Carvalho, Mariana da Conceição Nicolau de, 1992-

O malware enquanto meio de obtenção de prova

http://hdl.handle.net/11067/7568

Metadados

Data de Publicação 2024

Resumo Os meios de obtenção de prova são ferramentas essenciais para o sucesso de uma investigação criminal, os quais são usados pelas autoridades judiciárias e órgãos de polícia criminal para obtenção da prova necessária no processo penal. Entre os meios de obtenção de prova assentes no nosso Código Processo Penal, a interceção das comunicações é uma das principais técnicas de investigação no âmbito da criminalidade organizada, a qual é considerada um método oculto de investigação. Concretamente, a ...

The means of obtaining evidence are essential tools for the success of a criminal investigation, which are used by judicial authorities and criminal police bodies to obtain the required evidence in criminal proceedings. Among the means established in our Criminal Law, the interception of communications is one of the main methods in the organized crime context, which is considered a covert method of investigation. Specifically, the interception of communications involves a transgression into th...

Palavras Chave Malware (Software para computadores) - Direito e legislação - Portugal, Investigação criminal - Inovações tecnológicas, Prova digital - Portugal, Prova Penal - Portugal, Processo penal - - Portugal

Tipo masterThesis

Revisão de Pares Não

Coleções [ULL-FD] Dissertações

UNIVERSIDADE LUSÍADA

FACULDADE DE DIREITO

Mestrado em Direito

O *malware* enquanto meio de obtenção de prova

Realizado por:
Mariana da Conceição Nicolau de Carvalho

Orientado por:
Prof.ª Doutora Ana Bárbara Pina de Morais de Sousa e Brito

Constituição do Júri:

Presidente:	Prof. Doutor José Alberto Rodríguez Lorenzo González
Orientadora:	Prof.ª Doutora Ana Bárbara Pina de Morais de Sousa e Brito
Arguente:	Prof.ª Doutora Raquel Preciosa Tomás Cardoso

Dissertação aprovada em: 10 de julho de 2024

Lisboa

2024

UNIVERSIDADE LUSÍADA

FACULDADE DE DIREITO

Mestrado em Direito

O *malware* enquanto meio de obtenção de prova

Mariana da Conceição Nicolau de Carvalho

Lisboa

Março 2024

UNIVERSIDADE LUSÍADA

FACULDADE DE DIREITO

Mestrado em Direito

O *malware* enquanto meio de obtenção de prova

Mariana da Conceição Nicolau de Carvalho

Lisboa

Março 2024

Mariana da Conceição Nicolau de Carvalho

O *malware* enquanto meio de obtenção de prova

Dissertação apresentada à Faculdade de Direito da Universidade Lusíada para a obtenção do grau de Mestre em Direito.

Área científica: Ciências Jurídico-Criminais

Orientadora: Prof.ª Doutora Ana Bárbara Pina de Morais de Sousa e Brito

Lisboa

Março 2024

FICHA TÉCNICA

Autora Mariana da Conceição Nicolau de Carvalho
Orientadora Prof.ª Doutora Ana Bárbara Pina de Morais de Sousa e Brito
Título O *malware* enquanto meio de obtenção de prova
Local Lisboa
Ano 2024

CASA DO CONHECIMENTO DA UNIVERSIDADE LUSÍADA - CATALOGAÇÃO NA PUBLICAÇÃO

CARVALHO, Mariana da Conceição Nicolau de Carvalho, 1992-

O *malware* enquanto meio de obtenção de prova / Mariana da Conceição Nicolau de Carvalho ; orientado por Ana Bárbara Pina de Morais de Sousa e Brito. - Lisboa : [s.n.], 2024. - Dissertação de Mestrado em Direito, Faculdade de Direito da Universidade Lusíada.

I - BRITO, Ana Bárbara Pina de Morais de Sousa e, 1970-

LCSH
1. Malware (Software para computadores) - Direito e legislação - Portugal
2. Investigação criminal - Inovações tecnológicas
3. Prova digital - Portugal
4. Prova penal - Portugal
5. Processo penal - Portugal
6. Universidade Lusíada. Faculdade de Direito - Teses
7. Teses - Portugal - Lisboa

1. Malware (Computer software) - Law and legislation - Portugal
2. Criminal investigation - Technological innovations
3. Electronic evidence - Portugal
4. Evidence, criminal - Portugal
5. Criminal procedure - Portugal
6. Universidade Lusíada. Faculdade de Direito - Dissertations
7. Dissertations, academic - Portugal - Lisbon

LCC
1. KKQ4679.C37 2024

Das estrelas até aqui, que estejam tão orgulhosos de mim como eu serei deles a minha vida toda.

