INSTITUTO SUPERIOR BISSAYA BARRETO

CIBERCRIME E PROVA DIGITAL

Maria da Conceição Fernandes Ribeiro

Dissertação apresentada para obtenção do grau de Mestre
em Ciências Jurídico-Forenses

Orientador:
Prof. Doutora Cristiane Reis
Co-Orientador:
Mestre Sara Moreira

Coimbra, fevereiro de 2015

Dedico aos que mais amo, aos meus pais, à minha irmã e ao Avelino

"Por onde os utilizadores navegam deixam rastos da sua presença online. O navegador que usa é como um saco de pão furado que deixa migalhas por toda a parte"

SAPOTEK

Índice

Introdução

A Internet é algo que entra na maioria das nossas casas. Quando assim não é, facilmente lhe acedemos em cafés, bibliotecas, escolas e universidades. Este acesso fácil à Internet pode expor um utilizador menos experiente a situações de vulnerabilidade.

O ciberespaço facilitou em muito o nosso quotidiano, desde logo: no comércio, na compra de produtos e serviços sem necessidade de deslocação; permitiu efetuar transações bancárias e controlar investimentos financeiros; agilizou comunicações e o acesso à informação; e possibilitou a prestação de serviços públicos ao cidadão, que pode ser notificado através desses meios se assim o desejar, e tudo isto, a um custo reduzido.

Nas últimas décadas, o nosso legislador tem vindo a manifestar uma crescente preocupação no combate ao Cibercrime. Neste intuito, a Lei 109/2009, de 15 de Setembro, que aprova a Lei do Cibercrime, fornece um elenco de novas disposições processuais sobre os meios de obtenção de prova, direcionadas precisamente para crimes previstos nessa lei, cometidos por meio de um sistema informático, ou em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico (artigo 11.º).

Com a globalização, os avanços tecnológicos expandem-se a uma velocidade outrora impensável por todo o mundo. Por outro lado, todo este avanço poderá ser um veículo para a lesão de bens jurídicos, visto facilitar o cometimento de crimes tradicionais e criando em simultâneo novas modalidades criminológicas. Mas, como afirma HELENA CARRAPIÇO, *"a tecnologia é uma faca de dois gumes: se pode ser manipulada no âmbito de atividades ilícitas, também pode ser utilizada para combater estas últimas"*[1], onde a polícia judiciaria e o tribunal serão os privilegiados na realização da justiça.

A informática trouxe novos desafios ao direito e criou novas divergências doutrinárias.

O presente trabalho que agora iniciamos, pretende dar um humilde contributo para o estudo e clarificação da Lei do Cibercrime, que trouxe novos ilícitos penais e novas disposições processuais ao Direito Penal.

Assim, tendo em vista a análise desta Lei, estruturamos o nosso estudo em três capítulos, o primeiro é dedicado ao Cibercrime. Neste, começamos por justificar a necessidade do processo

[1] CARRAPIÇO Helena, O Crime Organizado e as Novas Tecnologias: Uma faca de dois gumes, p. 177. Disponível em http://www.idn.gov.pt/publicacoes/nacaodefesa/textointegral/NeD111.pdf consultado em 04-02-2014

penal acompanhar as exigências sociais. Seguidamente, faremos uma descrição da evolução legislativa, de índole internacional e nacional, procuramos saber se o direito penal tradicional é suficiente para responder a estas novas criminalidades praticadas através da internet. Fazemos alusão a algumas das definições de cibercrime e especificamos alguns dos *"modus operandi"* desta criminalidade.

Pretendeu-se analisar as disposições materiais contidas na Lei 109/2009, de 15 de setembro. Procurou-se averiguar se é possível responsabilizar os prestadores de serviços pelas quebras de segurança e pelos conteúdos colocados na Internet que possibilitam a lesão de bens jurídicos.

O segundo capítulo é dedicado à prova em processo penal, começamos com uma breve referência aos diferentes modelos processuais a modos de entender o nosso atual sistema processual. Dedicamos uma breve análise aos princípios gerais relativos à prova onde questionamos se no nosso ordenamento jurídico admite a revelação coativa de *password*. Abordamos os novos meios de obtenção de prova trazidos pela lei do cibercrime, ou seja, da obtenção da prova eletrónico-digital e terminando com uma alusão ao regime das proibições de prova em processo penal e suas implicações.

No terceiro capítulo mencionamos o reforço que a Lei do Cibercrime trouxe à Cooperação Internacional.

Por último, tecemos algumas considerações conclusivas do nosso estudo.

1. Cibercrime

1.1. Necessidade do processo penal acompanhar novas exigências da sociedade

Aprendemos com Figueiredo Dias que "*as soluções concretas dos problemas básicos do Direito Processual Penal dependam fundamentalmente do estádio de evolução e desenvolvimento social e cultural de uma certa comunidade, do grau de maturidade logrado pela sua consciência jurídica, das conceções jurídicas de base e das concretas formas de atuação estadual que aí vigoram, enfim, na tradição histórica nela vivente (...). O direito processual penal é o produto de uma longa evolução dirigida à escolha dos meios conducentes à realização ótima das tarefas próprias da administração da justiça penal*."[2]

Como afirma Vieira Neves, *"(...) a efetivação do processo penal visa essencialmente a realização da justiça e a descoberta da verdade material, a protecção dos direitos fundamentais e o restabelecimento da paz jurídica, através da aplicação de uma sanção penal ao arguido que violou específicos bens jurídicos que ascenderam à discursividade penal"*[3].

O uso da informática é cada vez mais recorrente em todos os sectores da vida em sociedade, desde a defesa nacional, passando pela atividade científica, económica e financeira, na saúde, na educação, na segurança social e na Administração Pública em geral[4]. Porém surgem também práticas delituosas, abrindo portas à criminalidade organizada e podendo também colocar em risco sectores fulcrais à comunidade, tais como: distribuição de energia, transportes, telecomunicações, serviços de urgência e mercados financeiros[5].

Com o evoluir da nossa sociedade, hoje cada vez mais *"dependente"* do mundo dito *"virtual"*, sentiu-se necessidade de criminalizar certas condutas lesivas de bens jurídicos, praticadas através da informática. O conceito material de crime, como nos diz Figueiredo Dias[6],

---

[2] DIAS, Jorge de Figueiredo, Clássicos Jurídicos, Direito Processual Penal, pp.59 e 60

[3] NEVES, Rosa Vieira, A Livre Apreciação da Prova e a Obrigação de Fundamentação da Convicção (na Decisão Final Penal, p. 79

[4]MARTINS, A. G. Lourenço, Criminalidade Informática, Direito da Sociedade da Informação, vol. IV, Coimbra Editora, 2003. ISBN 972-32-1169-6, p. 9

[5] Cfr. Daniel Martin/ Frédéric-Paul Martin, "Nouvelles technoligies de l´information et criminalité, in Revue du Marché Commun et de lÚnion européenne, n.º 421, 1998, p. 544. Apud MARTINS, A. G. Lourenço, Criminalidade Informática, Direito da Sociedade da Informação, vol. IV, Coimbra Editora, 2003. ISBN 972-32-1169-6, p. 11.

[6] DIAS, Jorge de Figueiredo, Temas Básicos da Doutrina Penal: sobre os fundamentos da doutrina penal; sobre a doutrina geral do crime, Coimbra Editora, 2001. ISBN 972-32-1012-6, pp. 43-62.

é essencialmente constituído pela noção de bem jurídico, definido como sendo "*a expressão de um interesse, da pessoa ou da comunidade, na manutenção ou integridade de um certo estado, objeto ou bem em si mesmo socialmente relevante e por isso juridicamente reconhecido como valioso*", O conceito de crime não é sinónimo de bem jurídico, contudo, este último é o seu conteúdo material. O objetivo do direito penal é a tutela subsidiária (de "ultima ratio") de bens jurídicos com dignidade penal. Sublinhando, que a realidade do crime não depende somente do conceito material, mas também da construção social, depende da reação social, quer pelas instâncias formais (legislador, polícia, Ministério Público, Juiz), quer pelas instâncias informais (família, escolas, igrejas, clubes, vizinhos) de controlo.

Sentida a necessidade pela sociedade da regulamentação penal dos crimes informáticos, veio o nosso legislador criar normas subjetivas e adjetivas na Lei do Cibercrime (LC).

Já Faria Costa em 1998 reparou na necessidade de o Direito Penal regulamentar os crimes praticados na Internet, nas palavras do Autor, *"A informação automatizada é uma realidade tão essencial que se, por hipótese - e não se está, por certo, a entrar no domínio da ficção científica -, se bloqueasse, totalmente e à escala mundial, o fluxo informacional automatizado, ainda que por breves horas, todos convêm em considerar que o caos se institucionalizaria. Ora, uma realidade tão importante, tão essencial para se empregar a expressão exata, que gera e suporta interesses materiais de somas astronómicas, rapidamente se impõe, repete-se, como uma questão a que o direito penal, se bem que em ultima ratio, não pode ficar indiferente."*[7]

Tendo surgido novas exigências ao direito penal e ao processo penal fruto da globalização, veio o nosso legislador consagrar instrumentos que visam diminuir constrangimentos à investigação. Seguidamente, referiremos os contributos europeus que estiveram na génese da nossa lei.

1.2. Evolução Legislativa

Ulrich Sieber sintetizou o desenvolvimento da legislação sobre a criminalidade informática em quatro fases: inicialmente, e em primeiro lugar, surgem nos anos 70 as primeiras preocupações do legislador na proteção da vida privada, perante os novos métodos de recolha,

[7] COSTA, José Francisco de Faria, Algumas reflexões sobre o estatuto dogmático do chamado "Direito Penal Informático", Direito Penal da Comunicação, alguns escritos. Coimbra Editora, 1998. ISBN 972-32-0850-4, p. 116.

armazenamento, transferência e interconexão de dados pessoais potenciados pela informática; num segundo momento, nos anos 80 já se dedica especial atenção à delinquência económica específica da informática, aparecendo dificuldades em considerar propriedade uma realidade imaterial ou não tangível (manipulação de computador ou modificação de programas); ainda em meados dos anos 80 e em terceiro lugar, dão-se emendas legislativas destinadas a melhorar a salvaguarda da propriedade intelectual (como aconteceu com a proteção de programas de computador por meio do direito de autor e proteção da topografia dos produtos semicondutores); em quarto lugar, caminha-se para reformas legislativas no campo de direito processual de modo a facilitar investigações.[8] Lourenço Martins apresenta-nos ainda uma quinta vaga que respeita ao Direito Internacional, reconhecendo que nesta criminalidade, as fronteiras desaparecem e têm natureza planetária[9]. O direito deve ultrapassar, do mesmo modo, os limites fronteiriços e atuar à escala global, sob pena de insucesso.

O nosso legislador optou por seguir os quadros europeus para regulamentação interna. É nesse contexto que surge a Resolução n.º9(89) do Conselho da Europa transposta para o nosso ordenamento jurídico através da Lei da Criminalidade Informática n.º 109/91, de 17 de agosto.

Após os trágicos acontecimentos do 11 de Setembro de 2001, ouviram-se várias vozes no seio da União Europeia, a clamar por maiores margens de liberdade na investigação dos crimes de terrorismo, organização terrorista e criminalidade altamente organizada, havendo quem, defende-se inclusivamente, a ingerência nas telecomunicações pela polícia, desprovidas da prévia autorização do Juiz[10]. Foi então, aprovada a Lei n.º5/2002, de 11 de janeiro, sobre *"Medidas de combate à criminalidade organizada e económico-financeira, devendo salientar-se que logo no n.º1 esta lei estabelece "(...) um regime especial de recolha de prova, quebra de segredo profissional(...)"*[11].

A Decisão-Quadro 2005/222/JAI do Conselho, de 24 de fevereiro de 2005, relativa a ataques contra sistemas de informação, visa lutar contra a cibercriminalidade e promover a

[8] In U. Sieber, "Les crimes informatiques et d´autres crimes dans le domaine de la technologie informatique", in Revue Internationale de Droit Penel, AIDP, Érès, Colóquio de Wurzbourg, Outubro de 1992, p.55. Apud MARTINS, A. G. Lourenço, Criminalidade Informática, Direito da Sociedade da Informação, vol. IV, Coimbra Editora, 2003. ISBN 972-32-1169-6, pp. 10-11.
[9] MARTINS, A. G. Lourenço, Criminalidade Informática, Direito da Sociedade da Informação, vol. IV, Coimbra Editora, 2003. ISBN 972-32-1169-6, p. 10.
[10] SANTOS, Cristina Máximo dos, As novas tecnologias da informação e o sigilo das telecomunicações, Lisboa, 2004, separata da Revista do Ministério Público, N.º 99, p.115.
[11] Idem, p. 99.

segurança da informação, tendo como objetivo principal o reforço da cooperação entre as autoridades judiciárias e outras autoridades competentes, mediante uma aproximação das legislações de Direito Penal para combater os ataques contra sistemas de informação (nomeadamente pirataria, vírus e ataques de negação de serviço).

A Convenção sobre o Cibercrime do Conselho da Europa (primeiro Tratado Internacional sobre criminalidade sobre sistemas de computadores, redes ou dados), adotada em Budapeste em 23 de novembro de 2001, contou com a colaboração de peritos internacionais de todo o mundo com o objetivo de harmonizar legislações (processuais e materiais) de modo a facilitar a cooperação internacional nas investigações[12]. Nela se estabeleceram os seguintes objetivos: impedir os atos praticados contra a confidencialidade, integridade e disponibilidade de sistemas, redes e dados informáticos, bem como a utilização fraudulenta destes; assegurar a incriminação desses comportamentos, facilitando a eficácia do procedimento criminal tanto a nível nacional como internacional (conforme ao preâmbulo da referida convenção)[13].

Importará, também, referenciar a Lei n.º41/2007, de 18 de agosto, alterada pela Lei n.º 46/2012, de 29 de agosto, que dispõe quanto aos dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas. No artigo 6.º deste diploma consagrava (uma vez que fora revogado) que *"os dados de tráfego relativos aos assinantes e utilizadores tratados e armazenados pelas empresas que oferecem redes e ou serviços de comunicações eletrónicas devem ser eliminados ou tornados anónimos quando deixem de ser necessários para efeitos da transmissão da comunicação" (artigo 6.º n.º1) sendo "permitido o tratamento de dados de tráfego necessários à faturação dos assinantes e ao pagamento de interligações"* (artigo 6.º n.º2).

Ulteriormente, surge a Lei n.º 32/2008, de 17 de julho respeitante à conservação de dados nas comunicações eletrónicas, Lei da Retenção de dados de tráfego (que transpôs para a ordem jurídica interna a Diretiva n.º 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de março). Nesta Lei, o nosso legislador optou por um período máximo de um ano para a conservação dos dados enquanto a Diretiva 2006/24/CE tinha estabelecido como limite máximo o período de dois anos, tendo vindo a derrogar o referido artigo 6.º da lei 41/2007, de 18 de

[12] VERDELHO, Pedro; BRAVO, Rogério; ROCHA, Manuel Lopes – Leis do Cibercrime, Vol. 1, pp. 27, disponível em http://www.centroatl.pt/titulos/direito/imagens/excerto-ca-leisdoCibercrime1.pdf , consultado em 22-12-2013

[13] Diário da República, 1.ª série — N.º 179 — 15 de Setembro de 2009

agosto. Sublinhe-se, contudo, que a conservação de dados terá como finalidade exclusiva a investigação, deteção e repressão de crimes graves[14] por parte das autoridades competentes, e só pode ser ordenada ou autorizada por despacho fundamentado do Juiz (artigo 3.º n.ºs 1 e 3 da Lei de retenção de dados).

O nosso atual regime jurídico do Cibercrime provém essencialmente de influência europeia, mais precisamente da Convenção do Cibercrime, pelo que faremos algumas considerações sobre esta Convenção.

1.3. Convenção sobre Cibercrime do Conselho da Europa

Um estudo de 1997 que revelava grandes disparidades legislativas, fez com que representantes de quarenta e um Estados Membros do Conselho da Europa e quatro Estados exteriores (Estados Unidos da América, Canadá, Japão e África do Sul), elaborassem os trabalhos que resultaram na Convenção sobre Cibercriminalidade.[15]

Entre nós, através da Resolução da Assembleia da Republica n.º 88/2009 e Decreto do Presidente da República n.º 92/2009, ambos publicados a 15 de setembro, Portugal ratificou a Convenção sobre o Cibercrime adotada em Budapeste em 23 de novembro de 2001, o que levou a Assembleia da República a aprovar a atual Lei do Cibercrime, n.º 109/2009, de 15 de setembro realizando-se desse modo os compromissos internacionais a que o nosso Estado se vinculou nesse tratado de direito internacional.

Esta Convenção veio substituir a Recomendação n.º R (89) 9 sobre criminalidade relacionada com computadores. Foi criada a Convenção com o intuito de alcançar essencialmente três objetivos: harmonizar legislações e os crimes neles previstos; estender às jurisdições de Estados Membros determinados instrumentos processuais de produção de prova modernos e adequados à investigação da cibercriminalidade; por último, pretende facilitar a cooperação internacional e viabilizar investigações[16]. Com a globalização, os danos dos cibercrimes podem fazer-se sentir em várias jurisdições, devendo encarar-se esta criminalidade

[14] Para efeitos deste diploma, «crimes graves» são os 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 – alínea g) do n.º 1 do artigo 2.º

[15] MARTINS, A. G. Lourenço, Criminalidade Informática, Direito da Sociedade da Informação, vol. IV, Coimbra Editora, 2003. ISBN 972-32-1169-6, p.38.

[16] Ponto 16 do relatório explicativo da Convenção sobre Cibercrime disponível em http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/ETS_185_Portugese-ExpRep.pdf

à escala mundial, daí que seja manifesto na Convenção a necessidade dos vários Estados se dotarem de instrumentos processuais de produção de prova aptos a comprovar os crimes praticados em ambiente digital sendo que a cooperação internacional facilita e agiliza a recolha da prova.[17]

Lourenço Martins dá-nos, de um modo sucinto, uma análise dos principais objetivos a alcançar nesta convenção, que segundo o Autor:

> *"Visa prevenir os atentados à confidencialidade, integridade e disponibilidade dos sistemas informáticos, das redes e dos dados, bem como o uso fraudulento de tais sistemas, redes e dados, assegurando-se a incriminação dos comportamentos respectivos (direito penal material); visa ainda a adopção de poderes processuais suficientes para a detecção, investigação e perseguição contra estas infracções penais, quer no plano nacional quer internacional. Dedica particular atenção à pornografia infantil (artigo 9.º) cometida através das redes e às infracções relativas à propriedade intelectual e aos direitos conexos.*
>
> *No direito processual, avultam as medidas para conservação rápida de dados informáticos registados, conservação, divulgação rápida de dados relativos ao tráfico das mensagens, podendo haver injunções para divulgação de dados que estejam na posse ou sob controlo de alguém, nomeadamente de um fornecedor de serviços em rede, busca e apreensão de dados informáticos armazenados, colheita de dados relativos ao tráfico em tempo real, intercepção de conteúdos.*
>
> *Um outro capítulo é dedicado a regras de cooperação internacional, e dentro deste a disposições específicas sobre a conservação de dados informáticos e sua rápida divulgação, e entreajuda respeitante a poderes de investigação.*
>
> *Finalmente, as Partes providenciarão por um ponto de contacto permanente (rede 24/7) para assistência imediata nestas investigações, designadamente recolha de provas sob forma electrónica de uma infracção penal."*[18]

Dispõe no seu próprio texto, que a aplicação das disposições processuais deverá sempre observar as condições e salvaguardas dos direitos nacionais (artigo 15.º, n.º2) e dos instrumentos

[17] VERDELHO, Pedro, "A Convenção sobre Cibercrime do Conselho da Europa - Repercussões na Lei Portuguesa", in Direito da Sociedade da Informação, Coimbra Editora, 2006, pp. 257-258. ISBN 978-972-32-1411-3

[18] MARTINS, A. G. Lourenço, Criminalidade Informática, Direito da Sociedade da Informação, vol. IV, Coimbra Editora, 2003. ISBN 972-32-1169-6, pp. 38-39.

internacionais na área dos direitos humanos (artigo 15.º, n.º1). A convenção não afasta normas específicas de um mecanismo de investigação do direito interno e consagra que os meios de obtenção de prova deverão observar a regra da proporcionalidade.[19]

Esta Convenção veio inovar com a consagração nos artigos 16.º e 17.º, de dois meios expeditos de obtenção de prova (visa a obtenção de informação de forma rápida e urgente, dada a velocidade com que circula a informação em ambiente digital): a "*conservação expedita de dados informáticos armazenados*", aplicável a todo o tipo de dados guardados no computador ou sistema de computadores (inclui os dados de tráfego); e a "*conservação expedita e divulgação parcial de dados de tráfego*", aplicando-se somente aos dados de tráfego (permitem conhecer o percurso de uma determinada comunicação, aprofundamos melhor o que se entende por estes dados em momento ulterior). Enquanto que no primeiro consagra a conservação, no segundo admite-se a divulgação, pois, os demais dados (excetuando os dados de tráfego), como por exemplo o conteúdo de uma comunicação, só poderão ser revelados após serem cumpridas as *"(...)formalidades do tipo das exigidas para outras medidas potencialmente lesivas de interesses e direitos dos cidadão"*, ou seja, providos da devida ordem judicial. A preservação expedita de dados de tráfego e de conteúdo e a revelação expedita de dados de conteúdo vieram assim modificar as regras gerais consagradas na nossa legislação, relativamente ao sigilo nas comunicações.[20]

A Convenção consagra ainda a responsabilização das pessoas coletivas[21] nas situações de omissão de supervisão ou controlo da parte de um legal representante da pessoa coletiva, de

[19] VERDELHO, Pedro, A convenção do cibercrime do Conselho da Europa - repercussões na lei portuguesa...p. 269.

[20] VERDELHO, Pedro, "A Convenção sobre Cibercrime do Conselho da Europa - Repercussões na Lei Portuguesa", Direito da Sociedade da Informação, vol. VI Coimbra Editora, 2006, pp.269-271. ISBN 978-972-32-1411-3

[21] Paulo de Sousa Mendes apresenta os seguintes argumentos contra a responsabilidade criminal de pessoas colectivas: estas não têm capacidade de ação, nem capacidade de culpa e o Direito Penal não prescinde do princípio da culpa; a punição da pessoa colectiva prejudica os membros inocentes e os trabalhadores da empresa; "*As penas adequadas à natureza das pessoas colectivas são diferentes das penas cominadas às pessoas singulares (por exemplo: a dissolução da sociedade, o encerramento da empresa, etc.). É muito possível que a aplicação dessas sanções fosse compatível com um direito administrativo sancionatório, que é menos garantista e seria mais eficaz (o nosso direito de mera ordenação social). Por outro lado, muitas sociedades são utilizadas pelos titulares dos seus órgãos ou pelos seus representantes exclusivamente ou predominantemente para praticar ilícitos penais. Paradoxalmente, são estes os casos nos quais a necessidade de punição da pessoa colectiva é menos efectiva na prática porque os representantes da pessoa colectiva não exercem o seu direito de defesa no processo; por consequência, a mesma acaba sendo condenada (apesar da vigência do princípio in dubio pro reo), mas isso não quer dizer que a sanção seja eficaz, seja porque a pessoa colectiva não tem património, seja porque medidas como bloqueio das contas bancárias da pessoa colectiva não resultam efectivas, etc. em suma, é uma condenação meramente simbólica e cremos que tudo aquilo que é meramente simbólico é contraproducente em termos penais."*

alguém que sob a sua autoridade e em seu benefício pratique um ato ilícito[22] (artigo 12.º da Convenção e ponto 125 do Relatório Justificativo da Convenção sobre Cibercrime (versão Portuguesa[23])).

A responsabilização das pessoas coletivas, no direito penal português já é pacífica em termos legislativos há muito tempo. Hoje, tal expressamente consagrado no artigo 11.º do Código Penal, que surge em 2007. No entanto, já havia essa responsabilização pelo menos desde 1984 com o Decreto-lei n.º 28/84 de 20 de Janeiro, no âmbito das preocupações do direito penal económico[24]. A fundamentação para essa responsabilidade passa pela analogia material entre a culpa individual e a responsabilidade por culpa, relativamente às pessoas coletivas. Enquanto na imputabilidade formal (idade) o direito penal diz que o menor não ascende à discursividade penal, nas pessoas coletivas o Direito Penal "liberta, cria, expande" aquilo que os órgãos das pessoas coletivas assumem como vontade própria e, por isso, tem o direito penal legitimidade para as responsabilizar, penalmente.[25] É certo que não se pode aplicar penas de prisão às pessoas coletivas, mas estas poderão ser punidas, criminalmente, mediante penas especificamente aplicáveis às pessoas coletivas[26], tais como, admoestação, multa ou dissolução.

Já no artigo 3.º n.º1 da Lei da criminalidade informática (Lei n.º 109/91, de 17 de Agosto, alterada pelo Decreto-Lei n.º 323/2001, de 17 de Dezembro, e revogada pela Lei n.º 109/2009, 15 de setembro), o nosso legislador consagrou que *"As pessoas colectivas, sociedades e meras associações de facto são penalmente responsáveis pelos crimes previstos na lei, quando cometidos em seu nome e no interesse colectivo pelos seus órgãos ou representantes".*

Basta, portanto, que o agente individual tenha atuado no desempenho da função ou por causa dela, à semelhança da responsabilidade civil e delitual da sociedade comercial por atos ilícitos de quem legalmente a represente (artigo 6.º n.º5 do Código das Sociedades Comerciais), assim como na responsabilidade do comitente pelos atos do comissário, quando o facto seja

---

MENDES, Paulo de Sousa, *" A responsabilidade de pessoas colectivas no âmbito da criminalidade informática em Portugal",* in Direito da Sociedade da Informação, Vol. IV, Coimbra Editora, 2003. ISBN 972-32-1169-6. pp.398-399

[22] VERDELHO, Pedro, "A Convenção sobre Cibercrime do Conselho da Europa - Repercussões na Lei Portuguesa", Direito da Sociedade da Informação, pp. 267-268

[23] Conselho da Europa, Minuta em português do Relatório Explicativo da Convenção sobre o Cibercrime, de 23-11-2001, disponível em http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/ETS_185_PortugeseExpRep.pdf, consultado em 18-12-2013

[24] COSTA, José de Faria, Direito penal económico, Quarteto, Coimbra 2003, ISBN 989-558-004-5, p. 49

[25] Idem, p. 51

[26] Idem, p.97

praticado por trabalhador subordinado no exercício das funções, ou seja, quando o facto caiba na definição do objeto do próprio contrato de trabalho, haverá imputação da responsabilidade da pessoa coletiva[27].

No nosso ordenamento jurídico, admite-se a possibilidade destas responderem criminalmente, a título excecional (artigo 11.º do Código Penal), nos crimes fiscais, crimes contra a economia, crimes de terrorismo e nos crimes informáticos (artigo 9.º Lei do Cibercrime, Lei 109/2009, de 15 de setembro).

Da transposição para a ordem jurídica Interna da Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação, e da adaptação do direito interno à Convenção sobre Cibercrime do Conselho da Europa, veio a Lei 109/2009, de 15 de Setembro (doravante designada Lei do Cibercrime) consagrar disposições penais materiais e processuais, disposições relativas à cooperação internacional em matéria penal, relativas ao domínio do Cibercrime e recolha da prova em suporte eletrónico (n.º 1 da referida Lei).

De seguida, tentaremos responder à seguinte questão: o direito penal primário é suficiente para regulamentar os crimes ditos informáticos ou pelo contrário exige-se a autonomização do Direito Penal Informático?

1.4. Regulamentação do cibercrime: divergências doutrinárias relativamente à sua localização

Surgem divergências doutrinárias quanto à questão a saber se o Direito Penal Clássico será suficiente para responder à complexidade que envolve os crimes praticados no ambiente Web. Entre os Autores que respondem positivamente, temos: José de Faria Costa[28]; Ana Mercedes Oubinã[29]. Outros Autores defendem que deveria existir um Direito Penal da

[27] MENDES, Paulo de Sousa, *"A responsabilidade de pessoas colectivas no âmbito da criminalidade informática em Portugal" op. cit.*. pp. 402-403

[28] COSTA, José Francisco de Faria, Algumas reflexões sobre o estatuto dogmático do chamado "Direito Penal Informático", Direito Penal da Comunicação, alguns escritos. Coimbra Editora, 1998. ISBN 972-32-0850-4, pp.103-119

[29] *In* OUBIÑA, Ana Mercedes da Silva claro, "As telecomunicações, a vida privada e o direito penal", Direito Penal Hoje - Novos desafios e novas respostas, Organizadores: Manuel da Costa Andrade e Rita Castanheira Neves, Coimbra Editora, 2009, p.36. *Apud LEITE, Ana Raquel Gomes, CRIMINALIDADE INFORMÁTICA – INVESTIGAÇÃO E MEIOS DE OBTENÇÃO DE PROVA. Dissertação apresentada no âmbito do 2.º Ciclo de*

Informática, ou seja um direito penal secundário, desde logo: Vladimir Aras[30]; Silva Dias; Ana Raquel Gomes Leite31; Benjamim Silva Rodrigues[32]; Pedro Simões Dias (defende um Direito das Tecnologias da Informação e da Comunicação).[33]

Concordamos com Faria Costa ao afirmar que a criminalidade informática consiste numa área específica de incriminação penal, podendo com os instrumentos do direito penal clássico continuar a estudar-se essa área específica da incriminação, referente à informática[34]. "*O direito penal informático não deve ser visto como afirmação inequívoca de uma autónoma e nova disciplina jurídico-penal, mas antes como indício, nominativo ou não, de uma precisa área da incriminação penal.*"[35] Segundo o Autor, para que ocorresse uma autonomização do direito penal informático deveria autonomizar-se do mesmo modo, um direito penal patrimonial, um direito penal dos crimes contra a vida, um direito penal dos crimes contra a integridade física, e assim sucessivamente. Ou seja, teríamos uma parte especial com diferentes e autónomas áreas ou zonas de incriminação. Contudo, admite também, que as novas áreas de incriminação podem ter uma determinada autonomia, acrescentando que (essas novas áreas de incriminação) se *"sustentam"* daquilo que a parte geral do Código Penal lhes dá, a título gratuito.[36]

Estudos em Direito, Faculdade de Direito da Universidade de Coimbra, sob orientação da Professora Doutora Helena Isabel Gonçalves Moniz Falcão Oliveira,Coimbra 2013, p.16

[30] *In* ARAS, Vladimir, "Crimes de informática - uma nova criminalidade", 2001, disponível na Internet, in http://informatica-juridica.com, consultado em 29/01/2013. *Apud LEITE, Ana Raquel Gomes, CRIMINALIDADE INFORMÁTICA – INVESTIGAÇÃO E MEIOS DE OBTENÇÃO DE PROVA. Dissertação p. 15*

[31] *LEITE, Ana Raquel Gomes, CRIMINALIDADE INFORMÁTICA – INVESTIGAÇÃO E MEIOS DE OBTENÇÃO DE PROVA. Dissertação apresentada no âmbito do 2.º Ciclo de Estudos em Direito, Faculdade de Direito da Universidade de Coimbra, sob orientação da Professora Doutora Helena Isabel Gonçalves Moniz Falcão Oliveira, p.17*

[32] Nas palavras do Autor: *"O actual processo penal português padece de algumas insuficiências que trazem algumas dificuldades à efectiva operatividade de um modelo dinâmico-reversivo. De facto, todo o processo penal foi pensado para o "ambiente físico", pelo que, nalgumas circunstâncias, só a custo os vários meios de (obtenção da prova) poderão ser de alguma utilidade em sede de obtenção da prova electrónico-digital".* RODRIGUES, Benjamim Silva - DIREITO PENAL PARTE ESPECIAL, Tomo I, DIREITO PENAL INFORMÁTICO DIGITAL, Contributo para a Fundamentação da sua Autonomia Dogmática e Científica à Luz do novo Paradigma de Investigação Criminal: a Ciencia Forense Digital e a Prova Digital, com prefácio da D.ª Sara Antunes. [S.L.]: Coimbra Editora, Limitada, 2009. ISBN: 978-989-95779-5-4, p. 733.

[33] DIAS, Pedro Simões, *"O «Hacking» enquanto crime de acesso ilegítimo. Das suas especialidades à utilização das mesmas para a fundamentação de um novo direito",* p. 56, consultado em http://www.uria.com/documentos/publicaciones/1580/documento/art04.pdf?id=2108, consultado em 10-10-2014.

