UNIVERSIDADE CATÓLICA PORTUGUESA

Cibercrime

&

A problemática da prova ilicitamente obtida por particulares no processo penal português

Ana Filipa Nunes Pereira

Mestrado em Direito

Faculdade de Direito | Escola do Porto

2022

UNIVERSIDADE CATÓLICA PORTUGUESA

Cibercrime

&

A problemática da prova ilicitamente obtida por particulares no processo penal português

Ana Filipa Nunes Pereira

Orientador: Senhor Professor Doutor José Manuel Damião da Cunha

Mestrado em Direito

Faculdade de Direito | Escola do Porto

2022

Aos que já partiram.

“It doesn’t matter who you are, where you come from. The ability to triumph begins with you. Always.”

- *Oprah Winfrey*

Agradecimentos

Ao Senhor Professor Doutor José Manuel Damião da Cunha pela mentoria, apoio, dedicação, conselhos e disponibilidade.

Às Ineses. À Maria. À Natália. À Vanessa. À Carolina. Ao João. Aos amigos que levo da Faculdade por, de mão dada, terem caminhado junto a mim desde o primeiro dia.

À Faculdade de Direito da Universidade Católica do Porto por ter sido a minha casa durante seis anos e por me ter visto crescer.

À Sónia e à Sofia por me acompanharem não só neste percurso académico, como na vida.

E aos meus pais, porque o melhor fica sempre para o fim. Obrigada por serem e por estarem, mas principalmente por acreditarem em mim.

Resumo

A presente dissertação propõe uma análise aos problemas e consequências resultantes do surgimento da tecnologia e, principalmente, da internet, enquanto ferramentas impulsionadoras de uma nova realidade criminal.

Com este estudo pretende-se uma reflexão não só relativa ao surgimento de novos tipos criminais ou de novas ferramentas do crime, fruto da criminalização de condutas lesivas levadas a cabo no ciberespaço, como de problemas que se levantam a nível processual, mais concretamente, das provas ilegalmente obtidas por particulares e a sua (in)admissibilidade no processo penal português.

Palavras-chave: cibercrime; *hacker*; processo penal; prova; particulares.

Abstract

The present dissertation proposes an analysis of the problems and consequences product of the emergence of technology and, especially, the internet, as driving tools of a new criminal reality.

This study aims to reflect on the emergence not only of new crimes or criminal tools as a result of the criminalization of harmful conducts that take place in the cyberspace, but also on problems that arise at a procedural level, more specifically, the evidence that is unlawfully obtained by private individuals and its (in)admissibility in the Portuguese criminal courtrooms.

Keywords: cybercrime, hacker, criminal proceeding; evidence; private individuals.

Índice

Advertência

A tradução da bibliografia estrangeira é da nossa autoria.

Lista de Siglas e Abreviaturas

APAF - Associação Portuguesa de Árbitros de Futebol

AR - Assembleia da República

Art. - Artigo

Arts. – Artigos

Cap. - Capítulo

CIA - Central Intelligence Agency

CP - Código Penal

CPP - Código de Processo Penal

CRP - Constituição da República Portuguesa

DIAP - Departamento de Investigação e Ação Penal

DL - Decreto-Lei

EUA - Estados Unidos da América

IP - Internet Protocol

LPDP - Lei de Proteção de Dados Pessoais

MIT - Massachusetts Institute of Technology

MP – Ministério Público

NSA - National Security Agency

ONU - Organização das Nações Unidas

Pág. - Página

Págs. - Páginas

PJ - Polícia Judiciária

PR - Presidente da República

Proc. - Processo

RGICSF - Regime Geral das Instituições de Crédito e Sociedades Financeiras

Séc. - Século

Ss. - Seguintes

TC - Tribunal Constitucional

TRG - Tribunal da Relação de Guimarães

TRL - Tribunal da Relação de Lisboa

TSE - Tribunal Superior Eleitoral

UNC3T - Unidade Nacional de Combate ao Cibercrime e a Criminalidade Tecnológica

Introdução

Sendo o Direito resultado da cultura humana, uma vez tratar-se de um corpo normativo criado para apaziguar as expectativas e interesses divergentes do ser humano, o mesmo não poderá conceber-se como uma realidade estática. Muito pelo contrário. Enquanto realidade humana, esta ordem normativa varia não apenas no tempo, como no espaço, de forma a acompanhar a evolução social, resultante da ocorrência de múltiplas mudanças culturais, sociais, económicas e até políticas, de forma a garantir a sua vigência.

É, assim, papel do legislador procurar novas formas de responder a desafios ou problemas que vão surgindo, na medida em que as soluções consagradas já não se afiguram suficientes.

Ora, é inegável, nos tempos correntes, que as Novas Tecnologias da Informação e da Comunicação – e em especial a internet – vieram alterar de forma significativa não apenas o quotidiano do simples cidadão comum, como também das empresas e até do próprio Estado, que nelas confia algumas das suas principais funções, como a defesa e a segurança. Mas, se por um lado estes avanços tecnológicos trouxeram vantagens, problemas também lhes estão associados.

Desde logo, estas novas formas de comunicação proporcionaram o aparecimento de uma nova realidade criminal: o cibercrime. Realidade complexa e obscura, o cibercrime tem a si associadas não apenas questões de direito substantivo, como levanta também problemas de índole processual, problemas estes que o legislador não pôde ignorar, tendo, neste sentido, ido à procura de soluções à altura dos desafios existentes.

Mais que procurar respostas absolutas, pretende-se, com a presente exposição, abordar questões que achamos relevantes e que derivam desta nova realidade criminal. Nestes termos, optamos por organizar a presente dissertação em três capítulos: o primeiro será dedicado ao cibercrime, onde, para além de uma análise do conceito, suas características e estatísticas recentes, será feito um balanço dos esforços legislativos nacionais e internacionais para o combate do problema; o segundo capítulo terá como foco uma análise aprofundada da comunidade *hacker* e a criminalização do *hacking* como atividade, bem como o estudo do *hacktivismo* como fenómeno de insurgência política emergente nas últimas décadas; por fim, o último capítulo abordará a importância da prova no processo penal, desde o regime estabelecido no artigo 125º do CPP, ao sistema

de proibição de prova regulado pelo artigo 32º, nº 8 da CRP e artigo 126º da do CPP, terminando com uma reflexão sobre a questão das provas obtidas ilicitamente por particulares e a sua (in)admissibilidade no processo penal, fazendo ainda referência ao mediático Caso Rui Pinto.

1. A sociedade da informação e as novas formas de criminalidade

1.1. A internet como ferramenta impulsionadora de uma nova realidade criminal

Em meados do séc. XX, pleno auge da Guerra Fria, o mundo aguardava de forma expectante pelo vencedor da disputa entre dois blocos não só opostos geograficamente, mas completamente antagónicos no que toca a ideais. Do envio do primeiro homem à lua à corrida ao armamento, EUA e União Soviética disputaram uma acérrima competição a que o mundo assistiu de forma expectante, não apenas a nível económico ou político, mas também a nível tecnológico. E, numa altura em que a informação era uma das mais importantes formas de poder, acabou por nascer, pela mão dos americanos, aquilo que hoje conhecemos como a internet[1].

Em menos de um século, a vida como era conhecida mudou radicalmente. A internet e a tecnologia criaram *"*uma população mundial, [...] num cibermundo sem fronteiras espaciais, territoriais, sociais, económicas, culturais, etárias, linguísticas e raciais, surgindo a chamada *"*Sociedade de Informação[2]". Da partilha de fotos e vídeos nas redes sociais, à facilidade e comodidade das compras online às várias plataformas de *streaming* que nos permitem ter acesso a uma diversidade vasta de conteúdo, é inegável que a internet e os avanços tecnológicos a que assistimos no último século mudaram drasticamente a sociedade moderna. A proliferação da tecnologia levou, assim, a mudanças notáveis na forma como os indivíduos se relacionam não só entre si, mas com o mundo ao seu redor.[3]

Este rápido desenvolvimento da internet e inovação tecnológica, aliadas à globalização, transformaram a forma como socializamos e fazemos negócios[4]. Mais que uma forma de lazer, esta corrida ao conhecimento e informação é encarada como fundamental na sociedade atual, na medida em que a competitividade comercial assim o exige, sendo que as tecnologias de informação fazem parte integrante de um mundo cada vez mais globalizado[5]. Nos dias de hoje, com especial incidência nos países mais

[1] Kremling & Parker, 2018, pág. 31.
[2] Dias, 2012, pág. 64.
[3] Holt, Bossler & Seigfried-Spellar, 2018, pág. 17.
[4] Clough, 2010, pág. 3.
[5] Amador, 2012, pág. 1.

desenvolvidos, a internet tem um papel fulcral ao nível de todas as infraestruturas estratégicas e nevrálgicas do país, como governamentais, de segurança, económicas, de telecomunicações, educacionais, energéticas, de saúde e serviços de socorro e emergência[6].

Contudo, ainda que este desenvolvimento tecnológico tenha sido esmagadoramente positivo, uma sociedade tão dependente destas novas tecnologias é também uma sociedade mais vulnerável. Como afirma VENÂNCIO[7], se enquanto instrumento da atividade económica, cultural e social a informática começa a assumir o papel de elemento essencial de desenvolvimento, por outro, enquanto instrumento potenciador e facilitador da prática de ilícitos, a informática passou também a ser o centro de muitos receios. Na verdade, "as vantagens da internet que levaram a uma explosão de utilizadores e de volume de circulação de informação, também levaram à multiplicação de condutas lesivas e ilícitas, praticáveis e praticadas, na internet, ou por intermédio dela[8]."

Neste sentido, ainda que a Sociedade da Informação tenha nascido como um "campo à margem do Direito", o papel central que assume e a sua importância social, cultural e económica, não podiam deixar o direito alheado desta realidade[9]. Podemos afirmar que a mente humana está sempre um passo à frente do legislador e, à medida que os tempos vão mudando, também a realidade criminal se vai alterando. Assim, não só surgem novos comportamentos capazes de lesar bens jurídicos importantes – e que, por isso, devem ser criminalizados – como assistimos também ao surgimento de novos instrumentos para a prática de atos ilícitos já tipificados[10]. Se antes a prática de um crime de furto, por exemplo, requeria uma proximidade física entre criminoso e vítima, nos tempos correntes, o mesmo pode ocorrer estando estas duas pessoas separadas por centenas de quilómetros.

É neste sentido, e tendo em conta esta nova realidade, que o legislador procurou e tem procurado acompanhar a evolução social e criminalizar comportamentos que, há menos de cinquenta anos, não eram sequer hipotéticos.

---

[6] Dias, 2012, pág. 64.
[7] Venâncio, 2011, pág. 14.
[8] Dias, 2012, pág. 65.
[9] Venâncio, 2011, págs. 14 e 15.
[10] Importante é também realçar que a tecnologia e a internet servem não apenas como meio para a prática de atos criminosos, como também facilitam a comunicação e troca de informação entre agentes do crime, prática muito comum, por exemplo, nas redes de pornografia infantil.

1.2. O cibercrime

Tentar reduzir esta nova realidade criminal a um único conceito é tarefa árdua. Entre crime digital, crime informático, cibercrime e crime informático-digital, existem conceitos para todos os gostos e feitios, podendo quase afirmar-se que existem tantas definições e conceitos como tipos legais tipificados[11]. Se, por exemplo, PARKER, em 1976, se serviu do conceito de crime informático, já WALL e FURNELL, em 2001, optaram pelo termo de cibercrime[12].

Ainda que nos pareça banal a expressão a que subsumimos esta nova realidade criminal, a verdade é que esta pode, se interpretada em sentido estrito, excluir determinadas condutas que também merecem tutela penal. Por exemplo, as definições que se focam mais no computador ou na informática, como crime informático ou digital, podem não incorporar *networks*; outras, como cibercrime ou crimes virtuais, parecem focar-se de forma quase que exclusiva na internet[13].

Parece poder afirmar-se que uma das maiores dificuldades no estudo desta nova realidade é a falta de consenso quanto ao conceito para a definir. Contudo, e tendo em consideração a mais relevante legislação internacional[14], referir-nos-emos, daqui em diante, a esta realidade como cibercrime.

O conceito de cibercrime surgiu nos anos 90 do século passado e, apesar de sinónimo dos conceitos acima elencados, foi utilizado por WALL e FURNELL para se referir, em termos genéricos, à forma única como a tecnologia é usada para facilitar a prática da atividade criminal[15]. Na verdade, o cibercrime não se refere apenas a um único tipo de comportamento criminal, segundo YAR; refere-se antes a um conjunto de ofensas que partilham uma importante caraterística, nomeadamente, o facto de serem cometidas através de um computador e de tecnologia eletrónica digital[16].

[11] Clough, 2012, pág. 9.
[12] *Cit. por.* Holt, 2016, pág. 6.
[13] Clough, 2012, pág. 9.
[14] Convenção sobre o Cibercrime pelo Conselho da Europa, adotada em Budapeste em 23 de novembro de 2011.
[15] *Cit. por*. Holt, Bossler & Seigfried-Spellar, 2018, pág. 27.
[16] Guedes, Moreira & Cardoso, 2021, pág. 5.

ANTUNES e RODRIGUES[17] descrevem o cibercrime como qualquer crime que ocorre no ciberespaço[18], incluindo-se no leque dos crimes as ações praticadas com recurso à internet, onde acabam por se incluir também os crimes informáticos, ou seja, aqueles praticados contra os sistemas informáticos, os dados e as informações alojados nos sistemas de informação.

Mas, se aquando do surgimento destas novas formas de criminalidade se revelou importante a distinção entre cibercrime e crime informático, em meados da primeira década do ano dois mil, o facto de quase todos os computadores se encontrarem, de alguma forma, conectados à rede, acabou por diminuir esta necessidade de diferenciação segundo WALL[19]. Assim, estes dois termos tornaram-se quase como que sinónimos, tanto no campo científico, como nos media, no que toca a crimes relacionados com a tecnologia[20].

Mas, para além da discussão existente à volta da expressão ou definição mais adequada para definir esta nova realidade criminal, outras divergências se levantam no que toca à tipologia e classificação dos crimes[21].