Aos meus pais.

AGRADECIMENTOS

O presente relatório é uma conquista precedida de muitos sacrifícios, tanto pessoais quanto profissionais.

Nesse sentido, a minha primeira palavra de agradecimento é dirigida à Ex.ª orientadora, Sr.ª Dr.ª Ana Bárbara de Sousa e Brito que, desconhecendo o desfecho do meu pedido, prontamente aceitou guiar-me nesta tão importante etapa, partilhando toda a sua disponibilidade e os mais sábios conselhos.

Em segundo lugar, agradeço ao Sr. º Dr. º Pedro Casquinha, atual Procurador da República Portuguesa e antigo inspetor da Polícia Judiciária, com quem tive o privilégio de partilhar ideias e pensamentos sobre o tema, obtendo sempre os melhores ensinamentos e sugestões.

De igual forma, a minha gratidão para com o Sr. º Dr. º Hélder Cordeiro, Procurador da República Portuguesa, pela sua disponibilidade e ajuda ao longo deste projeto. Para mim, sempre será um exemplo de dedicação e brio profissionais.

Um enorme agradecimento aos meus colegas de trabalho, mormente do Juízo Local Criminal 1 do Tribunal da Amadora que, mesmo com as minhas ausências, sempre me dirigiram palavras de ânimo e coragem para este percurso. Desta forma, e com especial relevo à atual secretária judicial, por quem, para além da relação laboral nutro um grande carinho e admiração, querida Graça Inácio, o meu maior bem-haja por tudo.

Aqui incluo também uma referência de respeito e admiração às minhas magistradas, Sr.ª Dr.ª Patrícia Lopes e Sr.ª Dr.ª Cristina Rodrigues, o meu obrigada pela vossa compreensão e acima de tudo pela força que sempre me transmitiram para alcançar este objetivo.

Não se olvidam os amigos e colegas que sempre estiveram disponíveis, tanto para a troca de enriquecedoras ideias como tão somente para ouvirem os meus desabafos.

Por último, mas não menos importante, ao meu braço direito, aquele que está sempre presente nos bons e maus momentos, aquele que levo para a minha vida toda com um amor indeterminável, ao meu estimado irmão – José Carvalho - por acompanhar de perto as minhas conquistas e, mais do que isso, por aturar o meu mau feitio naqueles dias em que nada parecia correr bem.

‘‘Liberdade é o direito de fazer tudo o que as leis permitem”.

MONTESQUIEU, Barão (1979) - Do Espírito das Leis, p. 166. São Paulo: Editora Nova Cultural

APRESENTAÇÃO

O *Malware*
enquanto meio de obtenção de prova

Mariana da Conceição Nicolau de Carvalho

Os meios de obtenção de prova são ferramentas essenciais para o sucesso de uma investigação criminal, os quais são usados pelas autoridades judiciárias e órgãos de polícia criminal para obtenção da prova necessária no processo penal.

Entre os meios de obtenção de prova assentes no nosso Código Processo Penal, a interceção das comunicações é uma das principais técnicas de investigação no âmbito da criminalidade organizada, a qual é considerada um método oculto de investigação.

Concretamente, a interceção das comunicações consiste numa intromissão nas comunicações telefónicas e/ou digitais das pessoas visadas, sem o seu conhecimento.

Por outro lado, é ainda admissível em processo penal a recolha de imagens e respetivo som, através de sistemas de videovigilância, para captação, gravação e tratamentos destas, de acordo com o preconizado na Lei n.º 95/2021, de 29 de dezembro.

Sem prejuízo, para que seja considerado legal, o recurso aos referidos meios, deve ser levado a cabo o cumprimento de todas as previsões legalmente estabelecidas, dado o seu impacto nos bens jurídicos dos visados (direito à palavra, imagem, privacidade, entre outros), razão pela qual a delimitação e utilização cautelosa dos meios ocultos de obtenção de prova se apresenta com importância extrema.