[34] COSTA, José Francisco de Faria, Algumas reflexões sobre o estatuto dogmático do chamado "Direito Penal Informático", Direito Penal da Comunicação, alguns escritos,p. 117

[35]Idem, p.119

[36] COSTA, José de Faria, Direito penal económico, Quarteto, Coimbra 2003, ISBN 989-558-004-5, p. 24

Dias Ramos[37], pelo contrário, defende *"(...)que se crie legislação Penal Informático-Digital, que abarque num só código normas de direito objetivo e subjetivo. Que se cortem as amarras com situações do passado, mormente que se deixe de considerar que o correio eletrónico seja comparável com o correio tradicional ou que exista a tentação de equiparar formas antigas de cometimento de crimes com as novíssimas formas de atuação a nível informático".*

Já Pedro Verdelho[38], defendeu que a opção legislativa mais coerente com a tradição portuguesa seria a elaboração de um código sectorial, à semelhança do que ocorreu *"(...)com a criminalidade relacionada com estupefacientes, com os crimes contra a economia e com a criminalidade fiscal, cujos quadros penais e processuais penais, diferentes dos previstos na legislação penal e processual penal, estão definidos em diplomas especiais"*. Aponta ainda duas outras razões: *"(...)por um lado, a incoveniência de ver em diplomas estruturantes do ordenamento penal regras especiais, de excepção, apenas aplicáveis a uma parcela muito restrita dos tipos de ilícitos; por outro, a conveniência prática, para os operadores judiciários, de ver sistematizados todos os normativos referentes a um sector específico da criminalidade."*

Dá Mesquita[39] refuta este entendimento (argumentos também apresentados na exposição de motivos da Lei do Cibercrime), argumentando a originalidade desta Lei em matéria de regras processuais, denotando que esta não prevê normas especiais em sentido técnico-jurídico, mas regras de obtenção de prova em suporte eletrónico, aplicáveis a um elenco de crimes mais amplo do que os crimes de tabela das escutas telefónicas. Alega ainda, que os normativos processuais em causa, não se reportam a *"um sector específico da criminalidade"*, pelo que é de «conveniência prática» dos operadores judiciários, que os mesmos não estejam inseridos em legislação aparentemente dirigida apenas *"a um sector específico da criminalidade"*. Conclui o seguinte *"(...) impunha-se a integração das regras no código de Processo Penal, pois, para usar as mesmas expressões da exposição de motivos, essa seria «a opção mais coerente com a tradição portuguesa», em face da «geral inconveniência» de ver dispersas em leis extravagantes regras gerais carecidas de enquadramento no Código de Processo Penal*

[37] RAMOS, Armando Dias, A prova digital em processo penal: o correio electrónico, chiado editora, 1.º ed. Novembro 2014, ISBN 978-989-51-2383-4, p. 114

[38] VERDELHO, Pedro, "A Convenção sobre Cibercrime do Conselho da Europa - Repercussões na Lei Portuguesa", Direito da Sociedade da Informação p. 276

[39] MESQUITA, Paulo Dá, Processo Penal, Prova e Sistema Judiciário, 1.ª ed: Setembro 2010, Coimbra Editora. ISBN 978-972-32-1842-8, pp.98-99

enquanto «diploma estruturante», e a «conveniência prática, para os operadores judiciários, de aí ter sistematizados todos os normativos» que não são apenas aplicáveis «a um sector específico da criminalidade» no Código de Processo Penal".[40]

1.5. Possíveis definições de Cibercrime

São várias as expressões utilizadas para designar crimes da internet: cibercrime; crime digital; crime informático; crime informático-digital. Não há consenso quanto à expressão, à definição, nem quanto à tipologia e classificação destes crimes.[41] Persiste a inexistência de um conceito de *"criminalidade informática"* expressamente consagrado na legislação, ou uniformemente sedimentado na doutrina e jurisprudência.[42]

De acordo com a Comissão Europeia, Cibercrime "*são os actos criminosos praticados com recurso a redes de comunicação electrónicas e sistemas de informação ou contra este tipo de redes e sistemas". Esta realidade consegue abarcar as formas tradicionais de crime, publicação de conteúdos ilícitos em meios de comunicação eletrónicos, e crimes exclusivos das redes eletrónicas, isto é, ataques contra sistemas de informação, bloqueio de serviços e pirataria. Sendo que "os crimes podem ser praticados em grande escala e pode ser muito grande a distância entre o acto criminoso e os seus efeitos*".[43]

Apresentam-se aqui diversas definições do cibercrime existentes no nosso mundo académico. Neste sentido, Garcia Marques e Lourenço Martins alertam para o facto de inexistir uma definição concreta de "criminalidade informática", e acrescentam que "*é frequente encarar a criminalidade informática como todo o acto em que o computador serve de meio para atingir um objectivo criminoso ou em que o computador é alvo simbólico desse acto ou em que o computador é objecto do crime*"[44].

---

[40] Idem, p.101.

[41] In SILVA RODRIGUES, Direito Penal Especial, Direito Penal Informático-Digital, Coimbra, 2009, p.168-194; SOFIA CASIMIRO, A responsabilidade civil pelo conteúdo da informação transmitida pela Internet, Coimbra, Almedina, 2000, p. 19. Apud DIAS, Vera Elisa Marques – A problemática da investigação do Cibercrime. p. 65, disponível em http://www.datavenia.pt/ficheiros/edicao01/datavenia01_p063-088.pdf, consultado em 29-01-2014

[42] VENÂNCIO, Pedro Dias, - Lei do Cibercrime - anotada e comentada, p. 16

[43] Conforme Boletim da Ordem dos Advogados, mensal n.º65, Abril 2010. CIBERCRIME *"pode ser muito grande a distância entre o acto criminoso e os seus efeitos"*. P.36, disponível em http://www.oa.pt/upl/%7B3d49f105-1ff4-426f-8c50-ddaee1b8acbb%7D.pdf, consultado em 26-11-2013

[44] In GARCIA MARQUES E LOURENÇO MARTINS, Direito da informática, 2.ª ed., Almedina, Coimbra, 2006, pp. 639 e ss. APUD VENÂNCIO, Pedro Dias, LEI DO CIBERCRIME, ANOTADA E COMENTADA, 1.ª ed., Coimbra Editora, p. 16

Parece-nos que deve ser dado um sentido amplo ao termo computador, de modo a abranger outras tecnologias (telemóveis, tablets, etc), ou seja, dispositivos com capacidade de computação. Já na Convenção sobre o cibercrime, na alínea a) do artigo 1.º é-nos dado o conceito de sistema informático, tendo " *(...) como elemento fulcral um ou mais computadores podendo ser constituído por dispositivos de qualquer tipo, desde que estejam interconexados ou relacionados e processem dados de forma automática, através de utilização de um programa*". Na nossa atual Lei do Cibercrime, é considerado "*«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"* (artigo 2.º alínea a) da Lei 109/2009 de 15 de Setembro), abarcando, igualmente, redes não constituídas por computadores (entre outras, redes de terminais de pagamento, telefones ou outro tipo de dispositivos periféricos).[45]

Romeo Casabona[46], define Cibercrime como *"el conjunto de conductas relativas al acceso, apropiación, intercambio y puesta a disposición de información en redes telemáticas, las cuales constituyen su entorno comisivo, perpetradas sin el consentimiento o autorización exigibles o utilizando información de contenido ilícito, pudiendo afectar a bienes jurídicos diversos de naturaleza individual o supraindividual".*

O termo *"Cibercrime"* define de forma genérica uma panóplia de crimes praticados com recurso a novas tecnologias de informação e de comunicação, ou seja, cabem naquele conceito atuações criminais clássicas, mas também novos crimes. Deve distinguir-se a *"criminalidade informática"* (a informática é alvo do crime) da *"criminalidade praticada com recurso a meios informáticos"* (a informática é meio de execução do crime)[47].

---

[45]VERDELHO, Pedro, *"A Convenção sobre Cibercrime do Conselho da Europa - Repercussões na Lei Portuguesa"*, Direito da Sociedade da Informação, Coimbra Editora, 2006, p. 260. ISBN 978-972-32-1411-3

[46] *In ROMEO CASABONA, « De los delitos informáticos al Cibercrimen. Una aproximación conceptual y político-criminal», pg.11. Apud DÍAZ, Leyre Hernández, Aproximación a un concepto de derecho penal informático, in DERECHO PENAL INFORMÁTICO, Primera edición, 2010, Civitas, Editorial Aranzadi, ISBN 978-84-470-3429-1, p.44*

[47] *VERDELHO, Pedro; BRAVO, Rogério; ROCHA, Manuel Lopes – Leis do Cibercrime, Vol. 1, pp. 27-28, disponível em* http://www.centroatl.pt/titulos/direito/imagens/excerto-ca-leisdoCibercrime1.pdf, consultado em 22-12-2013

Os crimes de sabotagem informática, crime de dano relativo a dados ou programas informáticos, e o crime de interceção ilegítima são considerados por Pedro Simões Dias[48] como sendo *"crimes informáticos técnicos"*, que se podem definir como *"as condutas criminalmente desvaliosas, simultaneamente praticadas com a utilização técnica de estruturas e sistemas informáticos e em que estes bens constituem o objecto da acção, lesando o bem jurídico segurança dos sistemas informáticos".* O mesmo autor refere-se à criminalidade informática como sendo criminalidade levitacional *("a criminalidade informática é levitacional por oposição à criminalidade tradicional"*)[49], sendo os tipos levitacionais de cariz técnico a sabotagem informática, o acesso ilegítimo e a interceção ilegítima[50].

A cibercriminalidade consiste num facto praticado com recurso às tecnologias de informação[51] e pode abarcar inúmeras condutas ilícitas, "*desde el delito económico, como el fraude informático, el robo, la falsificación, el computer hacking, el espionaje informático, el sabotaje, la extorsión informática, la piratería comercial y otros crímenes contra la propiedad intelectual, la invasión de la intimidad, la distribución de contenidos ilegales y dañosos, la incitación a la prostitución y otros crímenes contra la moralidad, y el crimen organizado (Rodríguez Bernal, 2007: 9). Pero a diferencia de otros tipos de delitos, el cibercrimen se vale del ciberespacio para realizar sus actividades delictivas."*[52]

Pedro Verdelho reconhece três grupos distintos naquilo que vulgarmente se vê referido como cibercrime: os crimes que recorrem a meios informáticos (abrange infrações descritas no Código Penal e, portanto, sistematicamente não autonomizadas, tais como a devassa por meio da informática - prevista no artigo 193.º, revogado tacitamente pelos artigos 7.º n.º 1 e artigo 3.º alínea b) da Lei n.º 67/98 e o crime de burla informática e nas comunicações com previsão no artigo 221.º); os crimes referentes à proteção de dados pessoais (assegurada pela Lei 67/98, de

[48]DIAS, Pedro Simões, "O «Hacking» enquanto crime de acesso ilegítimo. Das suas especialidades à utilização das mesmas para a fundamentação de um novo direito", p. 5 7(p.233 se consultar no manual da nota de rodapé 34), disponível em http://www.uria.com/documentos/publicaciones/1580/documento/art04.pdf?id=2108, consultado em 10-10-2014

[49] DIAS, Pedro Simões, O "Hacking" enquanto crime de acesso ilegítimo. Das suas especialidades à utilização das mesmas para a fundamentação de um novo direit, in Direito da Sociedade da Informação, vol. VIII, Coord. Prof. Doutor José de Oliveira Ascenção, Coimbra Editora, 2009. ISBN 978-972-32-1710-0,p. 232

[50] Idem, p.240

[51] *SANTOS, Paulo; BESSA, Ricardo; PIMENTEL, Carlos, CYBERWAR: O fenómeno, as tecnologias e os actores, p. 5*

[52] MEDERO, Gema Sánchez. Cibercrimen, Ciberterrorismo y Ciberguerra: Los Nuevos Desafíos Del s. XXI. 239-267. Revista Cenipec. 31.2012. Enero- Diciembre. ISSN: 0798-9202. pág 244, disponível em http://www.saber.ula.ve/bitstream/123456789/36770/1/articulo9.pdf, consultado em 25-08-2014

26 de Outubro que prevê ilícitos criminais específicos); e os crimes informáticos propriamente ditos[53] (aqueles que constam na Lei n.º 109/2009, de 15 de Setembro).

São muitos e os mais variados os *"modi operandi"* neste tipo de criminalidade, mencionamos de seguida alguns dos mais conhecidos.

A *"técnica do salame"*, onde o autor retira pequeníssimas importâncias de várias contas (cêntimos) de terceiros, com pouca alteração dos saldos, movimentando-as para uma conta em seu nome ou de um cúmplice[54].

A *"bomba lógica"* ou "programa-*crash*", que consiste em instruções clandestinas para atuação em determinado momento, logo que verificada certa condição ou evento[55].

O *"Vírus"*, que é um conjunto de instruções que se podem reproduzir rapidamente, e que levam à inutilização de dados, ficheiros e programas, ou mesmo à paralisação de um sistema informático[56].

O *"Phishing"*[57], que em linguagem de computação, *"(...)é uma forma de fraude eletrônica, caracterizada por tentativas de adquirir dados pessoais de diversos tipos; senhas, dados financeiros como número de cartões de crédito e outros dados pessoais. O ato consiste em um fraudador se fazer passar por uma pessoa ou empresa confiável enviando uma comunicação eletrônica oficial. Isto ocorre de várias maneiras, principalmente por email, mensagem instantânea, SMS, dentre outros. Como o nome propõe (Phishing), é uma tentativa*

[53]Relativamente aos crimes informáticos propriamente ditos o autor fez referência à Lei 109/91, de 17 de Agosto, que a data se encontrava em vigor, sendo só ulteriormente substituída pela Lei 109/2009, de 15 de Setembro. VERDELHO, Pedro, *"Cibercrime"*, in Direito da Sociedade da Informação (IV), pp. 356-368

[54] MARTINS, A. G. Lourenço, Criminalidade Informática, Direito da Sociedade da Informação, vol. IV, Coimbra Editora, 2003. ISBN 972-32-1169-6, pp.13-14

[55] Idem, Ibidem.

[56] MARTINS, A. G. Lourenço, Criminalidade Informática, Direito da Sociedade da Informação, vol. IV, Coimbra Editora, 2003. ISBN 972-32-1169-6, pp.13-14

[57] *"Esta actividade é facticamente complexa e traduz-se, antes de mais, na remessa massiva de mensagens de correio electrónico (utiliza portanto a técnica do spam). Tais mensagens incluem um link para uma página na WWW. Esta página será normalmente a reprodução aproximada de uma outra (esta autêntica), por exemplo de um banco ou de uma entidade emissora de cartões de crédito. Conterá elementos identificadores da entidade autêntica e imagens a ele referentes. Porém, será falsa, por ser construída e gerida por terceiros, sem autorização da entidade cujos sinais pretende imitar. Se a vítima usar o link para aceder à página falsa, deparar-se-à com uma página parecida com a do seu banco, ou da entidade gestora do seu cartão de crédito. Desta forma, os criminosos obtêm dados confidênciais que lhes permitirão aceder às contas bancárias das vítimas , transferindo o dinheiro que aí houver para contas suas. Ou utilizar os respectivos cartões de crédito, em seu proveito."* VERDELHO, Pedro, Phishing e outras formas de defraudação nas redes de comunicação, in Direito da Sociedade da Informação, Vol. VIII, coord. Prof. Doutor José de Oliveira Ascensão, Coimbra Editora, 2009. ISBN 978-972-32-1710-0, p. 413.

de um fraudador tentar "pescar" informações pessoais de usuários desavisados ou inexperientes".[58]

Por sua vez, o *"Pharming"*, através de *spam* do correio eletrónico, envia ficheiros ocultos, que se auto-instalam nos computadores ou sistemas informáticos das vítimas, e que uma vez instalados, alteram de modo oculto e automático, os arquivos do sistema. Desde logo ficheiros que contém os favoritos e o registo de *cookies*[59]. O objetivo final visa que quando o utilizador acede a um determinado *site*, o sistema reencaminha-o para um outro site semelhante, mas falso[60] de forma muito semelhante ao *Phishing*;

"Keylogger" é um programa que uma vez instalado no computador, passa a identificar todas as nossas batidas no teclado, e assim, quando escrevemos um endereço eletrónico (link) no nosso *browser*, ele envia essa informação ao seu detentor ou criador, que pode estar em qualquer parte do mundo[61].

Ataques do tipo *Distributed Denial of Service* ou DDoS são capazes de levar a que *websites* e redes fiquem indisponíveis[62].

Outros termos serão apresentados de forma mais aprofundada ao longo deste trabalho.

As condutas quando praticadas mediante recurso à Internet poderão também levar à prática de ilícitos criminais tais como: burlas no arrendamento de imóveis e na venda de bens, vendas ilegais, jogo ilegal, difamações e injúrias (artigos 180.º e 182.º do CP) praticadas através da Internet, furto de identidade, danos nos sistemas informáticos, pornografia infantil (artigos 188.º, 113.º e 172.º, n.º3 alínea d) do CP), crimes contra a auto determinação pessoal (*cybertalking*, *cyberbulling*).[63] Ameaça (artigo 153.º n.º1 CP), discriminação racial ou religiosa (artigo. 240.º do CP), casinos virtuais ilegais e devassa por meio da informática (artigo. 193.º do CP).

---

[58] Retirado da Wikipédia, disponível em http://pt.wikipedia.org/wiki/Phishing, consultado em 01-12-2014

[59] É *"um pedaço de informação que um site da web pode colocar no disco rígido do seu computador, para (por exemplo) "reconhecê-lo" num futuro acesso. Um cookie pode ser utilizado para manter um rastreio das suas visitas num site. Normalmente, é necessárioautorizar a gravação de cookies, mas isso depende da configuração de cada browser*.MATOS, José A. de, dicionário de informática e novas tecnologiaspp.95-96

[60] VERDELHO, Pedro, Phishing e outras formas de defraudação nas redes de comunicação,op.cit. p. 415

[61] GLENNY, Misha, DARK MARKET, Como os hackers se tornaram a nova máfia, do autor do bestseller McMÁFIA, traduzido por Michelle Hapetian, civilização Editora, 2012, ISBN 978-972-26-3443-4, p. 49

[62] Idem, p.18

[63] Cfr. SANTOS, Paulo; BESSA, Ricardo; PIMENTEL, Carlos , CYBERWAR: O fenómeno, as tecnologias e os actores, pp.18-23

As violações de direitos tanto podem incidir sobre bens coletivos, pondo em causa interesses da comunidade (pedofilia, incitamento ao terrorismo), como em bens privados, na lesão de direitos de uma pessoa singular[64]. Fala-se hoje no receio da chamada *"guerra cibernética"*, consistindo na possibilidade de um Estado através da internet *"invadir"* outro Estado e ao mesmo tempo inutilizar as tecnologias, comunicações, redes de transporte e redes de abastecimentos de combustíveis com consequências nefastas para os cidadãos (tais como falha na entrega de produtos essenciais, alimentos, medicamentos, etc.)[65].

"O vírus tornou-se a arma dos tempos tecnológicos"[66]. Sendo um programa informático que consiste num conjunto de instruções que se podem reproduzir rapidamente e levam à inutilização de dados, ficheiros e programas, ou mesmo à paralisação de um sistema informático, com ampla capacidade de difusão[67]. "*A distinção mais simples, ainda que incompleta, entre vírus, worms e trojans, conhecidos colectivamente por "malware", faz-se com base no seu método de transmissão - os vírus através de anexos de e-mail contaminados, os trojans, através de downloads, enquanto os worms têm a capacidade de se reproduzirem num computador anfitrião, para, depois, se servirem dos programas de comunicação neles existentes para se transmitirem a outras máquinas. Mas, na sua essência, todos eles causam danos no computador.*[68]"

Para melhor compreendermos o conceito em apreço não nos podemos eximir de falar nas várias designações atribuídas aos agentes que praticam estes crimes: os *hackers* que acedem a sistemas de informação sem a tal estarem autorizados, criam e utilizam aplicações maliciosas ("Vírus informáticos"); os *Phreakers* manipulam centrais telefónicas de modo a utilizarem as redes de comunicações de modo ilegítimo (*blackboxing* - consiste na perturbação das linhas telefónicas visando impedir ou diminuir a taxa a pagar à operadora); os *Crackers* descompilam ou removem proteções de programas de modo a terem acesso gratuito e sem restrições; os *Lammers* utilizam ou vendem os trabalhos dos *hackers*; os *Cypherpunks* ou criptoanarquistas

[64] ASCENÇÃO, José de Oliveira, "O Ilícito em rede", Direito da Sociedade da Informação e Direito de Autor, APDI, vol. X, Coimbra Editora, 2012, p.111. ISBN 978-972-32-2018-6
[65] Documentário do canal História, O Livro dos Segredos T3 - Ep. 32.
[66] PEREIRA, Joel Timóteo Ramos, Direito da Internet e Comércio Electrónico, Quid Iuris? Sociedade Editora, Lisboa, 2001. ISBN 972-724-113-1. p. 249
[67] MARTINS, A. G. Lourenço, Criminalidade Informática, Direito da Sociedade da Informação, vol. IV, Coimbra Editora, 2003. ISBN 972-32-1169-6, p. 14
[68] GLENNY, Misha, DARK MARKET, Como os *hackers* se tornaram a nova máfia, op cit. p. 49

recorrem à encriptação para protegerem comunicações maliciosas numa rede informática pertencente a terceiros; entre outros que praticam ilícitos através da internet.[69]

"*O crime na internet evoluiu do simples "hacker", em regra, inocente e aventureiro que desafia as barreiras pelo simples prazer de as ultrapassar, para um multimilionário negócio do crime, assumindo em determinados casos uma nova figura de terrorismo e do crime organizado (pedofilia, droga, terrorismo internacional) "*[70].

Face ao que se expôs supra, poderão os prestadores de serviços ser responsabilizados penalmente pelas quebras de segurança e conteúdos disponibilizados na Internet suscetíveis de lesarem bens jurídicos?

1.6. Prestadores de serviços: responsabilização pelas quebras de segurança e conteúdos disponibilizados

Relativamente à responsabilização dos prestadores intermediários de serviços[71] pelas quebras de segurança que permite a lesão de bens jurídicos dos utilizadores/vítimas, temos a Lei do Comércio Electrónico, Decreto-Lei 7/2004, de 7 de janeiro (alterado pelo Decreto-Lei n.º 62/2009, de 10 de Março e pela Lei n.º 46/2012 de 29 de Agosto), que veio transpor para a ordem jurídica interna a Diretiva n.º 2000/31/CE, do Parlamento Europeu e do Conselho, de 8 de Junho de 2000 (Diretiva do Comércio Electrónico).

A lei 7/2004, de 07 de Janeiro, de comércio eletrónico no mercado interno e tratamento de dados pessoais faz referência aos de prestadores intermediários de serviços em rede *"são os que prestam serviços técnicos para o acesso, disponibilização e utilização de informações ou serviços em linha independentes da geração da própria informação ou serviço"* (artigo 4.º n.º 5), este conceito abrange também: o prestador intermediário de serviços de transmissão de comunicações em rede (artigo 15.º, n.º1); aos prestadores intermediários do serviço de armazenagem em servidor (artigo 16.º, n.º1); e os prestadores intermediários de serviços de associação de conteúdos em rede (artigo 17.º).

---

[69] SANTOS, Paulo; BESSA, Ricardo; PIMENTEL, Carlos – CYBERWAR: O fenómeno, as tecnologias e os actores, p.56

[70] PEREIRA, Joel Timóteo Ramos, Direito da Internet e Comércio Electrónico, Quid Iuris? Sociedade Editora, Lisboa, 2001. ISBN 972-724-113-1. p. 240

[71] "Prestador de serviços": qualquer pessoa, singular ou colectiva, que preste um serviço do âmbito da sociedade da informação (artigo 2.º al. b) da Directiva n.º 2000/31/CE, do Parlamento Europeu e do Conselho, de 8 de Junho de 2000)

Segundo artigo 2.º alínea d) da Lei do Cibercrime, é *"«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 respetivos utilizadores"*. Dispõe na lei 7/2004, de janeiro, nos artigos 12 e 14.º, que estes, não têm responsabilidade pelos conteúdos e práticas ilícitas dos utilizadores º[72], contudo, nos termos do artigo 16.º, será responsabilizado *"pela informação que armazena se tiver conhecimento de actividade ou informação cuja ilicitude for manifesta e não retirar ou impossibilitar logo o acesso a essa informação"*. O artigo 18.º admite que as partes possam recorrer a uma entidade administrativa (ANACOM) para decidir no período de 48 horas se o conteúdo pode ou não ser disponibilizado. Esta decisão pode ser modificada posteriormente caso as partes recorram a juízo, uma vez que, só com decisão judicial a solução se torna definitiva[73].

No nosso ordenamento jurídico, o prestador intermediário de serviços é civilmente responsável: pela informação que armazena se tiver conhecimento de atividade ou informação cuja ilicitude for manifesta e não retirar ou impossibilitar logo o acesso a essa informação conforme ao artigo 16.º n.º1 da Lei 7/2004, de 7 de janeiro; perante as circunstâncias que conhece, o prestador do serviço tenha ou deva ter consciência do carácter ilícito da informação (artigo 16.º n.º 2.º da referida lei); e quando o destinatário do serviço atuar subordinado ao prestador ou for por ele controlado (artigo 16.º n.º3 da citada lei). Estabelece no artigo 17.º desta lei "Os prestadores intermediários de serviços de associação de conteúdos em rede, por meio de instrumentos de busca, hiperconexões ou processos análogos que permitam o acesso a conteúdos

---

[72] ***Artigo 12.º (Ausência de um dever geral de vigilância dos prestadores intermediários de serviços)***
"Os prestadores intermediários de serviços em rede não estão sujeitos a uma obrigação geral de vigilância sobre as informações que transmitem ou armazenam ou de investigação de eventuais ilícitos praticados no seu âmbito".
Artigo 14.º (Simples transporte)
1 - O prestador intermediário de serviços que prossiga apenas a actividade de transmissão de informações em rede, ou de facultar o acesso a uma rede de comunicações, sem estar na origem da transmissão nem ter intervenção no conteúdo das mensagens transmitidas nem na selecção destas ou dos destinatários, é isento de toda a responsabilidade pelas informações transmitidas.
2 - A irresponsabilidade mantém-se ainda que o prestador realize a armazenagem meramente tecnológica das informações no decurso do processo de transmissão, exclusivamente para as finalidades de transmissão e durante o tempo necessário para esta.

[73]ASCENÇÃO, José de Oliveira, "O Ilícito em rede", Direito da Sociedade da Informação e Direito de Autor, APDI, vol. X, Coimbra Editora, 2012, pp.112-113. ISBN 978-972-32-2018-6.

ilícitos estão sujeitos a regime de responsabilidade correspondente ao estabelecido no artigo anterior).

Portanto, tomando conhecimento, de um qualquer conteúdo ilícito, ou de práticas ilícitas mesmo perante denúncia feita por pessoas singulares, devem os fornecedores intermediários de serviços retirar de imediato essa informação perante ilicitude manifesta.[74]

Relativamente a Mail Servers (servidores de correio eletrónico) que tenham conhecimento de que se usam e-mails com o seu domínio e alojamento para fins ilícitos, e nada façam para remover ou bloquear esses utilizadores, ou criem barreiras no acesso à informação pelas autoridades competentes, não poderão ser responsabilizados penalmente, exceto quando desobedecerem a despacho judicial.

Quanto aos ISP (*Internet Service Provider*)[75], de acordo com artigo 13º do Decreto-Lei 7/2004, de 7 de Janeiro, sob a epígrafe *"Deveres comuns dos prestadores intermediários dos serviços", "Cabe aos prestadores intermediários de serviços a obrigação para com as entidades competentes: a) De informar de imediato quando tiverem conhecimento de atividades ilícitas que se desenvolvam por via dos serviços que prestam; b) De satisfazer os pedidos de identificar os destinatários dos serviços com quem tenham acordos de armazenagem; c) De cumprir prontamente as determinações destinadas a prevenir ou pôr termo a uma infração, nomeadamente no sentido de remover ou impossibilitar o acesso a uma informação; d) De fornecer listas de titulares de sítios que alberguem, quando lhes for pedido".*

Gonçalves Teixeira[76] aduz que, "*Se a atividade em que assenta o serviço prestado pelo ISP for "puramente técnica, automática e de natureza passiva, o que implica que o prestador de serviços da informação não tem conhecimento da informação transmitida ou armazenada, nem o controlo desta"*[77]*, ficará em nosso ver este ISP isento de qualquer responsabilização no*

[74] ASCENÇÃO, José de Oliveira, "O Ilícito em rede", Direito da Sociedade da Informação e Direito de Autor, APDI, vol. X, Coimbra Editora, 2012, p.111. ISBN 978-972-32-2018-6.

[75] Internet Service Provider (ISP) é "*uma empresa que fornece, a particulares ou empresas, uma forma de acesso ou a presença na Internet. Estas empresas poderão facultar serviços de apoio na área da criação e administração de homepages.*" .MATOS, José A. de, Dicionário de Informática e Novas Tecnologias, 3.ª ed. aumentada, FCA - Editora de Informática, LDA. ISBN 978-972-722-469-2, p. 204

[76] Teixeira, Paulo Alexandre Gonçalves - O FENÓMENO DO PHISHING: ENQUADRAMENTO JURÍDICO-PENAL, Dissertação para obtenção do grau de Mestre em Direito, especialidade em Ciências Jurídico-Criminais, orientador : Prof. Doutor Fernando Conde Monteiro. Fevereiro 2013, Lisboa, pp. 75-78, disponível em http://repositorio.ual.pt/bitstream/11144/301/1/O%20fen%C3%B3meno%20do%20Phishing%20%E2%80%93%20Enquadramento%20Jur%C3%ADdico-Penal%20%282013-02%29.pdf, consultado em 27-08-2014

[77] Considerando 42 da Directiva 2000/31/CE, de 8 de Junho de 2000

que concerne às informações transmitidas, em concreto as que são susceptíveis de encerrarem conteúdos ilícitos.". Posição com a qual concordamos, porque o ISP possibilita o acesso à rede e a transmissão de informações, seria impossível e até injusto serem punidos por crimes cometidos por terceiros, torna-se difícil apurar se têm ou não conhecimento dos crimes, dado o vasto número de utilizadores na internet e, além disso, estes não podem aceder ao conteúdo privado dos utilizadores, sob pena de violação do direito à privacidade. Contudo, quando não colaborem com as autoridades judiciárias competentes poderão sempre incorrer no crime de desobediência previsto e punível no artigo 348.º do Código Penal.

De acordo com o artigo 21 da Lei 12.965, de 23 de Abril de 2014 *"O provedor de aplicações de internet que disponibilize conteúdo gerado por terceiros será responsabilizado subsidiariamente pela violação da intimidade decorrente da divulgação, sem autorização de seus participantes, de imagens, de vídeos ou de outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado quando, após o recebimento de notificação pelo participante ou seu representante legal, deixar de promover, de forma diligente, no âmbito e nos limites técnicos do seu serviço, a indisponibilização desse conteúdo"*.[78]

Em 2014, um criador de serviço de partilha de ficheiros, criou o *BTuga* um *site* em que permitia aos utilizadores encontrar os chamados *torrents*, que servem para os utilizadores disponibilizarem e acederem a ficheiros entre os computadores uns dos outros, através de uma rede chamada "*peer-to-peer"*, ou ponto-a-ponto, foi condenado pelo Tribunal Criminal de Lisboa a duas multas que totalizam 12.600 euros, pelo crime de usurpação de direitos de autor[79].

Feita uma breve referência a algumas das condutas praticadas e dos vários agentes, importa-nos de seguida fazer uma análise dos crimes tipificados na Lei do Cibercrime que punem este tipo de criminalidade.

[78] A Lei 12.965, de 23 de abril de 2014, estabelece princípios garantias, direitos e deveres para o uso da Internet no Brasil, disponível em http://www2.camara.leg.br/legin/fed/lei/2014/lei-12965-23-abril-2014-778630-publicacaooriginal-143980-pl.html com acesso 01-12-2014

[79] PEREIRA, João Pedro, notícia publicada no jornal público em 14-01 de 2014, disponível em http://www.publico.pt/tecnologia/noticia/criador-do-servico-de-partilha-btuga-condenado-a-multas-de-12600-euros-1619654 com acesso em 05-01-2015

1.7. Disposições Penais Materiais

De um modo geral, as fontes que levaram à criação destas normas foram essencialmente, a convenção sobre Cibercrime do Conselho da Europa e a Decisão-Quadro 2005/222/JAI, do Conselho, de 24 de Fevereiro de 2005, relativa a ataques contra sistemas de informação.