Numa perspetiva internacional, o sistema de categorização que mais simpatizantes acolheu foi o de WALL. Este, tendo em conta as várias formas através das quais a tecnologia e a internet poderiam ser usadas para o cometimento de ilícitos criminais, acabou por criar um dos mais organizados e reconhecidos sistemas de categorização dos diversos tipos de cibercrime[22]. Segundo o autor, os cibercrimes poderiam organizar-se em quatro categorias distintas: *cyber-violence*, *ciber-deception*, *cyber-pornography* e *cyber-trespass*. Na categoria de *cyber-violence* incluir-se-iam os atos idóneos a provocar dor psicológica ou física nos outros e daí ligados à infração de leis relacionadas com a proteção da pessoa; *cyber-deception* referir-se-ia ao ato de roubar, onde se incluiriam, por exemplo, a violação dos direitos de propriedade intelectual; na categoria de *cyber-pornography* incluir-se-iam atos violadores de leis relativas à decência e obscenidade; e,

[17] *Cit. por.* Correia, 2021, pág. 53.
[18] O conceito de ciberespaço apareceu pela primeira vez em 1984, numa obra intitulada de "*Neuromancer*", da autoria de William Gibson, para descrever o meio eletrónico das redes de computadores onde as comunicações ocorrem em tempo real, *in* Gelbstein, 2013, pág. 118. Atualmente pode ser considerado como o espaço virtual onde os utilizadores comunicam e interagem entre si, *in* Kremling & Parker, 2018, pág. 47.
[19] *Cit. por.* Holt, Bossler & Seigfried-Spellar, 2018, pág. 27.
[20] Holt & Bossler, 2016, pág. 6.
[21] Dias, 2012, pág. 65.
[22] Holt, Bossler & Seigfried-Spellar, 2018, pág. 38.

por fim, *cyber-trespass* referir-se-ia ao ultrapassar de fronteiras por parte de alguém não autorizado, violando-se princípios de confidencialidade e integridade[23].

Por outro lado, e numa perspetiva interna, VENÂNCIO, que acaba por se socorrer do conceito de criminalidade informática, entende existirem duas categorias distintas às quais deve ser subsumida esta nova realidade criminal: os crimes em que a informática é usada como mero instrumento da prática do crime e crimes em que a informática é elemento integrador do tipo legal. Na primeira categoria incluir-se-iam os crimes em que

> *As tecnologias da informação e comunicação podem ser utilizadas enquanto instrumento (muitas vezes mais eficazes quer nos danos causados, quer no encobrimento da identidade dos seus autores) para a prática de crimes usuais da realidade corpórea e cujo tipo legal está previsto[24] sem considerar a utilização dos meios tecnológicos como um elemento integrador do crime.[25]*

Por outro lado, a segunda categoria seria dedicada aos crimes cuja função é a proteção da informática ou de "produtos informáticos", caso em que a informática integra já o tipo legal de crime – o seu objeto – e que surgem numa tentativa do Direito Penal acompanhar a evolução social tendo em conta a "crescente importância das tecnologias da informação e comunicação na organização e funcionamento das relações económicas, culturais e sociais, [merecendo, por isso] uma proteção equivalente à proteção [...] dada a bens corpóreos[26]". Mas, há que ter em conta que, neste último caso, o bem jurídico protegido não é, em exclusivo, a realidade informática[27].

Contudo, a maioria da doutrina portuguesa, entre os quais OLIVEIRA ASCENSÃO e PEDRO VERDELHO[28], acaba por apoiar o seu estudo numa categorização quadripartida, distinguindo: crimes que recorrem a meios informáticos, onde é exemplo o crime de devassa por meio de informática e burla informática[29]; crimes relativos à proteção de dados ou da propriedade, onde são exemplos os crimes tipificados na Lei nº

---

[23] Guedes, Moreira & Cardoso, 2021, pág. 54.
[24] Segundo o autor, incluir-se-ia nesta categoria, por exemplo, o crime de difamação: se é verdade que este já se encontrava previamente tipificado na legislação penal e outrora poderia ser praticado com recurso, por exemplo, a jornais ou revistas, hoje pode ser praticado através de blogues e redes sociais, como o *Instagram*, *Facebook* ou *Twitter*.
[25] Venâncio, 2011*,* pág. 18.
[26] Venâncio, 2011*,* págs. 19 e 20.
[27] Venâncio acaba por fazer referência aos crimes contra programas informáticos ou bases de dados, cuja finalidade é a proteção dos direitos de autor, enquanto "direito fundamental do criador intelectual", *in* Venâncio, 2011*,* pág. 20.
[28] Dias, 2012, pág. 67.
[29] Arts. 193º e 221º do CP, respetivamente.

67/98, de 26 de outubro[30] e Lei nº 69/98, de 28 de outubro; os crimes informáticos em sentido estrito, onde o bem ou meio informático é elemento do tipo, sendo praticados "contra ou através do computador[31]", onde se inscrevem os crimes da Lei do Cibercrime[32]; e, finalmente, os crimes relacionados com o conteúdo, onde se poderão incluir, a título exemplificativo, os crimes relacionados com os direitos de autor.

Por outro lado, esta forma de sistematização acaba também por divergir tendo em conta o sistema jurídico em estudo. Se, por exemplo, o Departamento de Justiça do EUA adota uma classificação tripartida onde divide o cibercrime entre crimes em que o computador ou rede é o alvo da atividade criminal (como o *hacking*), crimes em que o computador é utilizado meramente como meio de perpetração do crime (como o *stalking*) e crimes em que o uso do computador é aspeto incidental do cometimento do crime, mas poderá servir como meio de suporte de prova (como, por exemplo, moradas no computador de um suspeito, anteriores à prática de um crime de homicídio)[33], já a Comissão Europeia, lançando também mão de uma categorização tripartida, acaba por organizar o cibercrime nas seguintes categorias: os crimes tradicionais mas cometidos com o auxílio do computador e redes informáticas, os crimes relacionados com o conteúdo, nomeadamente a publicação de conteúdo ilícito e os crimes exclusivos das redes eletrónicas.

Em suma, independentemente da expressão utilizada ou do sistema de categorização de preferência, tem se entendido comummente que, quando nos referimos a cibercrime, acabamos por nos referir a uma realidade composta por um alargado conjunto muito heterogéneo de tipos legais de crime, onde além dos ilícitos descritos na Lei do Cibercrime se incluem também outros crimes incluídos no Código Penal, e diferentes outras fontes legais avulsas.

[30] Transposição da Diretiva nº 95/46/CE, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.
[31] Dias, 2012, pág. 65.
[32] Lei nº 109/2009, de 15 de setembro.
[33] Clough, 2010, pág. 10.

1.3. Dados estatísticos

A par do que se tem assistido na Europa e no mundo, também tem sido observado em Portugal um aumento do cibercrime[34]. Segundo o relatório elaborado pelo Gabinete de Cibercrime da Procuradoria-Geral da República[35], entre 1 de janeiro e 31 de dezembro de 2021 registaram-se um total de 1160 denúncias – mais das do dobro registadas em 2020[36] - das quais 195 originaram a abertura de inquérito e 25 foram encaminhadas para a PJ[37]. Entre estas, os crimes mais comuns foram o *phishing*, as burlas online, os ataques informáticos, *stalking* e *sextortion*, violação de direitos de autor e fraude através de utilização da plataforma *MBWAY* na realização de pagamento.

No último ano, as denúncias recebidas "aumentaram de forma exponencial, designadamente após a eclosão da pandemia resultante da COVID-19[38]" e, especialmente, nos períodos de confinamento[39].

Contudo, e apesar de a pandemia ter, indubitavelmente, contribuído para o aumento deste tipo de criminalidade, a tendência é para subir de "forma constante e consistente"[40], tendência que se vinha já a assistir desde 2016, pois, apesar de se tratar de uma atividade criminal altamente complexa, é também ela muito aliciante.

Desde logo, a inexigência de uma proximidade entre a vítima e o agente do crime que outrora não se verificava, e o caráter transfronteiriço ou extraterritorial da internet, tornam apelativo o recurso a estas novas tecnologias para a atividade criminosa. Como refere VERA MARQUES DIAS,

> *Através das redes informáticas internacionais o utilizador consegue aliar a quantidade á velocidade, pois são permitidas enormes transferências de dados e informação, por todo o globo, à velocidade de segundos. Com a ausência de*

[34] Ministério Público, 2022, pág. 3.
[35] O Gabinete Cibercrime é um gabinete de coordenação nacional, tendo sido criado em 2012, pelo Conselho Superior do Ministério Público. Apesar de não possuir atribuições funcionais de investigação criminal, passou, desde 2016, e de forma a tentar colmatar o aumento deste tipo de criminalidade, a receber denúncias (via e-mail) ligadas à atividade do mesmo, encarregando-se, depois, do processamento da informação através de um sistema de triagem, e procedendo ao envio das denúncias que reúnem os elementos e condições necessárias para a abertura de inquérito para o DIAP de Lisboa.
[36] Em 2020 foram registadas um total de 544 denúncias segundo o Gabinete Cibercrime.
[37] Falamos neste caso de denúncias que, apesar de não preencherem os critérios necessários que levam à abertura de inquérito, contêm informação relevante para eventuais investigações pendentes ou estudo de fenómenos criminosos.
[38] Ministério Público, 2022, pág. 5.
[39] Nomeadamente, entre os meses de março e maio de 2020 e em fevereiro de 2021.
[40] Ministério Público, 2022, pág. 7.

fronteiras estaduais desaparece todo o controlo feito "entre portas" e potencia[-se] a criação de um mundo sem lei[41].

Perde-se, neste sentido, a noção do tempo e do espaço: associado às novas tecnologias, a forma como é cometido o cibercrime acaba por diferir, no que toca ao modo e lugar, da restante realidade criminal[42]. O agente do crime, desde o conforto da sua casa, consegue atingir não só qualquer pessoa a qualquer altura, mas também uma grande quantidade de pessoas onde quer que estas se encontrem, o que leva não só a uma ampla janela de oportunidades para os agentes do crime e a uma maior dificuldade na investigação e consequente punição pelas entidades judiciárias[43], como também a um exponencial agravamento dos danos das condutas criminosas[44].

Por outro lado, e ao contrário de outras formas mais tradicionais no que toca à comunicação, a internet veio permitir que comuniquemos mais, de forma mais rápida, fácil e barata. O desenvolvimento tecnológico e a maior concorrência entre empresas levaram a uma redução de preços e, consequentemente, veio possibilitar que a maioria da população tenha acesso a este tipo de tecnologia e ferramentas. Aliás, tal tornou não só mais fácil a troca e o acesso à informação, como o seu armazenamento pois, uma vez desmaterializada, a mesma chega a caber num pequeno bolso[45].

No que toca aos crimes tradicionais que agora são cometidos com recurso à informática, salienta-se o fator da deslocalização. VENÂNCIO refere uma "deslocação criminosa para a internet, com uma deslocação criminosa na internet[46]". Esta valência e as ferramentas proporcionadas pelo ambiente digital, a facilidade com que se deslocaliza e "esconde" conteúdo, aliado ao caráter anónimo e à aparente impunidade, torna esta atividade apelativa para o agente do crime.

E, poderá considerar-se que este anonimato, ou o uso de uma identidade que não lhes pertence, é uma das caraterísticas mais atrativas para os agentes do cibercrime. A possibilidade de usar um IP falso, por exemplo, e a natureza moderna das redes de

[41] Dias, 2012, pág. 71.
[42] Amador, 2012, pág. 10.
[43] Falamos neste caso de crimes que podem ser cometidos por uma pessoa que se encontre no território de um Estado que poderá ser diferente do Estado em que se encontra a vítima e até do Estado onde o resultado do crime se acabará por produzir. Este leque variado de ordens jurídicas em confronto, onde vigoram regimes jurídicos distintos, origina uma grande dificuldade não só quanto à investigação, mas também quanto à punição dos agentes do crime.
[44] Dias, 2012, pág. 71.
[45] Clouch, 2010, pág. 7.
[46] Venâncio, 2011, pág. 6.

comunicação que determina que a informação passe por um vasto número de jurisdições antes mesmo de chegar ao seu destino final, faz com que seja extremamente difícil rastrear este tipo de comunicação até à fonte de origem, o que, consequentemente, diminui o risco de descoberta e punição dos agentes do crime[47].

Foi assim descoberto, pelos utilizadores, um campo fértil e vulnerável, de lucro fácil, com riscos físicos inexistentes, a baixo custo e com uma grande probabilidade de impunibilidade não só para o cometimento de novos delitos, como também para revisitar os crimes tradicionais, agora com a exponencial ajuda e cumplicidade da internet[48].

1.4. Evolução legislativa

Perante estes dados estatísticos, percebe-se a necessidade de prevenção e combate a este novo tipo de realidade criminal. Neste sentido, e desde cedo, o legislador, tanto nacional como internacional, consciente das mudanças provocadas na sociedade moderna pela tecnologia, procurou fazer um esforço de forma a conseguir prevenir e proteger a sociedade contra a criminalidade no ciberespaço, nomeadamente, através "da adoção de legislação adequada e da melhoria da cooperação internacional[49]". Tendo em consideração a extraterritorialidade como caraterística indissociável do cibercrime, a comunidade internacional sentiu a necessidade de reunir esforços e intensificar a sua cooperação no que toca ao combate mesmo[50], uma vez que as lacunas existentes e as diferentes legislações acabavam por dificultar a luta contra este tipo de criminalidade.

Neste sentido, e desde logo, destacar-se-á a Convenção do Conselho da Europa, de 23 de novembro de 2001, também conhecida como Convenção do Cibercrime, aprovada pelo Conselho da Europa em Budapeste, e que Portugal subscreveu no mesmo ano[51], como a primeira grande tentativa de prevenção e combate, a nível internacional, ao

[47] Clouch, 2010, pág. 6.
[48] Dias, 2012, pág. 65.
[49] Preâmbulo da Convenção do Conselho da Europa, de 23 de novembro de 2001.
[50] "Convictos da necessidade de prosseguir, com caráter prioritário, uma política criminal comum, com o objetivo de proteger a sociedade contra a criminalidade no ciberespaço, designadamente, através da adoção de legislação adequada e da melhoria da cooperação internacional", *in* Preâmbulo da Convenção do Conselho da Europa, de 23 de novembro de 2001.
[51] Contudo, esta apenas foi ratificada por Portugal em 2009, por Resolução da Assembleia da República nº 88/2009 e pelo Decreto do Presidente da República nº 92/2009, ambos publicados a 15 de setembro.

cibercrime. Tentou-se "proteger a sociedade contra a criminalidade no ciberespaço, designadamente, através da adoção de legislação adequada e da melhoria da cooperação internacional[52]". Desde logo, dedicou-se o Cap. I ao esclarecimento de conceitos, como sistema informático e dados informáticos, passando-se depois à criminalização de um conjunto de comportamentos[53] considerados lesivos dos bens jurídicos que se pretendiam proteger. Foram ainda pensados um conjunto de medidas reguladoras da obtenção de prova digital e mecanismos que promovessem e permitissem uma cooperação entre Estados a nível internacional.