O *malware* é uma categoria de *software* de computador que tem como objetivo causar danos ou controlo indevido em sistemas de computador e dispositivos móveis eletrónicos, sendo intencionalmente criado para ser prejudicial e malicioso. Todavia, dele também se poderá extrair uma nova funcionalidade, sendo esta cooperante com o sistema penal, no sentido de obtenção provas, as quais seriam impossíveis de adquirir por qualquer outra via.

Tal mecanismo permite, à semelhança dos acima referidos, a captura de imagens e/ou som, seja através das câmaras fotográficas, microfones ou até mesmo por acesso ao dispositivo eletrónico em questão.

Porém, coloca-se a questão relativamente à (im)possibilidade do seu uso no âmbito da investigação criminal, atenta a sua imperativa invasão pessoal no que respeita aos direitos fundamentais do cidadão, impondo-se desta forma uma análise crítica e fundamentada sobre a aplicação deste como meio de obtenção de prova, subsumindo-o igualmente como um método oculto de obtenção de prova.

Palavras-chave:

Meios de obtenção prova; escutas telefónicas; captura de imagens; direitos fundamentais.

ABSTRACT

O *Malware*
as a means of obtaining evidence

Mariana da Conceição Nicolau de Carvalho

The means of obtaining evidence are essential tools for the success of a criminal investigation, which are used by judicial authorities and criminal police bodies to obtain the required evidence in criminal proceedings.

Among the means established in our Criminal Law, the interception of communications is one of the main methods in the organized crime context, which is considered a covert method of investigation.

Specifically, the interception of communications involves a transgression into the telephone and/or digital communications of individual targets, without their knowledge.

On the other hand, the collection of images and their sound through a video surveillance system is also admissible in criminal proceedings for the capture, recording, and processing of these, under Law No. 95/2021, of december 29th.

Nevertheless, for the use of these means to be considered legal, compliance with all legally established provisions must be ensured, given their impact on an individual's legal rights (right to speech, image, privacy, among others), which is why the delimitation and cautious use of covert means of obtaining evidence is of utmost importance.

Malware is a category of computer software designed to cause damage or unauthorized control over computer systems and mobile devices, intentionally created to be harmful and malicious. However, it can also be repurposed to serve the criminal justice system by obtaining evidence that would otherwise be impossible to acquire by any other means.

Similar to the mechanisms mentioned, this method allows for capture of images and/or sound, whether through cameras, microphones, or even access to the electronic device in question.

However, questions arise regarding the (im)possibility of its use in criminal investigations, given its interference with basic privacy rights. The need for a critical and reasoned analysis of its application as a means of evidence, even considering its underhanded feature, is considered crucial.

Keywords:

Means of obtaining evidence; wiretapping; image capture; fundamental rights.

ABREVIATURAS E SIGLAS

al.	Alínea
ANEPC	Autoridade Nacional de Emergência e Proteção Civil
art.º	Artigo
arts.	Artigos
CC	Código Civil
CEDH	Convenção Europeia dos Direitos do Homem
Cfr.	Confrontar
cit.	Citado
CP	Código Penal
CPP	Código de Processo Penal
CRP	Constituição da República Portuguesa
DUDH	Declaração Universal dos Direitos Humanos
Disp.	Disponível em
ed.	Edição
Ex.	Exemplo
id.	Idem
JIC	Juízo de Instrução Criminal
LCC	Lei do Cibercrime
n.	Nota
nº	Número
nos	Números
OPC	Órgãos de polícia criminal
p.	Página
RGPD	Regulamento Geral de Proteção de Dados
ss.	Seguintes
UE	União Europeia
vol.	Volume

SUMÁRIO

INTRODUÇÃO

A matéria dos meios de obtenção de prova é fundamental no âmbito do processo penal, dado que, sem ela, é impossível proceder à recolha dos elementos essenciais para ser feita a prova do que realmente aconteceu, quer no sentido do cometimento do crime, como no sentido da sua não realização e, por inerência, facultando a possibilidade de o juiz decidir em conformidade.

Efetivamente, para se demonstrar o cometimento de um crime e, assim, sancionar alguém pelo seu ato é essencial que a investigação reúna provas legalmente admissíveis e em número e peso suficientes para convencer o Tribunal de que o arguido é, de facto, culpado.