Procedemos, à análise dos artigos da Lei do Cibercrime, onde colocamos alguns dos "*modi operandi*" referidos supra, na tentativa de exemplificar um pouco as condutas abrangidas pela norma.

1.7.1. Crime de falsidade informática (artigo 3.º)

O artigo 3.ºda lei do cibercrime prevê o crime de falsidade informática, que no n.º 1 desta norma, consagra *"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"*.

De modo geral, corresponde às ditas falsificações que ocorrem no mundo físico com regulamentação no Código Penal (artigo 256.º), sendo que estas, no entanto, são praticadas em ambiente digital. Do mesmo modo, esta norma visa proteger os seguintes interesses: a segurança, a fiabilidade, a força probatória dos documentos ou outros instrumentos essenciais à vida jurídica quotidiana[80], ou seja, visa proteger a segurança das relações jurídicas.

No Decreto-Lei n.º 290-D/99, de 2 de Agosto, regula-se a validade, eficácia e valor probatório dos documentos eletrónicos (não designados de informáticos) e a assinatura digital (especialmente nos artigos 2.º a 7.º). No artigo 3.º alude-se à forma e força probatória do documento eletrónico em confronto com os artigos 376.º e 368.º do Código Civil e 167.º do Código de Processo Penal[81].

Os elementos objetivos tipificadores do crime de falsidade informática consistem em *" (...) introduzir, modificar, apagar ou suprimir dados informáticos ou por qualquer outra forma*

[80] Cfr. MARTINS, A. G. Lourenço, Criminalidade Informática, Direito da Sociedade da Informação, vol. IV, Coimbra Editora, 2003. ISBN 972-32-1169-6, p. 22. E PEREIRA, Joel Timóteo Ramos, Direito da Internet e Comércio Electrónico, Quid Iuris? Sociedade Editora, Lisboa, 2001. ISBN 972-724-113-1. p. 248

[81] MARTINS, A. G. Lourenço, Criminalidade Informática, Direito da Sociedade da Informação, vol. IV, Coimbra Editora, 2003. ISBN 972-32-1169-6, p. 24

interferir num tratamento informático de dados, produzindo dados ou documentos não genuínos", sendo o elemento subjetivo *"a intenção de provocar engano nas relações jurídicas"*.

Este artigo 3.º consagra também duplo dolo: o agente do crime deverá estar imbuído do intuito de *"provocar engano nas relações jurídicas"* e com intenção que os documentos digitais falsificados *"sejam considerados ou utilizados para finalidades juridicamente relevantes"*, como se fossem verdadeiros[82].

Quando estas ações 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 (n.º2 do mesmo artigo).

Este tipo criminal pune também a falsificação exercida sobre dados informáticos inseridos em cartões SIM (Subscriber Identity Module, ou módulo de identificação do assinante). Estes cartões de plástico contêm uma estrutura semicondutora (o chip), onde está gravada informação digital que permite ao respetivo titular utilizar um telemóvel para aceder a uma rede telefónica móvel. A lei ao fazer referência *a "outros dispositivos (...) que permitem o acesso a serviços de acesso condicionado"*, abrange por exemplo, o caso dos cartões ou outros equipamentos que permitam o acesso a sinal de televisão por cabo. Tratando-se de cartões bancários, deve atender-se ao artigo 267.º n.º 1 alínea c) e ao artigo 262.º n.º 1 do Código Penal, pois estas normas equiparam os cartões bancários à moeda, do mesmo modo que a "contrafação" de um cartão bancário é equiparada a *"contrafação"* de moeda.[83]

De acordo com o n.º 3 do artigo 3.º, basta que o agente use documento produzido a partir de dados informáticos e atue com intenção de causar prejuízo a outrem ou de obter um benefício ilegítimo, para si ou para terceiro. Não se exige que o engano provocado se repercuta nas relações jurídicas como consagra o n.º1 do artigo em apreço.

No n.º4 deste artigo é consagrada uma tutela antecipada, bastando a importação, distribuição, venda ou detenção para fins comerciais[84], de qualquer dispositivo que permita o

[82] VERDELHO, Pedro, Lei n.º 109/2009, de 15 de Setembro, in Comentário das leis penais extravagantes, vol. 1, [coord. de] ALBUQUERQUE, Paulo Pinto de Lisboa: Universidade Católica Editora, 2010. ISBN 978-972-54-0282-5, p. 506

[83]Idem, pp. 506-508

[84] RODRIGUES, Benjamim Silva, Da Prova Penal, Tomo IV, Da Prova-Electrónico-Digital e da criminalidade Informático-Digital, 1.ª Ed. Rei dos Livros, 2011. ISBN 978-989-8305-18-3. p.136

acesso a sistema ou meio de pagamento, sistema de comunicações ou a serviço de acesso condicionado, para que seja aplicada ao agente, uma pena de prisão de 1 a 5 anos. Este artigo não veio revogar expressamente o estipulado no artigo 104 da Lei n.º 5/2004, Lei das Comunicações eletrónicas, mas passou a prever as possibilidades já aí previstas[85], desde logo, no n.º1 alínea a) que proíbe "fabrico, importação, distribuição, venda, locação ou detenção, para fins comerciais, de dispositivos ilícito. O n.º 2 do artigo 104, na alínea a) define *"«Dispositivo ilícito» um equipamento ou programa informático concebido ou adaptado com vista a permitir o acesso a um serviço protegido, sob forma inteligível, sem autorização do prestador do serviço"*.

O artigo 128.º do Regime Geral das Infrações Tributárias (doravante designado por RGIT), sob a epígrafe de "Falsidade informática e software certificado" estabelece que "Quem criar, ceder ou transacionar programas informáticos, concebidos com o objetivo de impedir ou alterar o apuramento da situação tributária do contribuinte, quando não deva ser punido como crime, é punido com coima variável entre (euro) 3750 e (euro) 37 500" (Redação dada pelo artigo 155.º da Lei n.º 64-B/2011, de 30 de Dezembro). As condutas previstas neste artigo 128.º do RGIT são, no essencial, subsumíveis às condutas previstas no n.º 4 do artigo 3.º da LC. Ainda assim, essa sobreposição não é total pois, este n.º 4 do artigo 3.º da LC apenas penaliza criminalmente as condutas associadas a dispositivos suscetíveis de serem utilizados para a prática das condutas agravadas do n.º2 do mesmo artigo, aquelas que *"incidem 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",* ficando todas as demais situações de criação, cedência ou transação de dispositivos suscetíveis *"de impedir ou alterar o apuramento da situação tributária do contribuinte"* abrangidos pela norma contraordenacional do artigo 128.º do RGIT".[86]

O bem jurídico tutelado por este crime de falsidade informática é, segundo a jurisprudência, a *"integridade dos sistemas de informação"*[87]. Já no entender de Alexandre Gonçalves, o bem jurídico em causa é a segurança das relações jurídicas. Concordamos com

[85] VERDELHO, Pedro, Lei n.º 109/2009, de 15 de Setembro, in Comentário das leis penais extravagantes, p. 508

[86] VENÂNCIO, Pedro Dias, LEI DO CIBERCRIME, ANOTADA E COMENTADA, 1.ª ed., Coimbra Editora, 2011. ISBN 978-972-32-1906-7, p. 41.

[87] Acórdão do Tribunal da Relação de Lisboa, de 30-06-2011, Processo nº 189/09.3JASTB.L1-5, com relatora FILOMENA LIMA, disponível em http://www.dgsi.pt; Acórdão do Tribunal da Relação do Porto, de 17-09-2014, Processo nº 2013/13.3JAPRT.P1, relator COELHO VIEIRA, disponível em http://www.dgsi.pt

este Autor, pois, com a falsidade informática, à semelhança do que acontece com os documentos falsificados, uma página de Internet falsificada, coloca em causa a segurança das relações jurídicas.

Consubstancia o crime de falsidade informática um *website* falsificado, em tudo semelhante a um site de uma entidade bancária, induzindo desse modo um utilizador em erro.

Segundo Acórdão do Tribunal da Relação do Porto, preenchem todos os elementos típicos do crime de falsidade informática previsto e punível (doravante designado p.p.) pelo artigo 3º, nºs 1 e 3, da Lei 109/2009 de 15 de Setembro, o *"arguido, ao criar informaticamente contas nas quais produziu dados de perfil não genuíno da ofendida através da utilização dos seus dados pessoais que, simulando ser a própria, introduziu no sistema informático para criar, via internet, em sítio próprio da plataforma da rede social do facebook, imagem psicológica, caráter, personalidade e identidade da ofendida que não correspondiam à realidade, com a intenção de serem considerados genuínos e, através das contas referenciadas, fingindo ser a ofendida, divulgar conteúdos íntimos da sua vida pessoal, provocando dessa forma engano, com a intenção de que fossem tomadas por verdadeiras e reais aquelas contas, dessa forma causando prejuízo à honra e imagem da ofendida, como era seu desiderato"*[88].

Coloca-se a questão de se saber se uma página de internet cabe no conceito de documento constante da alínea a) do artigo 255.º do CP, e se uma página de internet falsa (*Phishing*) se insere no tipo de falsidade informática. Quanto à utilização de dados pessoais para obtenção de ganhos patrimoniais, a doutrina e a jurisprudência têm-se dividido, havendo quem considere que estamos perante crime de burla informática (artigo 221.º, n.º1 do CP), argumentando com a *"utilização não autorizada de dados"*. Outros consideram estarmos perante um furto (artigo 203.º do CP), afastando o artigo 221.º por os dados em causa não serem informáticos.[89]

1.7.2. Crime de dano relativo a programas ou outros dados informáticos (artigo 4.º)

O artigo 4.º prevê o crime de dano relativo a programas ou outros dados informáticos. Esta norma visa proteger a integridade dos dados informáticos (definido no artigo 2.º alínea b)

[88] Acórdão do Tribunal da Relação do Porto, de 24-04-2013, Processo N.º 585/11.6PAOVR.P1, com relatora FÁTIMA FURTADO, disponível www.dgsi.pt

[89] VERDELHO, Pedro, Pishing e outras formas de defraudação nas redes de comunicação, in Direito da Sociedade da Informação, Vol. VIII, coord. Prof. Doutor José de Oliveira Ascensão, Coimbra Editora, 2009. ISBN 978-972-32-1710-0, pp.414-415

quer da destruição, quer da inutilização dos mesmos. No n.º 3 deste artigo pune-se a propagação de dispositivos ou programas ou outros dados informáticos, elaborados com a finalidade de cometimento de crimes de dano informático, penaliza *"quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos"*. É um tipo legal de crime de perigo, uma vez que não exige a efetiva consumação dos danos, nem exige a tentativa para punição da conduta. Este preceito distingue-se do crime de dano previsto no artigo 212.º do Código Penal, por neste se exigir a consumação do dano[90] e respeitar a objetos corpóreos, onde se inserem danos causados a equipamentos, sistemas e redes informáticos enquanto *"hardware informático"* (componente físico)[91]. Já no ilícito previsto na LC persiste a intangibilidade do objeto[92].

Pedro Verdelho refere que neste n.º3 se descreve "verdadeiramente um novo tipo de crime, cujo objeto é a difusão daquilo a que genericamente se chama "*malware*" (expressão que abrange os tradicionais vírus informáticos mas também todos os outros programas maliciosos). Este novo tipo de crime inspira-se claramente nas normas do artigo 6.º da Convenção sobre Cibercrime, que declaram proibida e punível a conduta de quem *"ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos que possam ter com consequência a prática do crime de dano."* Pune-se, por exemplo, a mera difusão de vírus por via de *spam*, mesmo que esses vírus ou outro *malware* não tenham chegado a produzir os efeitos pretendidos.[93].

Aquando da discussão pública anterior à aprovação parlamentar desta Lei, questionou-se se este alargamento poderia por em causa as atividades de segurança dos sistemas das redes informáticas, por entenderem que os atos de teste aos mecanismos de segurança desses sistemas se qualificavam como crime. Estas condutas não preenchem o tipo, uma vez que se exige que o

[90] VENÂNCIO, Pedro Dias, LEI DO CIBERCRIME, ANOTADA E COMENTADA, 1.ª ed., Coimbra Editora, 2011. ISBN 978-972-32-1906-7, pp. 46-47

[91] RODRIGUES, Benjamim Silva, Da Prova Penal, Tomo IV, Da Prova-Electrónico-Digital e da criminalidade Informático-Digital... p.141

[92] RODRIGUES, Benjamim Silva, Da Prova Penal, Tomo IV, Da Prova-Electrónico-Digital e da criminalidade Informático-Digital... p.139

[93]VERDELHO, Pedro, Lei n.º 109/2009, de 15 de Setembro, in Comentário das leis penais extravagantes, p. 510.

agente atue *"sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema"*[94].

A posição maioritária da doutrina considera que o bem jurídico protegido é o património, já Silva Rodrigues[95] defende que o artigo em apreço protege os dados ou programas informáticos, ou mais rigorosamente "*a integridade dos fluxos informacionais e comunicacionais e informático-digitais que flúem pelas redes ou sistemas informáticos*". No entender de Pedro Verdelho[96], a tutela penal é a defesa da integridade e fiabilidade de dados e ao bom funcionamento dos programas informáticos, o interesse protegido não é apenas a integridade patrimonial (como ocorre no crime de dano previsto no Código Penal), *"além da integridade dos dados informáticos, enquanto propriedade do lesado, protege também este tipo de ilícito a integridade, funcional desses dados, que se refere à disponibilidade e utilizabilidade eficaz dos dados informáticos"*. Em nossa opinião, tanto Silva Rodrigues como Pedro Verdelho apesar de usarem terminologias diferentes, ambos defendem que, o bem jurídico em apreço é a integridade dos dados ou programas informáticos, posição com a qual nos identificamos.

Estamos perante um crime semipúblico, uma vez que depende de queixa, pois o n.º6 do artigo em apreço não faz qualquer referência ao n.º 5, logo, a *contrario sensu*, o procedimento criminal não depende de queixa, sendo portanto um crime público quando *"o dano causado for de valor consideravelmente elevado"*.

O n.º1 deste artigo prevê *"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"*. Esta norma pode abranger também dados pessoais, abrangidos pelo conceito de dados informáticos, porém, perante esse tipo de dados deve dar-se prevalência à norma 45.º (Viciação ou destruição de dados pessoais) da Lei 67/98, de 26 de Outubro, Lei da Proteção de Dados Pessoais (doravante designada - LPDP), dado estabelecer no seu n.º1 *"Quem, sem a devida autorização, apagar, destruir, danificar, suprimir ou modificar dados pessoais, tornando-os inutilizáveis ou*

[94] Idem, Ibidem,
[95] RODRIGUES, Benjamim Silva, Da Prova Penal, Tomo IV, Da Prova-Electrónico-Digital e da criminalidade Informático-Digital, pp.141-142
[96] VERDELHO, Pedro, Lei n.º 109/2009, de 15 de Setembro, in Comentário das leis penais extravagantes, pp. 510-511

afectando a sua capacidade de uso, é punido com prisão até dois anos ou multa até 240 dias"[97]. O legislador, ao consagrar no artigo 30.º da Lei do Cibercrime que *"O tratamento de dados pessoais ao abrigo da presente lei efetua-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 respetivo capítulo VI."*, quis esclarecer expressamente essa preferência. Acrescente-se que, enquanto o crime da Lei do Cibercrime é geral, o da LPDP é especial, uma vez que visa especificamente o dano informático, quando o dano incidir sobre dados pessoais.

Sublinhe-se que além destas, podem ocorrer muitas outras situações de sobreposição legal entre tipos de crime praticados em ambiente digital, o mesmo facto pode simultaneamente corresponder a dois ilícitos, e nestes casos, a solução poderá passar pelo elemento subjetivo, desde logo, pela intenção do agente.

Importa também diferenciar este crime de dano relativo a programas ou outros dados informáticos, da burla informática prevista e punida no artigo 221.º n.º 1 do Código Penal, consagra *"Quem, com intenção de obter para si ou para terceiro enriquecimento ilegítimo, causar a outra pessoa prejuízo patrimonial, interferindo no resultado de tratamento de dados ou mediante estruturação incorrecta de programa informático, utilização incorrecta ou incompleta de dados, utilização de dados sem autorização ou intervenção por qualquer outro modo não autorizada no processamento, é punido com pena de prisão até três anos ou com pena de multa"*. Consistindo na produção de um engano para obter uma vantagem, estamos perante crime doloso, uma vez que subjacente a esta atuação, está a intenção de obter enriquecimento ilícito ou causar prejuízo patrimonial, e o seu bem jurídico tem natureza iminentemente patrimonial. *"Esta vertente de predominante protecção do património é, aliás, o critério que irá permitir separar este crime de vários dos crimes previstos na Lei do Cibercrime, entre eles, do crime de dano relativo a programas ou outros dados informáticos, previsto no artigo 4.º da Lei do Cibercrime"*.[98]

1.7.3. Crime de sabotagem informática (artigo 5.º)

É importante estabelecermos a destrinça do crime de dano relativo a programas ou outros dados informáticos e a sabotagem informática prevista no artigo 5.º. Enquanto no artigo 4.º, o

[97] *In* Benjamim Silva Rodrigues Direito Penal – Parte Especial, p. 453 *Apud* VENÂNCIO, Pedro Dias, LEI DO CIBERCRIME, ANOTADA E COMENTADA, p. 50.
[98] VERDELHO, Pedro, Lei n.º 109/2009, de 15 de Setembro, in Comentário das leis penais extravagantes,p. 511.

objeto do crime é o dano de programas ou de outros dados informáticos[99], a sabotagem (artigo 5.º) respeita a sistemas informáticos[100].

Estabelece no n.º1 do artigo 5.º *"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."* No seu n.º 2, pune-se igualmente, *"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"*. Ou seja, a difusão de vírus e de outros programas maliciosos, cujo objetivo seja o de provocar sabotagem informática, constitui uma clara antecipação da tutela penal a realidades que anteriormente eram atos preparatórios da prática de outros crimes. *" (...) Esta antecipação visa incriminar as novas atividades relacionadas com o controlo malévolo das redes. Será o caso da montagem de botnets por via do estabelecimento de uma rede de computadores zumbi, de forma a que essas estruturas possam ser utilizadas para as mais diversas actividades ilegais. No que respeita à sabotagem, será por exemplo o caso da sua utilização para provocar as falhas técnicas conhecidas como DoS e DDoS[101]. Portanto, pelo n.º2 pune-se a difusão de software destinado à criação destas redes ilegais com estes propósitos"* [102].

---

[99]São *«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"* (artigo 2.º al.b) LC).

[100] É *«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"* (artigo 2.º al. a) LC)

[101] *"Distributed Denial of Service - DDoS, o DDoS, conhecido também como DOS - Denial of Service, refere um tipo de procedimento ilegal na Internet, em que um sistema sofre um ataque, sobre diversas formas, ou de várias fontes, com o objectivo de forçar o total constrangimento e subsequentemente a incapacidade de responder a mais pedidos. Isto resulta literalmente numa negação de serviços, forçando, na maior parte das vezes, o encerramento (shutdown) do sistema."* MATOS, José A. de, Dicionário de informática e das novas tecnologias, p. 119

[102] VERDELHO, Pedro, Lei n.º 109/2009, de 15 de Setembro, in Comentário das leis penais extravagantes, p. 514.

Um dos "*modus operandi"* que cabe no âmbito do crime de sabotagem é o "*spam*", consiste no envio de correspondência eletrónica não solicitada, sendo que o internauta nunca solicitou nem se registou para receber esses emails. Ramos Pereira[103] defende que " *(...) a prática do "spamming" poderá configurar sabotagem informática, na medida em que interfere em sistema informático, actuando com a intenção de entravar ou perturbar o funcionamento de um sistema informático ou de comunicação de dados à distância. Na verdade, o spammer não deseja apenas "informar" sobre um determinado evento;ele pretende perturbar o próprio sistema informático e, por isso, envia um número elevado da mesma mensagem ou de diversas mensagens visando entravar e perturbar e perturbar os servidores. Essa sua conduta constitui sabotagem informática*".

A emissão de mensagens em inúmeras quantidades supõe que se detenha um igual número de endereços de correio eletrónico e tratando-se de dados pessoais (artigo 3.º alínea a), da Lei de Protecção de Dados Pessoais, Lei n.º 67/98, de 26 de Outubro), a manutenção dessa base de dados só poderia ser efetuada para finalidades legítimas (artigo 5.º n.º1 alínea b) da referida lei), logo, a emissão de *spam* constitui ilícitos criminais nos termos do artigo 43.º, n.º1, dessa lei.[104]

Na sabotagem será feita uma agravação da pena, quando haja lesão de sistemas informáticos essenciais à sociedade, como o impedimento do normal funcionamento dos serviços públicos, abastecimentos, saúde, bem-estar económico das pessoas (artigo 5.º n.5 alínea b) da LC). Segundo Pedro Verdelho[105], *"A situação fáctica a que a norma se dirige corresponde a uma grande ameaça dos tempos modernos, criada pelos chamados grandes ataques informáticos com séria perturbação das comunicações informáticas (os chamados DoS e DDoS)"*. Quando o dano emergente da perturbação for de valor elevado (quando exceda 50 unidades de conta avaliadas no momento da prática do facto - artigo 202.º al a) CP), a pena é de prisão de um a cinco anos, conforme o disposto no n.º 4 do artigo 5.º. Tratando-se de dano de valor consideravelmente elevado (aquele valor que exceda 200 unidades de conta avaliadas no

[103] PEREIRA, Joel Timóteo Ramos, Direito da Internet e Comércio Electrónico. Quid Iuris?, Sociedade Editora, Lisboa, 2001. ISBN 972-724-113-1, pp. 250-251.

[104] VERDELHO, Pedro, Phishing e outras formas de defraudação nas redes de comunicação, in Direito da Sociedade da Informação, Vol. VIII, coord. Prof. Doutor José de Oliveira Ascensão, Coimbra Editora, 2009. ISBN 978-972-32-1710-0,PP.412-413

[105] VERDELHO, Pedro, Lei n.º 109/2009, de 15 de Setembro, in Comentário das leis penais extravagantes,p.513

momento da prática do facto - artigo 202.º alínea b) do CP), a moldura penal será de um a dez anos de prisão, de acordo com o nº5 alínea a) do artigo 5.º.

À semelhança do já mencionado no artigo 4.º, também poderá ocorrer que uma determinada conduta possa, cumulativamente, preencher o tipo de crime de sabotagem informática (visa proteger um sistema informático) e de sabotagem previsto no artigo 329.º do Código Penal (visa proteger *"meios de comunicação ou vias de comunicação, instalações de serviços públicos ou destinadas ao abastecimento e satisfação de necessidades vitais da população, infra-estruturas de valor relevante para a economia, a segurança ou a defesa nacional"*)[106], devendo fazer-se uma análise casuística (do caso concreto), de modo a decidir se deve prevalecer a dignidade da norma ou antes o meio utilizado; deve fazer-se uma ponderação que vá de encontro ao espírito do legislador.

1.7.4. Crime de acesso ilegítimo (artigo 6.º)

O crime de acesso ilegítimo (artigo 6.º) pune quem violar a confidencialidade de sistemas informáticos, independentemente do objetivo que levou o agente a praticar o crime, ou seja, mesmo que não exista o intuito lucrativo ou um qualquer prejuízo de terceiros, pune também quem produzir, vender, distribuir, ou por qualquer outra forma disseminar, ou introduzir num ou mais sistemas informáticos, dispositivos ou programas, um conjunto executável de instruções, código, ou outros dados informáticos destinados a produzir o acesso a sistemas informáticos alheios (n.º2). Neste n.º2, " *(...) a lei pretende nomeadamente punir o chamado roubo de identidade, recorrente e preocupante actividade criminógena moderna. (...) Por este novo tipo de crime pune-se a actuação daqueles que, recorrendo a meios informáticos fraudulentos obtém informação confidencial pertencente a terceiros (por exemplo os seus códigos de acesso a sítios na Internet: nomes de utilizadores, logins, passwords), que lhes permitam aceder a contas de correio electrónico, contas bancárias on-line ou a todos os restantes tipo de sítios de acesso restrito ou condicionado. Anota-se que aquilo que se pune nesta disposição do n.º 2 é apenas a obtenção ilegítima de dados de acesso a locais reservados do mundo virtual. Neste novo crime não se abrange a eventual utilização desses dados*" (a utilização desses dados terá outros enquadramentos, poderá ser por via da burla informática p.p. no artigo 221.º do Código penal), ou eventualmente pelo n.º1 deste artigo 6.º).[107]

[106] VENÂNCIO, Pedro Dias, LEI DO CIBERCRIME, ANOTADA E COMENTADA...p.54
[107]VERDELHO, Pedro, Lei n.º 109/2009, de 15 de Setembro, in Comentário das leis penais extravagantes...p. 517

A pena é agravada até três anos ou multa, se o acesso for conseguido através de violação de regras de segurança (n.º3); será agravada de um a cinco anos, se o agente tiver tomado conhecimento de segredo comercial ou industrial, ou de dados confidenciais, protegidos por lei, ou quando o benefício ou vantagem patrimonial obtidos, forem de valor consideravelmente elevado (n.º4). Admite-se a punição da tentativa, exceto nos casos previstos no n.º2.

Nas palavras de Simões Dias, é crime de acesso ilegítimo quando alguém consegue penetrar num sistema informático ou numa rede informática[108], e é caracterizado por ser um crime informático técnico, praticado através de uma infraestrutura técnica, volátil e praticado à distância[109]. Na opinião do Autor, o bem jurídico tutelado pela norma não é o domicílio informático (como defendido por Alma-Perroni, Manuel António Lopes Rocha, Manuel Lopes Rocha, Garcia Marques e Lourenço Martins, Galdieri, Giorgio Pica[110]). Defende que o bem jurídico em causa é a *"segurança dos sistemas informáticos"* e abrange três dimensões: a primeira consiste na confiança na utilização dos sistemas (ocorrendo violação das plataformas informáticas, haverá medo e insegurança na utilização dos equipamentos); a segunda respeita aos danos nos bens informáticos (rutura de programas, danificação de estruturas do equipamento informático, destruição de documentos e conteúdos); e a terceira é relativa à tutela dos conteúdos (mantidos em documentos, registos e programas que vão ao encontro da privacidade). A economia não sobrevive sem estas plataformas (indústrias, comércio, serviços tradicionais e as entidades públicas) nem é desejável a descredibilização e desconsideração das atividades feitas *online*, quer pelos operadores (empresas) quer pelos utilizadores (consumidores). Defende também o Autor, o facto de estarmos perante um bem jurídico intermédio uma vez que é vocacionado quer para a esfera individual quer para a vertente coletiva.[111]

Diversamente, Ramos Pereira entende que *"Este preceito visa proteger o "domicílio informático"*, correspondendo assim a conduta do criminoso informático à *"introdução em casa alheia"*[112].

---

[108] DIAS, Pedro Simões, O "Hacking" enquanto crime de acesso ilegítimo. Das suas especialidades à utilização das mesmas para a fundamentação de um novo direit, in Direito da Sociedade da Informação, vol. VIII, Coord. Prof. Doutor José de Oliveira Ascenção, Coimbra Editora, 2009. ISBN 978-972-32-1710-0, p. 235

[109] Idem, p. 232

[110] Idem, pp.236-237

[111] DIAS, Pedro Simões, O "Hacking" enquanto crime de acesso ilegítimo. Das suas especialidades à utilização das mesmas para a fundamentação de um novo direito, in Direito da Sociedade da Informação, vol. VIII, Coord. Prof. Doutor José de Oliveira Ascenção, Coimbra Editora, 2009. ISBN 978-972-32-1710-0, pp. 245-251

[112] PEREIRA, Joel Timóteo Ramos, Direito da Internet e Comércio Electrónico, Quid Iuris? Sociedade Editora, Lisboa, 2001. ISBN 972-724-113-1. p. 251 (refere-se o autor ao anterior artigo 7.º da Lei 109/91)

Nas palavras de Silva Rodrigues[113], procura-se proteger a *"«formal esfera da privacidade e do segredo» ou a «integridade do sistema informático lesado», a partir de uma ideia (nova) de inviolabilidade do domicílio informático"*.

1.7.5. Crime de interceção ilegítima (artigo 7.º)

O crime de interceção ilegítima previsto no artigo 7.º pune a interferência nas comunicações eletrónicas, e visa proteger a segurança e privacidade das comunicações[114]. Interceção consiste no *"acto destinado a captar informações contidas num sistema informático, através de dispositivos electromagnéticos, acústicos, mecânicos ou outros"* (artigo 2.º alínea e)). Nas palavras de Benjamim Silva Rodrigues, trata-se *"(…)de proteger o exclusivo, inviolabilidade, segurança dos fluxos informacionais e comunicacionais que estruturam ou circulam pelos sistemas ou redes informáticos e redes de serviços e comunicações eletrónicas publicamente acessíveis e disponíveis"*[115]. No entender de Pedro Verdelho[116], o bem jurídico protegido é a privacidade na comunicação de dados sublinhando o referido Autor que *"(…) esta infração representa a mesma violação da privacidade de comunicações que as tradicionais escutas e gravações de conversas telefónicas entre pessoas. A inviolabilidade das "telecomunicações e demais meios de comunicação" é garantida pelo Artigo 34.º, n.º4, da Constituição da República Portuguesa, estando igualmente contemplada no Artigo 8.º da Convenção Europeia dos Direitos do Homem*".

O artigo 7.º n.º3, crime de interceção ilegítima, é um crime de perigo abstrato, bastando a simples detenção de aparelhagem destinada à violação do segredo das comunicações, não se exigindo a efetiva concretização[117]. É suficiente que haja intenção de praticar os atos do tipo objetivo, ou seja, a consumação deste tipo de crime não exige a obtenção efetiva de informações, bastando proceder de forma a captar informações[118].

Dias Venâncio chama-nos à atenção para o facto de poder existir uma sobreposição entre os crimes de violação de correspondência ou de telecomunicações (artigo 194.º CP), e de

[113] RODRIGUES, Benjamim Silva, Da prova Penal, Tomo IV, Da Prova-Electrónico-Digital e da Criminalidade Informático Digital, p.163
[114] VENÂNCIO, Pedro Dias, Lei do Cibercrime Anotada e Comentada...p. 67
[115] RODRIGUES, Benjamim Silva, Da prova Penal, Tomo IV, Da Prova-Electrónico-Digital e da Criminalidade Informático Digital, op. cit. p.176
[116] VERDELHO, Pedro, Lei n.º 109/2009, de 15 de Setembro, in Comentário das leis penais extravagantes...p. 518
[117] RODRIGUES, Benjamim Silva, Da prova Penal, Tomo IV, Da Prova-Electrónico-Digital e da Criminalidade Informático Digital, p. 175
[118] VERDELHO, Pedro, Lei n.º 109/2009, de 15 de Setembro, in Comentário das leis penais extravagantes...p. 518

interceção ilegítima relativamente à interceção da mensagem escrita ou comunicação áudio, ou vídeo em ambiente digital, sublinhando que o mesmo já não se verifica, quando se trate de interceção de transmissão de dados informáticos (artigo 2.º alínea b)) de natureza diversa[119].

Pedro Verdelho[120] reconhece que este tipo de crime, especialmente previsto para *"transmissões de dados informáticos que se processam no interior de um sistema informático, a ele destinadas ou dele provenientes",* colide quanto ao interesse que visa proteger (sublinhado nosso), com normas do Código Penal, nomeadamente com o artigo 192.º, n.º1 alínea a), que pune como devassa da vida privada *"quem, sem consentimento e com intenção de devassar a vida privada das pessoas, designadamente a intimidade da vida familiar ou sexual: a) Interceptar, gravar, registar, utilizar, transmitir ou divulgar conversa ou comunicação telefónica"*. Contudo, existem também diferenças quanto ao dolo, pois no tipo descrito no artigo 7.º da Lei do Cibercrime o dolo é genérico, sendo suficiente a intenção livre e deliberada de praticar as ações aí descritas. Já no artigo relativo a devassa do artigo 192.º n.º1 alínea a) do Código Penal, o dolo é específico, sendo que as ações típicas descritas neste artigo, não se incluem no artigo 7.º da Lei do Cibercrime, onde são também distintos os tipos objetivos.

Nos crimes até agora estudados: falsidade informática (artigo 3.º n.º4); dano relativo a programas ou outros dados informáticos (artigo 4.º n.º3); sabotagem informática (artigo 5.º n.º2); acesso ilegítimo (artigo 6.º n.º2); e de interceção ilegítima (artigo 7.º n.º3), o nosso legislador teve o cuidado de antecipar a tutela penal, punindo também a mera difusão de dispositivos aptos ao cometimento destes crimes.