Importante revelou-se também a Decisão-Quadro nº 2005/222/JAI[54] do Conselho, de 24 de fevereiro de 2005[55], que, acompanhando as linhas orientadoras da Convenção do Cibercrime, teve como objetivo reforçar a cooperação[56] entre autoridades judiciárias, mediante uma "aproximação das suas disposições de direito penal em matéria de ataques contra os sistemas de informação[57]", de forma a dar-se uma resposta mais eficaz a este tipo de ameaças, o que pressupõe uma abordagem global em matéria de segurança das redes e da informação; ou ainda a Diretiva nº 2006/24/CE do Parlamento e do Conselho, de 17 de julho, esta já referente à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou redes públicas de comunicações.

A verdade é que foram muitos e notáveis, ao longo dos anos, os esforços da comunidade internacional em criar um sistema mais coeso no que toca ao combate do cibercrime[58]. Mais recentemente, merece ainda destaque a Diretiva 2019/713 do Parlamento Europeu e do Conselho, de 17 de abril de 2019[59], relacionada com o combate

[52] Preâmbulo da Conselho da Europa, de 23 de novembro de 2001.
[53] Crime de acesso ilegítimo, interceção ilegítima, interferência de dados, interferência de sistemas, uso abusivo de dispositivos, falsidade informática, burla informática, infrações relacionadas com pornografia infantil e infrações relacionadas com a violação de direitos de autor e direitos conexos, respetivamente.
[54] Posteriormente substituída pela Diretiva 2013/40/UE do Parlamento Europeu e do Conselho, de 12 de agosto de 2013, relativa a ataques contra os sistemas de informação, também conhecida como Diretiva sobre o Cibercrime.
[55] Transporta para a ordem jurídica interna pela Lei nº 109/2099, de 15 de setembro.
[56] Destaca-se, neste sentido, o art. 11º da Decisão-Quadro 2005/222/JAI do Conselho, de 24 de fevereiro de 2005.
[57] Considerando 2 da Decisão-Quadro 2005/222/JAI do Conselho, de 24 de fevereiro de 2005.
[58] Entre os quais se destacam a criação da Agência Europeia para a Segurança das Redes e da Informação, pelo Regulamento (CE) nº 460/2004 do Parlamento Europeu e do Conselho, de 10 de março de 2004; a Resolução de 12 de setembro de 2013 sobre a estratégia da UE para a cibersegurança em ciberespaço aberto, seguro e protegido; e o Regulamento (UE) 2016/794 do Parlamento Europeu e do Conselho, de 11 de maio de 2016, que cria a Agência da União Europeia para a Cooperação Policial (Europol).
[59] E que veio substituir a Decisão-Quadro 2001/413/JAI do Conselho.

à fraude e à contrafação de meios de pagamento que não em numerário. Pretendeu-se fazer uma atualização e complementarização em matéria de fraude informática e sobre sanções, prevenção, assistência às vítimas e cooperação internacional uma vez que, com o aumento exponencial da economia digital, surgiram novas tecnologias de pagamento, e, consequentemente, um aumento das oportunidades de fraude.

No que toca ao direito interno, o corpo legislativo português "vai-se desenvolvendo [...], em parte por evolução autónoma; mas, e sobretudo, introduzido por desenvolvimentos externos, particularmente os resultantes de diretrizes da Comunidade Europeia[60]". Há que destacar, contudo, que desde cedo se previa na nossa ordem jurídica a possibilidade de crimes especificamente praticados por meios informáticos[61]; contudo, apenas com a Lei nº 109/91, de 17 de agosto, se veio "completar de modo abrangente o leque de crimes informáticos em sentido estrito[62]". Conhecida como a Lei da Criminalidade Informática, nesta foram tipificadas algumas condutas e previstas penas acessórias; contudo, a mesma não possuía um regime jurídico próprio para a recolha de prova em ambiente digital, o que veio a ser objeto de preocupação a nível internacional, nomeadamente, com a Convenção do Cibercrime, onde foram previstos um conjunto de mecanismos processuais especificamente destinados a garantir e regular o modo de obtenção da chamada "prova digital"[63]. Assim, até 2009, aquando da revogação da Lei nº 109/91, de 17 de agosto pela Lei nº 109/2009, de 15 de setembro[64], a mesma era recolhida nos termos "definidos pelos artigos 187º[65] e seguintes do Código de Processo Penal, por força da remissão legal comtemplada no artigo 189º, número 1[66]".

Mais tarde, através da Resolução da AR nº 88/2009 e do Decreto do PR nº 92/2009, ambos publicados a 15 de setembro, e em consequência da transposição da Decisão-Quadro nº 2005/222/JAI, do Conselho, de 24 de fevereiro, surge a Lei 109/2009, de 15

[60] Ascenção, 2001, pág. 9.
[61] Nomeadamente os crimes de devassa por meios informáticos (art. 193º), violação de correspondência ou de telecomunicações (art. 194º) e burla informática e nas telecomunicações (art. 221º), todos eles previstos no CP de 1982.
[62] Venâncio, 2011*,* pág. 21.
[63] Marques, 2014, pág. 3.
[64] E apesar de estes mecanismos processuais acabarem por ser estabelecidos na Convenção do Cibercrime (2001).
[65] A recolha de prova digital encontrava-se sujeita ao regime das escutas telefónicas, regime este de aplicação bastante restrita, o que, por vezes, acabava por dificultar o curso das investigações e até, em alguns casos, pôr em causa a subsistência das próprias; por outro lado, nos casos em que o crime a investigar não fosse subsumível ao elenco de crimes previstos no art. 187º CPP, a recolha de prova digital seria considerada inadmissível, *in* Marques, 2014*,* págs. 3 e 4.
[66] Marques, 2014*,* pág. 3.

de setembro, conhecida como a Lei do Cibercrime. A Lei do Cibercrime não foi propriamente uma novidade no ordenamento jurídico português pois, apesar de revogadora da Lei da Criminalidade Informática, que já se revelava, na altura, insuficiente e desadequada face ao aparecimento de novas formas de atuação criminosa no ciberespaço[67], a Lei do Cibercrime herdou parte relevante do que aquela já estabelecia, embora adaptando-se à regulamentação internacional[68].

Contudo, se poucas foram as alterações quanto às condutas criminalizadas, o mesmo não sucedeu em relação aos já mencionados mecanismos de obtenção de prova digital. Passou assim no Cap. III a prever-se um conjunto de mecanismos processuais, que não se aplicariam apenas aos tipos legais previstos naquela lei, como também aos cometidos por meio de um sistema informático e em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico[69].

Por outro lado, no âmbito da cooperação internacional, e na linha da Decisão-Quadro nº 2005/222/JAI, esta lei trouxe-nos também novidades: regulou-se um conjunto de medidas cujo objetivo era a cooperação entre Estados e a prestação de assistência no âmbito de investigações e procedimentos, assim como na recolha de prova[70], e que se revelavam essenciais visto que, tratando-se de um tipo de criminalidade complexa, os procedimentos tradicionais tendem a fracassar[71].

Recentemente, de forma a dar cumprimento à Diretiva 2018/713 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, a Lei do Cibercrime foi alterada pela Lei 79/2021, de 14 de novembro, tendo sido aditados sete novos artigos que passam a tipificar condutas relacionadas com a contrafação de cartões e uso de outros dispositivos de pagamento[72], assim como a sua aquisição ou outras condutas relacionadas com a transmissão ou disponibilização[73], prevendo-se mesmo a punição de atos preparatórios e possível agravação[74].

---

[67] Marques, 2014, pág. 8.
[68] Carvalho, García & Feijoo, 2018, pág. 53.
[69] Regulou-se, entre outros, a pesquisa de dados informáticos (art. 15º), a sua apreensão (art. 16º) e preservação (art. 12º).
[70] Nomeadamente pontos de contacto permanente (art. 21º), preservação e revelação expedita de dados informáticos (art. 22º), acesso a dados informáticos (arts. 24º e 25º) e interceção de comunicações (art. 26º).
[71] Dias, 2012, pág. 84.
[72] Nomeadamente, os arts. 3º A e 3º B.
[73] Nomeadamente, o art. 3º C.
[74] Para os casos em que tais atos sejam praticados por funcionário – art. 3º F.

Contudo, e como já realçamos, não só da Lei do Cibercrime se constitui o corpo de normas nacionais destinadas ao seu combate. Não existe uma "agregação total numa lei específica[75]", mas sim uma dispersão por vários diplomas. Para além dos crimes que se encontram previstos na Lei do Cibercrime e no CP – violação de correspondência e telecomunicações, devassa por meio de informática, burla informática e nas comunicações e pornografia infantil – outros diplomas merecem referência: a Lei nº 67/98, de 26 de outubro, mais conhecida como a Lei de Proteção de Dados; o DL nº 252/94, de 20 de outubro ou Lei da Proteção Jurídica de Programas de Computador; o DL nº 63/85, de 14 de março, vulgarmente conhecido como Código dos Direitos de Autor e Direitos Conexos; e a Lei 15/2001, de 5 de junho ou Regime Geral das Infrações Tributárias.

Conclui-se que, independentemente da discussão que se assiste na doutrina sobre o enquadramento jurídico do cibercrime na sociedade do risco[76], a verdade é que inegáveis têm sido os esforços por parte do legislador e da comunidade internacional em criar um sistema de combate ao cibercrime mais eficiente e coerente, de forma a melhor proteger esta sociedade que fez da tecnologia um elemento essencial de sobrevivência.

[75] Carvalho, García & Feijoo, 2018, pág. 54.
[76] Neste sentido, Dias, 2012, págs. 79 e ss.

2. *Hackers* – análise de uma comunidade anónima

2.1. Surgimento e evolução do conceito

Concebido como um mágico da tecnologia capaz de aceder aos sistemas mais bem protegidos pelo público em geral, o *hacker* é a figura que mais destaque merece quando nos referimos aos agentes do cibercrime.

O termo *hacker* e aquilo que mais tarde veio a constituir a "*hacker culture*" emergiu da atividade desenvolvida pelos estudantes de engenharia do MIT, em 1950[77]. O termo era usado pelos estudantes para se referirem à atividade lúdica por eles levada a cabo com recurso à tecnologia, atividade esta encarada pelos estudantes como "*goofing off*" e "*fooling around*". O *hacking* era por eles considerado um meio de resolver problemas de forma não convencional tendo em conta as técnicas de engenharia e computação à data conhecidas. Estas soluções, elegantes e inovadoras para os problemas em causa, eram denominadas de "*hacks*", e os seus autores, consequentemente, como "*hackers*"[78], tendo, por isso, "as primeiras gerações deste grupo [acabado por participar] no desenvolvimento dos computadores[79]".

Esta perceção do *hacker* como um programador habilidoso continuou a expandir-se na década de 60, onde se observou uma expansão do número de pessoas a ser referenciadas pelo termo[80]. Com a expansão da tecnologia a outros campos para além do meio universitário, surgiu a cultura da programação que se guiava por uma série de ideias que ficaram conhecidas por "*Hacker Ethic*"[81].

A noção de *hacking* foi assim evoluindo ao longo dos anos, especialmente quando os computadores pessoais começaram a surgir nos finais do século, e "subsequentemente, o interesse neles do público, em geral, e dos media[82]", onde rapidamente foram difundidas histórias sobre grupos de *hackers* maliciosos de forma a captar o interesse do público. Foi

[77] Brenner, 2012, pág. 16.
[78] Holt, Bossler & Seigfried-Spellar, 2018, pág. 94.
[79] Dias, 2012, págs. 67 e 68.
[80] Ferreira & Guedes, 2021, pág. 183.
[81] Falamos de uma cultura que defendia que a informação deveria ser livre e estar ao acesso de todos, de que os *hackers* deveriam ser julgados pelas suas competências e que o processo de aprendizagem subjacente à atividade deveria ser ilimitado, dado que o computador era visto como instrumento capaz de melhorar consideravelmente a vida das pessoas, *in* Ferreira & Guedes, 2021, pág. 183 e Steinmetz, 2016, págs. 25 e ss.
[82] Ferreira & Guedes, 2021, pág. 183.

nesta altura que o *hacking* passou, pela primeira vez, a ser conotado com a prática de crimes, conotação esta posteriormente exacerbada com o *The Hackers Manifesto*[83], publicado em 1986, na revista *Phrac*k[84].

A partir dos anos 90[85], esta tendência manteve-se. A par da redução dos preços da tecnologia, assistiu-se ao crescimento contínuo da comunidade *hacker* e desenvolvimento do *hacking* enquanto atividade. A possibilidade de intrusão e controlo não autorizado de dispositivos aumentou, observando-se, ao mesmo tempo "um crescimento da complexidade das ferramentas a serem utilizadas no *hacking* e uma alteração das suas funcionalidades, que passaram a estar focadas no ataque e apropriação de informação[86], o que contribuiu para o processo de criminalização do *hacking* enquanto atividade. Longe estavam os dias em que a maioria da comunidade pugnava pela transparência e liberdade de informação e melhoramento das habilidades informáticas; a motivação por detrás da atividade passara agora a estar ligada à sede de enriquecimento que era conseguido, frequentemente, através da intrusão e apropriação de informação em sistemas em relação aos quais não tinham acesso, forçando os Estados, consequentemente, a procurar a criminalização deste tipo de condutas.

Assim, se aquando do surgimento do termo o mesmo era encarado como uma forma inovadora para problemas por solucionar, o *hacking* possui hoje uma conotação predominantemente negativa, sendo o termo utilizado para se referir a um conjunto de atividades ilícitas levadas a cabo na tentativa ou no ganho de acesso não autorizado a sistemas de tecnologias de informação[87]. Aliás, as principais caraterísticas do *hacking* é a atividade ser simples, magistral e ilícita[88].