Neste sentido, o Ministério Público pode muitas vezes ter a convicção de que um indivíduo em particular é responsável pelo cometimento de um crime, mas ser incapaz de demonstrar todos os elementos objetivos e subjetivos do tipo e demais elementos do crime através de provas legalmente admissíveis.

Assim, para obter as provas necessárias, o Ministério Público e os órgãos de polícia criminal (OPC) empregam uma variedade de poderes e procedimentos. São esses poderes e procedimentos, quando exercidos de forma adequada, que poderão possibilitar uma correta condenação de um arguido em Tribunal.

No entanto, na obtenção da prova, tanto o Ministério Público como os órgãos de polícia criminal estão sujeitos a um rigoroso cumprimento da lei, designadamente da lei constitucional, uma vez que uma condenação encerra, em si mesma, uma necessária restrição dos direitos fundamentais.

Neste sentido dispõe, desde logo, o art.º 18.º n.º 1 e n.º 2 da Constituição da República Portuguesa[1].

Concretizando o sentido do preceito constitucional, o art.º 125.º do Código de Processo Penal estabelece que apenas "São admissíveis as provas que não forem proibidas por lei"[2], que é o mesmo que dizer que todas as provas que violarem a lei são inválidas.

[1] Cfr. https://www.parlamento.pt/Legislacao/Paginas/ConstituicaoRepublicaPortuguesa.aspx (consultado a 05/03/2023)
[2] Cfr. https://dre.pt/dre/legislacao-consolidada/decreto-lei/1987-34570075 (consultado a 08/03/2023)

Neste sentido, o art.º 126.º, n. º 1 e 2 CPP enuncia que são nulas, não podendo ser utilizadas, as provas obtidas mediante tortura, coação ou, em geral, ofensa da integridade física ou moral das pessoas.

Concomitantemente, o n.º 3 do referido artigo esclarece ainda que, ressalvados os casos previstos na lei, são igualmente nulas, não podendo ser utilizadas, as provas obtidas mediante intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações sem o consentimento do respetivo titular[3].

O meio de obtenção de prova objeto do nosso estudo envolve a utilização do *malware*. De acordo com o Dicionário da Língua da Porto Editora, verificamos que *malware* é definido como o "*software* cujo objetivo é perturbar ou danificar um computador ou uma rede de computadores (é o caso dos vírus informáticos)"[4].

Neste sentido, se o *malware* se destina a prejudicar um computador ou rede de computadores, questiona-se: como pode o mesmo ser admitido no âmbito da investigação penal?

Ora, a verdade é que o uso de *malware* como meio de obtenção de provas aumentou nos últimos anos devido à sua eficácia para contrariar as medidas anti-forenses adotadas por criminosos no âmbito do cibercrime. Ademais, os crimes cometidos através de meios eletrónicos têm aumentado drasticamente, o que incentiva ao uso desta ferramenta do lado da investigação.

Sem prejuízo, o tema continua a suscitar imensas dúvidas, designadamente no que respeita à sua constitucionalidade.

Em face do exposto, com vista a um entendimento completo e sustentado do tema em apreço, entendemos pertinente dividir o presente estudo em seis capítulos distintos.

No primeiro capítulo faremos um enquadramento geral do tema, abordando os conceitos de investigação criminal em ambiente digital, tecnologias de informação e comunicação ao serviço da investigação criminal, os meios ocultos de investigação criminal e será ainda apresentada uma breve resenha histórica da evolução legislativa no que respeita à investigação criminal em ambiente digital.

[3] *Id*.
[4] Cfr. https://www.infopedia.pt/dicionarios/lingua-portuguesa/malware (consultado a 13/03/2023)

No segundo capítulo exploraremos o conceito de *malware*, as suas modalidades e mecanismos de utilização. Faremos uma distinção entre figuras afins, discutindo especificamente as denominadas de Cavalos de Troia, *logic bombs*, *spyware*, *keyloggers* e *screen loggers*, *rootkits*, vírus, *worms*, *blended threats* e *bots*.

No terceiro capítulo, focar-nos-emos nos direitos fundamentais e princípios constitucionais afetados por estes meios de prova ocultos. Abordaremos o direito à reserva da intimidade da vida privada, à palavra, à imagem, à inviolabilidade do domicílio, ao segredo das comunicações, à integridade e confidencialidade dos sistemas informáticos, bem como o princípio da proporcionalidade.