Nas palavras de Pinto de Albuquerque[121], *"existe uma relação de concurso aparente (consunção) entre o crime de burla informática e os crimes de falsidade informática (artigo. 3º Lei do Cibercrime), dano relativo a dados ou programas informáticos (artigo. 4º Lei do Cibercrime), sabotagem informática (artigo. 5º Lei do Cibercrime), acesso ilegítimo (artigo. 6º Lei do Cibercrime) e a interceção ilegítima (artigo. 7º Lei do Cibercrime), sendo estes factos prévios não puníveis."*

[119] VENÂNCIO, Pedro Dias, Lei do Cibercrime Anotada e Comentada, op. cit.p. 68

[120] VERDELHO, Pedro, Lei n.º 109/2009, de 15 de Setembro, in Comentário das leis penais extravagantes...pp. 518-519

[121] *ALBUQUERQUE, Paulo Pinto de, Comentário do Código Penal à luz da Constituição da República Portuguesa e da Convenção dos Direitos do Homem, 2.ª ed. actualizada, Lisboa: Universidade Católica Editora, 2010, p. 691. ISBN 978-972-54-0272-6*

1.7.6. Crime de reprodução ilegítima de programa protegido (artigo 8.º)

O artigo 8.º prevê o crime de reprodução ilegítima de programa protegido. Sublinhe-se que esta norma respeita somente a programas de computador, ou seja, a reprodução, divulgação ou comunicação ao público não autorizada, de programa informático protegido por Lei (n.º1). Preenche o tipo ilícito, o ato de fazer uma cópia de um programa informático, para um suporte autónomo de dados (CD Rom, *pen disk*, disco rígido ou outro suporte de dados), ou para o instalar num computador. Contrariamente ao que acontece quanto ao direito de autor clássico, a lei considera crime a realização de cópias para uso privado de programas (exceto quando o titular do direito sobre o programa tenha autorizado a cópia[122]). Esta norma incrimina ainda, quem reproduz e quem divulga programa de computador sem a devida autorização do legítimo proprietário.

Não inclui a reprodução de outros dados informáticos, nem de bases de dados (regulados pelo Decreto-Lei 122/2000, de 4 de Julho, que transpõe para o ordenamento português a Diretiva do Parlamento e do Conselho n.º 96/9/CE) ficando também de fora a tutela de outros direitos de autor, legalmente protegidos pelo Decreto-Lei n.º 252/94, de 20 de Outubro (que transpôs para Portugal a Diretiva n.º 91/250/CEE, do Conselho)[123]. Neste Decreto-Lei, mais precisamente no artigo 14.º, remete para o artigo 9.º da Lei 109/91 a violação do direito de autor sobre programas de computador, devendo fazer-se uma interpretação corretiva e atualista, esta remissão deve fazer-se para o atual artigo 8.º da Lei do Cibercrime[124], que pune também quem ilegitimamente reproduzir topografia[125] de um produto semicondutor[126] ou a explorar comercialmente ou importar, para estes fins, uma topografia ou um produto semicondutor fabricado a partir dessa topografia.

---

[122] VERDELHO, Pedro, Lei n.º 109/2009, de 15 de Setembro, in Comentário das leis penais extravagantes...p. 520

[123] Curso de formação avançada à distância CIBERCRIME E PROVA DIGITAL, organizado pela e-UNIFOJ do centro de Estudos sociais (CES) da Universidade de Coimbra e coordenado por Pedro Verdelho, decorreu entre 06 de Outubro e 05 de Dezembro Modulo II, Cibercrime, Os crimes Informáticos ou Cibercrimes, pp.1-6, disponível em http://opj.ces.uc.pt/e-learning/moodle/course/view.php?id=10, consultado em 23/10/2014.

[124] VERDELHO, Pedro, Lei n.º 109/2009, de 15 de Setembro, in Comentário das leis penais extravagantes...p. 522

[125] Consiste, numa *"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"* - artigo 2.º al. f)

[126] Consiste na "*forma final ou intermédia de qualquer produto, composto por um substracto 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 2.º al g)

Importa também referir que quando os ilícitos não preveem a punição da tentativa deve seguir-se a regra geral estabelecida no artigo 23.º n.º1 do Código Penal, ou seja, será punida quando ao crime consumado respetivo corresponda pena superior a três anos de prisão. Contudo, " (…) *é notório, apesar da existência de normas e regulamentação a ela ligadas quer a nível internacional e nacional, que o internauta sente uma ausência de controlo ao nível social, da acção reguladora das instâncias formais e informais de combate ao crime, bem como uma inexistência dos complexos sociais de rotulação e estigmatização.*"[127] Além disso, muitas das vezes, as entidades formais de controlo, não chegam a tomar conhecimento do crime. Os lesados acarretam os prejuízos e optam por formatar os computadores (particulares) e quando estão em causa grandes empresas com receio da publicidade negativa, "*preferem suportar os custos destes crimes ao invés de divulgarem as suas fragilidades*"[128] Contribuindo assim, para as chamadas cifras negras.[129]

Analisadas as normas penais que a Lei do Cibercrime trouxe ao nosso ordenamento jurídico, vamos de seguida e de forma geral apreciar em que termos deve ocorrer a obtenção da prova para que possa ser valorada em tribunal.

[127] SANTOS, Paulo; BESSA, Ricardo; PIMENTEL, Carlos – CYBERWAR: O fenómeno, as tecnologias e os actores, p. 5

[128] BARROS, Juliana Isabel Freitas - O NOVO PROCESSO PENAL: OS MEIOS DE OBTENÇÃO DE PROVA DIGITAL CONSAGRADOS NA LEI 109/2009, DE 15 DE SETEMBRO, Dissertação apresentada no âmbito do 2.º ciclo de Estudos em Direito da Faculdade de Direito da Universidade de Coimbra, Área de especialização: Mestrado em Ciências Jurídico-Forenses, Orientadora: Professora Doutora Helena Moniz, Coimbra, 2012., p.16

[129] *"É vulgar falar-se nas cifras negras dos crimes, expressão com a qual pretende abranger-se os crimes cujos autores não são nunca julgados. Não se trata daqueles que prescrevem antes de chegar a julgamento, nem daqueles cujas investigações se arrastam indefenidamente. Os crimes incluídos nas cifras negras são aqueles que nunca chegam ao conhecimento das autoridades policiais ou judiciais. São aqueles crimes cujas vítimas preferem esquecer, ou aqueles crimes dos quais nunca se soube que foram praticados. A polícia e os tribunais nunca chegam a saber da sua existência. Os danos e prejuízos sofridos pelas vítimas ficam por reparar e os respectivos responsáveis ficam por castigar."* VERDELHO, Pedro, "*Cibercrime"*, in Direito da Sociedade da Informação, Vol. IV, Coimbra Editora, 2003. ISBN 972-32-1169-6, p.351

2. A prova no processual penal português

2.1. Modelo Processual Penal

A prova nem sempre foi obtida e valorada pelos tribunais como é hoje, de um modo breve, aludimos ao percurso percorrido que levou ao aparecimento do nosso atual modelo processual penal de estrutura acusatória integrado pelo princípio da investigação.

O sistema inquisitório tinha como objetivo satisfazer os interesses do Estado na tarefa de punir, reunindo numa só pessoa, o Juiz, as funções de investigar, acusar e de julgar. Tinha natureza secreta para que não ocorresse o desaparecimento das provas e eram admitidos todos os meios probatórios, incluindo a tortura[130].

Já no sistema acusatório, o indivíduo é parte no processo, sendo-lhe reconhecidos direitos, é um verdadeiro processo de partes, sendo estas que acarretam os elementos probatórios ao processo, onde ao Juiz incumbe dirigir o processo e decidir[131]. A trave mestra deste modelo consiste essencialmente na separação entre a entidade que acusa e a entidade que julga[132]

O sistema misto ou eclético procurou concretizar vantagens dos dois sistemas, sendo o processo dividido em duas partes: a fase de instrução, destinada a investigar o crime e os seus agentes, era dirigida por um magistrado especializado; a iniciativa e a titularidade da ação penal encontrava-se nas mãos de um oficial do poder executivo junto do poder judicial. A instrução era escrita, secreta e não contraditória. A fase de julgamento destinada a apreciação e valoração da prova estava organizada segundo o modelo acusatório, prevalecia a oralidade, e a publicidade da audiência de julgamento.[133] *"Este sistema fundeia-se na relação dialéctica decorrente da necessidade sentida pela comunidade de perseguir os culpados pelos crimes cometidos - incumbindo ao Estado a tarefa pública de exercer o seu ius puniendi - mas, em cada caso concreto, assegura-se ao arguido a possibilidade de exercer os seus direitos de defesa, evitando-se os perigos decorrentes de uma real aniquilação da condição humana (do arguido)*

[130] NEVES, Rosa Vieira, A Livre Apreciação da Prova e a Obrigação de Fundamentação da Convicção (na Decisão Final Penal)...pp. 58-65
[131] Idem, Ibidem
[132] MENDES, Paulo de Sousa, Lições de Direito Processual Penal, p. 27
[133] Idem, p. 31

em prol da busca, levada ao extremo no sistema inquisitório, da descoberta da verdade material".[134]

No nosso código de Processo Penal de 1929, a instrução era da competência de um juiz, cabendo ao Ministério Público (doravante designado por MP) apenas promover as diligências concretas de instrução (artigo 35.º). Com o Decreto-Lei n.º 35.007 introduziram-se profundas alterações na instrução, havia uma fase de instrução preparatória da competência do MP, que visava a descoberta dos indícios da existência do crime e do seu agente. Havia ainda depois desta fase, uma fase de instrução contraditória da competência do Juiz, obrigatória nos processos de querela, devia o MP requerer a instrução contraditória no mesmo ato em que deduzia acusação. Este Decreto-Lei, preparado por Cavaleiro Ferreira mediante atribuição da instrução preparatória ao MP, que se adotou o princípio do acusatório.[135]

Aquando da Revolução de 25 de Abril de 1974, o programa do Movimento das Forças armadas (MFA), tinha como prioridade a dignificação do processo penal, surgiu o Código de Processo Penal de 1987, que veio atribuir o domínio da fase de inquérito, na forma de processo comum ao MP. Em 2007 ocorre uma revisão do CPP.[136]

O nosso modelo processual é de estrutura acusatória[137] integrada por um princípio da investigação[138], pois a entidade que acusa e define o objeto do julgamento é diferente da que julga, havendo também contribuição por parte da acusação e da defesa. O tribunal pode ordenar oficiosamente todos os meios de prova cujo conhecimento lhe afigure necessário à descoberta da verdade e à boa decisão da causa" (não há um verdadeiro ónus da prova[139], artigo 340.º n.º1 do CPP), faculdade esta que permite que a todo tempo se faça junção de documentos requerida

---

[134].NEVES, Rosa Vieira, A Livre Apreciação da Prova e a Obrigação de Fundamentação da Convicção (na Decisão Final Penal), pp. 58-65

[135] MENDES, Paulo de Sousa, Lições de Direito Processual Penal, p.35

[136] Idem, pp.35-41

[137]Relativamente aos modelos: "*Enquanto o inquisitório exprime uma confiança na bondade do poder e na sua capacidade de alcançar a verdade, o acusatório deriva de uma desconfiança no poder enquanto fonte autónoma da verdade".* v.g. FERRAJOLI, 1998:619; WEIGEND, 2003: 168; HERRMAN/SPEER, 1994: 523. *Apud* MESQUITA, Paulo Dá, A PROVA DO CRIME E O QUE SE DISSE ANTES DO JULGAMENTO, Estudo sobre a prova no Processo Penal Português, à Luz do sistema Norte-Americano, p.244

[138] A nossa Lei Ordinária consagra no artigo 32.º n.º5 o princípio da contraditoriedade: "*O processo criminal tem estrutura acusatória, estando a audiência de julgamento e os actos instrutórios que a lei determinar subordinados ao princípio do contraditório*"

[139]Nas palavras de Fernando Gonçalves e Manuel João alves, "*Num puro sistema acusatório conjugado com o princípio da inocência, a acusação tem o ónus de provar os factos que imputa ao arguido. Se o não conseguir, nem por isso a defesa tem qualquer ónus de provar a inocência para que a absolvição surja.*" in A prova do crime, meios legais para a sua obtenção, p. 146

pelas partes, sem que haja necessidade de alegar e provar a impossibilidade de os juntar no decurso do inquérito ou da instrução[140] na procura da verdade material, acentuando que *"não valem em julgamento, nomeadamente para o efeito de formação da convicção do tribunal, quaisquer provas que não tiverem sido produzidas ou examinadas em audiência"* (artigo 355.º do CPP).

Na fase de inquérito, compete ao MP a respetiva direção (artigos 263.º n.º1 e 264.º n.º1 do CPP), na fase de instrução a direção é da competência do Juiz de instrução, que difere do Juiz de julgamento, sendo este que aprecia e valora a prova produzida sobre a factualidade vertida nos autos, podendo ordenar a realização de quaisquer diligências probatórias que se lhe afigure necessário à descoberta da verdade e à boa decisão da causa (artigo 340.º do CPP) por força do princípio de investigação. Não há paridade entre o MP e o arguido dado que durante a fase preliminar do processo, o MP tem ao seu dispor meios humanos (os órgãos de polícia criminal) e meios técnicos e tecnológicos para investigar que o arguido não tem. Além disso, não impende sobre nenhum dos sujeitos qualquer ónus da prova (diferentemente do que ocorre no âmbito civil), pois não vigora o princípio do dispositivo, nem o da auto-responsabilidade probatória das partes. Não poderá então o processo penal ser visto como um processo de partes, mas é reconhecida uma participação específica e dinâmica a cada um dos sujeitos processuais nos vários momentos do processo.[141]

2.2. A prova em processo Penal

A prova consiste no *"esforço metódico através do qual são demonstrados os factos relevantes para a existência do crime, a punibilidade do arguido e a determinação da pena ou medida de segurança aplicáveis"*[142]. "As provas têm por função a demonstração da realidade dos factos" (artigo 341.º do Código Civil) sendo que *"constituem objecto da prova todos os factos juridicamente relevantes para a existência ou inexistência do crime, a punibilidade ou não punibilidade do arguido e a determinação da pena ou da medida de segurança aplicáveis"*

[140]MESQUITA, Paulo Dá, A PROVA DO CRIME E O QUE SE DISSE ANTES DO JULGAMENTO, Estudo sobre a prova no Processo Penal Português, à Luz do sistema Norte-Americano... p.258

[141] NEVES, Rosa Vieira, A Livre Apreciação da Prova e a Obrigação de Fundamentação da Convicção (na Decisão Final Penal)...pp.81-86

[142] MENDES, Paulo de Sousa, As proibições de prova no processo penal, Jornadas de Direito Processual Penal e Direitos Fundamentais, Coordenação Científica de Maria Fernanda Palma, Almedina, 2004, p. 132 ou 133 (verificar)

e havendo pedido civil, valem também os fatos relevantes para determinação da responsabilidade civil (artigo 124.º n.os 1 e 2 do CPP). Não pode ser alcançada a todo e qualquer custo, na regulamentação desta matéria (no livro III, artigos 124.º a 190.º do CPP), denota-se a preocupação do legislador no respeito pelos imperativos constitucionais atinentes à dignidade da pessoa humana, à integridade pessoal e à intimidade da vida privada e familiar, próprios de um Estado de Direito Democrático[143].

Existem vários tipos de prova: a prova perfeita que leva à conclusão de que o agente praticou ou não o ilícito-típico; a prova imperfeita que carece da conjugação com outras provas para que se chegue a uma conclusão; a prova direta dá-se quando incide diretamente sobre os factos que se pretendem provar; e a prova indiciária que é uma prova indireta, obtida através da indução e de um raciocínio empírico, da ciência ou da técnica verifica-se (induz-se) o facto que se quer provar, parte-se de um facto conhecido (que indicia) para o facto desconhecido que se procura provar, o indício é necessário quando o facto respeite a uma só causa, mas quando possa ser atribuído a várias causas já será um indício provável ou possível; as provas pessoais são recolhidas pela declaração da própria pessoa e pelos comportamentos desta quando presta depoimento (expressões), na prova real ou prova pessoal passiva, a pessoa é antes objeto de observação, não importando nestas o alcance das declarações.[144] No nosso ordenamento jurídico não há um elenco taxativo das provas admissíveis, há liberdade de prova desde que não seja prova proibida por lei (artigo 125.º do Código do Processo Penal - CPP).[145]

Antes de aprofundarmos as características da prova eletrónico-digital importa-nos aludir de modo sucinto aos princípios que estão subjacentes.

2.3. Princípios relativos à prova

Em respeito do princípio da legalidade da prova (artigo 2.º do CPP), consta no artigo 125.º do CPP que *"são admissíveis todas as provas que não forem proibidas por lei"*, a nossa Constituição contempla serem *"nulas todas as provas obtidas mediante tortura, coacção,*

[143] GONÇALVES, Fernando; ALVES, Manuel João, A PROVA DO CRIME, Meios Legais para a sua Obtenção, Almedina, 2009, ISBN 978-972-40-3971-8, p.121

[144] JESUS, Francisco Marcolino de, Os Meios de Obtenção da Prova em Processo Penal, 2011, Almedina. ISBN 978-972-40-4428-6. pp. 75-79

[145] SILVA, Germano Marques da, curso de processo penal, II, Editorial Verbo, 1999, p. 114. Apud JESUS, Francisco Marcolino de, Os Meios de Obtenção da Prova em Processo Penal, 2011, Almedina. ISBN 978-972-40-4428-6. p. 81

ofensa da integridade física ou moral da pessoa, abusiva intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações" (artigo 32.º n.º8) e *"é proibida toda a ingerência das autoridades públicas na correspondência, nas telecomunicações se nos demais meios de comunicação, salvo os casos previstos na lei em matéria de processo criminal"* (artigo 34.º n.º4) correspondendo aos métodos proibidos previstos no artigo 126.º do CPP.

As proibições de prova (dedicamos um estudo mais aprofundado no ponto 2.5) constituem um limite à descoberta da verdade enquanto as regras de produção de prova visam disciplinar os processos e modos de a alcançar.[146]

No artigo 127.º do CPP está consagrado o princípio da livre apreciação da prova[147], esta é apreciada segundo as regras da experiência e a livre convicção da entidade competente, exceto quando haja disposição legal em sentido diferente, tal como acontece na prova pericial, segundo o artigo 163.º do CPP: *" 1 - O juízo técnico, científico ou artístico inerente à prova pericial presume-se subtraído à livre apreciação do julgador. 2 - Sempre que a convicção do julgador divergir do juízo contido no parecer dos peritos, deve aquele fundamentar a divergência"*[148]. Porém, *"Sempre que a convicção do julgador divergir do juízo contido no parecer dos peritos, deve aquele fundamentar a divergência" (n.º2 do mesmo artigo), trata-se de uma presunção iuris tantum que pode ser afastada mediante prova em contrário, devendo ser fundamentada, apresentando o juiz os motivos da divergência do seu juízo valorativo. "O que equivale a dizer que, em sede de apreciação da prova, o julgador poderá afastar o juízo técnico e científico contido no parecer emitido pelo perito, desde que, ele próprio, possua conhecimentos de igual*

[146] GONÇALVES, Fernando; ALVES, Manuel João, A PROVA DO CRIME, Meios Legais para a sua Obtenção...p. 128

[147] Este modo de valoração da prova resultada Revolução Francesa de 1789, e a sua implementação deve-se essencialmente à instituição do tribunal de juri, onde aos jurados era permitido uma garantia de imparcialidade face às decisões proferidas pelos magistrados, que julgavam de acordo com as leis emadas pelo monarca "Entendia-se que o critério último da verdade residia na íntima convicção dos jurados, que, despojados das "amarras" legalmente impostas pelo legislador em sede de valoração da prova, assentavam aquela convicção na força da razão, e não na vontade, em última instância, do soberano." Atente-se que deixar nas mãos dos jurados a valoração da prova aumenta a probabilidade de cometimento de erro judiciário. NEVES, Rosa Vieira, A Livre Apreciação da Prova e a Obrigação de Fundamentação da Convicção (na Decisão Final Penal), Coimbra Editora, 2011, ISBN 978-972-32-1929-6, PP.56-58

[148] O mesmo acontece com o valor probatório dos documentos autênticos e autenticados (artigo 169.º do CPP, quanto à confissão integral e sem reservas do arguido em audiência de julgamento, quando o crime for punível com pena de prisão até cinco anos (artigo 344.º do CPP) e quanto a pedido cível (artigo 84.º do CPP) a sentença penal que aprecie e julgue o pedido civel de indemnização faz caso julgado material em processo civil. GONÇALVES, Fernando; ALVES, Manuel João, A PROVA DO CRIME, Meios Legais para a sua Obtenção...pp. 142-143

valor técnico ou científico que possam colocar em crise a conclusão firmada no relatório pericial."[149]

A liberdade a que referida neste artigo, como ensina Castanheira Neves, *"não é, nem deve implicar nunca o arbítrio, ou sequer a decisão irracional, puramente impressionista-emocional que se furte, num incondicional subjectivismo, à fundamentação e à comunicação"*[150].

A prova surge como fundamento e limite da atividade jurisdicional, fundamento porque sem a produção e constatação da mesma não haveria decisão quer condenatória quer absolutória e limite porque o julgador não pode decidir pela condenação sem prova ou contra a prova produzida. Surgem contudo limitações a este princípio da livre apreciação da prova, dado o valor probatório atribuído à prova pericial, aos documentos autênticos e autenticados e ao valor do caso julgado[151].[152]

Anteriormente, só era valorada a confissão do arguido em sede de audiência de discussão e julgamento, com as alterações de 2013 ao Código de Processo Penal, introduzidas pela Lei n.º20/2013, a principal marca distintiva dessas alterações consiste na aceitação como meio de prova das declarações feitas pelo arguido anteriormente ao julgamento. Dantes, as declarações do arguido só podiam ser valoradas se fossem produzidas em audiência, conforme o anterior artigo 357.º, n.º1, com as alterações desta Lei, veio tornar possível aproveitar as declarações processuais do arguido anteriores ao julgamento. Cremos juntamente com Sousa Mendes, que se coloca em causa a estrutura acusatória do direito penal, assim com, alguns princípios jurídicos que vão desde o contraditório, a igualdade de armas, da oralidade, da imediação, podendo também desencadear na prática reação do arguido de antecipar o silêncio para uma fase anterior ao julgamento, limitando assim a recolha de informações na investigação.[153]

[149] NEVES, Rosa Vieira, A Livre Apreciação da Prova e a Obrigação de fundamentação da Convicção (na decisão final penal)...pp. 94-95
[150] *In* NEVES, A. Castanheira, Sumários de Processo Criminal (ed. policopiada), Coimbra, 1968, p. 53. Vol. II, n.º144. *Apud* SILVA, Germano Marques da, DIREITO PROCESSUAL PENAL PORTUGUÊS, Noções gerais, sujeitos processuais e objecto, p. 96.
[151] Vide. NEVES, Rosa Vieira, A Livre Apreciação da Prova e a Obrigação de fundamentação da Convicção (na decisão final penal), pp. 92-104
[152] idem, pp. 91-93
[153] MENDES, Paulo de Sousa, Lições de processo penal, pp. 48-49

A prova pericial[154] é dos meios probatórios mais utilizados na recolha de prova dos crimes informáticos.

O Juiz não pode deixar de fundamentar a sua decisão (artigos 205.º n.º1 CRP e 97.º n.º5 do CPP), conforme o artigo 374.º n.º2 do CPP, onde consta "*Ao relatório segue-se a fundamentação, que consta da enumeração dos factos provados e não provados, bem como de uma exposição tanto quanto possível completa, ainda que concisa, dos motivos, de facto e de direito, que fundamentam a decisão, com indicação e exame crítico das provas que serviram para formar a convicção do tribunal*" sob pena de nulidade da sentença (artigo 379.º do CPP). A fundamentação das decisões judiciais assegura a aceitação pelas instâncias superiores, e possibilita um controlo por parte dos sujeitos processuais e do público em geral, concretizando assim, as garantias de defesa do arguido (artigos 32.º n.º1 da CRP e 10.º e 11.º da Declaração Universal dos Direitos Humanos)[155].

Segundo o princípio da investigação ou da verdade material, o tribunal não está limitado pela prova dos factos feitos pela acusação e defesa, pois tem o poder/dever de investigação oficiosa. *"Definido o objecto do processo pela acusação e delimitado consequentemente o objecto do julgamento, o tribunal deve procurar a reconstrução histórica dos factos, deve procurar por todos os meios processualmente admissíveis alcançar a verdade histórica, independentemente ou para além da contribuição da acusação e da defesa; contrariamente ao que sucede no processo civil, não existe ónus da prova em processo penal. O tribunal pode e deve ordenar oficiosamente toda a produção de prova que entenda por necessária ou conveniente para a descoberta da verdade."*[156]

Como corolários deste princípio, temos o princípio *in dubio pro reo* e o princípio da imediação.

Segundo o primeiro, havendo dúvida quanto à matéria probatória, a decisão deve ser a mais favorável ao arguido, concretizando assim o princípio da presunção da inocência, o Juiz não pode abster-se de decidir *("non liquet")* e as consequências de não se conseguir provar devem ser sofridas por quem tinha obrigação de fazer prova, o Ministério Público e subsidiariamente o Juiz.

---

[154]Artigo 151 do CPP: "A prova pericial tem lugar quando a percepção ou a apreciação dos factos exigirem especiais conhecimentos técnicos, científicos ou artísticos"

[155] JESUS, Francisco Marcolino de, Os Meios de Obtenção da prova em processo Penal...pp.100-102

[156] SILVA, Germano Marques da, DIREITO PROCESSUAL PENAL PORTUGUÊS: Noções Gerais, sujeitos processuais e objecto, Vol.I, 7.ª ed. Isboa: Universidade Católica Editora, 2013. ISBN 978-972-54-0399-0, p. 96

No que toca ao princípio da imediação, é-lhe atribuído dois sentidos: o primeiro consiste na utilização dos meios de prova originais; o segundo pressupõe a oralidade do processo, concretiza-se na relação de proximidade comunicante entre o tribunal e os participantes no processo de modo a existir uma perceção do material (probatório) que levará à decisão. O Princípio da Contraditoriedade certifica-se na estruturação da audiência de julgamento, compreende um debate ou discussão entre a acusação e a defesa, onde são apresentadas as razões de facto e de direito, as provas, e é questionado o valor das mesmas, ficando excluída a possibilidade de condenação com base em elementos de prova que não tenham sido discutidos em audiência.[157]

Parece-nos importante aludirmos ao princípio *nemo tenetur* no levantamento da questão sobre se seria admissível a revelação coativa da *password* para desencriptação de dados obtidos em buscas ao domicílio mas estando os discos rígidos cifrados - teriam os arguidos que entregar as passwords dos computadores apreendidos[158]? Esta questão surgiu num acórdão inglês[159], onde o tribunal *ad quem* entendeu que sendo os dados cifrados incriminatórios, e o acesso a esses dados dependa da revelação da *password*, então esse conhecimento poderá ser incriminatório. Entendeu ser um caso de possível aplicação do privilégio contra a auto-incriminação, mas como este admite exceções legais, o tribunal invocou o princípio da proporcionalidade, e estando os dados na posse da polícia de forma legal, a revelação da *password* é uma medida proporcional, levando a uma pena de prisão de dois anos (artigo 53.º da RIPA) a sua não revelação.

Relativamente ao nosso ordenamento jurídico, Figueiredo Dias e Costa Andrade reparam que, não obstante, o princípio *nemo tenetur*, na vertende de direito ao silêncio do arguido, seja na sua dimensão de privilégio contra uma auto-incriminação, não esta consagrado expressamente na constituição da república portuguesa, a doutrina e a jurisprudência são unânimes quanto à vigência desse princípio no nosso direito processual penal, ainda quanto à sua natureza constitucional. Desde logo, pela consagração jurídico-constitucional de valores ou

[157] GONÇALVES, Fernando; ALVES, Manuel João, A prova do crime, meios legais para a sua obtenção, pp. 144-149

[158] Nesta análise seguimos de perto o estudo de: PINTO, Lara Sofia, Privilégio contra a auto-incriminação versus colaboração do arguido, in PROVA CRIMINAL E DIREITO DE DEFESA, estudos sobre teoria da prova e garantias de defesa em processo penal, Reimpressão, coord. Teresa Pizarro Beleza e Frederico de Lacerda da Costa Pinto, Almedina, Coimbra, 2011, ISBN 978-972-40-4090-5, pp.91-116

[159] É o Acórdão [2008] EWCA Crim 2117 do *Supreme Court of Judicature (Criminal Divisio), Disponível em: http://www.bailii.org/ew/cases/EWCA/Crim/2008/2177.html*

direitos fundamentais como a dignidade humana, a liberdade de ação, e a presunção da inocência. A lei processual penal contém normas que asseguram esse princípio, tais como o direito ao silêncio do arguido (artigo 343.º, n.º1 , artigo 345.º, n.º1), assim como o dever de esclarecimento ou advertência sobre os direitos decorrentes daquele princípio (nos artigos 58.º, n.º2, 61.º, n.º1, alínea h), 141.º, n.º4, alínea a))[160].

Sofia Pinto teceu as seguintes conclusões: "*Já no que toca ao enquadramento deste caso face ao Direito Português, podemos afirmar que estamos no âmbito de aplicação do direito ao silêncio (artigo61.º/1, d) CPP, em virtude de estarmos perante uma declaração do arguido (a revelação da password) que é incriminatória (como resulta do exposto). Ora, no panorama legal português, não há uma previsão legal no sentido de estabelecer uma excepção ao princípio nemo tenetur (direito ao silêncio), ao contrário do que se passa na lei inglesa. Daqui decorre que não será exigível a revelação da password (porquanto constitui uma declaração incriminatória), sob pena de violação do estatuto processual do arguido. Conclui-se, pois, que não é exigível a colaboração do arguido neste caso (i.e. não tem de revelar a password de desencriptação) na medida em que não existe uma disposição legal que imponha essa colaboração em concreto"*[161].

Não vamos neste estudo aprofundar todos os meios de prova (a prova testemunhal, as declarações do arguido, do assistente e das partes civis, a acareação, o reconhecimento, a reconstituição do facto, a perícia e o documento, constam do livro III, Título II, artigos 128.º e seguintes) e meios de obtenção de prova (o exame, a revista e a busca, a apreensão e a escuta telefónica, constam do livro III, Título III, artigos 171.º e seguintes) previstos no Código de Processo Penal, sob pena de nos desviarmos do nosso tema.

Pinto de Albuquerque[162] distingue-os do seguinte modo: *"Os meios de obtenção de prova visam a detecção de indícios da prática do crime, constituindo um meio de aquisição para o processo de uma prova"pré-existente" e, em regra, contemporânea ou preparatória do crime. Os meios de prova formam-se no momento da sua própria produção no processo,*

[160]DIAS, Jorge de Figueiredo; ANDRADE, Manuel da Costa, Supervisão, direito ao silêncio e legalidade da prova, p.45
[161]PINTO, Lara Sofia, Privilégio contra a auto-incriminação versus colaboração do arguido, p. 116
[162] ALBUQUERQUE, Paulo Pinto de, Comentário do Código de processo Penal: à luz da Constituição da República Portuguesa e da Convenção Europeia dos Direitos do Homem, 3.ª ed. actualizada, Universidade Católica Editora, 2009, ISBN 978-972-54-0202-3, p. 315

visando a "reprodução" ("avaliação") do facto e, nessa medida, constituindo um meio de aquisição para o processo de uma prova "posterior" à prática do crime".

Seguidamente, procedemos à análise das disposições processuais previstas na Lei do Cibercrime, para obtenção de prova nos crimes previstos nessa lei, e também para outros crimes previstos no Código Penal praticados com recurso a meios informáticos (artigo 11.º da mencionada Lei).

2.4. Obtenção da Prova Digital

Com a globalização, os agentes deste tipo de criminalidade conseguem adaptar-se e cometer os ilícitos mais facilmente, tornando-se difícil para os sistemas formais de controlo, acompanharem o ritmo dessa criminalidade, uma vez que a investigação encontra entraves ou limites processuais, na salvaguarda de direitos fundamentais.

Não existem ainda muitas definições de prova digital, uma vez que a Lei em apreço entrou em vigor em 2009 e serem poucos os Autores nacionais que se dedicam a este tema, apresentamos em seguida duas definições distintas.