Ainda assim, o *The Jargon File*[89] acaba por fornecer oito definições onde, apesar desta onda crescente de conotação negativa ao termo, sete são positivas. Por exemplo, a primeira define o *hacker* como "uma pessoa que disfruta da exploração de detalhes da

[83] Considerado o pilar da cultura *hacker*, e em oposição ao *Hacker Ethic* e ao conceito de *hacking* dos anos 60, o *The Hacker Manifesto*, da autoria daquele que era intitulado *The Mentor*, apelava a um conjunto de condutas criminais do *hacker* o que acabou por criar uma divisão na comunidade e uma mudança definitiva da perceção dos atos exploratórios e maliciosos, *in* Ferreira & Guedes, 2021, pág. 183.
[84] Holt, Bossler & Seigfried-Spellar, 2018, pág. 103.
[85] Altura em que, como vimos no capítulo anterior, começaram a surgir, por parte dos Estados, as primeiras tentativas de combate a este tipo de criminalidade.
[86] Ferreira & Guedes, 2021, págs. 183 e 184.
[87] Ferreira & Guedes, 2021, pág. 181.
[88] Jordan, 2004, pág. 7.
[89] Glossário Informático, atualmente publicado sob o nome *Hacker´s Dictionary*.

programação de sistemas e como aumentar as suas capacidades, opondo-se à restante maioria dos usuários, que preferem apenas aprender o mínimo necessário[90]"; já a última descreve o *hacker* como um "intrometido com intenções maliciosas que tenta descobrir informações confidenciais bisbilhotando[91]". Tal permite-nos, de certa forma, perceber a dicotomia existente entre a perceção do público em geral e das legislações relativamente aos *hackers* e ao *hacking* e a perceção que estes têm de si e dos atos por eles praticados.

2.2. O crime de acesso ilegítimo como emblema do *hacking*

Vimos que o *hacking* passou de um comportamento lúdico a ato criminoso, foi meio de guerra cultural, sendo, na atualidade, um fenómeno multifacetado, moralmente ambíguo e legalmente complexo[92].

Segundo YAR, quando um *hacker* ganha acesso a um sistema e tem propósitos maliciosos, existem seis atividades que frequentemente acontecem: o furto de recursos computacionais, de propriedade ou de informação confidencial, a sabotagem, alteração ou destruição do sistema, a desfiguração de sites, *denial of service attacks* e a distribuição de software malicioso[93]. E, todos estes comportamentos podem, na opinião de JOÃO MACEDO, ser subsumidos a três grandes categorias: a manipulação, a espionagem e a sabotagem[94].

Falamos de atos altamente intrusivos e violadores de direitos constitucionalmente protegidos[95]; logo, compreende-se a necessidade de atuação do direito penal, enquanto direito de *ultima ratio*, de se chegar à frente e criminalizar este tipo de comportamentos, criminalização esta que, no nosso ordenamento jurídico, como vimos, não se encontra condensada num único diploma legal.

Enquanto emblema do *hacking*, merece especial destaque o crime de acesso ilegítimo. Previsto e punido no art. 6º da Lei do Cibercrime, o crime de acesso ilegítimo

[90] Anonymous, 2000.
[91] Anonymous, 2000.
[92] Ferreira & Guedes, 2021, pág. 186.
[93] *Cit. por* Ferreira & Guedes, 2021, pág. 185.
[94] Militão, 2012, pág. 258.
[95] Como, por exemplo, os sistemas informáticos ou domicílio informático, ou ainda bens jurídicos dos utilizadores, entre os quais se destacam o direito à palavra, à imagem e à reserva da intimidade e vida privada.

abrange, segundo VENÂNCIO, as infrações relativas às ameaças à segurança (confidencialidade, integridade e disponibilidade) e confiança nos sistemas informáticos[96].

Nos termos do nº 1, será punido quem, sem permissão legal ou sem autorização do proprietário, titular do direito do sistema ou parte dele, de qualquer modo aceder a um sistema informático, prevendo-se uma pena de prisão até 1 ano ou de multa até 120 dias. Falamos de um crime em que alguém consegue "penetrar [...] num sistema informático ou uma rede informática [...] sem que o respetivo titular o tenha autorizado ou para além do consentimento expresso produzido pelo titular do sistema ou rede informáticos"[97], um crime onde, em primeira linha, o bem jurídico protegido é a segurança dos sistemas informáticos, a proteção do designado domicílio informático, algo que, quando violado, é quase que semelhante à introdução em casa alheia[98].

BENJAMIM SILVA RODRIGUES descreve o crime de acesso ilegítimo como o crime necessário para cobrir o "*hacking informático*". A criminalização da conduta descrita pelo legislador, tratou-se, no geral, numa tentativa de tutelar a "integridade do sistema informático lesado", a partir de uma ideia nova de "inviolabilidade do domicílio informático" – "a construção deste tipo legal de crime assenta na noção de ilegitimidade consubstanciada na falta de autorização para aceder a um sistema ou rede informáticos ou intercetar comunicações que se processam numa rede ou sistema informático"[99]. Tem-se sustentado que o mesmo tutela indiretamente outros valores, por impedir que o agente fique em circunstância de lesar outros bens jurídicos, tratando-se, nessa medida, de um crime de perigo.

Este sistema informático é assim considerado um lugar onde se encontram alojados dados de alguém; aliás, a tendência é para considerar que a relação entre os dados informáticos e o sistema informático é a mesma da relação entre o domicílio físico e a pessoa em si. Contudo, existem autores que discordam desta associação, entendendo não dever reduzir-se os atos tipificados no crime de acesso ilegítimo como incidindo num "domicílio informático"[100] e que o bem jurídico que se pretende proteger é, apenas, o sistema informático enquanto património do lesado e não a informação a que se possa ter

[96] Venâncio, 2011*,* pág. 59.
[97] Dias, 2016, pág. 58.
[98] Ac. do TRC, de 15 de outubro de 2008, proc. nº 368/07.8TAFIG.C1, disponível em www.dgsi.pt
[99] Rodrigues, 2009, pág. 159.
[100] Ver mais *in* Dias, 2016*,* págs. 59 e ss.

acesso através da prática do crime. Contudo, parece-nos não ser esta a posição da doutrina e jurisprudência maioritária[101].

Por outro lado, no nº 2 do mesmo artigo, punem-se os agentes que, acedendo ao sistema, acabem por ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas, um conjunto executável de instruções, um código ou outros dados informáticos destinados a produzir ações não autorizadas descritas no nº 1. Neste caso, e ao contrário do nº 1, o crime apenas se consumará com a efetiva prática do mesmo, não sendo punível a simples tentativa, nos termos do nº 6. E, assim como nas situações do nº 4, o procedimento criminal dispensa a necessidade de queixa-crime pelo lesado.

Resta-nos realçar o facto de se prever a agravação do tipo legal em dois casos distintos: a primeira relacionada com o meio pelo qual foi praticado o crime (nº 3); o segundo relacionado com os benefícios retirados da prática do crime pelo autor do mesmo (nº 4).

2.3. O perfil do *hacker*: caraterísticas, motivações e figuras afins

Quando pensamos na figura por detrás do cibercrime, uma realidade criminal complexa e onde identidade dos seus agentes é maioritariamente anónima, tendemos a criar uma imagem visual de "um génio na área da informática, perito em computadores e programação, homem, estudante com um Q.I. acima da média, introvertido, associal e que age pelo desafio da superação da máquina[102]". Mas será esta imagem correspondente à realidade?

Estudos recentes[103] demonstram que a comunidade *hacker* – ainda que a grande maioria aja sob o anonimato e seja relutante em dar entrevistas ou participar em estudos – é, efetivamente, composta maioritariamente por indivíduos do sexo masculino e com idade inferior a 30 anos, com empregos bem remunerados, maioritariamente na área da

[101] Veja-se, neste sentido, o Ac. TRL de 7 de março de 2018, proc. nº 5481/11.4TDLSB.L1-3 e o Ac. do TRG de 12 de abril de 2021, proc. nº 19719.8GCBRG.G1, ambos disponíveis em www.dgsi.pt
[102] Dias, 2012, págs. 68.
[103] Bachmann, 2010.

segurança. Aliás, dados do *The 2021 Hacker Report*[104] indicam que 82% da comunidade se considera um "*part-time hacker*".

Num outro estudo conduzido por STEINMETZ em 2012, os indivíduos que compunham o universo estatístico identificaram-se, maioritariamente, como membros de classe média, ainda na faculdade ou com algum tipo de educação superior[105]; ainda assim, as suas habilidades informáticas eram, usualmente, resultado de uma conjugação de formação e conhecimento adquiridos de forma autónoma[106]. Dado interessante é o facto de a maioria ter tido contacto com um computador, pela primeira vez, ainda na primeira década de vida, e a sua primeira experiência ligada ao *hacking* ainda antes de atingirem a maioridade.

Por outro lado, o mesmo estudo acaba por desconstruir a ideia do *hacker* como um ser solitário e com capacidades de socialização pouco desenvolvidas. Pelo contrário, seis dos indivíduos entrevistados eram casados e dois deles divorciados, sendo que quatro deles tinham filhos[107].

Relativamente às motivações subjacentes à atividade, o *The 2021 Hacker Report* indica como a maior motivação subjacente ao *hacking* a intenção de aprender (85%), seguindo-se o enriquecimento (76%), o entretenimento (65%), a pretensão de avançar na carreira (62%) e, por fim, a intenção de proteger e defender (47%). Estes fatores, mais do que nos permitirem conhecer melhor a atividade em si, permitem-nos distinguir e categorizar diferentes tipos de *hackers*, sendo que a maioria da literatura científica acaba por aderir a uma classificação tripartida: *black hats*, *white hats* e *gray hats*.

Na categoria dos *black hats*, também conhecidos como os "*bad guys*" ou "*crakers*[108]", incluem-se os hackers movidos por intenções maliciosas, sendo estes, consequentemente, aqueles que mais atenção recebem por parte dos media. Falamos de criminosos no sentido literal do termo, que procedem, entre outras, à interceção de comunicações online, ao acesso e recolha de dados e informações em relação aos quais não possuem consentimento para aceder e à criação e implantação de *malware* em

[104] Hackerone Team, 2021.
[105] Steinmetz, 2016, pág. 42.
[106] Holt, Bossler & Seigfried-Spellar, 2018, pág. 91.
[107] Steinmetz, 2016, pág. 43.
[108] O termo "*cracker*" emergiu na cultura *hacker* para reconhecer e separar *hackers* com intenções maliciosas daqueles que atuavam de acordo com o *The Hacker Ethic*, *in* Holt, Bossler, & Seigfried-Spellar, 2018, pág. 91.

computadores alheios com o objetivo de obterem vantagens ilegítimas ou de danificar sistemas informáticos[109]. Distinguem-se dos restantes por adotarem condutas não éticas – e ilícitas, movidos por interesses egoístas e pessoais – atos estes que podem ser considerados quase como que vandalismo informático.

Merece destaque, neste caso, o grupo *CyberTeam*, liderado por "Zambrius"[110] e composto por jovens adolescentes que se assumem como "*black hats*" e parecem operar simultaneamente em Portugal e no Brasil, e que assumem uma postura "rebelde e provocadora"[111], tendo confessado a autoria dos ataques informáticos contra o TSE do Brasil em 2020[112].

No polo oposto temos os *white hats* ou "*ethical hackers*". Referimo-nos neste caso a indivíduos que usam as suas habilidades informáticas na procura de vulnerabilidades em programas de software e no fornecimento de programas informáticos que protejam os sistemas de serem invadidos de forma maliciosa. A maioria dos *hackers* incluídos nesta categoria é geralmente contratada por empresas para testarem os seus sistemas de segurança e ajudarem a melhorar as suas medidas de prevenção[113]. Há, contudo, que realçar que estes *hackers*, "mesmo não tendo objetivos maliciosos, podem ou não estar autorizados a aceder ao sistema informático, sendo que, ao não estarem, poderão praticar um crime à luz do art. 6º da Lei do Cibercrime[114]".

Na última categoria encontram-se os *grays hats*, situando-se estes, como o próprio nome sugere, na zona cinzenta entre os *white* e *black hats*. Considerados como oportunistas por MOORE, falamos de *hackers* que se inserem numa categoria híbrida e cujo "modus operandi não se limita a aceder ao sistema informático para notificar o dono das suas vulnerabilidades. Adicionalmente, o *hacker* propõe um valor pecuniário para corrigir o problema que encontrou[115]".

[109] Ferreira & Guedes, 2021, pág. 189.
[110] Conhecido por "Zambrius", o jovem *hacker* português natural da Ericeira, foi condenado em 2022 a 6 anos de prisão por ter cometido 28 crimes de acesso ilegítimo agravado, desvio de dados e dano informático, estando entre as entidades ofendidas a APAF, a operadora de telecomunicações MEO, a Universidade Nova e o portal MyBenfica. Ver mais *in* Franco, 2022.
[111] Arruda, 2021.
[112] Lusa, 2020.
[113] Kremling & Parker, 2018*,* pág. 196.
[114] Ferreira & Guedes, 2021, pág. 189.
[115] Ferreira & Guedes, 2021, págs. 189 e 190.

2.4. Hacktivismo

Da Primavera Árabe à suposta influência de eleições por meio de ataques informáticos, podemos facilmente perceber que o ciberespaço é, ao mesmo tempo, uma ferramenta de comunicação, mas também em si um espaço onde a política é criada, exercida e desafiada[116].

Resultante da combinação das palavras *hack* e ativismo, o *hacktivismo* é um fenómeno emergente de ação popular e orientado para a promoção de ideais políticos através da utilização das capacidades informáticas dos seus membros[117]. Ao contrário dos *hackers* – tendo eles a intenção de repararem um sistema ou de o danificar – os *hacktivistas* "são *hackers* com o propósito de espalhar uma mensagem política[118]". Segundo ADERSON, o fenómeno do *hacktivismo* relaciona-se com o apoio de causas anarquistas, ativistas e movimentos de protesto e onde a prática dos crimes informáticos é politicamente motivada pela defesa de causas em que acreditam[119].