Depois do devido enquadramento, iniciamos no quarto capítulo uma abordagem aprofundada ao *malware* enquanto meio oculto de investigação criminal, sublinhando a sua relevância no nosso ordenamento jurídico e analisando detalhadamente os regimes jurídicos já em vigor (escutas telefónicas e Lei do Cibercrime, sistema de videovigilância, registo de voz e imagem e localização de celular) os quais poderão afetar, ainda que de forma menos invasiva, os mesmos direitos fundamentais a este meio de prova que aqui se apresenta.

No capítulo seguinte passamos a mencionar breves notas de direito comparado e bem assim algumas decisões jurisprudenciais, as quais se apresentam com bastante pertinência para o tema em apreço, designadamente com vista a ser possível verificar como os vários conceitos abordados se compaginam com a atuação prática.

Por último, no sexto capítulo discutiremos a possível abrangência dos regimes jurídicos abordados no capítulo IV a um futuro regime jurídico sobre o *malware* – que apresentamos. Neste, para além de referir os fundamentos basilares da sua concretização, faremos referências aos crimes por ele abrangidos, o procedimento e os órgãos responsáveis pela sua aplicação.

Cremos que, desta forma, será possível, para além de realizar uma análise aprofundada sobre os conceitos, as modalidades e as implicações jurídicas do *malware*, efetuar uma visão crítica sobre os meios ocultos de investigação criminal e os princípios do processo penal que possam estar neles envolvidos, bem como apresentar um regime jurídico consistente e proporcional aplicável no nosso ordenamento jurídico.

CAPÍTULO I- A INVESTIGAÇÃO CRIMINAL EM AMBIENTE DIGITAL

1- AS TECNOLOGIAS DE INFORMAÇÃO E COMUNICAÇÃO AO SERVIÇO DA INVESTIGAÇÃO CRIMINAL

O conceito de tecnologias de informação e comunicação é fundamental para entendermos como as informações são transmitidas e processadas no dia-a-dia.

Começando pela definição de telecomunicação, verificamos que a mesma abrange uma ampla variedade de processos técnicos que são essenciais para a obtenção, processamento, tratamento, conservação e transmissão de dados[5].

E, de acordo com André Inácio (2009, p. 61), o conceito de tecnologias de informação e comunicação abrange

> (…) todas as formas de tecnologias destinadas à criação, armazenamento, troca e utilização de informação nos seus diversos formatos, possibilitando a inclusão das tecnologias de computação e de telecomunicações num mesmo conceito, englobando para além do processamento de dados, os sistemas de informação, a engenharia de software e a informática, sem descurar o 'fator humano', questões administrativas e organizacionais. [6.]

A sociedade contemporânea tem experimentado os efeitos da globalização e das novas tecnologias de comunicação, os quais trazem consigo uma série de benefícios. Com efeito, as novas formas de comunicação têm contribuído positivamente em diversos âmbitos, tanto a nível económico, como educacional e cultural, superando obstáculos que antes pareciam intransponíveis.

Desde o término da Segunda Guerra Mundial, as barreiras ao comércio e às transações financeiras internacionais têm sido gradualmente eliminadas, impulsionando a liberalização e o desenvolvimento do comércio global. O colapso do bloco comunista, ocorrido nos anos 90, no antigo bloco oriental, incentivou o crescimento de novas economias de mercado livre e o aumento significativo dos fluxos transfronteiriços de pessoas, mercadorias e capitais.[7]

[5] Cfr. ANDRADE, Manuel da Costa (2009) – *Bruscamente no Verão passado, a reforma do Código de Processo Penal,* Coimbra Editora, p.146.
[6] Cfr. INÁCIO, André (2016) – *Tecnologias de Informação e Segurança Pública: Um Equilíbrio Instável*, Revista Científica Sobre Cyberlaw, CIJC, Faculdade de Direito de Lisboa, n.º 1, janeiro 2016, p. 61.
[7] Cfr. https://www.infopedia.pt/apoio/artigos/$muro-de-berlim (consultado a 06/04/2023)

No que diz respeito aos benefícios económicos, a globalização e as tecnologias de informação e comunicação permitiram a expansão do comércio internacional, possibilitando o acesso a novos mercados e a oferta de produtos e serviços diversificados, o que impulsionou o crescimento económico em muitos países, criando empregos, aumentando a produtividade e estimulando a inovação.