RODRIGUES, define prova eletrónico-digital "*como qualquer tipo de informação, com valor probatório, armazenada [em repositório electrónico-digitais de armazenamento] ou transmitida [em sistemas e redes informáticas ou rede de comunicações electrónicas, privadas ou publicamente acessíveis], sob a forma binária ou digital".*[163]

Dias Ramos define esta prova "*como sendo toda a informação passível de ser obtida ou extraída de um dispositivo eletrónico (local, virtual ou remoto) ou de uma rede de comunicações. Pelo que esta prova digital, para além de ser admissível, deve ser também autêntica, precisa e concreta"*[164]. Dá-mos preferência a esta última definição por ser mais clara que a anterior.

As principais características da prova digital[165] são: que esta assume carácter temporário, pelo de decurso do tempo a prova pode deixar de existir; é fungível, dada a facilidade de

[163] RODRIGUES, Benjamin Silva. DA PROVA PENAL – Tomo IV, DA PROVA ELECTRÓNICO – DIGITAL E DA CRIMINALIDADE INFORMÁTICO – DIGITAL, p.39

[164] RAMOS, Armando Dias, A prova digital em processo penal, p. 86

[165] Quanto ao modo como deve ser recolhida e preservada a prova remetemos para MARQUES, Pedro Penha Leitão da, Informática forense, recolha e preservação da prova digital, Dissertação de mestrado, sob orientação de Prof. Doutor Rui Alves Pires, maio, 2013, Universidade Católica Portuguesa, Faculdade de Engenharia, disponível em

substituição dos dados informáticos por outros; é volátil, pois facilmente se escondem esses dados, podendo ser ocultados ou suprimidos, do suporte original; por fim, cumpre-nos salientar a fragilidade da prova, cujo manuseamento deverá ser cuidadosamente efetuado[166]. Como bem repara Miren Josune Pérez Estrada, *"(...) no se puede cuestionar que la evolucíon tecnolólica ha supuesto un incrementode la calidad de vida y un desarrollo en laestructura social y económica. Se habla ya de una nueva civilización caracterizada por la instantaneidad y la desaparicíon de las distancias, pero tambíen es evidente que este gran avance tecnológico perjudica, en ocasiones, los intereses ajenos. Aparecen nuevos medios para delinquir y ello conlleva la necesidad de investigar dichos delitos a través de los, tambíen, nuevos medios tecnológicos"*[167].

A Lei do Cibercrime consagrou esses novos modos de investigar, que abordaremos em seguida. Inserimos também alguma jurisprudência onde se manifestam entendimentos sobre as disposições processuais.

O Artigo 11.º da Lei em estudo, define qual o âmbito de aplicação das normas processuais contidas nessa Lei, excetuando o disposto nos artigos 18.º e 19.º, pode aplicar-se a crimes: a) previstos nessa lei; b) cometidos por meio de um sistema informático; ou c) em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico. Acresce ainda que essas normas não prejudicam a lei sobre conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações telefónicas publicamente disponíveis ou de redes públicas de comunicação (Lei 32/2008, de 17 de Julho), esta lei não abrange os dados de conteúdo, que se encontram cobertos pela definição de dados informáticos da Lei do Cibercrime *são "«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"*.[168]

10-10-2014.http://repositorio.ucp.pt/bitstream/10400.14/13191/1/Disserta%C3%A7%C3%A3o%20-%20Recolha%20e%20preserva%C3%A7%C3%A3o%20da%20prova%20digital.pdf com acesso

[166]RAMOS, Armando Dias, A prova digital em processo penal, p. 88

[167] ESTRADA, Miren Josune Pérez, La investigacíon del delito a través de las nuevas tecnologías. Nuevos medios de investigagíon en el processo penal, in DERECHO PENAL INFORMÁTICO, José Luis de la Cuesta Arzamendi (director), Primera edición, 2010, Civitas, ISBN 978-84-470-3429-1, pp. 306-307

[168] MESQUITA, Paulo Dá, Processo Penal, Prova e Sistema Judiciário...pp.108-110

2.4.1. Preservação expedita de dados (artigo 12.º)

As empresas de exploração de serviços de telecomunicações solicitaram pareceres à Procuradoria Geral da República quanto aos termos e conteúdo da colaboração com as autoridades de investigação criminal, relativamente aos serviços de comunicações que prestam, e é nesse contexto que surge o parecer n.º 16/94 e respectivo parecer complementar.

No que toca à proteção de dados[169] face à informática, e no que concerne ao serviço telefónico em geral, a Procuradoria Geral da República[170] seguiu as orientações de YVES POULLET e FRANÇOISE WARREN que distinguem "*(...)três espécies de dados ou elementos; os dados relativos à conexão à rede, ditos dados de base; os dados funcionais necessários ao estabelecimento de uma ligação ou comunicação e os dados gerados pela utilização da rede (p. ex. localização do utilizador, localização do destinatário, duração da utilização, data e hora, frequência), dados de tráfego; dados relativos ao conteúdo da comunicação ou da mensagem, dados de conteúdo*"[171].

A Lei do Cibercrime no artigo 2.º alínea c) estabelece que são 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"*.

A jurisprudência tem vindo a defender que o acesso a dados associados a um endereço de IP (*Internet Protocol*)[172] configura um pedido de dados de tráfego, conforme definição legal

---

[169] Em linguagem informática, configura dados, "*Factos, noções ou instruções representados de uma forma conveniente para um processo de comunicação*". MATOS, José A. de, Dicionário de Informática e Novas Tecnologias, 3.ª ed. aumentada, FCA - Editora de Informática, LDA. ISBN 978-972-722-469-2, p. 103.

[170] *Em pareceres anteriores do Conselho Consultivo (v. o Parecer n.º 21/2000, de 16 de Junho de 2000, homologado e publicado no Diário da República n.º 198, II Série, de 28 de Agosto de 2000, que originou a Directiva n.º 5/2000 – Despacho de 7 de Agosto de 2000, o Parecer n.º 16/94-Complementar, de 2 de Maio de 1994, publicado em Pareceres, edição da Procuradoria-Geral da República, vol. VI, pág. 535 e segs., e ainda o Parecer n.º 16/94, de 24 de Junho de 1994, que originou a Circular n.º 13/94, da Procuradoria-Geral da República) estabelecia-se uma distinção entre três categorias de dados: dados de base, dados de tráfego e dados de conteúdo."* Informação retirada de parecer do Conselho Consultivo da PGR com o n.º P000792008, disponível em http://www.dgsi.pt/pgrp.nsf/0/b90edf9f8e8a47e480257515003eb4e8, consultado em 08-10-2014

[171] *In YVES POULLET e FRANÇOISE WARREN, "Noveaux compléments au service teléphonique et protection des donnés: à la recherche d'un cadre conceptuel" - in Droit de L'Informatique et des Télécoms, 7 éme année; 1990/91, 1, pág. 19 e segs. que se seguiu de perto." Apud site oficial da Procuradoria Geral da República, pareceres VII, utilização da informática, disponível em http://www.pgr.pt/pub/Pareceres/VII/2.html, consultado em 08-10-2014*

[172] Entende-se por IP ou Internet Protocol, "O protocolo que especifica o formato de pacotes de dados e esquemas de endereçamento que existe na Internet e outras redes. Este protocolo pode ser combinado com o TCP (Transmission Control Protocol), responsável pela ligação virtual entre a fonte e o destino".MATOS, José A. de,

(alínea d) do número e artigo 2.º) da Lei n.º 41/2004, de 18 de Agosto *"dados de tráfego" são «quaisquer dados tratados para efeitos do envio de uma comunicação através de uma rede de comunicações electrónicas ou para efeitos de facturação da mesma». Mais explicitamente refere o considerando (15) da Directiva n.º 2002/58/CE, de 12 de Julho de 2002, transposta para o ordenamento jurídico português pela Lei n.º 41/2004, que "uma comunicação pode incluir qualquer informação relativa a nomes, números ou endereços fornecida pelo remetente de uma comunicação ou pelo utilizador de uma ligação para efectuar a comunicação. Os dados de tráfego podem incluir qualquer tradução desta informação pela rede através da qual a comunicação é transmitida, para efeitos de execução da transmissão. Os dados de tráfego podem ser, nomeadamente, relativos ao encaminhamento, à duração, ao tempo ou ao volume de uma comunicação, ao protocolo utilizado, à localização do equipamento terminal do expedidor ou do destinatário, à rede de onde provém ou onde termina a comunicação, ao início, fim ou duração de uma ligação. Podem igualmente consistir no formato em que a comunicação é enviada pela rede".*

Quando se pedem a identificação e morada do utilizador do serviço (considerados dados de base[173]), é da competência do Ministério Público efetuar o pedido. No entanto quando se pretende obter informação mais alargada no âmbito do tráfego terá que ser solicitada com autorização judicial[174].

"Assim a identificação de um determinado endereço de IP conjugada com a identidade de quem o utilizou num dado dia e hora não revela informação sobre o percurso da comunicação nem sobre outro eventual tráfego comunicacional da pessoa em causa. Apenas comprova que essa mesma comunicação (e apenas essa) foi efetuada por via daquele número técnico de acesso à Internet. (...) com essa informação apenas se estabelece ligação entre uma determinada comunicação que se conhece já e a respectiva origem (...) Obter a identificação do utilizador de um endereço de IP (...) num determinado dia e hora não é susceptível de revelar informação privada ou confidencial e apenas permite confirmar que uma comunicação - que a

Dicionário de Informática e Novas Tecnologias, 3.ª ed. aumentada, FCA - Editora de Informática, LDA. ISBN 978-972-722-469-2, pp.202-203

[173] Acórdão do Tribunal da Relação de Évora, de 7 de dezembro de 2012, Processo nº 72/11.2DFTR-A.E1, com relator MARTINHO CARDOSO, disponível em http://www.dgsi.pt; Acórdão do Tribunal da Relação de Lisboa, de 18 de janeiro de 2011, Processo nº 3142/09.3PBFUN-A.L1-5, com relator FILOMENA CLEMENTE LIMA, disponível em http://www.dgsi.pt

[174] Acórdão do Tribunal da Relação de Évora, de 13 de Novembro de 2012, Processo nº 315/11.2PBPTG-A.E1, com relator GILBERTO CUNHA, disponível em http://www.dgsi.pt

investigação conhecia já - ocorreu" Sendo nestes casos competente o Ministério Público, conforme Acórdão do Tribunal da relação de Lisboa de 19 de Junho de 2014[175].

A Lei do Cibercrime prevê neste artigo a preservação de dados de tráfego por determinação das autoridades judiciárias a terceiros que não se encontrem abrangidos na Lei 32/2008, esta impõe aos fornecedores de serviço a conservação de dados que só serão utilizados em processo quando esteja em causa criminalidade grave – artigo 3.º e depende de despacho fundamentado por Juiz para que se utilizem esses dados- Enquanto a preservação dos dados ordenados ao abrigo do artigo 12.º da LC servem de prova no processo que levou à ordem de preservação.

A preservação expedita de dados terá aplicabilidade também noutros crimes que não os catalogados como crimes graves, desde que respeitem a processos relativos a crimes previstos na Lei do Cibercrime, cometidos por meio de um sistema informático, ou em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico, resulta da conjugação do artigo 12.º com o artigo 11.º da Lei do cibercrime[176].

Quando no decurso do processo for necessário obter dados informáticos específicos armazenados num sistema informático podendo ser: um documento eletrónico nos termos do DL n.º290D/99, de 2 de Agosto; um programa de computador, protegido ou não nos termos do DL n.º252/94, de 20 de Outubro; dados pessoais, para efeitos da Lei 67/98, de 26 de Outubro; ou ainda dados de tráfego ou dados de localização, nos termos da Lei 41/2004, de 18 de Agosto[177]. Incluindo dados de tráfego, para produção de prova e existindo receio fundamentado de possível perda, alteração, ou futura indisponibilidade desses dados, a autoridade judiciária competente, ordena a quem tenha disponibilidade ou controlo destes, designadamente ao Fornecedor de Serviços, que preserve os dados em causa (conforme ao artigo 12.º n.º1).

O órgão de polícia criminal pode ordenar a preservação dos dados quando devidamente autorizado pela autoridade judiciária competente ou quando haja urgência ou perigo na demora, sendo que nestas situações, deve dar-se notícia imediata do facto à autoridade judiciária, transmitindo-lhe o relatório previsto no artigo 253 do Código de Processo Penal (n.º2.º do artigo em apreço).

---

[175] Acórdão do Tribunal da Relação de Lisboa, de 19-06-2014, Processo nº 1695/09.5PJLSB.L1-9, com relator MARGARIDA VIEIRA DE ALMEIDA, disponível em http://www.dgsi.pt

[176] Acórdão do Tribunal da Relação de Coimbra, de 26-02-2014, Processo nº 559/12.0GBOBR-A.C1, com relator FERNANDO CHAVES, disponível em http://www.dgsi.pt

[177] VENÂNCIO, Pedro Dias, Lei do cibercrime, p.99

A ordem de preservação descrimina a natureza dos dados, origem e destino, e o período de tempo de preservação até um máximo de três meses (n.º3). Aquele a quem foi dada a ordem terá de imediato que preservar os dados e garantir a confidencialidade da aplicação da medida processual (n.º4 do artigo 12.º). Esta regra, sendo adjetiva, não impõe àquele a quem foi ordenado a preservação dos dados, nenhuma sanção se o não fizer, nem remete diretamente para alguma disposição de direito substantivo, assim como nas demais disposições do código de processo penal, nem precisa de o fazer, uma vez que o Código Penal já pune o crime de desobediência no artigo 348.

Coloca-se a questão de saber qual a sanção para aqueles que tenham o acesso aos dados e que se recusem a cooperar com o que lhes fora ordenado. Parece-nos que também no artigo 12.º n.º4 poderia constar *"(…) sob pena de punição por desobediência"*, à semelhança do prescrito no artigo 14.º n.º1 da lei em apreço. Silva Rodrigues entende que o Juiz de instrução criminal é competente a requerimento do Ministério Público, no seguimento da evolução legislativa recentemente ocorrida em matéria das escutas, no artigo 187.º, n.º1 do Código de Processo Penal[178].

Num recente acórdão do Tribunal de Justiça da União Europeia, de 8 de Abril de 2014[179], decidiu-se que a Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de março

[178] RODRIGUES, Benjamim Silva, Da prova penal, tomo IV, p. 521.

[179] Estabelece o Acórdão do Tribunal de Justiça da União Europeia, de 8 de Abril de 2014 "Quanto à questão de saber se a ingerência que a Diretiva 2006/24 comporta se limita ao estritamente necessário, importa salientar que esta diretiva impõe, nos termos do seu artigo 3.°, conjugado com o seu artigo 5.°, n.° 1, a conservação de todos os dados relativos ao tráfego respeitante à rede telefónica fixa, à rede telefónica móvel, ao acesso à Internet, ao correio eletrónico através da Internet e às comunicações telefónicas através da Internet. Assim, visa todos os meios de comunicação eletrónica cuja utilização está muito divulgada e é de importância crescente na vida quotidiana de todos. Além disso, em conformidade com o seu artigo 3.°, a referida diretiva abrange todos os assinantes e utilizadores registados. Comporta, portanto, uma ingerência nos direitos fundamentais de quase toda a população europeia.[...]Em segundo lugar, a esta ausência geral de limites acresce que a Diretiva 2006/24 não estabelece critérios objetivos que permitam delimitar o acesso das autoridades nacionais competentes aos dados e a sua utilização posterior para prevenir, detetar ou agir penalmente contra infrações suscetíveis de ser consideradas suficientemente graves, à luz da amplitude e da gravidade da ingerência nos direitos fundamentais consagrados nos artigos 7.° e 8.° da Carta, para justificar tal ingerência. Pelo contrário, a Diretiva 2006/24 limita‑se a remeter, no seu artigo 1.°, n.° 1, de forma genérica, para as infrações graves tal como definidas no direito nacional de cada Estado‑Membro [...] no que respeita às regras relativas à segurança e à proteção dos dados conservados pelos fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações, há que concluir que a Diretiva 2006/24 não prevê garantias suficientes, como exige o artigo 8.° da Carta, que permitam assegurar uma proteção eficaz dos dados conservados contra os riscos de abuso e contra qualquer acesso e utilização ilícita dos mesmos. Com efeito, em primeiro lugar, o artigo 7.° da Diretiva 2006/24 não estabelece regras específicas e adaptadas à grande quantidade de dados cuja conservação é imposta por esta

de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Diretiva 2002/58/CE, é inválida, por entender que se violam direitos fundamentais de todos os cidadãos na conservação de dados, quando só uma minoria pratica esses crimes. Parece-nos que essa declaração de invalidade da Diretiva, não levará à revogação da Lei 32/2008, pois o nosso legislador foi prudente e consagrou requisitos apertados para que se utilizem os dados preservados pelos fornecedores de serviço, desde logo, crimes graves e despacho fundamentado de Juiz, respeitando-se assim direitos constitucionalmente protegidos.

Pedro Verdelho sublinha que a lei está em vigor, uma vez que ainda não foi revogada, e que o nosso legislador teve o cuidado de elencar os crimes e enunciou o período de conservação dos dados, algo que a Diretiva não definiu. Como não se sabe quais os dados que vão fazer falta é preferível que se gravem todos, em muito boa parte, a lei portuguesa responde às criticas do tribunal de justiça, daí ainda estar em vigor. Não se trata de uma Diretiva de Processo Penal, mas sim, de mercado interno. À data da mesma não havia ainda o tratado de Lisboa que incumbiu aos Estados Membros a regulamentação das garantias.[180] Independentemente do que vier a decidir-se sobre esta questão, deve respeitar-se o sagrado princípio da proporcionalidade na medida a tomar. Se não se conservarem os dados pelo período de um ano ou se não forem alcançados os dados em tempo útil, subsequentemente não se faz prova do cometimento ou não cometimento do crime, sendo suficiente para que toda a investigação seja condenada ao insucesso[181].

---

diretiva, ao caráter sensível destes dados e ao risco de acesso ilícito aos mesmos, regras que se destinariam, designadamente, a regular de maneira clara e estrita a proteção e a segurança dos dados em causa, a fim de garantir a sua plena integridade e confidencialidade. Além disso, também não foi prevista uma obrigação precisa de os Estados‑Membros estabelecerem tais regras. Face ao exposto, há que considerar que, ao adotar a Diretiva 2006/24, o legislador da União excedeu os limites impostos pelo respeito do princípio da proporcionalidade à luz dos artigos 7.°, 8.° e 52.°, n.° 1, da Carta. ", disponível em http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=PT&mode=req&dir=&occ=first&part=1&cid=128161, consultado em 27-06-2014

[180] Num workshop com o tema: PROVA DIGITAL EM PROCESSO PENAL - Velhos limites a novas necessidades, de 27 de Junho de 2014 (organizado pela Procuradoria-Geral da República, em colaboração com a Polícia Judiciária) Auditório do edifício Sede da Polícia Judiciária, Rua Gomes Freire, 174, Lisboa

[181] RAMOS, Armando Dias , A prova digital em processo penal: o correio electrónico, chiado editora, 1.º ed. Novembro 2014, ISBN 978-989-51-2383-4, p.88

Costa Andrade[182] alerta-nos para os perigos que podem advir da conservação de dados por entidades privadas, segundo o Autor:

> *A "privatização da investigação" conheceu recentemente um novo impulso com a privatização generalizada (pelo menos na Europa) das empresas de telecomunicação. A que estão confiadas as tarefas de intromissão, intercepção e gravação de telecomunicações e, em geral, da produção e "armazenamento" de dados processualmente relevantes, bem como a sua apresentação ao processo penal. E tanto no que respeita ao conteúdo e dados da comunicação como no que respeita aos dados de localização. Um quadro entretanto reforçado com o aparecimento de novos meios e procedimentos tecnológicos de comunicação, com destaque para a produção e transmissão de dados por internet, inteiramente nas mãos de privados. E a quem são, mais uma vez, cometidos meios de obtenção de prova , como a intromissão no correio electrónico, as diferentes formas da chamada busca online, a intercepção de comunicações telefónicas através da internet (VoIP). (…)*
>
> *"b) Se, nalguns casos, a intervenção dos privados se afigura inevitável e mesmo desejável, não pode esquecer-se que ela comporta os riscos e está exposta aos abusos conaturais aos "sistemas de contacto" (LUHMANN) entre o público e o privado. Perigos agravados e reforçados à medida do aumento da dimensão das empresas de telecomunicação, algumas delas à escala global (v.g., Google, Microsoft) e da crescente assimetria de poder entre aquelas empresas e os indivíduos. E mesmo entre elas e os próprios Estados. Tudo a antecipar a possibilidade de as intromissões arbitrárias nas telecomunicações e as utilizações abusivas dos dados deixarem de ser um exclusivo do Estado."*

2.4.2. Revelação expedita de dados de tráfego (artigo 13.º)

O Fornecedor de Serviços a quem foi ordenada a preservação dos dados, nos termos do artigo precedente, indica de forma imediata ou expedita, à autoridade judiciária competente ou ao órgão de polícia criminal, logo que o souber, outros fornecedores de serviço através dos quais aquela comunicação tenha sido efetuada, de modo a que se identifiquem todos os fornecedores

[182] ANDRADE, Manuel da Costa – "BRUSCAMENTE NO VERÃO PASSADO" A REFORMA DO CÓDIGO DE PROCESSO PENAL, Observações críticas sobre uma lei que podia e devia ter sido diferente.Coimbra Editora, 2009. ISBN 978-972-32-1726-1, pp.127-129

de serviço e assim assegurar a preservação dos dados de tráfego relativos a uma determinada comunicação.

Este artigo revela-nos a importância da cooperação dos fornecedores de serviço com a autoridade judiciária competente ou com o órgão de polícia criminal, ao terem de indicar outros fornecedores de serviço (independentemente do número) para apurar a via através da qual a comunicação foi efetuada.

Neste aspeto, Silva Rodrigues salienta que *"vigora, em matéria de divulgação expedita de dados, o princípio da suficiência, ou seja, de nada valerá a transmissão de dados cuja quantidade não seja suficiente para os efeitos de investigação criminal: (i) identificação, pela parte, dos fornecedores de serviços; e (ii) dos fornecedores de serviços; e (iii) da via pela qual a comunicação foi transmitida."*[183]

Não poderíamos encerrar este capítulo, sem tecer algumas conclusões, para melhor compreendermos estes novos mecanismos de obtenção de prova e quem terá legitimidade para solicitar a preservação e revelação de dados. Para o efeito, faremos uma breve alusão ao mencionado num parecer consultivo da Procuradoria Geral da República[184] a qual fora solicitada a pronunciar-se relativamente à questão, de saber se os órgãos de polícia, carecem de prévia autorização da autoridade judiciária para proceder ao visionamento de imagens colhidas por jornalistas, por outros funcionários e pelos demais colaboradores de órgãos de comunicação. Onde foram tomadas as conclusões que referimos seguidamente.

O Ministério Público é a entidade competente para a direção do inquérito e para a seleção dos atos dirigidos aos respetivos fins: investigar a existência de um crime, determinar os seus agentes e a responsabilidade deles, e descobrir e recolher as provas a modo à decisão sobre o exercício da ação penal.

Os órgãos de polícia criminal podem realizar atividades dirigidas aos fins do processo penal: a) Ao abrigo direto da lei, no caso de medidas cautelares e de polícia (sempre dependentes dos pressupostos urgência e perigo na demora); ou b) Por encargo do Ministério Público (caso em que é necessária a cobertura de um despacho de delegação de competência).

---

[183] RODRIGUES, Benjamim Silva, DIREITO PENAL PARTE ESPECIAL, Tomo I, DIREITO PENAL INFORMÁTICO DIGITAL, pág. 616.

[184] Parecer consultivo da Procuradoria Geral da República, n.º convencional PGRP00003238, com relator Paulo Dá Mesquita, disponível em http://www.dgsi.pt/pgrp.nsf/7fc0bd52c6f5cd5a802568c0003fb410/a734913d16b0f89480257af00043b68a, consultado em 26-01-2015

Os órgãos de polícia criminal apenas podem praticar atos de investigação criminal ao abrigo de despacho de delegação de competência depois da comunicação da notícia do crime ao Ministério Público, de acordo com os termos estabelecidos no despacho, e em respeito das competências reservadas ao juiz e ao Ministério Público.

Na impossibilidade de comunicação com o Ministério Público competente, o órgão de polícia criminal pode contactar qualquer magistrado ou agente do Ministério Público, e este pode determinar os atos urgentes de aquisição e conservação de meios de prova que considerar pertinentes, ao abrigo do disposto no artigo 264.º, n.º 4, do CPP.

A prática de atos relativos aos fins do inquérito por iniciativa própria do órgão de polícia criminal depende sempre da verificação dos pressupostos de necessidade e urgência.

As autoridades e os órgãos de polícia criminal, por iniciativa própria que na prossecução de fins do processo penal, poderão: a) relativamente a matérias que não integrem a reserva judiciária legal, praticar todos os atos cautelares necessários e urgentes para assegurar os meios de prova que não atinjam direitos protegidos por lei (artigo 249.º, n.º 1, do CPP); b) relativamente a matérias previstas nas reservas de competência das autoridades judiciárias, poderão realizar os atos permitidos por previsão legal especial dentro dos estritos pressupostos jurídico-normativos, estabelecidos pela lei.

A interpelação de jornalistas, diretores de informação, administradores ou gerentes de entidade proprietária de órgão de comunicação social, ou qualquer outra pessoa que nele exerça funções com vista à solicitação de documentos, ou quaisquer objetos que estejam na posse daquele órgão, para a prossecução de fins do processo penal, integram a competência reservada da autoridade judiciária que dirige o processo (por força do disposto no n.º 1 do artigo 182.º do CPP conjugado com o artigo 135.º, n.º 1, do CPP e o artigo 11.º, n.º 5, do Estatuto do Jornalista).

A solicitação de imagens captadas e na posse de órgãos de comunicação social para os fins do processo penal é, assim, matéria da competência reservada das autoridades judiciárias independentemente, de as imagens estarem ou não protegidas por sigilo profissional do jornalista.

Não é admissível que órgãos de polícia criminal, por iniciativa própria dirigida à prossecução de finalidades do processo penal, interpelem elementos de órgão de comunicação social com vista ao visionamento de imagens que estão na sua posse, e tenham sido captadas por jornalistas, outros funcionários ou demais colaboradores dessa entidade (por força do

disposto no n.º 1 do artigo 182.º do Código de Processo Penal, conjugado com o n.º 2 do artigo 135.º do mesmo diploma, o artigo 11.º, n.º 5, do Estatuto do Jornalista e artigos 11.º, n.º 1, alínea c), e 14.º, números 1 e 7, da Lei do Cibercrime).

Caso a autoridade ou órgão de polícia criminal tenha conhecimento que elementos de um órgão comunicação social recolheram imagens que podem ser relevantes para investigar a existência de um crime, determinar os seus agentes e a responsabilidade deles, deve comunicá-lo no mais curto prazo ao Ministério Público para este decidir ou promover o que tiver por conveniente.

Pode uma autoridade ou um órgão de polícia criminal entender que se afigura necessário à descoberta da verdade, em processo penal, obter imagens recolhidas e na posse de órgão de comunicação social (em suporte digital ou material). Nesse caso, e em relação às quais haja receio de que se possam perder, alterar ou deixar de estar disponíveis, existindo urgência ou perigo na demora, e não sendo possível contactar tempestivamente magistrado do Ministério Público, poderá ser ordenado a quem tenha disponibilidade ou controlo desses dados, que os preserve (sublinhado nosso), ao abrigo das disposições conjugadas dos artigos 55.º, n.º 2 e 249.º, n.º 1, do CPP e dos artigos 11.º, n.º 1, alínea c), e 12.º, n.º 2, da Lei do Cibercrime.

2.4.3. Injunção para apresentação ou concessão do acesso a dados (artigo14.º)

De acordo com o Relatório Explicativo da Convenção do Cibercrime, no ponto 167 onde consta que *"Por vezes, os dados de tráfego ou, pelo menos, alguns tipos de dados de tráfego, são partilhados entre os fornecedores de serviços envolvidos na transmissão da comunicação, para fins comerciais, técnicos ou de segurança. (...) Cada um deles tem em sua posse uma parte do puzzle, e cada uma destas partes necessita de ser examinada de forma a detectar-se a sua origem ou o seu destino"*.

A injunção consiste num mecanismo que poderá melhorar os resultados da investigação, particularmente junto de ISP não cooperantes, apresentando a possibilidade de os sujeitar à obrigação de fornecerem determinados dados[185], sob pena de punição por crime de

[185] VERDELHO, Pedro, A obtenção da prova no ambiente digital, notas que serviram de suporte a uma curta intervenção no *International Seminar on Seizing Evidence in the Internet*, organizado em Lisboa, a 5 e 6 de Maio de 2004, pela Polícia Judiciária e dirigido a agentes policiais da União Europeia, documento fornecido pelo Autor em Curso de formação avançada à distância CIBERCRIME E PROVA DIGITAL, organizado pela e-UNIFOJ do centro de Estudos sociais (CES) da Universidade de Coimbra e coordenado por Pedro Verdelho, decorreu entre 06 de Outubro e 05 de Dezembro, disponível em http://opj.ces.uc.pt/e-learning/moodle/course/view.php?id=10, consultado em 10-11-2014

desobediência[186] (artigo 14.º n.ºs 1 e 3). Dá Mesquita entende que a punição pelo crime de desobediência é uma medida processual e materialmente inadequada no plano jurídico prático para os fins pretendidos, defendendo que era preferível a aplicação de medidas compulsórias, em especial sanções pecuniária, que se adaptem às exigências de um procedimento célere: "*Entende-se que por via do art. 4.º do CPP se deve ponderar em função do caso concreto, nomeadamente, a aplicação do art. 519.º, n.º2, primeira parte, do Código de Processo civil, «aqueles que recusem a colaboração devida serão condenados em multa, sem prejuízo dos meios coercivos que forem possíveis*"[187].

O nosso legislador proibiu a injunção relativamente ao suspeito ou arguido nesse processo (artigo 14.º n.º5), já que isso poderia consubstanciar uma verdadeira auto-incriminação ou atuação processual menos leal e incompatível com o princípio da presunção da inocência de que normalmente gozam suspeito e arguido[188]. " *(...) O expediente da injunção também é aplicado aos fornecedores de serviço a quem pode ser ordenado que comunique, ao processo, os dados relativos aos seus clientes ou assinantes. Esta informação abrange toda aquela 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, nomeadamente, determinar*" as informações contidas nas alíneas a) a c) do n.º4 deste artigo.[189]

Consagra no n.º6 que 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. Como bem repara Silva Rodrigues, "*Tudo isto em nome dos valores ligados ao direito de defesa ou plenitude das garantias de defesa processuais penais, à privacidade ou reserva da intimidade ligada à saúde e que implica o sigilo dos dados "sensíveis" da saúde das pessoas, o sigilo bancário e o sigilo profissional do jornalista e a*

[186] **Artigo 348.º CPP - Desobediência**
1 - Quem faltar à obediência devida a ordem ou a mandado legítimos, regularmente comunicados e emanados de autoridade ou funcionário competente, é punido com pena de prisão até 1 ano ou com pena de multa até 120 dias se:
a) Uma disposição legal cominar, no caso, a punição da desobediência simples; ou
b) Na ausência de disposição legal, a autoridade ou o funcionário fizerem a correspondente cominação.
2 - A pena é de prisão até 2 anos ou de multa até 240 dias nos casos em que uma disposição legal cominar a punição da desobediência qualificada
[187] MESQUITA, Paulo dá, Processo Penal, Prova e Sistema Judiciário...p.113.
[188] RODRIGUES, Benjamim Silva, DA PROVA PENAL - Tomo IV, DA PROVA ELECTRÓNICO – DIGITAL E DA CRIMINALIDADE INFORMÁTICO – DIGITAL, p. 524.
[189] RODRIGUES, Benjamin Silva. DA PROVA PENAL, tomo II, Bruscamente, A(s) Face(s) Ocultas dos Métodos Ocultos de Investigação Criminal, Pág 445

respectiva liberdade de informação e expressão implicadas, todos direitos com assento constitucional, nomeadamente, nos artigos 26.º 34.º,35.º, 37.ºe 64.º da CRP 1976"[190].