Fenómeno relativamente recente e associado ao cibercrime, os ataques efetuados por estes visam sobretudo sistemas governamentais ou de grandes empresas privadas, impossibilitando o acesso aos mesmos por períodos de tempo indeterminado, costumando, também, substituir as páginas web de origem por mensagens que consideram ideológicas[120]. Falamos num *modus operandi* que se traduz na capacidade de romper e manipular as infraestruturas de tecnologias de informação digital e de comunicações, sistemas computacionais e processadores protegidos[121]. Neste sentido, e porque o *hacktivismo* usa técnicas oriundas da comunidade *hacker*, é difícil identificar ao certo onde é que o *hacking* acaba e o *hacktivismo* começa[122].

Sob o lema "nós não perdoamos, nós não esquecemos, esperem-nos", o grupo *Anonymous*, pioneiro deste tipo de atividade, é descrito por COLEMAN como sendo constituído por "muitas faces". Como o próprio nome indica, o grupo baseia-se na ideia do anonimato e no desaparecimento do individuo em função do coletivo. Apesar de ter

[116] Owen, 2021, pág. 64.
[117] Amador, 2012, pág. 57.
[118] Ferreira & Guedes, 2021, pág. 190.
[119] Domingues, 2015, pág. 40.
[120] Amador, 2012, pág. 57.
[121] Santos, 2015, pág. 87.
[122] Jordan & Taylor, 2004, pág. 2.

começado de forma caótica e controversa[123], nascendo primitivamente para o "*lulz*"[124], nos últimos anos o grupo contribuiu para a publicitação de uma série de causas, desde a exposição da prática de crimes de violação[125] até à "Operação Avenge Assange"[126], em finais de 2010, o que acaba por demonstrar que não existe, por detrás da sua atividade, "uma filosofia consistente ou uma agenda política[127]". Falamos de um grupo que recruta e coordena as suas atuações em fóruns online, e cujos métodos, ainda que movidos por nobres intenções[128], são "às vezes subversivos, muitas vezes rancorosos, geralmente imprevisíveis e frequentemente desdenhosos da etiqueta ou da lei"[129].

Por outro lado, ainda que os *hacktivistas* usualmente não beneficiem de amplo suporte político, os mesmos conseguem reunir um poder significativo. Como explica SORELL, o conhecimento avançado da tecnologia dá aos *hacktivistas* a capacidade de atacar infraestruturas, roubar segredos comerciais e expor informação governamental altamente classificada[130].

Desde logo, haverá que destacar-se o emblemático caso "*NSA Files*", protagonizado por Edward Snowden. Enquanto ex-trabalhador da CIA e NSA, Snowden, através do acesso que lhe foi conferido por um colega de trabalho[131], fez chegar ao conhecimento do público, em 2013, informação altamente privilegiada[132] que demonstrava a constante vigilância, por estas entidades, de comunicações e tráfego de dados entre cidadãos comuns. Através da informação por ele fornecida ao *The Guardian* e *The National Post*, o mundo ficou a conhecer a existência de programas de vigilância secretos, incluindo a interceção de dados telefónicos e eletrónicos, tanto americanos como europeus[133].

Ainda assim, a opinião do público em relação à "denúncia" levada a cabo por Snowden é bastante heterogénea: enquanto uns louvam a investigação e divulgação por

[123] Com ataques à Igreja da Cientologia, em 2008. Ver mais *in* Coleman, 2014, págs. 5 e ss.
[124] Gozo.
[125] Referimo-nos ao contributo do grupo para a resolução de um caso de violação que aconteceu em Steubenille, EUA, através da divulgação de fotografias e tweets incriminadores dos jovens que cometeram o crime, *in* Freeman, 2021, pág. 67.
[126] Falamos de uma operação que consistiu em ataques informáticos dirigidos às páginas web de instituições financeiras que haviam recusado a realização de donativos para a *Wikileaks*, entre as quais se destacam a PayPal e a MasterCard, i*n* Coleman*,* 2014*,* pág. 3.
[127] Coleman*,* 2014*,* pág. 3.
[128] Guiam-se, segundo os mesmos, por um conjunto de princípios fundamentais, entre os quais se destaca o bem-estar e a consciência coletiva, *in* Arruda*,* 2021.
[129] Coleman*,* 2014*,* pág. 7.
[130] Sorrel, 2015, pág. 392.
[131] Brenton, 2015.
[132] Corroborada por cerca de 1,7 milões de documentos, *in* Freeman, 2021, pág. 55.
[133] Norris, 2013, pág. 697.

ele levada a cabo de documentos confidenciais que suportam a prática destas atividades ilegais, por eles sendo apelidado de "*hacktivista*" ou "*whistleblower*", outros consideram a mesma como uma traição ao país. Aliás, o mesmo chegou a ser acusado, pelos EUA, de espionagem, roubo e conversão de propriedade do governo, de acordo com o *Espionage Act*, e, consequentemente, não lhe foi atribuído o estatuto de "*whistleblower*", o que levou a que pedisse asilo político à Rússia, onde reside atualmente[134].

Aliás, existem já plataformas direcionadas para a divulgação deste tipo de informação. É o que sucede, por exemplo, na plataforma *WikiLeaks*, uma organização transnacional que, através da sua plataforma online, publica e divulga informação vazada[135] – e secreta – informação esta não apenas inspirada em documentos confidenciais, mas também, geralmente, acompanhada dos mesmos e referentes a Estados ou empresas privadas com destaque no respetivo setor. Ainda que o nascimento da organização seja normalmente atribuído a Julian Assange, a *WikiLeaks*, guiada pelas ideias do *Hacker Ethic*, é produto de décadas de colaboração entre pessoas dedicadas à aplicação das suas capacidades informáticas a causas políticas[136].

Mas há que ter em conta que nem toda a informação é vazada por "*insiders*" ou "*whistleblowers*", sendo muita dela obtida por pessoas não relacionadas com o assunto em questão, e fornecida, posteriormente, à plataforma para que possa ser divulgada[137]. Aliás, foram já várias as vezes em que essas mesmas informações foram fornecidas pelo grupo *Anonymous* à plataforma.

JOSÉ PEDRO ARRUDA, no âmbito do estudo do tema, acaba por apontar a existência de grupos e páginas portuguesas no Facebook orientados para o *hacktivismo*, indicando como as que reúnem mais seguidores a *#Anonymous Legion Portugal*, a *#Anonymous Portugal*, a *#CyberTeam* e a *#Tugaleaks*[138], sendo que a maioria acaba por partilhar conteúdos comuns. Contudo, explica que a informação publicada não se trata verdadeiramente de "*leaks*", uma vez que não são reveladas informações nem documentos secretos; em vez disso, difundem-se notícias habitualmente de cariz polémico ou revelador de más práticas institucionais, que foram já publicados noutros

[134] Brenton, 2015, pág. 4.
[135] Também conhecidos por "*leaks*".
[136] Ludlow, 2010.
[137] Tenhamos por exemplo os e-mails da uma empresa de inteligência secreta americana, a Stratfor, que foram divulgados pela *WikiLeaks*, informação esta que não proveio de trabalhadores, mas da atividade levada a cabo pela *Anonymous*, *in* Brenton, 2015.
[138] Arruda, 2021.

órgãos, sendo apenas acrescentados pequenos textos introdutórios que visam "predispor o leitor a assumir uma posição"[139]. Os alvos de eleição destas páginas são, segundo o mesmo, instituições de poder nacionais, sobretudo partidos políticos com representação parlamentar, tribunais, forças de segurança e organismos do Estado e repartições públicas.

Numa entrevista, ROGÉRIO BRAVO, Inspetor-Chefe da UNC3T da PJ, questionado sobre o conceito de *hacktivismo*, entende que o mesmo não faz sentido. Como era de esperar, afirma que para a justiça, o *hacktivista* não existe, ponderando tratar-se de "uma categoria que podemos [ter] em termos de conceito, mas depois o crime que cometem pode ser de acesso ilegítimo, ou sabotagem, ou acesso ilícito a informação, por aí fora". Segundo o mesmo, "ou há autorização ou não há autorização. Se não há autorização, é crime", acabando mesmo por desvalorizar a prévia categorização que fizemos (*black hats, white hats...*), entendendo que a mesma, adotada da literatura anglo-saxónica, acaba por criar apenas "desinformação, sobretudo para os mais jovens, que podem assim acabar por envolver-se em atividades criminosas"[140].

Ora, esta mesma linha de orientação de que todos os acessos sem consentimento são crime à luz da lei esteve na origem da "Operação C4R3T05"[141] onde a PJ, em estreita ligação com o Gabinete do Cibercrime, operação esta que teve como finalidade o combate à criminalidade informática e tecnológica, "designadamente à atividade ilícita conhecida como "*hacktivismo*", efetuou 7 detenções no dia 26 de fevereiro de 2015. Em causa, estava a prática de crimes de sabotagem informática, dano informático, acesso ilegítimo e indevido, todos eles praticados contra diversos sistemas informáticos do Estado Português e empresas relevantes do setor privado[142]. ROGÉRIO BRAVO, a propósito da mesma, acaba por comentar não ter visto "consciência política nenhuma" pelos arguidos.

Pois a verdade é que, ainda que a motivação por detrás do *hacktivismo* possa ser uma causa que mereça destaque, a prática de crimes em defesa da mesma não justifica o fim. Num país e num mundo onde a internet assume um papel central, ataques informáticos de tamanha proporção podem pôr em risco a segurança e levar a consequências nefastas. Basta pensarmos, por exemplo, no facto de a internet ser a base

[139] Arruda, 2021.
[140] Arruda, 2021.
[141] Operação CARETOS.
[142] Ver mais *in* Polícia Judiciária, 2015.

de comunicação de muitas instituições de elevado prestígio, como as Forças Armadas, Serviços de Informações e o Governo[143].

[143] Domingues, 2015, pág. 61.

3. Investigações privadas: a problemática da prova ilicitamente obtida por particulares no processo penal

3.1. O papel da prova no processo penal português

No processo penal, enquanto instrumento último da descoberta da verdade material e do restabelecimento da paz jurídica, adquirida a notícia do crime e aberto o inquérito, têm lugar um conjunto de diligências que visam investigar a existência de um crime, determinar os seus agentes e respetiva responsabilidade, e descobrir e recolher provas, de forma a que se possibilite determinar, no caso concreto, se os comportamentos que constam na acusação do MP, e que foram, alegadamente, praticados pelo arguido, encontram correspondência com os factos previstos na estatuição da norma penal[144].

O processo penal compreende, assim, uma atividade cognitiva[145], e é com base nas diferentes provas apresentadas em juízo que se formará a convicção do magistrado sobre a verificação – ou não – da prática do crime. Neste sentido, ao contrário do CPP de 1929, o atual CPP consagrou inteiramente todo um *Livro* à matéria probatória[146] (arts. 124º a 190º do CPP), dedicando-lhe ainda um acervo importante de preceitos na disciplina da audiência (arts. 327º, 340º, 343º a 345º, 348º, 355º a 357º e 374º, nº 2), sem prejuízo de normas contidas em diplomas avulsos[147], o que traduz, mais que uma opção sistemática de "*arrumação*" do código pelo legislador, a centralidade e importância da prova enquanto coração do processo penal.

Toda a atividade probatória[148] é assim direcionada a *convencer* alguém de uma certa versão das coisas[149]. Pois, num regime respeitoso do devido processo legal, para alguém ser declarado culpado, afastando-se a presunção de inocência[150], é necessária a demonstração, mediante provas válidas, que permitam, além de qualquer dúvida razoável,

[144] Antunes, 2022, pág. 138.
[145] Badaró, 2019, pág. 15.
[146] Silva, 2011, pág. 547.
[147] Entre as quais se destacam a Lei 93/99, de 14 de julho (Lei de Proteção de Testemunhas) e a Lei 101/2001, de 25 de agosto (Ações Encobertas).
[148] Em sentido estritamente jurídico, a palavra prova pode abarcar desde o próprio meio de prova, até às formas através das quais as partes ou as autoridades judiciárias procuram demonstrar a veracidade dos factos alegados, *in* Ribeiro, 2014, pág. 1.
[149] Gonçalves, 2009, pág. 123.
[150] Art. 32º, nº 2 da CRP.

concluir pela culpa do arguido *lato senso*[151] ou pela procedência de um pedido de indemnização civil[152]. Além disso, a atividade probatória revela-se também importante para decidir sobre questões prévias, interlocutórias ou incidentais verificadas na pendência do processo, incluindo a determinação de factos relevantes para a verificação dos pressupostos das medidas de coação e garantia patrimonial[153].

Sendo a prova o centro de todo o processo penal, e a descoberta da verdade material o fim a atingir, o legislador português entendeu ser necessário consagrar um conjunto amplo e heterogéneo de meios de prova e de obtenção de prova. Neste sentido, e ao contrário do sistema de prova vigente na Idade Média que se regia pelo sistema *prova legal* ou *prova tarifada*,[154] consagrou no art. 125º do CPP o *princípio da legalidade da prova* que estabelece que serão admissíveis no processo todas as provas não proibidas por lei – mesmo que não previstas no CPP, prevendo-se, assim, a regra da não taxatividade dos meios de prova. A lei portuguesa não estabelece, ao contrário de outras legislações, "um critério substantivo especial para a admissibilidade das provas não previstas na lei, pelo que [... a admissibilidade das mesmas se rege] pelos critérios substantivos gerais do art. 340º[155]".

3.2. Limites à descoberta da verdade – as proibições de prova e o seu *efeito-á-distância*

Como referimos, o art. 125º do CPP estabelece um critério não taxativo da admissibilidade de meios de prova no processo penal; ainda assim, existem, na nossa legislação, enquanto ordenamento jurídico próprio de um Estado de Direito Democrático, onde o respeito pela dignidade da pessoa humana e pelos direitos, liberdades e garantias dos cidadãos se assume primordial, limites impostos à admissibilidade da prova no processo.