Do ponto de vista geral, a globalização e a conectividade digital abriram igualmente portas para o acesso ao conhecimento e à informação em tempo real. Através da *internet*, é hoje possível aprender e trocar experiências com pessoas de diferentes partes do mundo, em tempo real.

Também no contexto cultural a globalização tem possibilitado a disseminação e a diversificação das expressões artísticas e culturais, promovendo a interculturalidade e o diálogo entre diferentes tradições e identidades. As plataformas digitais permitem que produções culturais alcancem um público mais amplo e diversificado, promovendo a compreensão e a valorização da diversidade cultural.

No entanto, tanto a globalização como as novas tecnologias de informação e comunicação têm desafios e riscos, como a desigualdade económica, a exclusão digital ou a perda de identidade cultural. Assim, é fundamental adotar políticas e estratégias que promovam um desenvolvimento equitativo e inclusivo, garantindo que os benefícios da globalização sejam compartilhados por todos os indivíduos e comunidades.

Com o avanço e a popularização da informática, o número de utilizadores da *internet* em todo o mundo atingiu níveis sem precedentes, impulsionando a indústria de tecnologia da informação como uma fonte global de riqueza, com participação significativa tanto dos países desenvolvidos quanto dos em desenvolvimento.

Tal facto resultou na integração das economias nacionais num sistema global único, onde o desempenho das bolsas de valores e dos mercados de capitais representa um papel fundamental, afetando não apenas a economia, mas também a identidade cultural e social. Enquanto as barreiras ideológicas parecem cair, observamos a homogeneização económica, mas também a fragmentação política e social.[8]

[8] Cfr. https://www.incb.org/documents/Publications/AnnualReports/Thematic_chapters/English/AR_2001_E_Chapter_I.pdf (consultado a 06/04/2023)

Conforme se referiu já, todos estes factos contribuem para uma melhoria das condições de vida, mas também potenciam os riscos existentes, designadamente criando meios de proliferação de criminalidade.

Por conseguinte, também os mecanismos de investigação se têm de adaptar aos novos tempos, utilizando a tecnologia a seu favor.

Neste sentido, as tecnologias de informação e comunicação, sendo algo indissociável da atualidade e do dia-a-dia, têm desempenhado um papel cada vez maior na investigação criminal nos últimos anos, com as autoridades a utilizarem as referidas tecnologias para obter e analisar dados, identificar suspeitos, bem como, para reunir provas que são fundamentais para a resolução de crimes.

As tecnologias de informação e comunicação são utilizadas em diversas etapas da investigação criminal. Por exemplo, os órgãos de polícia criminal podem utilizar as redes sociais para identificar suspeitos ou analisar vídeos de câmaras de segurança para identificar veículos e pessoas envolvidas em crimes.

Por outro lado, as referidas tecnologias também são usadas para obter e armazenar provas, dado que a tecnologia forense permite a recuperação de dados de dispositivos eletrónicos, como telemóveis e computadores, que podem ser usados como prova no processo penal.

A análise de dados é outra área em que as tecnologias de informação e comunicação têm desempenhado um papel fundamental na investigação criminal, uma vez que os bancos de dados de informações criminais podem ser usados para identificar tendências e padrões que podem ajudar a prever onde e quando os crimes ocorrerão.

Também o âmbito da própria comunicação entre entidades responsáveis pela investigação é uma área em que as tecnologias de informação e comunicação são usadas. Os OPC podem usar sistemas de comunicação seguros para partilhar informações entre si, assim como com outras agências internacionais, o que pode ser particularmente útil em casos que envolvem organizações criminosas internacionais, onde a cooperação internacional é essencial para a resolução do crime.

No entanto, as tecnologias de informação e comunicação também apresentam desafios para a investigação criminal, sendo um desses grandes desafios o respeito por um conjunto de direitos fundamentais incluindo o direito à privacidade dos dados.

A título de exemplo, embora a recuperação de dados de dispositivos eletrónicos possa ser usada para ajudar na investigação criminal, também pode violar a privacidade dos indivíduos. Assim, os OPC necessitam de equilibrar a necessidade de obter prova com a necessidade de proteger a privacidade dos cidadãos, como sempre acontece no âmbito da investigação criminal e da descoberta da verdade material em processo penal.