2.4.4. Pesquisa de dados informáticos (artigo 15.º)

Pedro Verdelho, Rogério Bravo e Lopes Rocha sublinham que no *"n.º2 do Artigo 19.º da Convenção prevê-se algo não previsto no direito português, embora não proibido nem contrariado. Prevê-se aí que quando no decurso de busca a um sistema de computadores se note que os dados que se procuram estarão guardados noutro sistema de computadores, as entidades competentes, de forma expedita, estenderão a busca (ou o acesso similar a que se proceda) ao outro sistema. É uma inovação que importa consagrar na lei nacional, uma vez que as buscas, tal como elas estão desenhadas no sistema processual penal, em regra, não podem ser determinadas pelas entidades que na prática as executam (é exigida, como regra, a autorização da autoridade judiciária - Ministério Público ou Juiz-, sendo como regra, as buscas executadas por entidades policiais) "*[191], encontrando-se agora consagrada esta norma da convenção, no n.º5 do artigo em apreço.

Silva Rodrigues, relativamente ao artigo 15.º n.º1, refere-se à admissibilidade de *"pesquisa"* ou *"vasculhagem"*. O mesmo autor apela que este normativo deve sofrer uma interpretação restritiva, de modo a que a pesquisa não ocorra sem que à mesma presida a autoridade judiciária que a ordenou ou autorizou[192] (n.º1 in fine). Alega o autor que *"por força do artigo 32.º, n.º4 da CRP, esta autorização tem de ser judicial e, à semelhança do que ocorre com o 179.º, n.º3, do CPP, caberá ao juiz presidir a tal operação para que se mantenha a "chain of custody", ou seja, a força probatória de tais elementos, sob pena de se desconsiderar a valoração dos mesmos em virtude de não darem garantias de autenticidade, fidedignidade e não contaminação".*[193]

Uma vez que o n.º3 admite que o órgão de polícia criminal proceda a pesquisa sem prévia autorização (sublinhado nosso) da autoridade judiciária quando: haja consentimento por quem tiver a disponibilidade ou controlo desses dados, desde que o consentimento fique documentado

[190] Idem, Ibidem
[191] VERDELHO, Pedro; BRAVO, Rogério; ROCHA, Manuel Lopes – Leis do Cibercrime, Vol. 1, p.17, disponível em http://www.centroatl.pt/titulos/direito/imagens/excerto-ca-leisdoCibercrime1.pdf, consultado em 22-12-2013
[192] RODRIGUES, Benjamin Silva. DA PROVA PENAL, tomo II, Bruscamente, A(s) Face(s) Ocultas dos Métodos Ocultos de Investigação Criminal, pp.446-447
[193] Idem, p.. 447

(conforme alínea a)); ou nos casos de terrorismo, criminalidade violenta ou altamente organizada; ou quando haja fundados indícios de crime que ponha em grave risco a vida ou a integridade de qualquer pessoa (alínea b)). Devendo nestes casos, ser comunicado de imediato às autoridades judiciárias sob pena de nulidade. Nestes casos admite-se valoração *a posteriori* pela autoridade judiciária nos termos do n.º4 alínea a) do artigo 15.º.

Concordámos com as observações que Silva Rodrigues faz do n.º 3, sendo que na alínea a), o consentimento documentado, pode ser obtido de forma *"engenhosa, desleal e alguma artimanha"*. O consentimento (que poderá ser prestado com vícios ou não) permitirá aos órgãos de polícia criminal obter dados aos quais, sem esse consentimento, não teriam (sem recurso a outros expedientes) acesso. Dados que serão fundamentais para a condenação do suspeito.

Relativamente à alínea b) o Autor diz-nos que *"concretiza um verdadeiro direito (processual) penal do inimigo"*, visto que o terrorista ou o criminoso violento ou organizado ficam desapossados dos níveis democráticos mínimos de garantias dos seus direitos fundamentais à luz das legítimas expectativas e garantias processuais penais que gerou na sua mente em virtude do quadro geral processual penal e constitucional em vigor na ordem jurídica portuguesa"[194]. Com fundamento nos indícios retiram-se garantias processuais ao indivíduo.

Jakobs como precursor da teoria do Direito Penal do inimigo, defende que "o direito penal do cidadão, aplicável a todos os que pertencem a uma *"comunidade legal",* não deve valer para aqueles que se recusam a participar nela, tentando obter a aniquilação dessa comunidade (os *"terroristas"*) ou violando repetida e persistentemente as normas que os regem (*"os delinquentes por tendência perigosos)"*[195].

O regime excecional de pesquisa de dados informáticos, levado a cabo pelos órgãos de polícia criminal, sem previa autorização da autoridade judiciária competente, por razões de urgência, terá de respeitar o disposto no artigo 15.º n.º4, alíneas a) e b), sob pena de se reconduzir a prova proibida, insuscetível de valoração[196].

Quando no decurso de uma pesquisa, os órgãos de polícia, estejam convictos que os dados procurados se encontrem noutro sistema informático, ou numa parte diferente do sistema pesquisado e podendo o acesso dar-se através do sistema inicial, haverá lugar à extensão da

[194] Idem, p. 449
[195] DIAS, Jorge de Figueiredo, Direito penal, parte geral tomo I, 2ª Edição, Questões fundamentais, a doutrina geral do crime, Coimbra Editora, 2007, ISBN 978-972-32-1523-6. pág 36
[196] RODRIGUES, Benjamim Silva, Da prova penal, tomo IV, p. 527

medida a esses mesmos sistemas, mediante autorização ou ordem prévia da autoridade competente (números 1, 2 e 5 deste artigo).[197]

Importa denotar que o acesso e a pesquisa a um sistema informático pode fazer-se sem que o proprietário do mesmo tome conhecimento dessa medida. É isto que distingue a chamada busca *online*[198] (com natureza silenciosa e oculta) das ditas buscas tradicionais.[199]

O n.º6 do artigo 15.º, remete-nos para as regras de execução das buscas previstas nos artigos 174.º a 177.º do CPP e para o Estatuto do jornalista (Lei n.º1/99, de 1 de Janeiro, alterada pela lei n.º 64/2007, de 5 de Novembro e Retificação n.º 114/2007, de 20 de Novembro).

Dá Mesquita, sobre a questão terminológica entende que a busca de dados informáticos num sistema informático prevista neste artigo é intitulada de pesquisa, embora não se altere a sua natureza processual de busca. Acrescenta ainda que continuam a valer os cânones estabelecidos no artigo 174.º, nrs.1 e 2, do CPP.[200]

2.4.5. Apreensão de dados informáticos (Artigo 16.º)

Quando no decurso de uma pesquisa informática ou de outro acesso legítimo a um sistema informático, se encontrem dados ou documentos informáticos necessários a produção de prova para descoberta da verdade material, a autoridade judiciária competente autoriza a apreensão dos mesmos (n.º1 do artigo 16.º), no decurso de pesquisa informática legitimamente ordenada. Todavia, o órgão de polícia criminal pode efetuar apreensões sem previa autorização da autoridade judiciária, no decurso de pesquisa legitimada pelo artigo 15.º, e em situações de urgência ou de perigo na demora (n.º2).

---

[197] Idem, p. 528

[198] Segundo Manuel da Costa Andrade, a busca online consiste em *"aceder, de forma oculta e à distância, via internet, aos dados contidos num computador, observá-los e, sendo caso disso, copiá-los em maior ou menor medida. O que pode acontecer sob a forma de intromissão instantânea e descontínua ("espelho") ou de forma contínua, permitindo o registo das alterações ocorridas nos computadores-alvo (monitoring).* – "Bruscamente no verão passado" a reforma do código de processo penal,p.153

[199] Segundo Manuel da Costa Andrade, *"É o que bem ilustra a resposta, hoje praticamente unânime, ao problema da legalidade da chamada busca online. ao contrario do que, num primeiro momento, algumas vozes chegaram a advogar, é hoje pacífico o entendimento de que a lei processual penal vigente não prevê nem legitima a medida. O que vale, desde logo e sobretudo, para os dispositivos que prevêem e regulam a clássica figura da busca, que não oferecem o indispensável suporte normativo de que a nova medida carece. Desde logo, por causa da irredutível heterogeneidade teleológica e normativa que separa os dois meios de obtenção de prova. E que fazem particularmente crise no carácter oculto da busca online, contraposto à natureza aberta da busca tradicional."* – "Bruscamente no verão passado" a reforma do código de processo penal, p.150

[200] MESQUITA, Paulo Dá, Processo penal, prova e sistema Judiciário, pp.114-115

Quando esteja em causa conteúdo suscetível de revelar dados pessoais ou íntimos, que possam pôr em causa a privacidade do respetivo titular ou terceiro, esses dados são levados a juiz, que ponderará a sua junção aos autos, atendendo aos interesses do caso concreto.

As apreensões de prova a que nos temos vimos a referir nos nrs.º1.º, 2.º e 3.º têm que ser apresentadas no prazo máximo de 72 horas, à autoridade judiciária, para que esta proceda a validação (n.º4). Estando em causa segredo profissional, n.ºs5.º e 6.º remetem-nos para o CPP.

O n.º7.º do artigo 16.º consagra o princípio da proporcionalidade e adequação quanto ao modo e tipologias de formas de apreensão de dados informáticos, tendo em conta os interesses do caso concreto. Na hipótese do objeto de busca ser o computador do arguido, que por sua vez, é o seu material de trabalho e modo de subsistência, devê-lo-á ser-lhe devolvido o mais rapidamente possível, dando-se preferência aos meios menos onerosos para o investigado (e sempre que possível), em respeito do princípio da presunção da inocência. Quando a apreensão for efetuada, por realização de cópia de dados em suporte autónomo, a cópia será feita em duplicado (n.º8). O legislador Italiano, na Lei 48/2008, de 18 de Março (que procede à ratificação e implementação da Convenção do Conselho da Europa sobre Cibercrime, à qual tantas vezes já aludimos), optou por proceder à alteração de alguns artigos do Código de Processo Penal (artigos 254.º bis, 259.º, 260.º e 354.º), passando a exigir que a aquisição de dados de computador se faça *"(...)copiando-os (...)num suporte adequado, com um procedimento que garanta a conformidade dos dados obtidos com o original e a sua imutabilidade"*[201]. Na opinião de Silva Rodrigues a cópia deve ser feita em triplicado, ficando uma cópia como reserva e salvaguarda, outra será entregue ao suspeito ou arguido, para exercício do direito de defesa, e uma outra será usada pelas autoridades judiciárias em audiência de julgamento.[202] Dias Ramos defende que a palavra cópia deveria ser substituída por clonagem ou cópia de imagem, uma vez que existem ferramentas informáticas forenses específicas para o efeito, impedindo assim, posteriores alterações, de modo a não ser questionada a valoração da prova em sede de julgamento[203].

[201] RAMOS, Armando Dias, A prova digital em processo penal, p.90
[202] RODRIGUES, Benjamin Silva. DA PROVA PENAL, tomo II, Bruscamente, A(s) Face(s) Ocultas dos Métodos Ocultos de Investigação Criminal, pp.452-453
[203] RAMOS, Armando Dias, A prova digital em processo penal, p.90

Pedro Verdelho, Rogério Bravo e Lopes Rocha[204], referindo-se às medidas previstas no artigo 19.º da Convenção do Cibercrime adotada em Budapeste em 23 de Novembro de 2001, entendem que *"com excepção da mera apreensão de dados no seu suporte, que em nada se distingue da mera apreensão, todas estas medidas (incluindo apreensão de dados separadamente do seu suporte) são medidas específicas do espaço virtual. Não são por isso enquadráveis nos conceitos atuais da lei processual".*

2.4.6. Apreensão de correio eletrónico e registos de comunicações de natureza semelhante (artigo17.º)

Rita Castanheira Neves e Manuel da Costa Andrade, defenderam que o correio eletrónico deixa de ser comunicação para passar a ser ficheiro digital, no momento, em que a comunicação é recebida e lida pelo destinatário, pois até lá, é considerado comunicação, podendo ser intercetado, respeitando os requisitos de admissibilidade e as formalidades exigidas para as interceções de comunicações (em respeito pelo direito à inviolabilidade das comunicações), não podendo ser alvo de buscas. Diferentemente, Rogério Bravo e Romeo Casabona *"entendem que a comunicação acaba logo que chega ao terminal do destinatário"*.

Já Pedro Verdelho[205] *"defendeu idealmente (antes da solução legislativa consagrada no n.º1 do artigo do artigo 189.º do Código de Processo Penal), com base nestes três momentos, o regime estabelecido para as escutas telefónicas para a fase de transmissão do e-mail, o regime da apreensão de correspondência para a fase em que o e-mail já chegou ao destino mas ainda não foi lido pelo destinatário e o regime da apreensão de normais ficheiros escritos quando o e-mail já foi aberto e lido pelo destinatário"*[206]. Atente-se que todas as considerações doutrinárias acabadas de referir foram anteriores à Lei de Cibercrime agora em apreço, pelo que certamente terão contribuído para a atual previsão do artigo 17.º

Também na jurisprudência encontramos essa diferenciação de tratamento, nomeadamente, no Acórdão do Tribunal da Relação de Guimarães onde se pode ler que, "*Tal*

[204] VERDELHO, Pedro; BRAVO, Rogério; ROCHA, Manuel Lopes – Leis do Cibercrime, Vol. 1, p.18, disponível em http://www.centroatl.pt/titulos/direito/imagens/excerto-ca-leisdoCibercrime1.pdf, consultado em 22-12-2013

[205] PEDRO VERDELHO, "Apreensão do Correio Electrónico em Processo Penal", Revista do Ministério Público, Ano 25.º, n.º100, Outubro-Dezembro ,2004, pp.153-164: e "Técnica no Novo C.P.P.: Exames, Perícias e Prova Digital" Revista CEJ, 1.º Semestre 2008, n.º9 (Especial) – Jornadas sobre a revisão do Código de processo penal, pp. 145-171

[206] NEVES, Rita Castanheira – AS INGERÊNCIAS NAS COMUNICAÇÕES ELECTRÓNICAS EM PROCESSO PENAL. Natureza e respectivo regime jurídico do correio electrónico enquanto meio de obtenção de prova. Coimbra: Coimbra Editora, 2011. ISBN 978-972-32-1942-5, pp. 261-264

como acontece na correspondência efectuada pelo correio tradicional diferenciar-se-á a mensagem já recebida mas ainda não aberta da mensagem já recebida e aberta. Na apreensão daquela rege o art.° 179° do Código de Processo Penal, mas a apreensão da já recebida e aberta não terá mais protecção do que as cartas recebidas, abertas e guardadas pelo seu destinatário. E a mensagem recebida em telemóvel, atenta a natureza e finalidade do aparelho e o seu porte pelo arguido no momento da revista, é de presumir que uma vez recebida foi lida pelo seu destinatário. Na sua essência a mensagem mantida em suporte digital depois de recebida e lida terá a mesma protecção da carta em papel que tenha sido recebida pelo correio e que foi aberta e guardada em arquivo pessoal. Sendo meros documentos escritos, estas mensagens não gozam de aplicação de regime de protecção da reserva da correspondência e das comunicações"[207].

Com a consagração do artigo 17.º da Lei do Cibercrime, " (...) *não vem estabelecida qualquer distinção entre mensagens de correio electrónico e/ou registos de comunicações de natureza semelhante, armazenados em sistema informático, já acedidas, ou não, pelo respectivo destinatário; entre mensagens a abrir ou já abertas, tão pouco entre comunicações e mero arquivo informático, sendo que não podia o legislador ignorar a polémica a propósito instalada, potenciada pela reforma de 2007 do Código de Processo Penal*"[208]. Costa Andrade foi um dos Autores que teceu críticas ao novo código, apontando alterações que não foram devidamente feitas e importantes casos que o legislador se absteve de legislar. Assim, e nas palavras do Autor: " *(...) o legislador deve resistir à tentação e ao primeiro impulso de responder com leis – e sobretudo com leis incriminatórias - ao primeiro sinal de surpresa, de factos ou de problemas para os quais pareça não haver resposta na lei. Como de todos os lados se reconhece, a criminalização deve ser sempre o ponto de chegada de uma determinada reflexão sobre a dignidade penal e a carência de tutela penal do facto."*[209].

A lei especial do cibercrime, neste artigo 17.º remete assim para "o regime de apreensão de correspondência previsto no Código de Processo Penal, este encontra-se disciplinado no

[207] Acórdão do Tribunal da Relação de Guimarães, de 12-10-2009, Processo nº 1396/08.1PBGMR-A.G1, com relator TOMÉ BRANCO, disponível em http://www.dgsi.pt
[208] Acórdão do Tribunal da Relação de Guimarães, de 29-03-2011, Processo nº 735/10.0GAPTL-A.G1, com relator MARIA JOSÉ NOGUEIRA, disponível em http://www.dgsi.pt
[209] ANDRADE, Manuel da Costa – "BRUSCAMENTE NO VERÃO PASSADO" A REFORMA DO CÓDIGO DE PROCESSO PENAL, Observações críticas sobre uma lei que podia e devia ter sido diferente. Coimbra Editora, 2009. ISBN 978-972-32-1726-1, p. 37

artigo 179º, o qual estabelece desde logo no nº 1, que tais apreensões sejam determinadas por despacho judicial, "sob pena de nulidade" expressa (nº 1), e que "*o juiz que tiver autorizado ou ordenado a diligência é a primeira pessoa a tomar conhecimento do conteúdo da correspondência apreendida*". Tal aplica-se ao correio eletrónico já convertido em ficheiro legível, configurando um ato da competência exclusiva do Juiz de Instrução Criminal, nos termos do art.º 268º nº 1 alínea d) do CPP, artigo este, que estabelece que *"compete exclusivamente ao juiz de instrução, tomar conhecimento, em primeiro lugar, do conteúdo da correspondência apreendida"*, o que se estendeu ao conteúdo do correio eletrónico, por força da subsequente Lei nº 109/2009, de 15 de Setembro, constituindo a sua violação nulidade expressa absoluta e que se reconduz, a final, ao regime de proibição de prova, ou seja, a falta de exame da correspondência pelo juiz constitui uma nulidade prevista no art.º 120º nº 2 alínea d) do CPP, porque se trata de um ato processual legalmente obrigatório[210].

Contudo, em caso de urgência, isto é, de perda de informações úteis à investigação de um crime, em caso de demora, o juiz pode sempre autorizar a abertura imediata de correspondência (assim como de correio eletrónico), pelo órgão de polícia criminal, podendo este inclusivamente, ordenar a suspensão da remessa de qualquer correspondência nas estações de correios e de telecomunicações, nos termos dos nºs 2 e 3 do art.º 252º do Código de Processo Penal, devendo a ordem policial ser convalidada no prazo de 48 horas, sob pena de devolução ao destinatário caso não seja atempadamente convalidada, ou caso seja rejeitada a convalidação[211].

Silva Rodrigues, faz uma forte crítica a esta norma, pois segundo este Autor, o artigo 17.º ao remeter para a apreensão de correspondência previsto no CPP, para o artigo 179.º, n.º 3.º do CPP, denota "*uma qualquer confusão legislativa, já que a não ser que se admita uma (desproporcional) apreensão massiva dos correios electrónicos, já que o juiz não está presente e somente pode seleccionar após leitura, então, verifica-se que foi infeliz o legislador ao esquecer a regulamentação complexa do artigo 179.º, n.º3, do CPP, e ao esquecer a regulamentação inversa, a esta, consagrada no artigo 189.º n.º1 do CPP"*[212].

---

[210] Deste sentido vide Paulo Pinto de Albuquerque, *in* comentário do Código de Processo Penal, 2ª Edição, anotação 12ª ao art.º 179º, p. 495

[211] Acórdão do Tribunal da Relação de Lisboa, de 11-01-2011, Processo nº 5412/08.9TDLSB-A.L1-5, com relator RICARDO CARDOSO, disponível em http://www.dgsi.pt

[212] RODRIGUES, Benjamin Silva. DA PROVA PENAL, tomo II, Bruscamente, A(s) Face(s) Ocultas dos Métodos Ocultos de Investigação Criminal,pág. 454

Da leitura do artigo 17.º em conjunto com o artigo 179.º do CPP, o Juiz que tiver autorizado ou ordenado a diligência é a primeira pessoa a tomar conhecimento do conteúdo da correspondência apreendida.[213].

2.4.7. Interceção de comunicações (artigo 18.º)

Este artigo prevê a interceção de comunicações eletrónicas para processos relativos a crimes previstos na presente lei, ou cometidos por meio de um sistema informático, ou em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico, quando tais crimes se encontrem previstos no artigo 187.º do Código de Processo Penal (das alíneas a) e b) do n.º1.º do artigo 18.º da LC). Encontramos nesta previsão legal, os crimes para os quais se admite, como meio de obtenção de prova, a ingerência nas telecomunicações.

Respeitando, assim, a imposição do artigo 34.º n.º4 da CRP, só em processos de natureza penal, se admite a ingerência nas telecomunicações, cabendo à lei ordinária definir os limites em que ela pode ter lugar, ou seja, " *(...) não é em qualquer processo criminal que a ingerência das telecomunicações/escutas é admissível como meio de obtenção de prova, mas apenas e só para um determinado conjunto de crimes previamente definido por lei*"[214]. As exceções ao sigilo das comunicações devem revestir a forma de lei (reserva de lei), conforme o artigo 18.º nrs. 2 e 3 da CRP, só podendo ser aplicadas por um magistrado judicial (artigo 32.º, n.º4 da CRP). A norma 32.º n.º8 da CRP, comina com a nulidade das provas obtidas mediante abusiva intromissão na vida privada, ou nas telecomunicações.

Também o artigo 35.º da CRP consagra o direito fundamental à autodeterminação informacional.[215]

Na interceção e registo de transmissões de dados informáticos, remete o artigo18.º, n.º4, para as regras estabelecidas nos artigos 187.º a 190.º do CPP, relativas às escutas telefónicas, aplicam-se às comunicações eletrónicas os mesmos procedimentos e autorizações judiciais previstas para as "escutas telefónicas". *"Neste caso, falamos da intercepção de mensagens de correio electrónico em tempo real, ou seja, no seu trajecto do computador do emissor para o computador do receptor através da rede de servidores. Ou ainda a intercepção de mensagens*

[213] MESQUITA, Paulo Dá, Processo Penal, prova e sistema judiciário...p. 118
[214] SANTOS, Cistina Máximo dos, As novas tecnologias da informação e o sigilo das telecomunicações, Lisboa, 2004, separata da Revista do Ministério Público N.º99, p. 96
[215] Idem, Ibidem

trocadas através de processos de comunicação instantânea (usualmente designados por serviços de "chat", como são os casos do "IRC[216]", do MSN Messenger", ou do "ICQ")".[217]

Relativamente ao sigilo nas telecomunicações, o artigo 384.º, do CP pune a violação do segredo das comunicações por entidades públicas. Essa restrição a entidades públicas, deve-se ao facto do elemento histórico de criação da norma, pois aquando da sua criação, as telecomunicações estavam entregues às entidades públicas, diferentemente do que ocorre hoje em dia, dado o fenómeno da privatização. Porém, o artigo 194[218], sob a epígrafe *"violação de correspondência ou de telecomunicações"* pune quem se intrometa e divulgue o conteúdo das comunicações de terceiros.

A Lei 41/2004 (proteção de dados pessoais e privacidade nas comunicações eletrónicas), no nº 1 do seu Artigo 4º, estabelece que os fornecedores de serviço devem preservar a inviolabilidade das comunicações e dos dados de tráfego. Por outro lado, no nº 2 do mesmo artigo proíbe-se a interceção e a vigilância das comunicações.

O artigo 276º do Código Penal prevê a punição de quem detiver instrumento ou aparelhagem, especificamente destinados à montagem de escuta telefónica, ou à violação de telecomunicações, fora das condições legais (proíbe as escutas através de aparelho). Já os artigos 187.º, 188.º e 189.º do CPP e o artigo 18.º da LC admitem, excecionalmente, a interceção e gravação, desde que se respeitem determinados requisitos e condições (sob pena de nulidade artigo 190.º CPP). De acordo com o artigo 187.º do CPP, "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", tratando-se de crimes elencados nesse preceito.

---

[216] "Uma forma de comunicação que permite a troca de mensagens em tempo real". MATOS, José A. de, Dicionário de Informática e Novas Tecnologias...p. 203

[217] VENÂNCIO, Pedro Dias. LEI DO CIBERCRIME-ANOTADA E COMENTADA,pág.119

[218] **Artigo 194.º - Violação de correspondência ou de telecomunicações**

1 - 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

2.4.8. Ações encobertas (Artigo 19.º)

É comum a existência de grupos fechados no ambiente digital, com regras próprias para recrutamento de novos membros, trocando informações e onde, modo organizado, e com uma estrutura hierárquica, *"brincam"* com as falhas de segurança de sistemas informáticos de empresas e particulares. O agente encoberto terá, com toda a certeza, um importante papel no contributo da investigação criminal.

Neste artigo o legislador estendeu as disposições sobre as ações encobertas previstas na Lei 101/2001, de 25 de agosto àquelas que agora são tidas em *"em ambiente electrónico-digital"*[219], de acordo com o n.º 1 desta Lei, "*consideram-se acções encobertas aquelas que sejam desenvolvidas por funcionários de investigação criminal ou por terceiro actuando sob o controlo da Polícia Judiciária para prevenção ou repressão dos crimes indicados nesta lei, com ocultação da sua qualidade e identidade*".

Admite-se o regime das ações encobertas para crimes previstos na lei 109/2009, de 15 de Setembro e para crimes cometidos por meio de um sistema informático, quando lhes corresponda em abstrato, pena de prisão de máximo superior a 5 anos, ou ainda quando a pena for inferior, desde que 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 infrações económico-financeiras, bem como os crimes consagrados no título IV do Código do Direito de Autor e dos Direitos Conexos, são suscetíveis de investigação mediante recurso às ações encobertas (artigo 19.º, n.º1 alínea b)).

Dias Ramos[220], refere (e bem, em nosso entender), que na intervenção encoberta em sistemas informáticos, o legislador não criou uma norma processual específica para esta novíssima forma de investigação, nem procedeu à sua regulamentação sobre os meios técnicos a utilizar, remetendo apenas este artigo, para o regime aplicável às ações encobertas.

Dá Mesquita crítica esta previsão legal em dois aspetos: por um lado, no n.º1 deste artigo é ampliado de forma drástica o catálogo de crimes previsto no artigo2.º do Regime Jurídico sobre ações encobertas; por outro, no plano jurídico-constitucional, prevê-se uma medida de carácter excecional para um leque muito amplo de crimes (alguns dos quais enquadrados na

[219] RODRIGUES, Benjamin Silva. DA PROVA PENAL, tomo II, Bruscamente, A(s) Face(s) Ocultas dos Métodos Ocultos de Investigação Criminal, pág.456
[220] RAMOS, Armando Dias, A prova digital em processo penal, pp. 90-91

pequena criminalidade), sem que ocorra um aprofundamento normativo dos princípios da proporcionalidade e da necessidade[221].

Contrariamente ao que sucede em alguns países europeus, o nosso ordenamento jurídico não admite que, ao abrigo das ações encobertas, e com o intuito de por exemplo, combater a pedofilia, um agente encoberto se faça passar por uma criança menor, de modo a verificar, se o agente do crime, solicita à criança fotografias ou vídeos, ou até encontros. Tal consubstanciaria prova inadmissível de valoração, por ocorrerem à margem do paradigma constitucional e legalmente previsto no nosso sistema jurídico, em matéria probatória[222]. Estaríamos nessa situação perante a figura do agente provocador.

Costa Andrade, seguindo o pensamento de Meyer, dá-nos o conceito *de "homens de confiança"*, "*abrangendo todas as testemunhas que colaboram com as instâncias formais da perseguição penal, tendo como contrapartida a promessa da confidencialidade da sua identidade e actividade. Cabem aqui tanto os particulares (pertencentes ou não ao submundo da criminalidade) como os agentes das instâncias formais, nomeadamente da polícia (Untergrundfahnder, under cover agent, agentes encobertos ou infiltrados), que disfarçadamente se introduzem naquele submundo ou com ele entram em contacto; e quer se limitem à recolha de informações (Polizeispitzel Lockspizel, agent provocateur, entrapment),quer vão ao ponto de provocar eles próprios a prática do crime*"[223].

Importará, por ventura, fazer a distinção entre agente infiltrado e agente provocador. O primeiro, com a sua atuação, limita-se a obter a confiança do suspeito, tornando-se aparentemente um criminoso, e assim, ter acesso a informações, planos, processos, confidências, recolhendo desse modo prova de planos ilícitos. O agente provocador cria o próprio crime e o próprio criminoso, uma vez que induz o suspeito à prática de atos ilícitos, instigando-o e alimentando o crime. Tanto age como comprador, ou como fornecedor de bens e serviços ilícitos[224].

[221] MESQUITA, Paulo Dá, Processo Penal, prova e sistema judiciário, p. 126
[222] RODRIGUES, Benjamin Silva. DA PROVA PENAL, tomo II, Bruscamente, p. 130
[223] ANDRADE, Manuel da Costa, Sobre as proibições de prova em processo penal, Coimbra Editora, 1992, ISBN 972-32-0613-7, p. 220
[224] LAVOURA, Tiago Santos, "O agente infiltrado e o seu contributo para a investigação criminal", Dissertação para obtenção de grau de Mestre em ciências jurídico-forenses, Orientador Professor Doutor Figueiredo Dias, Co-orientador: Mestre Ana Pais, Coimbra, Lisboa, Instituto Superior Bissaya Barreto, pp.21-22

Para Fernando Gonçalves, Manuel João Alves e Manuel Monteiro Guedes Valente, agente infiltrado é "*o funcionário de investigação criminal ou terceiro, por exemplo, o cidadão particular, que actue sob o controlo da Polícia Judiciária que, com ocultação da sua identidade, e com o fim de obter provas para a incriminação do suspeito, ou suspeitos, ganha a sua confiança pessoal, para melhor o observar, em ordem a obter informações relativas às actividades criminosas de que é suspeito e provas contra ele(s), com as finalidades exclusivas de prevenção ou repressão criminal, sem contudo, o(s) determinar à prática de novos crimes.*"[225]

Alguns autores autonomizam a figura do agente infiltrado em relação ao agente encoberto, enquanto outros autores (a maioria da doutrina) entendem tratar-se da mesma realidade. Os argumentos apresentados por aqueles que defendem estarmos perante realidades distintas (Alves Meiréis), baseiam-se no facto de que são agentes encobertos aqueles que se inserem no mundo do crime, somente para observar os comportamentos dos criminosos, presenciando o crime, constatando os fatos, sem intervir, mas recolhendo informações essenciais à prevenção do crime[226].

Quanto ao agente provocador, atualmente é consensual, quer ao nível da doutrina, quer na jurisprudência, que a atuação do agente provocador é inadmissível face ao nosso ordenamento jurídico, não tendo previsão legal na Constituição da República Portuguesa, nem no Código de Processo Penal, nem na Lei 101/2001.[227]

Analisadas todas disposições processuais contidas na Lei em estudo. Importa-nos agora averiguar se o nosso processo penal consagra as chamadas "buscas online".

[225] In GONÇALVES, F., ALVES, M. J., VALENTE, M.G (2001). O novo regime jurídico do agente infiltrado (comentado e Anotado - Legislação Complementar). Coimbra: Livraria Almedina, pp. 91-93. Apud LAVOURA, Tiago Santos, "O agente infiltrado e o seu contributo para a investigação criminal", p. 35

[226] Idem, p. 23

[227] In SANTOS, Elsa Costa (2009), Tese de Mestrado - O agente infiltrado na experiência processual penal portuguesa. FDUC. Coimbra, pp. 127-131. Apud LAVOURA, Tiago Santos, "O agente infiltrado e o seu contributo para a investigação criminal", p. 53

2.4.9. A (in)admissibilidade das chamadas "buscas online" também denominadas "pesquisas de dados online" no ordenamento jurídico português

Quando o meio de obtenção de prova implicar um elevado grau de intrusão na privacidade do suspeito, tal deve estar expressamente previsto (artigo 26.º, n.º1 e 2 da Constituição da República Portuguesa), lido à luz do Acórdão do TEDH Vetter v. França, de 31.5.2005, e do Acórdão do Bundesverfassungsgericht de 12.4.2005), também de acordo com o imperativo da reserva de lei nestes domínios dos meios ocultos de investigação. Há também limites materiais intrínsecos dos meios atípicos de obtenção de prova, desde logo, a inamissibilidade da utilização de meios de obtenção de prova que permita uma "vigilância total", uma "vigilância" global com a qual possa ser construído um perfil completo da personalidade do arguido (expressões usadas nos parágrafos 60.º e 67.º referido Acórdão de 12.4.2005, repetidas no Acórdão Bundesverfassungsgericht de 27.2.2008 sobre infiltração em sistemas informáticos). Assim e neste sentido, tem relevância o acórdão do Tribunal Constitucional n.º 442/2007, onde se afirma a proibição de um retrato exaustivo do modo de vida do cidadão, sendo estes os argumentos que levam Paulo Pinto de Albuquerque a afirmar que não são admissíveis como meios atípicos de obtenção de prova, a infiltração em sistema informático.[228]

As exigências de reserva de lei justifica-se somente através de lei da Assembleia da República (ou mediante Decreto-Lei do Governo devidamente autorizado pela Assembleia da república), podendo autorizar e legitimar um qualquer método oculto de investigação, devendo nas palavras de Benjamim Silva Rodrigues[229], ter as seguintes características: *"*a) *clareza suficiente para correcta e rigorosa identificação do bem(ns) jurídico(s) ou direito(s) fundamentai(s) envolvido(s); b) correcta definição dos níveis de sacrifício a impor ao bem(ns) jurídico(s) ou direito(s) fundamental(ais) envolvido(s), com vista à sua contenção dentro dos níveis da não desestruturação ou aniquilamento do núcleo fundamental respectivo do(s) mesmo(s); c) Previsão da forma ou modalidade de técnica invasiva usada (ou a utilizar); d) previsão e prescrição precisa e clara do fundamento (Anlas), fim e limites da intromissão - princípio da vinculação ao fim (da recolha de informação)".*

[228] ALBUQUERQUE, Paulo Pinto de, Comentário do Código de Processo Penal, pp.316-317
[229] RODRIGUES, Benjamim silva, da prova penal, tomo II, Bruscamente, p.53

A reserva de lei de Juiz de instrução ou *"das liberdades" visa, essencialmente, assegurar uma tutela preventiva dos direitos fundamentais das pessoas, e evitar o uso de uma medida não justificada, cabendo ao juiz o controlo prévio da admissibilidade do uso do método oculto de investigação"* [230].