Desde logo, a dignidade da pessoa humana franqueia a nossa Constituição que a consagra logo no art. 1º e a impõe como princípio limite. Esta ganha assim valor próprio

[151] Badaró, 2019, pág. 13.
[152] Art. 124º do CPP.
[153] Albuquerque, 2008, pág. 330.
[154] Gonçalves & Alves, 2009, págs. 127 e ss.
[155] Albuquerque, 2008, pág. 330.

através da expressão normativa específica e pressupõe, inerentemente, o direito à vida, à integridade física, à liberdade e à reserva da intimidade da vida privada e familiar[156]. Pois, cabe ao Estado não apenas respeitar os direitos e liberdades fundamentais dos cidadãos, como também garantir a sua efetivação[157], uma vez que os mesmos são elementares para uma vida digna e livre. Logo, não poderá tentar obter-se a verdade a todo o custo, devendo procurar-se sim uma verdade obtida no "escrupuloso e integral respeito dos direitos fundamentais dos cidadãos, arguidos no processo[158]".

Consciente desse facto, o legislador entendeu ser necessário, e bem, consagrar um preceito de índole constitucional onde se salvaguardassem estes direitos fundamentais no âmbito do processo penal. Referimo-nos, desde logo, ao art. 32º, nº 8 da CRP que estabelece como consequência para a as provas obtidas mediante a violação de direitos e liberdades dos cidadãos[159], a nulidade, impondo, assim, um limite ao princípio da investigação e da descoberta da verdade material, que acabará sacrificada[160]. Pois, como afirma GERMANO MARQUES DA SILVA,

> *Não se combate o crime com atos atentórios da dignidade humana, mesmo quando eficazes, porque a eficácia na luta contra o crime não é o valor primeiro e em nome dela têm sido cometidos gravíssimos abusos como a história da justiça documenta. E, se para obstar aos abusos contra a dignidade humana, pela violação de direitos fundamentais, é necessário sacrificar outros interesses ou valores, a Constituição fez a opção que se impunha, cominando com a nulidade a prova obtida...*[161]

Este preceito constitucional encontra correspondência no CPP, mais concretamente no art. 126º, que, sob a epígrafe "*métodos proibidos de prova*" regula e esclarece, de forma mais detalhada, o regime da proibição de prova no processo penal[162]. Este artigo estabelece, desde logo, duas cominações distintas atento o bem jurídico violado: o nº 1 prevê que serão consideradas nulas e, consequentemente, não passiveis de valoração, as provas que sejam obtidas mediante tortura, coação ou, em geral, ofensa à integridade

---

[156] Gonçalves & Alves, 2009*,* pág. 13.
[157] Canotilho & Moreira, 2007, pág. 194.
[158] Gonçalves & Alves, 2009*,* pág. 15.
[159] Obtidas mediante tortura, coação, ofensa da integridade física ou moral, abusiva intromissão na vida privada, no domicílio, na correspondência e nas telecomunicações.
[160] Gonçalves & Alves, 2009*,* pág. 17.
[161] Silva, 2006, pág. 41.
[162] Chamamos a atenção para o facto de as proibições de prova configurarem "autênticos limites à descoberta da verdade material, "barreiras colocadas à determinação do objeto do processo", no dizer de Gôssel, [devendo as mesmas distinguir-se das] regras sobre a produção de prova [que configuram], diversamente, meras prescrições ordenativas da produção de prova, cuja violação não poderia acarretar a proibição de valorar como prova", *in* Ac. do STJ de 20/02/2008, proc. nº 07P4553, disponível em www.dgsi.pt

física e moral das pessoas, procedendo-se, no nº 2, a uma enumeração exemplificativa de condutas capazes de ofender os bens jurídicos a proteger no nº 1; já o nº 3 estabelece que serão igualmente nulas as provas obtidas mediante intromissão na vida privada, no domicílio, nas comunicações e na correspondência, salvo o consentimento do titular do direito em relação ao qual se verificou a intromissão ilegal.

Parece-nos claro que a intenção do legislador foi atribuir diferentes graus de proteção a diferentes bens jurídicos ao permitir que a utilização da prova obtida mediante intromissão na vida privada, caso o titular do próprio direito assim o consinta, mas não o permitindo quando o bem jurídico em causa é a integridade física, ainda que o mesmo seja um bem jurídico livremente disponível[163], ou a liberdade, fazendo-lhe sempre corresponder a consequência da nulidade[164].

Para PAULO PINTO DE ALBUQUERQUE, o art. 126º, nº 1 e 2 preveem aquilo a que chamamos *nulidades absolutas de prova*, ao contrário do art. 126º, nº 3, que prevê *nulidades relativas de prova*[165] e, para além das consequências associadas aos diferentes tipos de nulidade, o conhecimento das mesmas também varia, pois se as *nulidades absolutas de prova* podem ser conhecidas oficiosamente ou a requerimento dos sujeitos processuais, a prova ferida de uma *nulidade relativa* apenas poderá ser conhecida a requerimento do titular do direito violado.

Pela leitura do nº 3 do art. 118º, não é difícil concluir-se que a intenção do legislador, ao instituir o regime das proibições de prova previsto no art. 126º, foi instituir um regime autónomo face ao previsto nos arts. 118º e ss. do CPP, sendo esta mesmo uma não questão entre a doutrina; contudo, o mesmo não sucede quando a tarefa é determinar a extensão com que esta autonomia foi concebida[166] pois, se parte da doutrina[167] defende uma autonomia dogmática, encarando o regime das proibições de prova como um regime especial em relação ao regime geral das nulidades, outra parte[168] entende tratar-se de uma autonomia jurídica. Falamos, neste último caso, de uma autonomia "total, de maneira que não se socorrem, para nenhum efeito, na aplicação do artigo 126º, do regime dos arts. 118º e ss.", existindo uma absoluta separação entre estes dois regimes. Parece-nos ser esta

[163] Nos termos do art. 149º, nº 1 do CP.
[164] Que poderá ser invocada a todo o tempo, em ambos os casos.
[165] Albuquerque, 2008, pág. 335.
[166] Oliveira, 2017, págs. 260 e ss.
[167] Oliveira, 2017, págs. 260 e 261.
[168] Oliveira, 2017, págs. 261 e 262.

última a posição mais acertada, não só pela sistematização do CPP ou pela finalidade destas proibições de prova, mas também pelas diferenças notáveis entre regimes[169].

Resta-nos salientar ainda que, para além das provas proibidas no art. 126º do CPP, outras poderão ser reconhecidas pela doutrina e jurisprudência nos domínios em que o método de aquisição probatória concretamente utilizado importe uma intromissão injustificada nos direitos fundamentais do arguido ou outras pessoas, *maxime*, nas situações de afronta à dignidade humana ou à integridade pessoal ainda reconduzíveis ao âmbito de tutela do nº 8 do art. 32º da CRP[170]. Neste sentido decidiu o TC[171], alertando para o facto de, fruto da evolução das técnicas de investigação em consequência do constante avanço da ciência e da tecnologia, ser necessário uma atitude de "perseverante vigilância", sob pena de se lesarem direitos fundamentais, "no sentido de sancionar a sua admissão, formal e materialmente legitimidade, no processo penal".

Contudo, muitas vezes, é a aquisição de certo material probatório, á custa da violação de um método proibido, que vem possibilitar o avanço da investigação e o alcance de outros meios de prova[172]. A questão se coloca é, então, que valor atribuir às provas derivadas ou subsequentes das provas obtidas através dos métodos de prova proibidos?

Concretizando: como vimos no capítulo anterior, aceder ilegitimamente a uma caixa de correio eletrónico é considerado crime, nos termos do art. 6º da Lei do Cibercrime, o que, consequentemente, leva a que os e-mails a que se teve acesso não possam ser usados como prova no processo; mas o que dizer em relação ás informações nele contidas e que, por exemplo, poderão levar á descoberta de outros elementos essenciais da prática do crime que se investiga, como, por exemplo, a arma do crime ou mesmo o próprio cadáver? Serão estes também atingidos pela força da ilegalidade inicial?

---

[169] Tenha-se, como exemplo, o facto de as nulidades de prova poderem ser arguidas a todo tempo, diferentemente do regime geral das nulidades que prevê prazos curtos para o efeito ou o facto de as proibições de prova resistirem ao caso julgado havendo lugar a recurso extraordinário de revisão quando se descubra que foi utilizada prova proibida, enquanto as nulidades, mesmo as insanáveis, se consolidam na nossa ordem jurídica com o trânsito em julgado da decisão, *in* Oliveira, 2017, pág. 268.

[170] Silva, 2011, pág. 589.

[171] Ac. do TC nº 155/2007, de 19 de março de 2007, proc. 695/06, disponível em: https://www.tribunalconstitucional.pt/tc/home.html

[172] Morão, 2012, pág. 708.

Inspirada na *teoria dos frutos da árvore envenenada*, desenvolvida nos EUA, e na *teoria da nódoa*, desenvolvida na Alemanha[173], a solução[174] adotada pela doutrina portuguesa é a da contaminação da restante prova pela prova ferida de nulidade, quando entre elas exista um nexo de dependência cronológica, lógica e valorativa[175]. Neste sentido, e nas palavras de PAULO PINTO DE ALBUQUERQUE, o efeito à distância "há-de, pois, resultar de uma necessária ponderação do nexo que liga a prova proibida e a prova mediata dela resultante", sendo este *efeito-à-distância* da proibição de prova tanto maior quanto mais grave for a proibição de prova violada.

Ainda assim, existe, na opinião de HELENA MORÃO, uma importante convergência, quer na doutrina e jurisprudência nacionais[176], quer no plano do direito comparado, quanto à admissibilidade de limitações razoáveis a esse princípio, isto numa tentativa de conciliação dos valores protegidos pelas proibições de prova com a necessidade de conferir eficácia à justiça penal[177]. Falamos nos casos da *fonte independente*, da *mácula dissipada* e da *descoberta inevitável.*

Relativamente à *fonte independente*, a mesma 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. Incluem-se nesta exceção as situações em que a ilegalidade não foi *conditio sine qua non* da descoberta da verdade[178].

No caso da *mácula dissipada*, admite-se que uma prova, não obstante derivada de outra prova ilegal, seja aceite, sempre que os meios de alcançar aquela apresentem uma forte autonomia relativamente a esta, em termos tais que produzam uma decisiva atenuação da ilegalidade precedente[179].

---

[173] Costa Andrade, 2013, pág. 312.
[174] Alicerçada no conteúdo normativo do art. 122º do CPP, segundo o qual "as nulidades tornam inválido o ato em que se verificarem, bem como os que dele dependerem e aquelas puderem afetar".
[175] Albuquerque, 2008, pág. 338.
[176] Destacamos, neste sentido, o Ac. do TC nº 198/2004, de 24 de março de 2004, proc. nº 39/04, disponível em: https://www.tribunalconstitucional.pt/tc/home.html que, inspirado na jurisprudência americana, mais concretamente na decisão *Nardone v. United States* [308 U.S. 338 (1939), disponível em https://supreme.justia.com/cases/federal/us/308/338/ , desenvolveu de forma detalhada a questão.
[177] Morão, 2012, pág. 716.
[178] Gonçalves & Alves, 2009*,* pág. 139.
[179] *In* Ac. do TC nº 198/2004, de 24 de março de 2004, proc. nº 39/04, disponível em: https://www.tribunalconstitucional.pt/tc/home.html

Por fim, a *descoberta inevitável* tem lugar quando ficar demonstrado, pela acusação, que uma outra atividade investigatória, não levada a cabo, seguramente iria ocorrer na concreta situação, não fora a descoberta através da prova proibida conducente inevitavelmente ao mesmo resultado[180]. Falamos numa exceção assente na ideia de que a projeção do efeito da prova proibida não impossibilita a admissão de outras provas derivadas quando estas tivessem inevitavelmente sido descobertas, através de outra atividade investigatória legal[181]. Contudo, a admissão desta última exceção não é consensual: para PAULO PINTO DE ALBUQUERQUE, posição com a qual concordamos, não deve ser excluído o *efeito-à-distância* no caso dos "percursos hipotéticos de investigação", entendendo o autor que "nestes casos, a prova inicialmente proibida tem um efeito à distância destruidor da prova posterior, mesmo que esta pudesse a vir a ser descoberta de outra forma lícita[182]" devido à incerteza e dos juízos político-criminais inerentes a estes juízos hipotéticos.

3.3. A problemática da prova ilicitamente obtida por particulares e a sua utilização no processo penal português – *o Caso Rui Pinto*

Problema importante e alvo de discussão noutros ordenamentos jurídicos, mas ainda pouco discutido em Portugal, a "privatização da investigação penal" é um fenómeno com tendência para aumentar[183], surgindo com ele muitas dúvidas, uma delas sendo qual o regime aplicável à obtenção de prova ilicitamente recolhida por particulares – sejam eles jornalistas de investigação, investigadores privados ou o mais comum dos cidadãos.

Os cidadãos intervêm cada vez mais na investigação penal, oferecendo provas por si recolhidas o que, *prima facie*, nos parece uma intervenção saudável, pautando o processo penal de uma maior colaboração entre o cidadão comum e os OPC, tornando, consequentemente, a "investigação mais eficiente, e [a reposição da paz social] mais célere[184]". Contudo, é de fácil representação a escalada de situações em que a obtenção

[180] Gonçalves & Alves, 2009, págs. 139 e 140.
[181] *In* Ac. do TC nº 198/2004, de 24 de março de 2004, proc. nº 39/04, disponível em: https://www.tribunalconstitucional.pt/tc/home.html
[182] Albuquerque, 2008, pág. 339.
[183] Principalmente com o avanço da tecnologia.
[184] Costa, 2013, pág. 301.

de prova pelos particulares, à falta de qualquer tipo de vigilância ou controlo por parte de qualquer instância ou entidade, seja feita à custa da violação de direitos fundamentais constitucionalmente consagrados, pois, como vimos, a dificuldade com que um *hacker* informático hoje em dia acede à caixa de correio eletrónico de outrem é quase nula; assim como é quase nula a dificuldade com que alguém, com o seu próprio telemóvel, grava um vídeo ou conversa telefónica sem o consentimento do visado[185].

Neste sentido, o núcleo da questão reside em saber se, face à falta de menção, o regime das proibições de prova, previsto nos art. 32º, nº 8 da CRP e 126º do CPP, vincula igualmente os particulares, ou se destinam apenas aos órgãos incumbidos da prossecução penal e se será, nesse caso, sustentável a existência de dois regimes distintos consoante a prova seja obtida por autoridades públicas ou particulares.