Noutro âmbito, um dos grandes desafios que se tem apresentado cada vez mais complexo reporta-se à sofisticação das técnicas de criptografia e ao seu uso por parte de redes de crime organizado, o que torna a investigação criminal mais difícil e demorada.

2- OS MEIOS OCULTOS DE INVESTIGAÇÃO CRIMINAL

Na sequência dos desenvolvimentos tecnológicos que referimos, contata-se que a criminalidade organizada representa, na atualidade, uma ameaça significativa ao Estado de Direito Democrático.

A criminalidade organizada moderna é caracterizada por estruturas complexas, como redes globais de operações e realização de uma ampla gama de atividades ilícitas como tráfico de drogas, tráfico de seres humanos, branqueamento de capitais, lavagem de dinheiro, corrupção ativa ou passiva, extorsão, entre outras. As organizações criminosas estão cada vez mais adaptadas às novas tecnologias de informação e comunicação e, por conseguinte, têm cada vez mais capacidade de se imiscuírem em instituições governamentais, empresas e na sociedade em geral, minando a ordem social e comprometendo a segurança.[9]

A natureza transnacional da criminalidade organizada torna o seu combate um desafio bastante complexo, o qual requer cooperação internacional, partilha de informações, fortalecimento das capacidades de investigação e aplicação de medidas eficazes para desmantelar as referidas redes criminosas.

Conforme nos refere José Braz (2013, p. 296):

[9] Cfr. VALENTE, Manuel Monteiro Guedes (2017) - *Contributos para um Direito Penal Supranacional*, Ed. Abdul´s Angels, 2º ed., p. 30.

> A discussão e a estruturação do conceito crime organizado, dada a sua elevada subjetividade e natureza especulativa, tem lugar próprio na criminologia e na política criminal, onde os laboriosos esforços se têm desenvolvido no sentido de encontrar consensos quanto à definição de crime organizado ou de criminalidade organizada.[10]

De acordo com Cláudia Cruz Santos, existem três caraterísticas essenciais na caraterização do crime organizado, a saber:

- atividade permanente e racionalizada em moldes empresariais com intuito de obter lucro por meios ilícitos;
- a utilização (ou iminência de utilização) de violência;
- e a corrupção de funcionários — a que acrescerá, como consequência da globalização, a internacionalização.[11]

Por conseguinte, é necessário promover o fortalecimento do Estado de Direito, garantindo a aplicação eficaz da lei, a proteção dos direitos fundamentais, a prevenção da corrupção e a cooperação internacional para enfrentar a criminalidade organizada em todas as suas formas.

Neste sentido, as estratégias para enfrentar a criminalidade organizada têm evoluído para conseguirem acompanhar as mudanças nas táticas utilizadas pelas referidas organizações criminosas. E, uma das formas é, sem dúvida, a utilização de meios ocultos de investigação criminal.

Nas palavras de Eduardo Maia Costa (2014, p. 357), os meios ocultos de investigação são caraterizados, de forma genérica,

> pela utilização por parte da entidade investigadora de meios enganosos, dissimulados ou mesmo insidiosos contra a pessoa investigada que, assim (…), age espontaneamente, 'inocentemente', entregando informações e provas aos investigadores, ou praticando actos ilícitos, ou tendencialmente ilícitos, comportamentos esses que não assumiria se tivesse conhecimento do engano.[12]

Estes métodos de investigação visam possibilitar que a pessoa investigada atue espontaneamente, com vista a entregar informações ou a praticar atos ilícitos, os quais seguramente não ocorreriam se a mesma tivesse conhecimento que se encontrava a ser investigada.

[10] Cfr. BRAZ, José (2013) – *Investigação Criminal: A organização, o método e a prova: os desafios da nova criminalidade*. 3ª ed, Coimbra: Almedina, p. 296.
[11] Cfr. SANTOS, Cláudia Cruz (2001) – *O Crime de Colarinho Branco*, Stvdia Ivridica 56, Coimbra, pp. 88 e 87.
[12] Cfr. COSTA, Eduardo Maia (2014) – *Acções Encobertas (Alguns Problemas, Algumas Sugestões)*, Estudos em Memória do Conselheiro Artur Maurício, Coimbra Editora, p. 357.