Em anotação ao artigo 189.º do CPP, Pinto de Albuquerque[231] entende que esta *"disposição não é aplicável à infiltração on line em sistemas informáticos pessoais, como computadores pessoais e PDAs, com vista à obtenção de informações e dados do visado, sejam eles textos, imagens ou sons. Também neste caso, o carácter altamente intrusivo da infiltração impõe a reserva de lei e de juiz, razão pela qual esta infiltração não é presentemente admissível como meio atípico de obtenção de prova".*

Dias Ramos[232] alerta para a circunstância de não se dever confundir a pesquisa de dados informáticos com a *"pesquisa de dados online"*. A primeira surge no decurso de um processo em investigação (sublinhado nosso), por ser necessário à produção de prova (artigo 15.º, n.º1 da LC). Já quanto à pesquisa de dados online, ou seja, à intervenção encoberta em sistemas informáticos, o legislador não criou uma norma processual específica para esta nova forma de investigação, nem regulamentou os meios técnicos a utilizar; limitou-se a remeter o artigo 19.º da Lei do Cibercrime, para o regime aplicável às ações encobertas, previsto na lei n.º 101/2001, de 25 de agosto. Nas palavras do referido Autor *"A pesquisa de dados online pressupõe que um sistema informático esteja a ser "vigiado" ou sob interceção, tal qual como se fazem escutas telefónicas, vigilâncias ou seguimentos, como é o caso mais comum em processos de investigação de tráfico de estupefacientes. Uma vez que não contempla esta figura na lei de modo mais específico, tal como recorrendo a worms ou spyware, a mesma não poderá ser utilizada para desenvolver investigações e carrear prova para o inquérito, sob pena da prova obtida ser considerada nula"*.

Não deve confundir-se as ações encobertas com as "buscas online", nas primeiras, o agente infiltra-se em grupos, ou comunica com outros criminosos de modo a obter informações. Nas "buscas online", tratar-se-á de pesquisas que ocorrem fora do decurso de um processo, é uma medida muito invasora, na medida em que no acesso a sistemas informáticos sem quaisquer limites e sem estar acompanhado da presença do Juiz (caso se admitissem este tipo de buscas)

[230] Idem,pp.62 e 63
[231]ALBUQUERQUE, Paulo Pinto de, Comentário do Código de Processo Penal, p.528
[232] RAMOS, Armando Dias, A prova digital em processo penal, pp. 91-92

violaria os direitos fundamentais dos visados por essas medidas e seria prova absolutamente proibida.

A lei do Cibercrime procedeu à adaptação ao mundo virtual dos regimes das buscas e das apreensões (pelas figuras da pesquisa de dados informáticos, no artigo 15.º, da apreensão de dados informáticos no artigo 16.º e da apreensão de correio eletrónico e registos de comunicações de natureza semelhante, no artigo 17.º) e do regime das interceções de comunicações telefónicas (pela figura da interceção de comunicações, no artigo 18.º) [233].

Em jeito de conclusão, e relativamente ao que se acabou de referir, cumpre-nos salientar que a nova lei do Cibercrime não consagra um regime para as chamadas "buscas online", e os parâmetros em que deve ocorrer, fora de um processo de investigação, mas no decurso de um processo as pesquisas são feitas como se de buscas e apreensões se tratasse. Não obstante, haver quem denomine as pesquisas informáticas de "buscas online".

Feita uma análise aos novos meios de obtenção da prova eletrónico-digital, importará sublinhar que deve atender-se: por um lado, à privacidade das comunicações e dos dados pessoais; e por outro, à necessidade de uma eficaz investigação criminal, onde as normas do artigo 12.º ao artigo 19.º do diploma em apreço estabelecem os requisitos de acesso dos órgãos de investigação policial e dos Tribunais a estes dados, tendo os fornecedores de serviços responsáveis pelo tratamento desses dados, a obrigação de colaborar[234].

2.5. Proibições de prova

Já anteriormente fizemos algumas considerações sobre as proibições de prova. Também na prova eletrónico-digital se deve respeitar-se as imposições legais. Obviamente, que se fosse admissível no nosso Direito, a titulo de exemplo, a revelação coativa de *password*, os operadores de direito mais facilmente acederiam à prova. Todavia, existem limites que devem ser observados, para concretização dos direitos fundamentais.

"A expressão ´proibições de prova` (Beweeisverbote) foi inventada por Beling, que a utilizou pela primeira vez numa conferência inaugural proferida no ano 1902, em Tübingen.

[233] VERDELHO, Pedro, módulo 3, A perspetiva processual: Prova eletrónica em processo penal, p.2.documento fornecido pelo Autor em Curso de formação avançada à distância CIBERCRIME E PROVA DIGITAL, organizado pela e-UNIFOJ do centro de Estudos sociais (CES) da Universidade de Coimbra e coordenado por Pedro Verdelho, decorreu entre 06 de Outubro e 05 de Dezembro, disponível em http://opj.ces.uc.pt/e-learning/moodle/course/view.php?id=10 consultado em 10-11-2014

[234] VENÂNCIO, Pedro Dias. LEI DO CIBERCRIME-ANOTADA E COMENTADA, pág.99

Beling pretendia, através dessa designação, referir que existem limitações à descoberta da verdade material no processo penal, que o Estado se impõe a si mesmo, em parte como forma de respeitar a esfera da personalidade do cidadão investigado, noutra parte também como forma de preservar certos interesses públicos."[235]

As opiniões divergem quanto à relação do regime das nulidades com as proibições de prova. Numa corrente, encontramos os defensores de uma autonomia dogmática (Paulo de Sousa Mendes[236]), que reconhecem a diferença de regimes, o regime das nulidades visa responder à inobservância das exigências legais dos atos processuais, já o regime das proibições de prova, propõe-se a disciplinar a investigação criminal, estabelecendo limites cuja violação acarreta a ofensa dos mais relevantes direitos individuais. Entendem, portanto, que do ponto de vista jurídico, este regime estabelece uma clara relação de especialidade face ao das nulidades.[237]

Com argumentos de que que a autonomia dos dois regimes não é apenas dogmática, mas também uma autonomia jurídica, encontramos autores que defendem uma absoluta separação dos dois regimes (Manuel da Costa Andrade[238]), considerando que o regime das proibições de prova não depende de modo algum do regime das nulidades e consequentemente não existe nenhuma relação de especialidade daquele perante este.[239] *"Paulo Pinto de Albuquerque afirma que o artigo 118.º n.º3 estabelece o «o princípio do tratamento autónomo das proibições de prova (o regime das proibições de prova não se identifica nem se sobrepõe ao das nulidades nem ao das irregularidades)»*[240]

---

[235] BELING, Ernst, Die Beweisverbote als Grenzen der Wahrrheitserforschung im Stafprozess, Darmstadt: Wissenschaftliche Buchegesellschaft, 1903:3-6.Sobre a origem e desenvolvimento histórico do conceito, veja-se, por todos, AMBOS, Kai, Beweisverwertungsverbote: Grundlagen und Kasuistik - internationale Bezüge - ausgewählte Probleme, Berlin: Duncker & Humblot, 2010: 17-21. Apud MENDES, Paulo de Sousa da, Lições de Processo Penal, p. 177.

[236] *In* Manuel da Costa Andrade, Sobre proibições , cit, p.195; Paulo de Sousa Mendes, As proibições de prova no processo penal, in jornadas de Direito Processual Penal e Direitos fundamentais, Coimbra, Almedina,2004, pp. 148-149. *Apud* OLIVEIRA, Luís Pedro Martins de, Da autonomia do regime das proibições de prova, in PROVA CRIMINAL E DIREITO DE DEFESA, estudos sobre teoria da prova e garantias de defesa em processo penal, Reimpressão, coord. Tereza Pizarro Beleza e Frederico de Lacerda da Costa Pinto, Almedina, Coimbra 2011, ISBN978-972-40-4090-5, pp. 260-261

[237] OLIVEIRA, Luís Pedro Martins de, Da autonomia do regime das proibições de prova, in PROVA CRIMINAL E DIREITO DE DEFESA, pp.260-261

[238] in Manuel da Costa Andrade, Sobre proibições , cit, p.195; Apud OLIVEIRA, Luís Pedro Martins de, Da autonomia do regime das proibições de prova, in PROVA CRIMINAL E DIREITO DE DEFESA, p.260.

[239] Idem, pp.261-262.

[240] in Comentário do Código de Processo Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem, 2.ª ed., Lisboa, Universidade católica Editora, 2008, p. 299. Apud OLIVEIRA, Luís Pedro

O Código de Processo penal distingue os temas de prova proibidos (aqueles que a lei não permite que sejam investigados), os meios de prova proibidos (a lei não permite que se valorizem como meio de prova por lhes faltar um qualquer requisito legal) e os métodos proibidos de prova (constam do artigo 126. do CPP e do artigo 32.º n.º8 da CRPº).[241]

O efeito-à-distância das proibições de prova, segundo Sousa Mendes[242], "*é a única forma de impedir que os investigadores policiais, os procuradores e os juízes menos escrupulosos se aventurem à violação das proibições de produção de prova na mira de prosseguirem sequências investigatórias às quais não chegariam através dos meios postos à sua disposição pelo Estado de Direito*". Porém, esse efeito pode ser atenuado em determinados casos, nomeadamente, quando as provas secundárias poderiam ter sido obtidas na falta da prova primária.

> *"Segundo a teoria da árvore envenenada ou dos frutos da árvore envenenada (fruit of poisonous tree doctrine), desenvolvida nos Estados Unidos da América,e a teoria da nódoa (Makel-Theorie), desenvolvida na Alemanhã, as provas obtidas mediante métodos proibidos de prova, ofensivos dos direitos, liberdades e garantias, contaminam, através do efeito-à-distância as provas consequenciais ou subsequentes, não podendo, também estas, ser utilizadas.*
>
> *Através de uma longa evolução jurisprudencial, sobretudo nos Estados Unidos da América, o radicalismo destas teorias, como nos dá conta o Tribunal Constitucional, foi bastante atenuado, particularizando-se as circunstâncias em que uma prova reflexa deve ser excluída do efeito próprio das doutrinas referidas. São fundamentalmente três os grupos de circunstâncias: a chamada limitação da fonte independente; a limitação da descoberta limitada e a limitação da mácula.*
>
> *A **fonte independente**, que respeita a um recurso probatório destacado do inválido, usualmente com recurso a meio de prova anterior que permite induzir, probatoriamente, aquele a que o originário tendia, mas que foi impedido, ou seja, quando a ilegalidade não foi condictio sine qua nom da descoberta da verdade. Exemplo:Busca inicial ilegal na qual foram observados objectos próprios para o tráfico de estupefacientes, mas não*

Martins de, Da autonomia do regime das proibições de prova, in PROVA CRIMINAL E DIREITO DE DEFESA...p. 260.

[241] JESUS, Francisco Marcolino de, Os meios de obtenção da prova em processo penal...p.82.

[242] MENDES, Paulo de Sousa, Lições de Direito Processual Penal, Coimbra, Almedina, 2013, p. 192. ISBN 978-972-40-5205-2

os estupefacientes, seguida de uma busca com mandado, baseado numa causa provável anterior à primeira busca, em que o produto estupefaciente foi efectivamente encontrado. Tudo o que foi encontrado na primeira busca deve ser excluído como prova válida, o produto estupefaciente encontrado na segunda deve manter-se como elemento de prova válida.

A outra restrição à doutrina do fruto da árvore venenosa é ***descoberta inevitável****, que tem lugar quando se demonstre - pela acusação - que uma outra actividade investigatória, não levada a cabo, seguramente iria ocorrer na concreta situação, não fora a descoberta através da prova proibida conducente inevitavelmente ao mesmo resultado, ou seja, quando inevitavelmente, apesar da proibição, o resultado seria inexoravelmente alcançado. Exemplo: um interrogatório ilegal, levou o suspeito a localizar o cadáver da vítima. Este, porém, sendo certo que ocorriam concomitantemente buscas no local onde foi encontrado, viria seguramente, embora eventualmente mais tarde a ser descoberto.*

A terceira limitação à doutrina dos frutos da árvore venenosa é a da ***mácula dissipada*** *que conduz a que uma prova, não obstante derivada deoutra prova ilegal, seja aceite sempre que os meios de alcançar aquela representem uma forte autonomia relativamente a esta, em termos taos que produzam uma decisiva atenuação da ilegalidade precedente. Exemplo: a ilegalidade de uma detenção inicial, não assente em causa provável, não afecta uma posterior confissão voluntária e esclarecida quanto às suas consequências, tratando-se esta de um acto independente praticado de livre vontade."*[243]

Em Acórdão do Tribunal Constitucional n.º 198/2004, de 24 de março de 2004 (Moura Ramos), cuja doutrina foi reafirmada na Decisão Sumária do Tribunal Constitucional n.º13/2008, de 11 de janeiro de 2008 (Maria Lúcia Amaral) o tribunal constitucional afirmou a inteira vigência entre nós da doutrina da eficácia longínqua ou do efeito à distancia.

"No acórdão, tratava-se de apreciar a questão de inconstitucionalidade normativa de saber se a norma do artigo 122.º n.º1, pode ser interpretada como autorizando, face à

[243] GONÇALVES, Fernando; ALVES, Manuel João, A PROVA DO CRIME, Meios Legais para a sua Obtenção, Almedina, Coimbra, 2009, ISBN 978-972-40-3971-8 pp. 139-140. Vide também Paulo de Sousa Mendes, que faz uma análise pormenorizada às exceções ao efeito-à-distância em jurisprudência dos Estados Unidos da América, MENDES, Paulo de Sousa, Lições de Direito processual penal, pp.192-194

nulidade de intercepções telefónicas realizadas, a utilização de outras provas, distintas das escutas se a elas subsequentes, tais como declarações confessórias dos arguidos que não teriam existido se os arguidos soubessem da invalidade das escutas. O TC afirmou a inteira vigência entre nós da doutrina da eficácia longínqua ou do efeito à distância, mas, no caso em apreciação, invocando a doutrina estabelecida pelo Supremo Tribunal dos EUA no caso Wong Sun v. United States, considerou que a invalidade da prova primária não efetava uma posterior confissão voluntária e esclarecida quanto às suas consequências, tratando-se de um ato independente praticado de livre vontade. Em referência ao artigo 122.º, o TC considerou que "esta norma abre um espaço interpretativo no qual há que procurar relações de dependência ou de produção de efeitos (o art. 122.º, n.º1 do CPP fala em atos dependentes ou afetados pelo ato inválido) que, com base em critérios nacionais, exijam a projeção do mesmo valor que afeta o ato anterior. Finalmente o TC decidiu que "o entendimento do artigo 122.º, n.º1 do CPP, subjacente à decisão recorrida, segundo o qual este abre a possibilidade de ponderação do sentido das provas subsequentes, não declarando a invalidade destas, quando estiverem em causa declarações de natureza confessória, mostra-se constitucionalmente conforme, não comportando qualquer sobreposição interpretativa a essa norma que comporte ofensa ao disposto nos preceitos constitucionais invocados".[244]

A prova eletrónico-digital, como toda a prova, será admissível quando não for proibida por lei. Na análise ao artigo 17.º da Lei do cibercrime começamos por fazer referência às divergências doutrinárias e jurisprudências. Tratando-se de mensagens de correio eletrónico aberto e lido, aplicar-se-ia o regime dos simples documentos; caso as mensagens não tivessem sido abertas ou lidas, ser-lhe-ia aplicado o regime processual da correspondência. Com o surgimento da Lei do Cibercrime, passou a prever-se que, 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 autorizará ou ordenará por despacho que se proceda a uma pesquisa nesse sistema informático, devendo, sempre que possível, presidir à diligência, caso contrário, não havendo

[244] *In* AA.VV. Elementos de Estudo - Direito Processual Penal (coord.: Paulo de Sousa Mendes), 1.ª reimp., Lisboa: AAFDL, 2010, pp. 630-676. *Apud* MENDES, Paulo de Sousa, Lições de Direito Processual, pp. 194-195.

autorização do Juiz, a prova obtida será considerada nula, por violação do direito da privacidade do sujeito sobre quem foi efetuada pesquisa.

Em Acórdão do Tribunal da Relação do Porto[245], suscitou-se a questão, de se saber, se a prova obtida pelos polícias, designadamente, do conteúdo de mensagens do telemóvel do arguido, desprovida do seu consentimento e sem prévia autorização do juiz, valoradas no tribunal *a quo*, consubstanciará prova proibida e, como tal, nula. Vejamos: se tivesse existido consentimento do titular do direito, no acesso ao teor das mensagens, estaríamos perante um caso de proibição de prova relativa, sanável pelo consentimento do titular do direito protegido (artigo 126.º n.º3 do CPP). Contrariamente, caso o consentimento seja obtido mediante tortura, coação ou, ofensa da integridade física ou moral das pessoas, casos em que as proibições de prova qualificar-se-ão como absolutas e portanto insanáveis (artigo 126.º n.º1 do CPP).

O uso de prova proibida torna nula, toda e qualquer decisão, que nela se tenha fundamentado. Na verdade, conforme refere Pinto de Albuquerque[246],

> *"(…)a nulidade da prova proibida prejudica a sentença ou despacho (por exemplo, o despacho instrutório ou o despacho que determina uma medida de coacção)* ***se a prova proibida tiver sido utilizada na fundamentação da decisão****, bastando para o efeito que ela seja um dos meios de prova invocados, mesmo que não seja o elemento preponderante para a fundamentação da decisão do tribunal (também assim, Costa Andrade, 1992: 64 e 65). A* ***sentença fundada em provas nulas*** *(provas insanavelmente nulas ou provas cuja nulidade é sanável, mas não deva considerar-se ainda sanada) é, também ela, nula, nos termos do artigo 122.º, n.º 1. (…) O* ***fundamento do recurso da sentença ou do despacho*** *para conhecimento de uma nulidade da prova proibida reside no artigo 410.º, n.º 3, do CPP, aplicável por identidade de razão ao recurso de despacho interlocutório. Assim, a procedência da nulidade tem a* ***consequência*** *da repetição da sentença pelo tribunal recorrido, sem a ponderação da prova proibida."*

O tribunal *ad quem* considerou:*"ser prova proibida o uso por parte do órgão de polícia criminal, não autorizado judicialmente nem pelo arguido, das SMS´s gravadas no cartão SIM do telemóvel deste; em consequência disso, nulo o douto acórdão que nela se fundamentou, determinando-se que o Tribunal a quo profira um outro que a não contemple".*

[245] Acórdão do Tribunal da Relação do Porto, de 12-09-2012, Processo nº 787/11.5PWPRT.P1, com relator ALVES DUARTE, disponível em http://www.dgsi.pt
[246] ALBUQUERQUE, Paulo Pinto de, Comentário do Código de Processo Penal, p. 321

3. Cooperação Internacional

3.1. A fácil deslocação criminosa na web

É notória a evolução da nossa legislação, no sentido de punir os cibercrimes. Contudo, a rápida deslocação criminosa na web, pode criar constrangimentos ao nível da concretização do princípio da territorialidade, Segundo Ramos Pereira *"É difícil reconstituir o percurso das informações entre o ponto emissor e o ponto receptor , em virtude de os actos na internet serem praticados em diversos pontos, sabendo que os infractores em regra, dissimulam o efectivo ponto emissor"*, além disso, fácilmente se transferem os conteúdos para outros servidores de alojamento ou de aceso à internet e poderão sempre pedir o acesso a um servidor off-shore. Quando o armazenamento e divulgação de informação ilícita seja prestada por servidores estrangeiros tornar-se-á juridicamente difícil às autoridades de outro Estado proibirem os prestadores desses serviços de permitirem a prática de condutas ilícitas.[247]

Para determinar a competência dos tribunais portugueses, ou seja, *"Para aferição do locos delicti, basta que o crime tenha com o território português qualquer dos elementos de conexão previstos no art.º 7.º do Código Penal, a saber, a acção, omissão ou resultado típico. Em qualquer destas circunstâncias, considera-se o crime como praticado em Portugal e, consequentemente, aplicável o direito português e competentes os Tribunais Portugueses."*[248] Ainda nos factos praticados em território português independentemente da nacionalidade do agente (artigo 4.º, al. a) do CP), a bordo de um navio ou aeronaves portuguesas (artigo 4.º, al. b) do CP), aplica-se também a factos cometidos fora do território nacional nos casos expressamente previstos na lei (artigo 5.º CP)[249].

O artigo 27.º da LC veio alargar o âmbito dessas competências. Não se verifica nenhuma contradição com qualquer princípio estruturante do ordenamento jurídico nacional, que já prevê para outros crimes, a competência universal da lei portuguesa, desde logo, no artigo 5,º, n.º1, alínea a) do Código Penal[250]. Há crimes insuscetíveis de localização, que ultrapassam fronteiras

[247] PEREIRA, Joel Timóteo Ramos, Direito da Internet e Comércio Electrónico, Quid Iuris? Sociedade Editora, Lisboa, 2001. ISBN 972-724-113-1. p. 239
[248] PEREIRA, Joel Timóteo Ramos, Direito da Internet e Comércio Electrónico, Quid Iuris? Sociedade Editora, Lisboa, 2001. ISBN 972-724-113-1. p. 240
[249] Idem, p. 241
[250] VERDELHO, Pedro, A convenção sobre cibercrime do conselho da Europa - repercussões na Lei portuguesa, p. 273

físicas, sendo que a prática desses delitos ao extravasarem o âmbito estadual, converte-os em assunto público da comunidade internacional. Na verdade, foi a pirataria em alto mar que permitiu a primeira aplicação da técnica da competência universal no Direito Internacional.[251]

3.2. Necessidade de cooperação internacional

Os artigos 20.º a 26.º da Lei do Cibercrime vêm estipular as medidas de cooperação internacional[252] propostas nos artigos 23.º a 35.º da Convenção sobre o Cibercrime.

No artigo 20.º da Lei do Cibercrime, com epígrafe ***âmbito da cooperação internacional***, estabelece-se que as autoridades judiciárias competentes têm de cooperar com as entidades estrangeiras competentes para efeitos de investigações, ou procedimentos respeitantes a crimes

[251] ALMEIDA, Francisco António de Macedo Lucas Ferreira de, Os Crimes Contra a Humanidade no Actual Direito Internacional Penal, Dissertação para doutoramento em Ciências Jurídico-políticas pela Faculdade de Direito da Universidade de Coimbra, Almedina, ISBN 978-972-40-3761-5, DEPÓSITO LEGAL 288229/09, Fevereiro 2009. PP.166-167

[252] Para melhor denotarmos os contributos dessa regulamentação apresentamos dois casos de estudo distintos. **Caso 1**: não é um típico "caso de cibercrime", mas foram usadas as ferramentas de cooperação internacional da Convenção de Budapeste. Em 2005, um cidadão da Noruega atacou um banco em Oslo, pretendia roubar dinheiro mas, no decurso da operação, um agente policial morreu o assaltante fugiu e não foi possível detê-lo ou descobrir o seu paradeiro. Alguns dias mais tarde, a polícia efectuou uma busca à sua casa e aprendeu o seu computador descobriu que o assaltante era dono de uma conta de email de um fornecedor de serviços do Reino Unido a cooperação internacional foi solicitada às autoridades de Londres. Dias depois, o assaltante acedeu à sua conta de email para mandar uma mensagem no Reino Unido, a polícia obteve do ISP a informação necessária para concluir onde estava o assaltante. As autoridades espanholas e britânicas implementaram um sistema de alerta, cujo objectivo era o de conhecer, em cada vez que o assaltante utilizava a sua conta de correio electrónico, onde estava o mesmo, assim, em cada vez que utilizou a sua conta, a polícia britânica obteve o endereço IP do equipamento na origem da comunicação e comunicou-o de imediato à polícia espanhola. Então, a polícia espanhola obtinha do ISP espanhol dados sobre o dono ou utilizador do endereço IP, todas as ligações se faziam desde um ciber café de Madrid apesar de se tentar aproximar do café muito rapidamente, durante muito tempo a polícia não conseguiu chegar antes da partida do assaltante. Dias depois, o assaltante passou a utilizar a sua conta de email a partir de um ciber café de Málaga, era uma localidade muito mais pequena que Madrid numa pequena aldeia próxima de Málaga, foi possível pôr todos os ciber cafés da área sob vigilância permanente, depois de alguns dias de vigilância, a polícia britânica anunciou que o assaltante estava online, usando a sua conta de email e forneceu o respectivo endereço IP. Rapidamente, o ISP de Espanha informou a polícia espanhola sobre a localização concreta do ciber café, os agentes policiais na rua conseguiram identificar e deter o assaltante, que veio a ser extraditado para a Noruega
Caso 2: um típico "caso de cibercrime" mas as ferramentas de cooperação internacional não puderam ser usadas. A Estónia ratificou a Convenção de Budapeste em 2003. A Estónia sofreu um importante ataque, do tipo (DDoS distributed denial of service) em Abril e Maio de 2007, este ataque causou perturbações muito importantes na vida quotidiana das pessoas e das instituições públicas, páginas web ficaram fora de serviço e os servidores ficaram indisponíveis, foram executados vários ataques utilizando botnets – muitas páginas web estónias não estiveram disponíveis durante alguns dias. Identificaram-se se alguns IP suspeitos, mas apenas foi levada a julgamento uma pessoa, que acabou por ser condenada na verdade, era o único cidadão estónio, de entre os suspeitos que foi possível identificar todos os outros suspeitos usaram um IP de um Estado que não assinou a Convenção de Budapeste – e portanto, cuja lei não permite cooperar com outros Estados. Informação retirada de Curso de formação avançada à distância CIBERCRIME E PROVA DIGITAL, organizado pela e-UNIFOJ do centro de Estudos sociais (CES) da Universidade de Coimbra e coordenado por Pedro Verdelho, decorreu entre 06 de Outubro e 05 de Dezembro.

relacionados com sistemas ou dados informáticos, bem como para efeitos de recolha de prova, em suporte eletrónico de um crime, de acordo com as normas de transferência de dados pessoais, previstos na lei n.º 67/98, de 26 de Outubro.

Para esse efeito, seria necessária a existência de **ponto de contacto permanente** entre os vários Estados membros, para que essa cooperação internacional tivesse lugar. O artigo 21.º criou esse ponto, cabendo à Polícia Judiciária assegurar a manutenção de uma estrutura que garanta um ponto de contacto disponível permanentemente, isto é, vinte e quatro horas por dia, sete dias por semana (n.º1 do citado artigo).

Mantêm troca de informações, 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 (n.º2 do referido artigo). A assistência imediata prestada por esse ponto de contacto permanente passa pelas seguintes funções: "*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 22.º; 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 de perigo na demora; e) a transmissão imediata ao Ministério Público de pedidos relativos às medidas referidas das alíneas b) a d), fora dos casos aí previstos, tendo em vista a sua rápida execução"* (conforme o n.º3 do artigo em apreço).

Sempre que atue ao abrigo das referidas alíneas b) a d) do n.º3 do artigo 21.º a Polícia Judiciária dará notícia imediata do facto ao Ministério Público remetendo também o relatório previsto no artigo 253.º do Código de Processo Penal.

No artigo 22.º consagra-se a ***preservação e revelação expeditas de dados informáticos em cooperação internacional***. O artigo 29.º da Convenção consagra regras respeitantes à preservação expedita de dados armazenados num computador. Admite-se, nesta norma, a possibilidade de um Estado solicitar a outro a preservação expedita de dados, manifestando a intenção de, ulteriormente, lhe fazer um pedido formal de assistência, para realização de uma busca, apreensão ou diligência similar, devendo o Estado requerido tomar as diligências necessárias à preservação daqueles dados, respeitando a lei nacional. De acordo com o n.º3 deste artigo 29.º,não será necessário que se observe o requisito da dupla incriminação, como condição

da preservação dos dados (quanto aos crimes previstos na convenção, haverá, em princípio , dupla incriminação, o que não acontecerá nos demais crimes).[253]

Esta medida visa somente a preservação de dados por razões cautelares, sem implicar a sua revelação (prevista no artigo 30.º da Convenção). sendo que esta terá outras regras, mais estreitas, por isso, poderá haver preservação de dados sem que depois haja condições para a sua revelação ao Estado requerente.[254]

A preservação expedita de dados informáticos vem regulada nos n.os 1 a 9 do artigo 22.º da Lei do Cibercrime, e por sua vez, a comunicação à autoridade requerente encontra-se prevista nos n.os 10 e 11 do mesmo artigo. Pode ser solicitada a Portugal a preservação expedita de dados informáticos, armazenados em sistema informático localizado no nosso país, relativos a crimes previstos no artigo 11.º, com vista a apresentação de um pedido de auxílio judiciário para fins de pesquisa, apreensão e divulgação dos mesmos (artigo 22.º n.º1). Para este efeito, a entidade requerente deve especificar no pedido os seguintes elementos: *"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 de dados"* (artigo 22.º n.º 2).

A autoridade judiciária competente, em execução de uma solicitação de autoridade estrangeira, ordena a quem tenha disponibilidade ou controlo desses dados, designadamente a Fornecedor de Serviços que os preserve (nr.º3 do artigo em apreço).

Estipula ainda o n.º 4 deste artigo, que a preservação possa ser ordenada pela Polícia Judiciária, mediante autorização da autoridade judiciária competente ou quando haja urgência ou perigo na demora, devendo nestas situações dar notícia imediata ao Ministério Público e remeter-lhe o relatório previsto no artigo 253.º do Código de Processo Penal[255].

A ordem de preservação específica, sob pena de nulidade (sob pena de tal prova não poder ser valorada - proibição de valoração[256]): "*a) A natureza dos dados; b) Se forem*

[253] VERDELHO, Pedro, Cibercrime, Direito da Sociedade da informação, vol. IV op. cit. p. 379
[254] Idem, pp. 379-380
[255] RODRIGUES, Benjamim Silva, da Prova Penal, tomo IV, p. 536
[256] Idem, p. 537

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" (conforme ao artigo 22.º n.º5). Recebida essa ordem, deve o fornecedor de serviço preservar de imediato, os dados em causa pelo período estipulado, protegendo e conservando a sua integridade (N.º6). Poderá ser ordenada renovação da medida de preservação, por períodos sujeitos ao limite de três meses (limite previsto na alínea c) do n.º5), até ao limite máximo de um ano (n.º7).

No artigo 23.º com a epígrafe ***Motivos de recusa***, o legislador previu a possibilidade de se recusar a solicitação de preservação ou revelação expeditas de dados informáticos (n.º1), quando: "*a) Os dados informáticos em causa respeitarem a infracções 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"*. Poderá igualmente ser recusada quando houver fundadas razões para crer que a execução do 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 (n.º2).

O artigo 24.º- ***Acesso a dados informáticos em cooperação internacional*** - prevê no seu n.º1, a possibilidade de, em execução de pedido de autoridade estrangeira competente, a autoridade judiciária portuguesa competente 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. O mesmo sucede com os pedidos formulados pelas autoridades judiciárias portuguesas (n.º3). "*Há, depois, um princípio da aceleração ou de urgência, sempre que existam razões para crer que os dados informáticos em causa são «especialmente vulneráveis à perda ou modificação ou quando à cooperação rápida se encontre prevista em instrumento internacional aplicável» "*[257] (n.º2).