Ao contrário do que sucede na Alemanha[186], MANUEL DA COSTA ANDRADE entende que, apesar de em Portugal o regime das proibições de prova ser sobretudo dirigido às instâncias formais de controlo, a quem cabe prevenir os atentados e agressões que os métodos proibidos de prova representam, não se poderá excluir do seu âmbito de aplicação a atividade investigadora levada a cabo por particulares. Aliás, numa estreita comparação entre o ordenamento jurídico alemão e o português, o autor sustenta a sua argumentação no facto de o art. 126º vir codificado no livro *Da prova,* onde se regula a prova não apenas numa perspetiva dos órgãos pertencentes ao terceiro poder do Estado, mas onde se encontram proibições aplicáveis também a particulares. E,

> *Mal se compreenderia que, por um lado, o legislador português precludísse sem mais a valoração dos meios de prova [...] obtidas por particulares através de atentados ao direito à palavra ou à imagem (art. 167º)[187]; e por outro lado e ao mesmo tempo, admitisse as provas logradas por particulares à custa de atentados tão intoleráveis a eminentes bens jurídicos pessoais como os previstos nos art. 126º do CPP[188].*

[185] Costa, 2013, pág. 302.
[186] Onde as proibições de prova apenas só valem para os agentes das instâncias formais de controlo, ou para os particulares que intervêm em colaboração com eles e sob a sua orientação, *in* Costa Andrade, 2013, pág. 197.
[187] O art. 167º do CPP faz depender a validade da prova produzida por reproduções mecânicas da sua não ilicitude criminal (arts. 192º e 199º do CP). Ainda assim, a maioria da jurisprudência, especialmente relativa à videovigilância, parece fixar um critério flexível no que toca à admissão destes meios de prova, fundando-se em duas exigências: que o conteúdo das fotografias não diga respeito ao núcleo central do direito à vida privada do visado e que exista uma justa causa para a sua obtenção. Veja-se, neste sentido, o Ac. do STJ, de 28 de setembro de 2011, proc. nº 22/09.6YGLSB.S2, disponível em: www.dgsi.pt
[188] Costa Andrade, 2013, pág. 198.

De realçar ainda que, incluindo-se o art. 32º, nº 1 e 8 da CRP no capítulo dos *Direitos, Liberdades e Garantias*, os mesmos se encontram sob a alçada do art. 18º, nº 1, que prevê a aplicação e vinculação de entidades públicas e privadas aos preceitos constitucionais cujo escopo é a proteção de direitos constitucionalmente consagrados dos cidadãos[189].

Da mesma opinião partilha PAULO PINTO DE ALBUQUERQUE para quem os *sujeitos passivos* dos métodos proibidos de prova são não apenas o arguido ou a testemunha, como também o perito, assistente, partes civis e o intérprete; e os *sujeitos ativos* dos mesmos não só os agentes do Estado e os que agem sob a sua orientação, como quaisquer particulares que levem a cargo, por sua própria iniciativa[190], qualquer tipo de investigação, sendo as provas por eles obtidas mediante a violação dos requisitos do art. 126º do CPP feridas de nulidade e, consequentemente, não passíveis de valoração no processo em questão.

Na nossa ótica, adotar uma solução contrária a esta seria atribuir "carta-branca para o cidadão comum levar a cabo as suas próprias investigações criminais[191]", possibilitando que o mesmo tivesse poderes de investigação mais amplos que as próprias autoridades judiciárias, comprometendo-se todos os direitos e garantias fundamentais salvaguardadas através da consagração do regime do art. 32º, nº 8 da CRP e 126º do CPP. Pois, a proteção destes direitos não se encontra completa se não se fizer também contra os particulares[192].

JOSÉ NEVES DA COSTA vai mais longe ao afirmar que "há violação também quando o Estado não cumpre as suas obrigações de proteção dos bens jurídicos dos cidadãos, ou se aproveita das violações feitas por particulares para efetivar as suas pretensões[193]".

De realçar ainda que, a proibição da valoração da prova ilicitamente obtida por particulares se entende estender a momentos outros que não apenas audiência de julgamento. Neste sentido, não poderão ser usadas em momentos anteriores, nomeadamente para a denúncia da prática do crime e consequente abertura de

[189] Costa, 2013, pág. 321.
[190] Falamos de investigações levadas a cabo por particulares onde a intervenção do Estado apensa se dá *ex post, in* Costa, 2013, pág. 303.
[191] Freitas, 2019.
[192] Costa, 2013, pág. 320.
[193] Costa, 2013, pág. 320.

inquérito[194], a não ser que esteja em causa alguma das limitações do *efeito-à-distância* das proibições de prova.

Recentemente, e como vimos no capítulo anterior, muitos têm sido os escândalos, nacionais e internacionais[195], que ocupam grande parte do tempo de antena, relacionados com a divulgação de informação ilegalmente obtida, e que servem de suporte aos indícios da prática de vários crimes. Pense-se, por exemplo, no Caso Rui Pinto, *hacker* português criador da página *Football Leaks*, que é acusado de mais de 90 crimes[196], entre eles, o acesso ilegítimo à caixa de endereço eletrónico do Clube Sport Lisboa e Benfica e da filha do ex-presidente angolano, Isabel dos Santos, e posterior divulgação dos mesmos.

Percebido como criminoso por uns, e como herói ou *hacktivista* movido por motivos altruístas por outros, a verdade é que a obtenção de informação pelo *hacker* originou uma situação complexa: se, por um lado, o método ilegal através do qual a informação foi obtida não deve ser recompensado, por outro, as atividades ilegais que os documentos evidenciam também não devem deixar de ser investigadas e punidas.

Rui Pinto, que se negou a prestar declarações sobre os factos de que é acusado na primeira sessão de julgamento, acabou mesmo por afirmar não se considerar um *hacker*, mas um *whistleblower*. Ora, não podemos deixar de discordar com a afirmação do mesmo pois, não se prevê nenhum estatuto de *whistleblower* ou denunciante no ordenamento jurídico português que leve à isenção da responsabilidade criminal do mesmo. O que o ordenamento jurídico português conhece, por força de normas constitucionais e legais de caráter geral, é a possibilidade de transmissão de denúncias internas e externas de infrações penais ou administrativas[197].

Como esclarece NUNO BRANDÃO[198], o art. 244º do CPP estabelece a possibilidade, caso assim o cidadão o entenda, de fazer chegar ao MP a notícia de crime, tornando-se esta denúncia obrigatória quando em causa esteja um funcionário público, que tenha tido conhecimento da mesma no exercício e por causa das suas funções. Mais: o art. 245º, nº 6 do CPP admite mesmo a realização de denúncias anónimas dirigidas ao MP e às autoridades judiciárias quando a mesma seja acompanhada da demonstração de

[194] Costa, 2013, pág. 325.
[195] Pense-se no caso dos *Panama Papers*, do *Luanda Leaks* ou da *Primavera Árabe*.
[196] Entre os quais acesso ilegítimo, acesso indevido, sabotagem informática, violação de correspondência e tentativa de extorsão.
[197] Brandão, 2020, pág. 105.
[198] Brandão, 2020, pág. 105.

indícios da prática do crime, não sendo este anonimato razão suficiente para travar a abertura de inquérito. Contudo, e como denota o autor, falamos de uma regulação de caráter geral que não foi desenhada a pensar no *whistleblower*, mas sim no cidadão comum[199]. Aliás, a situação concreta nem sequer é acolhida no âmbito da recente Diretiva (UE) 2019/1937, que se aplica apenas no âmbito laboral, não conferindo qualquer tipo de proteção contra a ação penal do Estado.

Nas palavras do mesmo,

> *As leis portuguesas de whistleblowing nada preveem [...] nos casos em que para melhor se inteirar da suspeita ou para comprovar a denúncia, o whistleblower realize factos típicos de acesso ilegítimo a sistemas informáticos ou a correspondência eletrónica, ou viole segredos comerciais*[200].

In casu, não beneficiando o *hacker*, a nosso ver, do estatuto de *whistleblower*, e tendo o mesmo praticado crimes aquando da busca da informação que sustentava as suas suspeitas, não faria sentido o mesmo sair impune. Pois, ainda que a prova tenha sido por ele ilegalmente obtida[201] (pois as condutas levadas a cabo constituem, indubitavelmente, crime) sendo consequentemente, nula, não podendo poder ser valorada em processos movidos contra os agentes a que a informação respeita, a mesma poderá ser usada, com fim exclusivo, para proceder legalmente contra este. É esta a solução que resulta do art. 126º, nº 4 do CPP, que não prevê qualquer ação contraditória do Estado aquando da punição do "investigador particular", na medida em que essa acusação será independente da do aproveitamento da prova[202].

Ainda assim, alguns autores admitem, fazendo uso da *teoria da ponderação*, que, aplicando o *princípio da proporcionalidade*, concretiza os interesses a ponderar, pesando a gravidade do facto imputado, do direito do arguido e a gravidade dos interesses particulares violados no processo, que a prova obtida ilegalmente pelo particular possa vir a ser utilizada no processo[203]. Ora, não podíamos estar mais em desacordo pois, por mais importante que seja o interesse público da defesa da gravidade, prossecução do

[199] Existe, contudo, legislação que é tributário do "pensamento" do *whistleblowing* em determinados setores, como o bancário, do mercado de capitais, prevenção de branqueamento de capitais e do financiamento do terrorismo. Ver mais i*n* Brandão, 2020*,* págs. 106 e ss.
[200] Brandão, 2020*,* pág. 112.
[201] A não ser que exista consentimento do titular do direito lesado, inserindo-se, neste caso, no âmbito do art. 126º, nº 3 do CPP.
[202] Costa, 2013, pág. 323.
[203] Costa, 2013, pág. 327.

crime e reafirmação das normas penais violadas, esta solução – por se tratar de um critério subjetivo e que, a nosso ver, não é compatível com o *princípio da segurança jurídica* – coloca em causa o escopo de proteção do regime das proibições de prova. Concordamos com RUI SILVA LEAL que, a propósito do *hacker* Rui Pinto[204], afirmou que,

> *Não se pode, a meio de um jogo, mudar as regras. Não se pode dizer que em nome do interesse público uma prova que não é lícita passa a ser lícita. Não podem fazer isso. O interesse público é a justiça. Os magistrados não podem decidir contornar a lei em nome do alegado interesse público. Isso é um raciocínio que chega à desonestidade.*

Seria, a nosso ver, insustentável concluir de forma diferente. Prever um regime distinto para os particulares, capaz de os incentivar a "buscar a prova, a qualquer custo, para com ela obterem a condenação do agressor[205]" ou aceitar essa prova, em determinados casos, após ponderados os interesses em jogo, seria criar uma "sociedade justiceira que, sob a capa da justiça e da verdade decidem arbitrariamente invadir os nossos computadores, smartphones, ou qualquer outro dispositivo em relação ao qual confiamos – bem ou mal – os nossos segredos[206]".

Permitir que se valorem em tribunal provas ilicitamente obtidas por particulares é comprimir bastante a esfera de proteção dos direitos dos particulares e alimentar a desconfiança não só entre as pessoas[207], como a falta de confiança do cidadão no sistema judiciário. Este aproveitamento significaria a conivência com a prática de atos lesivos dos direitos fundamentais dos indivíduos visados pelo próprio Estado, e, quanto às proibições de prova assentes em ilicitude material, ditaria a condução de atos criminosos pelo Estado com o propósito de averiguar e esclarecer a prática criminosa de outrem, frustrando em absoluto a teleologia subjacente ao regime das proibições de prova[208].

[204] Câncio, 2020.
[205] Oliveira, 2021, *cit. por*. Bernardes, pág. 4.
[206] Freitas, 2019.
[207] Costa, 2013, pág. 324.
[208] Pereira, 2019, pág. 20.

Conclusão

Da exposição supra conclui-se que o cibercrime, ainda que se trate de um tipo de criminalidade relativamente recente e que tem vindo, como comprovam as estatísticas, a crescer exponencialmente, não só em Portugal como no mundo em geral, constitui uma realidade complexa de tratar, mas que se revela bastante atrativa do ponto de vista do agente do crime.

Nascida de uma atividade originalmente encarada como lúdica, tendo mesmo dado origem a uma comunidade própria que atua no ciberespaço, a mesma passou rapidamente a ser vista, por uma parte dos utilizadores, como um meio de lucro fácil e de risco diminuto; contudo, vimos também que a mesma é capaz de causar prejuízos substanciais, lesar vários bens jurídicos importantes e de afetar não apenas o cidadão comum, como empresas e Estados, sejam eles praticados com o intuito de obter vantagens económicas ou movidos por ideais políticos.

Consequentemente, desde cedo o legislador começou a desenvolver medidas de combate ao cibercrime, tendo mesmo sido feito um esforço para implementar medidas mais coesas a nível internacional e europeu, de forma a facilitar a cooperação entre Estados; assim como tem sido desenvolvido, pelo menos a nível interno, um trabalho sério, pelas autoridades judiciárias, no que toca à investigação deste tipo de criminalidade. É exemplo disso o Caso Rui Pinto e outros casos mediáticos, onde a prática de crimes informáticos, ainda que cometidos sob a égide da busca pela verdade, põe em causa não só direitos, liberdades e garantias constitucionalmente protegidos, como os pilares em que se funda o próprio processo penal.

Percebemos que, no contexto atual, a intervenção dos particulares no processo, mediante a contribuição com prova obtida de forma autónoma, assuma caráter cada vez mais comum; contudo, certas atuações, nomeadamente a prática de crimes para a obtenção da referida prova, comporta uma ameaça para a os direitos fundamentais tutelados pelo regime do art. 126º do CPP e 32º, nº 8 da CRP.

Neste sentido, defendemos que o regime das proibições de prova se aplica não só às autoridades judiciárias, que investigam e recolhem prova no exercício e por causa das suas funções, ao serviço do Estado enquanto titular do *ius puniendi*, como aos particulares que decidem levar a cabo, de forma autónoma e independente, as suas próprias

investigações, independentemente do interesse público. A ser utilizada a prova obtida, apenas o seria com o fim exclusivo de proceder contra o respetivo particular no caso de a atuação ter constituído crime.

