos ou multa até 240 dias:

a) O incumprimento de qualquer das regras relativas à protecção e à segurança dos dados previstas no artigo 7.º;

b) O não bloqueio dos dados, nos termos previstos no n.º 2 do artigo 7.º;

c) O acesso aos dados por pessoa não especialmente autorizada nos termos do n.º 1 do artigo 8.º

2 - A pena é agravada para o dobro dos seus limites quando o crime:

a) For cometido através de violação de regras técnicas de segurança;

b) Tiver possibilitado ao agente ou a terceiros o conhecimento de dados pessoais; ou

c) Tiver proporcionado ao agente ou a terceiros benefício ou vantagem patrimonial.

3 - A tentativa e a negligência são puníveis.

Artigo 14.º

Processos de contra-ordenação e aplicação das coimas

1 - Compete à CNPD a instrução dos processos de contra-ordenação e a respectiva aplicação de coimas relativas às condutas previstas no artigo anterior.

2 - O montante das importâncias cobradas em resultado da aplicação das coimas é distribuído da seguinte forma:

a) 60 % para o Estado;

b) 40 % para a CNPD.

Artigo 15.º

Aplicabilidade dos regimes sancionatórios previstos nas Leis n.os 67/98, de 26 de Outubro, e 41/2004, de 18 de Agosto

O disposto nos artigos 12.º a 14.º não prejudica a aplicação do disposto no capítulo vi da Lei n.º 67/98, de 26 de Outubro, e no capítulo iii da Lei n.º 41/2004, de 18 de Agosto.

Artigo 16.º

Estatísticas para informação anual à Comissão das Comunidades Europeias

1 - A CNPD transmite anualmente à Comissão das Comunidades Europeias as estatísticas sobre a conservação dos dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de uma rede pública de comunicações.

2 - Tendo em vista o cumprimento do disposto no número anterior, as entidades referidas no n.º 1 do artigo 4.º devem, até 1 de Março de cada ano, remeter à CNPD as seguintes informações, relativas ao ano civil anterior:

a) O número de casos em que foram transmitidas informações às autoridades nacionais competentes;

b) O período de tempo decorrido entre a data a partir da qual os dados foram conservados e a data em que as autoridades competentes solicitaram a sua transmissão; e

c) O número de casos em que as solicitações das autoridades não puderam ser satisfeitas.

3 - As informações previstas no número anterior não podem conter quaisquer dados pessoais.

Artigo 17.º
Avaliação

No fim de cada período de dois anos a CNPD, em colaboração com o Instituto das Comunicações de Portugal - Autoridade Nacional de Comunicações (ICP-ANACOM), procede a uma avaliação de todos os procedimentos previstos na presente lei e elabora um relatório detalhado, o qual pode incluir recomendações, cujo conteúdo deve ser transmitido à Assembleia da República e ao Governo.

Artigo 18.º
Produção de efeitos

A presente lei produz efeitos 90 dias após a publicação da portaria a que se refere o n.º 3 do artigo 7.º

Aprovada em 23 de Maio de 2008.
O Presidente da Assembleia da República, **Jaime Gama**.

Promulgada em 1 de Julho de 2008.
Publique-se.

O Presidente da República, **Aníbal Cavaco Silva**.
Referendada em 2 de Julho de 2008.
O Primeiro-Ministro, **José Sócrates Carvalho Pinto de Sousa**.