O nosso legislador consagrou também o ***acesso transfronteiriço a dados informáticos armazenados quando publicamente disponíveis ou com consentimento,*** no artigo 25.º. Segundo esta disposição, as autoridades estrangeiras competentes podem, sem necessidade de pedido prévio às autoridades portuguesas, e de acordo com as normas sobre transferência de

[257] Idem, p. 539

dados pessoais previstas na lei n.º 67/98, de 26 de Outubro, aceder a dados informáticos armazenados em sistema informático localizado em Portugal, quando publicamente disponíveis (alínea a)). Poderão, igualmente, 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 (alínea b)). No entender de Benjamim Silva Rodrigues, " *(...) não se trata de uma medida efectiva de cooperação, já que as autoridades estrangeiras competentes, sem necessidade de pedido prévio às autoridades portuguesas, de acordo com as normas vigentes, a nível europeu e português...*" podem aceder a esses dados informáticos publicamente disponíveis ou com consentimento da pessoa legalmente autorizada a divulgá-los[258] (referidos nas alíneas deste normativo).

De acordo com o preceituado no artigo 26.º - ***interceção de comunicações em cooperação internacional*** - em execução de pedido da autoridade estrangeira competente, pode ser autorizada pelo juiz a interceção de transmissão de dados informáticos realizada 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 interceção seja admissível, nos termos do artigo 18.º, em caso nacional semelhante. No entender de Benjamim Silva Rodrigues, é atribuído o papel de "*pivot*" à Polícia Judiciária Portuguesa "*Para recepção dos pedidos de intercepção de comunicações, considerou-se competente a Polícia Judiciária que, à semelhança do que ocorre na Lei n.º 144/99, os apresentará ao Ministério Público, para que, por sua vez, este os torne presentes ao Juiz de instrução da comarca de Lisboa para autorização*"[259].

Pedro Dias Venâncio, alerta para o facto de que não se deve desconsiderar os poderes atribuídos à Autoridade Nacional de Comunicações (ANACOM), enquanto entidade de supervisão central nos termos do disposto no artigo 35.º do DL n.º 7/2004, de 7 de Janeiro (Lei do Comércio Eletrónico-LCE). Tendo competência para adotar as providências restritivas (consistem na possibilidade "*de restringir a circulação de um determinado serviço da sociedade da informação proveniente de outro Estado Membro da União Europeia se lesar ou ameaçar gravemente: a) A dignidade humana ou a ordem pública, incluindo a protecção de menores e a repressão do incitamento ao ódio fundado na raça, no sexo, na religião ou na nacionalidade,*

[258] Idem, Ibidem
[259] Idem, p. 540

nomeadamente por razões de prevenção ou repressão de crimes ou de ilícitos de mera ordenação social; b) A saúde pública; c) A segurança pública , nomeadamente na vertente da segurança e defesa nacionais; d) Os consumidores, incluindo os investidores") previstas nos artigos 7.º e 8.º da LCE e as competências exclusivas de cooperação com as entidades de supervisão central dos demais Estados Membros da União Europeia, do artigo 9.º da referida LCE[260].

O artigo 32.º da convenção prevê uma forma de obtenção de prova no estrangeiro, sem recurso à cooperação Internacional, quando no decurso de uma investigação, obter de um computador localizado no estrangeiro dados de livre acesso, ou mediante autorização da pessoa com essa legitimidade[261], o inverso também pode acontecer como já referimos supra em referência ao artigo 25.º da LC.

A Lei do Cibercrime, nas disposições que acabamos de referir agilizou assim mecanismos de cooperação judiciária entre os países que aderiram à Convenção do Cibercrime[262].

[260] VENÂNCIO, Pedro Dias, Lei do Cibercrime, anotada e comentada, op. cit. pp. 92-93
[261] VERDELHO, Pedro, Cibercrime, Direito da Sociedade da informação, vol. IV, p. 380

Conclusão

Com este trabalho tentamos dar a conhecer um pouco melhor o que se entende por cibercrime e como ele é regulamentado no nosso ordenamento. Conforme defendido por Dias Simões, este conceito abrange vários crimes desde que praticados com recurso a novas tecnologias de informação e de comunicação, podendo inclusivamente a informática ser alvo do crime ou meio de execução.

A Lei do Cibercrime, Lei n.º 109/2009, de 15 de setembro, que veio substituir a Lei n.º 109/91, de 17 de agosto, resultou essencialmente da Convenção sobre o Cibercrime do Conselho da Europa adotada em Budapeste em 23 de novembro de 2001 e da Decisão-Quadro, 2005/222/JAI, do Conselho, de 24 de Fevereiro de 2005. Aplica-se a crimes previstos nesta lei, naqueles em que é necessária a recolha de prova através de meios informáticos e aqueles que ferem a integridade dos sistemas informáticos, bem como ataques a sistemas de informação e bloqueios de serviços, ou seja, cometidos por meio de um sistema informático.

Defendemos que o Direito Penal Clássico é suficiente para responder à criminalidade praticada com recursos aos meios informáticos, não se exigindo um novo ramo do Direito Penal.

Contudo não concordamos com o facto de as disposições processuais constarem de legislação extravagante, preferindo o entendimento de Dá Mesquita, segundo o qual deveriam estar consagradas no Livro III, relativo à prova, do Código de Processo Penal, titulo III, criando-se um capítulo V, por essas disposições se aplicarem também a outros crimes, além dos consagrados nesta Lei, ou que se fizesse uma remissão no Código de Processo Penal para esta Lei.

Seria ir longe demais responsabilizar os prestadores de serviços por eventuais quebras de segurança e pelos conteúdos disponíveis na internet, uma vez que podem nem sequer tomar conhecimento da informação transmitida ou armazenada. Contudo, no nosso entendimento, na eventualidade de estes desrespeitarem uma ordem da autoridade judiciária competente para remoção dos conteúdos, deveriam incorrer no crime de desobediência previsto no artigo 348.º do Código Penal, não obstante haver quem entenda que seria preferível aplicar uma sanção pecuniária compulsória.

A Lei do Cibercrime veio consagrar novas disposições penais materiais, onde surgem novos bens jurídicos, tais como a integridade dos sistemas informáticos de acordo com a nossa

jurisprudência, a integridade dos fluxos informacionais e comunicacionais e informático-digitais, de acordo com Silva Rodrigues, a integridade e fiabilidade de dados e ao bom funcionamento dos sistemas informáticos e privacidade na comunicação de dados, na esteira do entendimento de Pedro Verdelho, domicílio informático, como referem Ramos Pereira e Lopes Rocha, segurança dos sistemas informáticos, que se coadunam com o entendimento desta nova realidade.

Logo, com novos bens jurídicos, surgem outros desafios ao nosso ordenamento jurídico, nomeadamente aqueles que concernem ao processo penal e à prova. A prova eletrónico-digital deve fazer-se com respeito pelos princípios gerais de direito, bem como pelo regime das proibições de prova, sob pena de a prova obtida não ser, nem poder ser, valorada pelo Tribunal. Para tal, deve atender-se ao critério da proporcionalidade na decisão da medida probatória a tomar, deixando-se sempre que possível, prevalecer as medidas menos invasivas dos direitos fundamentais consagrados na Constituição da República Portuguesa.

Nos artigos 11.º a 19.º da Lei por nós exaustivamente analisada, são consagradas regras de preservação expedita de dados, de revelação de dados, a injunção, a pesquisa, e a apreensão de dados informáticos, apreensão de correio eletrónico e registo de comunicação de natureza semelhante, a interceção de comunicações e as ações encobertas, por remissão do artigo 19.º para a Lei n.º 101/2001, de 25 de agosto, contudo, esta lei não estabelece um regime processual, pondo em causa a valoração da prova obtida nestas, que foram uma inovação no nosso ordenamento jurídico e que, de alguma forma, vieram acautelar uma realidade que se encontrava desprovida de regulamentação jurídica.

Assim, criou-se um ponto de contacto permanente, como exigia a Convenção, facilitando o modo de obtenção de prova localizada em sistemas informáticos estrangeiros, contudo quando a prova se encontre num servidor localizado num país que não aderiu a esta convenção, dificilmente se obterá prova.

Os crimes clássicos podem efetuar-se mediante recurso às novas tecnologias. A prova digital consagra meios expeditos de a obter, através, designadamente da preservação expedita de dados, revelação de dados, pesquisas e apreensões, que veio facilitar as investigações. Continua o Juiz com importantíssimo papel de garantir os direitos fundamentais das pessoas, é o "Juiz das liberdades" a entidade com competência para autorizar a revelação de dados. Com

as Injunções permite-se que os fornecedores de serviços indiquem outros fornecedores onde também foram feitas ligações, a prova pode estar em vários sítios da Internet.

Quando no decurso de uma pesquisa se verifiquem ligações a um outro sistema informático é possível efetuar-se a extensão da pesquisa também a esse.

Exigem-se cuidados redobrados na recolha e preservação da prova, tendo também aqui os peritos um importante papel a desempenhar, quer na recolha quer no relatório a apresentar ao Juiz.

A Internet trará sempre novos desafios, não só ao Direito Penal, como também noutros ramos do Direito. Torna-se repetitivo nas notícias a afirmação "o sistema está em baixo!", a maioria dos serviços públicos e privados recorrem às novas tecnologias, as quebras de segurança de sistemas informáticos e a divulgação de dados, podem levar ao caos, questões às quais o Estado de Direito Democrático não pode ficar indiferente.

Bibliografia

ALBUQUERQUE, Paulo Pinto de, Comentário do Código Penal: à luz da Constituição da República Portuguesa e da Convenção dos Direitos do Homem, 2.º ed. actualizada, Lisboa: Universidade Católica Editora, 2010. ISBN 978-972-54-0272-6

- Comentário do Código de Processo Penal: à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem, 3.ª ed. actualizada, Lisboa, Universidade católica, 2009, ISBN 978-972-54-0202-3.

ALMEIDA, Francisco António de Macedo Lucas Ferreira de, Os Crimes Contra a Humanidade no Actual Direito Internacional Penal, Dissertação para doutoramento em Ciências Jurídico-políticas pela Faculdade de Direito da Universidade de Coimbra, Almedina, ISBN 978-972-40-3761-5, DEPÓSITO LEGAL 288229/09, Fevereiro 2009.

ALVES, Rita Duarte Ribeiro da Mota Ferreira - A Criminalidade Informática no Ordenamento jurídico-Penal Português. Em especial, as questões processuais. Dissertação apresentada no âmbito do 2º Ciclo de Estudos em Direito da Faculdade de Direito da Universidade de Coimbra, Área de Especialização em Ciências Jurídico-Forenses. Orientador: Professora Doutora Helena Moniz, Coimbra, 2012. (Disponível na biblioteca da FDUC).

ANDRADE, Manuel da Costa – "BRUSCAMENTE NO VERÃO PASSADO" A REFORMA DO CÓDIGO DE PROCESSO PENAL, Observações críticas sobre uma lei que podia e devia ter sido diferente.Coimbra Editora, 2009. ISBN 978-972-32-1726-1

- Sobre as proibições de prova em processo penal, Coimbra Editora, 1992, ISBN 972-32-0613-7

ARZAMENDI, José Luis de la Cuesta; BARRANCO, Noberto j. de la Mata [et al.] – Derecho Penal Informático. Primera edicíon, 2010. Editorial Aranzadi, SA. ISBN: 978-84- 470-3429-1.

ASCENÇÃO, José de Oliveira, "O Ilícito em rede", Direito da Sociedade da Informação e Direito de Autor, APDI, vol. X, Coimbra Editora, 2012. ISBN 978-972-32-2018-6.

BARROS, Juliana Isabel Freitas - O NOVO PROCESSO PENAL: OS MEIOS DE OBTENÇÃO DE PROVA DIGITAL CONSAGRADOS NA LEI 109/2009, DE 15 DE SETEMBRO, Dissertação apresentada no âmbito do 2.º ciclo de Estudos em Direito da Faculdade de Direito da Universidade de Coimbra, Área de especialização: Mestrado em Ciências Jurídico-Forenses, Orientadora: Professora Doutora Helena Moniz, Coimbra, 2012., p.16.

Boletim da ordem dos advogados, mensal n.º65, Abril 2010. CIBERCRIME "pode ser muito grande a distância entre o acto criminoso e os seus efeitos". P.36. Consult.26/11/2013. Disponível em:http://www.oa.pt/upl/%7B3d49f105-1ff4-426f-8c50-ddaee1b8acbb%7D.pdf

BRAZ, José, Investigação criminal, a organização, o método e a prova, os desafios da nova criminalidade, 2.ª edição, Almedina, Coimbra, 2010, ISBN978-972-40-4350-0

CARRAPIÇO Helena, O Crime Organizado e as Novas Tecnologias: Uma faca de dois gumes, p. 177. Disponível em http://www.idn.gov.pt/publicacoes/nacaodefesa/textointegral/NeD111.pdf consultado em 04-02-2014

COSTA, José Francisco de Faria, Algumas reflexões sobre o estatuto dogmático do chamado "Direito Penal Informático", Direito Penal da Comunicação, alguns escritos. Coimbra Editora, 1998. ISBN 972-32-0850-4

- Direito Penal Económico, Quarteto, coimbra 2003, ISBN 989-558-004-5

DÍAZ, Leyre Hernández, Aproximación a un concepto de derecho penal informático, in DERECHO PENAL INFORMÁTICO, Primera edición, 2010, Civitas, Editorial Aranzadi, ISBN 978-84-470-3429-1

DIAS, Jorge de Figueiredo, Clássicos Jurídicos, Direito Processual Penal, 1ª ED.1974, Reimpressão, Coimbra Editora, 2004, ISBN 972-32-1250-1, Depósito Legal n.º 208 109/2004

- Supervisão, direito ao silêncio e legalidade da prova, Almedina, Coimbra, 2009, ISBN 978-972-40-3763-9

-Direito penal, parte geral tomo I, 2ª Edição, Questões fundamentais, a doutrina geral do crime, Coimbra Editora, 2007. ISBN 978-972-32-1523-6.

-Temas Básicos da Doutrina Penal: sobre os fundamentos da doutrina penal; sobre a doutrina geral do crime, Coimbra Editora, 2001. ISBN972-32-1012-6

DIAS, Pedro Simões, "O «Hacking» enquanto crime de acesso ilegítimo. Das suas especialidades à utilização das mesmas para a fundamentação de um novo direito". Consult. 10-10-2014. Disponível em: http://www.uria.com/documentos/publicaciones/1580/documento/art04.pdf?id=2108

DIAS, Pedro Simões, O "Hacking" enquanto crime de acesso ilegítimo. Das suas especialidades à utilização das mesmas para a fundamentação de um novo direito, in Direito da Sociedade da Informação, vol. VIII, Coord. Prof. Doutor José de Oliveira Ascenção, Coimbra Editora, 2009. ISBN 978-972-32-1710-0

DIAS, Vera Elisa Marques – A problemática da investigação do Cibercrime. Consult. 22-12-2013. DataVenia Revista Jurídica Digital. N.º1, Julho-Dezembro, 2012. ISSN 2182-8242 Disponível na Internet:
http://www.datavenia.pt/ficheiros/edicao01/datavenia01_p063-088.pdf

ESTRADA, Miren Josune Pérez, La investigacíon del delito a través de las nuevas tecnologías. Nuevos medios de investigagíon en el processo penal, in DERECHO PENAL INFORMÁTICO, José Luis de la Cuesta Arzamendi (director), Primera edición, 2010, Civitas, ISBN 978-84-470-3429-1

GLENNY, Misha, DARK MARKET, Como os hackers se tornaram a nova máfia, do autor do bestseller McMÁFIA, traduzido por Michelle Hapetian, civilização Editora, 2012, ISBN 978-972-26-3443-4, depósito legal 349233/12.

GONÇALVES, Fernando; ALVES, Manuel João, A PROVA DO CRIME, Meios Legais para a sua Obtenção, Almedina, 2009, ISBN 978-972-40-3971-8

Helena Carrapiço, O Crime Organizado e as Novas Técnologias: Uma faca de dois gumes. Consult. 04-02-2014. Disponível em
http://www.idn.gov.pt/publicacoes/nacaodefesa/textointegral/NeD111.pdf

JESUS, Francisco Marcolino de, Os Meios de Obtenção da Prova em Processo Penal, Coimbra, 2011, Almedina. ISBN 978-972-40-4428-6.

LAVOURA, Tiago Santos, "O agente infiltrado e o seu contributo para a investigação criminal", Dissertação para obtenção de grau de Mestre em ciências jurídico-forenses, Orientador Professor Doutor Figueiredo Dias, Co-orientador: Mestre Ana Pais, Coimbra, Lisboa, Instituto Superior Bissaya Barreto.

LEITE, Ana Raquel Gomes, CRIMINALIDADE INFORMÁTICA – INVESTIGAÇÃO E MEIOS DE OBTENÇÃO DE PROVA. Dissertação apresentada no âmbito do 2.º Ciclo de Estudos em Direito, Faculdade de Direito da Universidade de Coimbra, sob orientação da Professora Doutora Helena Isabel Gonçalves Moniz Falcão Oliveira.

MARTINS, A. G. Lourenço, Criminalidade Informática, Direito da Sociedade da Informação, vol. IV, Coimbra Editora, 2003. ISBN 972-32-1169-6.

MATOS, José A. de, Dicionário de Informática e Novas Tecnologias, 3.ª ed. aumentada, FCA - Editora de Informática, LDA. ISBN 978-972-722-469-2

MEDERO, Gema Sánchez. Cibercrimen, Ciberterrorismo y Ciberguerra: Los Nuevos Desafíos Del s. XXI. 239-267. Revista Cenipec. 31.2012. Enero- Diciembre. ISSN: 0798-9202. pág 244. Consult. em 25-08-2014. Disponível em http://www.saber.ula.ve/bitstream/123456789/36770/1/articulo9.pdf

MENDES, Paulo de Sousa, *"A responsabilidade de pessoas colectivas no âmbito da criminalidade informática em Portugal",* in Direito da Sociedade da Informação, Vol. IV, Coimbra Editora, 2003. ISBN 972-32-1169-6.

- As proibições de prova no processo penal, Jornadas de Direito Processual Penal e Direitos Fundamentais,Coordenação Científica de Maria Fernanda Palma, Almedina, 2004

- Lições de Direito Processual Penal, Coimbra, Almedina, 2013. ISBN 978-972-40-5205-2

MESQUITA, Paulo Dá, A PROVA DO CRIME E O QUE SE DISSE ANTES DO JULGAMENTO, Estudo sobre a prova no Processo Penal Português, à Luz do sistema Norte-Americano, 1.ª Ed. Dezembro 2011. Coimbra Editora S.A. ISBN 978-972-32-1951-7.

- Processo Penal, Prova e Sistema Judiciário, 1.ª ed: Setembro 2010, Coimbra Editora. ISBN 978-972-32-1842-8

NEVES, Rita Castanheira – AS INGERÊNCIAS NAS COMUNICAÇÕES ELECTRÓNICAS EM PROCESSO PENAL. Natureza e respectivo regime jurídico do correio electrónico enquanto meio de obtenção de prova. Coimbra: Coimbra Editora, 2011. ISBN 978-972-32-1942-5

NEVES, Rosa Vieira, A Livre Apreciação da Prova e a Obrigação de Fundamentação da Convicção (na Decisão Final Penal), Coimbra Editora, 2011, ISBN 978-972-32-1929-6

OLIVEIRA, Luís Pedro Martins de, Da autonomia do regime das proibições de prova, in PROVA CRIMINAL E DIREITO DE DEFESA, estudos sobre teoria da prova e garantias de defesa em processo penal, Reimpressão, coord. Tereza Pizarro Beleza e Frederico de Lacerda da Costa Pinto, Almedina, Coimbra 2011, ISBN978-972-40-4090-5

PEREIRA, Joel Timóteo Ramos, Direito da Internet e Comércio Electrónico. Quid Iuris?, Sociedade Editora, Lisboa, 2001. ISBN 972-724-113-1

PINTO, Lara Sofia, Privilégio contra a auto-incriminação versus colaboração do arguido, in PROVA CRIMINAL E DIREITO DE DEFESA, estudos sobre teoria da prova e garantias de defesa em processo penal, Reimpressão, coord. Teresa Pizarro Beleza e Frederico de Lacerda da Costa Pinto, Almedina, Coimbra, 2011, ISBN 978-972-40-4090-5

RAMOS, Armando Dias , A prova digital em processo penal: o correio electrónico, Chiado Editora, 1.º ed. Novembro 2014, ISBN 978-989-51-2383-4

RODRIGUES, Benjamim Silva, DIREITO PENAL PARTE ESPECIAL, Tomo I, DIREITO PENAL INFORMÁTICO DIGITAL, Contributo para a Fundamentação da sua Autonomia Dogmática e Científica à Luz do novo Paradigma de Investigação Criminal: a Ciencia Forense Digital e a Prova Digital, com prefácio da D.ª Sara Antunes. [S.L.]: Coimbra Editora, Limitada, 2009. ISBN: 978-989-95779-5-4.

- DA PROVA PENAL, tomo II, Bruscamente… A(s) Face(s) Ocultas dos Métodos Ocultos de Investigação Criminal. 1.ª Edição, Rei dos Livros, 2010. ISBN 978-989-8305-06-0.

- DA PROVA PENAL – Tomo IV, DA PROVA ELECTRÓNICO – DIGITAL E DA CRIMINALIDADE INFORMÁTICO – DIGITAL. 1-ª Ed. [S.L]: Rei dos Livros, 2011. ISBN 978-989-8305-18-3.

SANTOS, Cistina Máximo dos, As novas tecnologias da informação e o sigilo das telecomunicações, Lisboa, 2004, separata da Revista do Ministério Público N.º99

SANTOS, Paulo; BESSA, Ricardo; PIMENTEL, Carlos – CYBERWAR: O fenómeno, as tecnologias e os actores. Janeiro 2008. FCA - Editora de Informática Lda. ISBN: 978-972-722-597-2

SILVA, Germano Marques da, DIREITO PROCESSUAL PENAL PORTUGUÊS: Noções Gerais, sujeitos processuais e objecto, Vol.I, 7.ª ed. Isboa: Universidade Católica Editora, 2013. ISBN 978-972-54-0399-0

Teixeira, Paulo Alexandre Gonçalves - O FENÓMENO DO PHISHING: ENQUADRAMENTO JURÍDICO-PENAL, Dissertação para obtenção do grau de Mestre em Direito, especialidade em Ciências Jurídico-Criminais, orientador : Prof. Doutor Fernando Conde Monteiro. Fevereiro 2013, Lisboa, pp. 75-78. Consult. 27-08-2014 disponível em: http://repositorio.ual.pt/bitstream/11144/301/1/O%20fen%C3%B3meno%20do%20Phishing%20%E2%80%93%20Enquadramento%20Jur%C3%ADdico-Penal%20%282013-02%29.pdf

VENÂNCIO, Pedro Dias, LEI DO CIBERCRIME, ANOTADA E COMENTADA, 1.ª ed., Coimbra Editora, 2011. ISBN 978-972-32-1906-7.

VERDELHO, Pedro; BRAVO, Rogério; ROCHA, Manuel Lopes – Leis do Cibercrime, Vol. 1, pp. 27-28 Consult. 22-12-2013. Disponível na Internet: http://www.centroatl.pt/titulos/direito/imagens/excerto-ca-leisdoCibercrime1.pdf

VERDELHO, Pedro, "A Convenção sobre Cibercrime do Conselho da Europa - Repercussões na Lei Portuguesa", Direito da Sociedade da Informação, vol. VI Coimbra Editora, 2006, p. 258. ISBN 978-972-32-1411-3.

- Cibercrime, Direito da Sociedade da Informação, Vol. IV, Coimbra Editora, 2003. ISBN 972-32-1169-6.

- Phishing e outras formas de defraudação nas redes de comunicação, in Direito da Sociedade da Informação, Vol. VIII, coord. Prof. Doutor José de Oliveira Ascensão, Coimbra Editora, 2009. ISBN 978-972-32-1710-0

-Lei n.º 109/2009, de 15 de Setembro, in Comentário das leis penais extravagantes, vol. 1, [coord. de] ALBUQUERQUE, Paulo Pinto de .Lisboa: Universidade Católica Editora, 2010. ISBN 978-972-54-0282-5

-A obtenção da prova no ambiente digital, notas que serviram de suporte a uma curta intervenção no *International Seminar on Seizing Evidence in the Internet*, organizado em Lisboa, a 5 e 6 de Maio de 2004, pela Polícia Judiciária e dirigido a agentes policiais da União Europeia, documento fornecido pelo Autor em Curso de formação avançada à distância CIBERCRIME E PROVA DIGITAL, organizado pela e-UNIFOJ do centro de Estudos sociais (CES) da Universidade de Coimbra e coordenado por Pedro Verdelho, decorreu entre 06 de Outubro e 05 de Dezembro. Disponível http://opj.ces.uc.pt/e-learning/moodle/course/view.php?id=10 acedido em 10-11-2014

VERDELHO, Pedro, módulo 3, A perspetiva processual: Prova eletrónica em processo penal, p.2.documento fornecido pelo Autor em Curso de formação avançada à distância CIBERCRIME E PROVA DIGITAL, organizado pela e-UNIFOJ do centro de Estudos sociais (CES) da Universidade de Coimbra e coordenado por Pedro Verdelho, decorreu entre 06 de Outubro e 05 de Dezembro. Disponível http://opj.ces.uc.pt/e-learning/moodle/course/view.php?id=10 acedido em 10-11-2014.

http://pt.wikipedia.org/wiki/Phishing

Conselho da Europa, Minuta em português do Relatório Explicativo da Convenção sobre o Cibercrime, de 23-11-2001, disponível em http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/ETS_185_Portugese-ExpRep.pdf, acedido em 18-12-2013.

Jurisprudência consultada

Acórdão do Tribunal da Relação de Évora, de 7 de Dezembro de 2012, Processo nº 3142/09.3PBFUN-A.L1-5, com relator FILOMENA CLEMENTE LIMA disponível em http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/5d335a57cd0118f280257acd00502b7c

Acórdão do Tribunal da Relação de Lisboa, de 18 de janeiro de 2011, Processo nº 3142/09.3PBFUN-A.L1-5, com relator FILOMENA CLEMENTE LIMA disponível em http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/0e870e9e2782243380257839005785c2

Acórdão do Tribunal da Relação de Évora, de 13 de Novembro de 2012, Processo nº 315/11.2PBPTG-A.E1 disponível em http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/6f0b16b32262478f80257abc00517327

Acórdão do Tribunal da Relação de Lisboa, de 19-06-2014, Processo nº 1695/09.5PJLSB.L1-9, com relator MARGARIDA VIEIRA DE ALMEIDA, disponível em http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/eb1460fa14510bf380257d080036a9b9;

Acórdão do Tribunal da Relação de Coimbra, de 26-02-2014, Processo nº 559/12.0GBOBR-A.C1, com relator FERNANDO CHAVES, disponível em http://www.dgsi.pt/jtrc.nsf/c3fb530030ea1c61802568d9005cd5bb/0e255b331c5eaecd80257c91005ae8bf;

Acórdão do Tribunal da Relação de Guimarães, de 12-10-2009, Processo nº 1396/08.1PBGMR-A.G1, com relator TOMÉ BRANCO, disponível em http://www.dgsi.pt/jtrg.nsf/86c25a698e4e7cb7802579ec004d3832/4c03909839f95d5f8025767e004f83fe;

Acórdão do Tribunal da Relação de Guimarães, de 29-03-2011, Processo nº 735/10.0GAPTL-A.G1, com relator MARIA JOSÉ NOGUEIRA, disponível em http://www.dgsi.pt/JTRG.NSF/86c25a698e4e7cb7802579ec004d3832/6aa96edf91e899b2802578a00054631f

Acórdão do Tribunal da Relação de Lisboa, de 11-01-2011, Processo nº 5412/08.9TDLSB-A.L1-5, com relator RICARDO CARDOSO, disponível em http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/e5ed1936deb44eb180257824004ab09d

Acórdão do Tribunal da Relação do Porto, de 12-09-2012, Processo nº 787/11.5PWPRT.P1, com relator ALVES DUARTE, disponível em http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/877e0322acde18d080257a8300393cc6

Acórdão do TJUE de 8 de Abril de 2014, disponível em http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=PT&mode=req&dir=&occ=first&part=1&cid=128161 consultado em 06/10/2014

Outros documentos acedidos na internet:

Conselho da Europa, Minuta em português do Relatório Explicativo da Convenção sobre o Cibercrime, de 23-11-2001, disponível em http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/ETS_185_Portugese-ExpRep.pdf, consultado em 18-12-2013

Wikipédia, disponível em http://pt.wikipedia.org/wiki/Phishing, consultado em 01-12-2014

Lei 12.965, de 23 de abril de 2014, estabelece princípios garantias, direitos e deveres para o uso da Internet no Brasil, disponível em http://www2.camara.leg.br/legin/fed/lei/2014/lei-12965-23-abril-2014-778630-publicacaooriginal-143980-pl.html com acesso 01-12-2014

Curso de formação avançada à distância CIBERCRIME E PROVA DIGITAL, organizado pela e-UNIFOJ do centro de Estudos sociais (CES) da Universidade de Coimbra e coordenado por Pedro Verdelho, decorreu entre 06 de Outubro e 05 de Dezembro Modulo II, Cibercrime, Os crimes Informáticos ou Cibercrimes, pp.1-6, disponível em http://opj.ces.uc.pt/e-learning/moodle/course/view.php?id=10, consultado em 23/10/2014.

Acórdão [2008] EWCA Crim 2117 do *Supreme Court of Judicature (Criminal Divisio), Disponível em: http://www.bailii.org/ew/cases/EWCA/Crim/2008/2177.html*

Parecer consultivo da Procuradoria Geral da República, n.º convencional PGRP00003238, com relator Paulo Dá Mesquita, disponível em http://www.dgsi.pt/pgrp.nsf/7fc0bd52c6f5cd5a802568c0003fb410/a734913d16b0f89480257af00043b68a, consultado em 26-01-2015

VERDELHO, Pedro, A obtenção da prova no ambiente digital, notas que serviram de suporte a uma curta intervenção no *International Seminar on Seizing Evidence in the Internet*, organizado em Lisboa, a 5 e 6 de Maio de 2004, pela Polícia Judiciária e dirigido a agentes policiais da União Europeia, documento fornecido pelo Autor em Curso de formação avançada à distância CIBERCRIME E PROVA DIGITAL, organizado pela e-UNIFOJ do centro de Estudos sociais (CES) da Universidade de Coimbra e coordenado por Pedro Verdelho, decorreu entre 06 de Outubro e 05 de Dezembro, disponível em http://opj.ces.uc.pt/e-learning/moodle/course/view.php?id=10, consultado em 10-11-2014

Site oficial da Procuradoria Geral da República, pareceres VII, utilização da informática, disponível em http://www.pgr.pt/pub/Pareceres/VII/2.html, consultado em 08-10-2014

Parecer do Conselho Consultivo da PGR com o n.º P000792008, disponível em http://www.dgsi.pt/pgrp.nsf/0/b90edf9f8e8a47e480257515003eb4e8, consultado em 08-10-2014

Parecer consultivo da Procuradoria Geral da República, n.º convencional PGRP00003238, com relator Paulo Dá Mesquita, disponível em

http://www.dgsi.pt/pgrp.nsf/7fc0bd52c6f5cd5a802568c0003fb410/a734913d16b0f89480257af00043b68a, consultado em 26-01-2015

http://tek.sapo.pt/extras/site_do_dia/sera_que_e_um_num_milhao_na_internet_1428713.html acedido em 26-01-2014

PEREIRA, João Pedro, notícia publicada no jornal público em 14-01 de 2014, disponível em http://www.publico.pt/tecnologia/noticia/criador-do-servico-de-partilha-btuga-condenado-a-multas-de-12600-euros-1619654 com acesso em 05-01-2015

MARQUES, Pedro Penha Leitão da, Informática forense, recolha e preservação da prova digital, Dissertação de mestrado, sob orientação de Prof. Doutor Rui Alves Pires, maio, 2013, Universidade Católica Portuguesa, Faculdade de Engenharia, disponível em http://repositorio.ucp.pt/bitstream/10400.14/13191/1/Disserta%C3%A7%C3%A3o%20-%20Recolha%20e%20preserva%C3%A7%C3%A3o%20da%20prova%20digital.pdf com acesso 10-10-2014