Aliás, decidir de forma diferente seria pôr em causa a integridade dos direitos fundamentais que o regime das proibições de prova estabelece e a finalidade que desempenha, atribuindo-se poderes de investigação mais amplos ao particular que ao próprio Estado. Ao permitir-se a procura da verdade a todo o custo, estar-se-ia a abrir portas para abusos contra a dignidade humana e demais direitos constitucionalmente protegidos e a criar-se um clima de desconfiança e insegurança incompatível com o postulado de um Estado de Direito Democrático.

Bibliografia

ALBUQUERQUE, Paulo Sérgio Pinto de (2008) – *Comentário do Código de Processo Penal: Á Luz da Constituição da República e da Convenção Europeia dos Direitos do Homem,* 2ª ed. atualizada. Lisboa: Universidade Católica Editora.

AMADOR, Nelson José Roque (2012) – *Cibercrime em Portugal: Trajetórias e Perspetivas de Futuro*, Dissertação de Mestrado em Ciências Policiais. Lisboa, Instituto Superior de Ciências Policiais e Segurança Interna.

ANDRADE, Manuel da Costa (2013) – *Sobre as Proibições de Prova em Processo Penal*, reimp. Coimbra: Coimbra Editora.

ANONYMOUS, *"Jargon File"*, v. 4.2.2., 20/Aug/2000, disponível em: https://vanderworp.org/wp-content/uploads/2019/06/jargon.pdf, consult. em 28/Mai/2022.

ANTUNES, Maria João (2022) – *Direito Processual Penal*, 4ª ed. Lisboa: Almedina.

ARRUDA, José Pedro – Hackers, Hacktivistas e Whistleblowers: o caso português, *Perspetiva em Ciências da Informação,* 26 (abril-junho 2021), disponível em: https://www.scielo.br/j/pci/a/pgQCPNRHYbJMw4nx6MpKZ3L/, consult. em 03/Mai/2022.

ASCENÇÃO, J. Oliveira (2001) – Direito Cibernético: A Situação em Portugal. *Direito e Justiça*, 15.

BACHMANN, M. – "The Risk Propensy Computer Hackers and Rationality", *International Journal of Cyber Criminology*, vol. 4 (janeiro 2010/julho-dezembro 2010), disponível em: https://www.cybercrimejournal.com/michaelbacchmaan2010ijcc.pdf, consult. em 15/Mai/2022.

BADARÓ, Gustavo – "Meios de Obtenção de prova: requisitos legais e standard de prova", *Revista Portuguesa de Ciência Criminal*, Ano 29, nº 1 (janeiro-abril 2019).

BERNARDES, Bianca Adélia Tudéia – *A Prova Ilícita Obtida por Particulares e a Sua Utilização no Processo Penal*, pág. 4, disponível em: https://repositorio.animaeducacao.com.br/bitstream/ANIMA/13961/1/Artigo%20-%20A%20PROVA%20ILICITA%20OBTIDA%20POR%20PARTICULAR%20E%20SUA%20UTILIZAÇÃO%20NO%20PROCESSO%20PENAL.pdf, consult. em 10/Jun/2022.

BRANDÂO, Nuno – "O Whistleblowing no Ordenamento Jurídicos Português", *Revista do Ministério Público*, Nº 161 (janeiro-março 2020).

BRENNER, Susan W. (2012) – *Cybercrime and the law: challenge, issues and outcomes*. Boston: Northwestern University.

BRENTON, Brian, "The Misinformers: Edward Snowden, Aaron Swartz and The Troubled Relationship Between Hacktivists, Mass Media and American Government", 2015, disponível em: https://www.academia.edu/26547917/The_Misinformers_Edward_Snowden_Aaron_Swartz_and_The_Troubled_Relationship_Between_Hacktivists_Mass_Media_and_American_Government, consult. em 04/Jun/2022.

CÂNCIO, Fernanda – "Afinal, Rui Pinto é Testemunha de Quê?", Diário de Notícias, 10/Set/2020, disponível em https://www.dn.pt/edicao-do-dia/10-ago-2020/afinal-rui-pinto-e-testemunha-de-que-12509667.html, consult. em 10/Jun/2022.

CANOTILHO, Gomes, Vital MOREIRA (2007) – Constituição da República Portuguesa Anotada, Vol. 1. Coimbra: Coimbra Editora.

CARVALHO, Francisco Proença de, Óscar Morales GARCÍA, Manuel Álvarez FEIJOO – "Regulamentação Supranacional Sobre Criminalidade Informática e Técnicas de Transposição. O Direito Penal Português e Espanhol Como

Paradigmas", *Actualidade Jurídica Uría Menéndez*, 48 – 2018, disponível em:
https://www.uria.com/documentos/publicaciones/5801/documento/art04.pdf?id=7877, consult. em 08/Mai/2022.

CLOUGH, Jonathan (2010) – *Principles of Cybercrime*. Cambridge: Cambridge University Press.

COLEMAN, Gabriella (2014) – *Hacker, Hoaxer, Whistleblower, Spy – The Many Faces of Anonymous*, Nova Iorque: Verso.

CORREIA, António (2021) – "Velhos Crimes, Novas Ferramentas; Novos Crimes, Novas Ferramentas", in *Cibercriminalidade: Novos Desafios, Ofensas e Soluções.* Lisboa: PACTOR – Edições de Ciências Sociais, Forenses e da Educação.

COSTA, José Neves da – "Do Aproveitamento em Processo Penal das Provas Ilicitamente Obtidas por Particulares", *Revista de Concorrência e Regulação*, Vol. 4, Nº 16 (2013).

DIAS, Pedro Simões – "O "Hacking" Enquanto Crime De Acesso Ilegítimo. Das Suas Especialidades À Utilização Das Mesmas Para A Fundamentação De Um Novo Direito", *Actualidad Jurídica Uría Menendez,* 14 (2016).

DIAS, Vera Marques – "A Problemática da Investigação do Cibercrime", *Data Venia, Revista Jurídica Digital*, Ano 1, Nº 1 (julho-dezembro 2012).

DOMINGUES, Elisabete Júlio (2015) - *Os Ciberataques como um Novo Desafio para a Segurança: O Hacktivismo*, Tese de Mestrado Integrado em Ciências Policiais. Lisboa, Instituto Superior de Ciências Policiais e Segurança Interna.

FERREIRA, João, Inês Sousa GUEDES (2021) – Hacking: Evolução, Perfis e Explicações Criminológicas, in *Cibercriminalidade: Novos Desafios, Ofensas e Soluções*. Lisboa: PACTOR – Edições de Ciências Sociais, Forenses e da Educação.

FRANCO, Hugo, "A história e a longa lista de crimes de Zambrius, o jovem hacker da Ericeira que vivia com os pais e a avó (e foi condenado a seis anos de prisão", *Expresso*, 12/jan/2022, disponível em: https://expresso.pt/sociedade/2022-01-12-A-historia-e-a-longa-lista-de-crimes-de-Zambrius-o-jovem-hacker-da-Ericeira-que-vivia-com-os-pais-e-a-avo--e-foi-condenado-a-seis-anos-de-prisao--b04fcdb6, consult. em 21/Mai/2022.

FREEMAN, Lindsay – "Hacked and Leaked: Legal Issues Arising From The Use of Unlwafully Obtained Digital Evidence In International Criminal Cases", *UCLA Journal of International Law and Foreign Affairs*, 25 (2021).

FREITAS, Pedro Miguel, "Criminoso ou Denunciante? A Ilusão do Justiceiro Privado", *Opinião*, 07/Set/2019, disponível em: https://repositorio.ucp.pt/bitstream/10400.14/30095/1/Criminoso%20ou%20denunciante.pdf, consult. em 03/Jun/2022.

GELBSTEIN, Eduardo – The War of Attriction in Cyber-Space or "Cyber-Attacks", "Cyber-War" and "Cyber-Terrorism", *IDN – Revista de Nação e Defesa*, Nº 135, 5ª série (2013).

GONÇALVES, Fernando, Manuel João ALVES (2009) – *A Prova do Crime: Meios Legais Para a Sua Obtenção*. Coimbra: Almedina.

GUEDES, Inês Sousa, Samuel MOREIRA, Carla CARDOSO (2021) – "Cibercrime: Conceptualização, Desafios e Perceções Públicas", in *Cibercriminalidade: Novos Desafios, Ofensas e Soluções.* Lisboa: PACTOR – Edições de Ciências Sociais, Forenses e da Educação.

HACKERONE TEAM, *The 2021 Hacker Report*, 08/Mar/2021, disponível em https://www.hackerone.com/resources/reporting/the-2021-hacker-report, consult. em 21/Mai/2022.

HOLT, Thomas J., Adam M. BOSSLER (2016) – *Cybercrime in Progress*. Oxon: Routledge.

HOLT, Thomas J., Adam M. BOSSLER, Kathryn C. SEIGFRIED-SPELLAR (2018), *Cybercrime and Digital Forensics, An Introduction*. 2ª ed., Oxon: Routledge.

JORDAN, Tim, Paul A. TAYLOR (2004) – *Hacktivism and Cyberwars – Rebels With a Cause?* London: Routledge.

KREMLING, Janine, Amanda M. Sharp PARKER (2018) - *Cyberspace, Cybersecurity and Cybercrime.* Califórnia: Sage Publications, Inc.

LUDLOW, Peter, "WikiLeaks and Hacktivist Culture", *The Nation*, 15/Set/2010, disponível em: https://www.thenation.com/article/archive/wikileaks-and-hacktivist-culture/, consult. em: 05/06/2022.

LUSA, "Grupo hacker português reinvindica ataque a 61 sites do Brasil este ano", *Público,* 25/Nov/2020, disponível em: https://www.publico.pt/2020/11/25/tecnologia/noticia/grupo-hacker-portugues-reivindica-ataque-61-sites-brasil-ano-1940563, consult. em 03/Jun/2022.

MARQUES, Maria Joana Xara-Brasil (2014) – *Os Meios de Obtenção de Prova na Lei do Cibercrime e o Seu Confronto Com o Código de Processo Penal*, Tese de Mestrado em Ciências Forenses. Lisboa, Universidade Católica Portuguesa.

MILITÃO, Renato Lopes – "A Propósito da Prova Digital No Processo Penal", *Revista da Ordem dos Advogados*, Ano 72, vol. 1 (janeiro-março 2012).

Ministério Público (2022), *Cibercrime: Denúncias Recebidas 2021 – Nota Informativa*. Lisboa, Gabinete Cibercrime, 25/Jan/2022, disponível em: https://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/denuncias-de-cibercrime-25-01-2022.pdf, consult. em 07/Mai/2021.

MORÃO, Helena – "Efeito-à-distância das Proibições de Prova e Declarações Confessórias – o Acórdão nº 198/2004 do Tribunal Constitucional e o

Argumento "The Cat is Out of the Bag", *Revista Portuguesa de Ciência Criminal*, Ano 22, nº 4 (2012).

NORRIS, Mark – "Bad "Leaker" or Good "Whistleblower"? – A Test", *Case Western Reserve Law Review*, vol. 63 (2013).

OLIVEIRA, Luís Pedro Martins (2017) – "Da Autonomia do Regime das Proibições de Prova", in *Prova Criminal e Direito de Defesa: Estudo Sobre Teoria da Prova e Garantias de Defesa em Processo Penal*. Coimbra: Almedina.

OWEN, Tim, Jessica MARSHALL (2021) – *Rethinking Cybercrime – Critical Debates*. UK: Palgrave Macmillan.

PEREIRA, Alexandra Filipa de Jesus (2019) – *A Vinculação dos Particulares Às Proibições de Prova*, Tese de Mestrado em Direito Penal. Lisboa: Faculdade de Direito da Universidade de Lisboa.

Polícia Judiciária (2015), Operação C4R3T05 (CARETOS), Lisboa, Diretoria de Lisboa e Vale do Tejo, disponível em: https://www.policiajudiciaria.pt/operacao-c4r3t05-caretos/, consult. em 07/Mai/2022.

RIBEIRO, Joana Clara Freire (2014) – *A (In)admissibilidade das Provas Proibidas em Processo Penal*, Tese de Mestrado Forense. Lisboa, Universidade Católica Portuguesa.

RODRIGUES, Benjamim Silva (2009) – *Direito Penal – Parte Especial – Tomo I – Direito Penal Informático-Digital.* Coimbra: Coimbra Editora

SANTOS, Ana Felícia Canilho Santos (2015) – *O Cibercrime: Desafios e Respostas do Direito*, Tese de Mestrado em Direito. Lisboa, Universidade Autónoma de Lisboa.

SILVA, Germano Marques da – "Produção e Valoração da Prova em Processo Penal", *Revista do CEJ*, Nº 4 (2006).

SILVA, Sandra Oliveira e – "Legalidade da Prova e Provas Proibidas", *Revista Portuguesa de Ciência Criminal*, Ano 21, nº 4 (2011).

SORREL, Tom – "Human Rights and Hacktivism: The Cases of Wikileaks and Anonymous", *Journal of Human Rights Practice,* vol. 7 (Novembro 2015).

STEINMETZ, Kevin F. (2016) – *Hacked – A Radical Approach to Hacker Culture and Crime*. Nova Iorque: NYU Press.

VENÂNCIO, Pedro Dias (2011) – *Lei do Cibercrime: Anotada e Comentada*. Coimbra: Coimbra Editora.

Jurisprudência

Nacional:

- Ac. do TC nº 155/2007, de 19 de março de 2007, proc. 695/06, disponível em: https://www.tribunalconstitucional.pt/tc/home.html

- Ac. do TC nº 198/2004, de 24 de março de 2004, proc. nº 39/04, disponível em: https://www.tribunalconstitucional.pt/tc/home.html

- Ac. do TRC, de 15 de outubro de 2008, proc. nº 368/07.8TAFIG.C1, disponível em: www.dgsi.pt

- Ac. do TRG de 12 de abril de 2021, proc. nº 19719.8GCBRG.G1, disponível em: www.dgsi.pt

- Ac. TRL de 7 de março de 2018, proc. nº 5481/11.4TDLSB.L1-3, disponível em: www.dgsi.pt

- Ac. do STJ, de 28 de setembro de 2011, proc. nº 22/09.6YGLSB.S2, disponível em: www.dgsi.pt

Internacional:

- *Nardone v. United States* [308 U.S. 338 (1939), disponível em: https://supreme.justia.com/cases/federal/us/308/338/