Como exemplos de métodos ocultos podemos referir as intercetações e escutas telefónicas, bem como as escutas ambientais através da recolha de imagem e/ou som de pessoas, a utilização de agentes encobertos ou a localização celular[13].

De acordo com Manuel da Costa Andrade (2009, p. 105), os métodos ocultos de investigação são:

> Aqueles métodos que representam uma intromissão nos processos de ação, inteiração, informação e comunicação das pessoas concretamente visadas, sem que as mesmas disso tenham consciência, conhecimento ou disso sequer se apercebam.[14]

E, conforme salienta João Gouveia de Caires (2019, p. 51 e 52):

> As características dos métodos ocultos são a intrusão desconhecida na esfera do visado (o que pressupõe uma atuação dissimulada ou desconhecimento intencional por parte dos poderes públicos), a deslealdade (que não deixa espaço de liberdade ao visado para, querendo, definir os fins da sua acção) e, no limite, a suscetibilidade de corroer os fundamentos do Estado de Direito Democrático (levando a que o Estado se comporte como mais uma permissão de actuação que o mesmo define a cada momento —, transformando o arguido em mero objeto de prova, deixando para a insustentável leveza retórica o estatuto de sujeito processual). É, ainda, atributo destes métodos a restrição intensa de direitos fundamentais, nomeadamente, de direitos, liberdades e garantias fundamentais quer num plano substantivo (v.g., o direito à intimidade e privacidade, à transitoriedade da palavra falada, à imagem, à inviolabilidade do domicílio, etc.), quer num plano adjetivo (v.g., o direito a um processo justo e equitativo, o contraditório, o nemo tenetur se ipsum accusare, a lealdade, etc.).[15]

A este propósito importa referir que, na utilização de meios ocultos de investigação criminal, nunca poderá ser o investigador a levar o investigado a praticar o crime, caso em que estaríamos perante a figura do agente provocador[16] (a qual não é admissível nos termos legais).[17]

---

[13] Cfr. CAIRES, João Gouveia de – *Métodos Ocultos na Criminalidade Económico-Financeira: entre a (A)Tipicidade e a Cumulação*, p. 52, Disp. *in* http://julgar.pt/wp-content/uploads/2019/05/JULGAR38-04-JC.pdf (consultado a 15/04/2023)

[14] Cfr. ANDRADE, Manuel da Costa (2009) – *Bruscamente no Verão passado, a reforma do Código de Processo Penal,* Coimbra Editora, p.105.

[15] Cfr. CAIRES, João Gouveia de – *Métodos Ocultos na Criminalidade Económico-Financeira: entre a (A)Tipicidade e a Cumulação*, p. 51 e 52, Disp. *in* http://julgar.pt/wp-content/uploads/2019/05/JULGAR38-04-JC.pdf (consultado a 17/10/2023)

[16] Sobre este conceito, Fernando Gonçalves, Manuel João Alves e Manuel Monteiro Guedes Valente salientam o Acórdão do Tribunal Europeu dos Direitos do Homem, Caso Teixeira de Castro c. Portugal (44/1997/828/1034) de 9 de Junho de 1998, no qual foi condenado o Estado português a pagar uma indemnização de dez milhões de escudos a um cidadão português, condenado pelos tribunais portugueses por tráfico de droga, «...por concluir que os agentes da PSP, aí referidos, com ocultação da sua qualidade, ao procederem à detenção do cidadão, no momento em que lhes entregou certa porção de heroína, que insistiram comprar, não atuaram como agentes infiltrados, mas sim como verdadeiros agentes provocadores do crime», Cfr. GONÇALVES, Fernando; ALVES, Manuel João; e VALENTE, Manuel Monteiro Guedes (2001) – *Lei e Crime, Lei e Crime - O Agente Infiltrado Versus o Agente Provocador - Os Princípios do Processo Penal*, Almedina, Coimbra, pp. 262 e ss.

[17] Sob pena de estarmos perante a verificação do preconizado no art.º 126.º do Código de Processo Penal:

Assim, o uso de meios ocultos de investigação é ainda um assunto controverso, pois levanta questões éticas e legais sobre a invasão de privacidade e os limites da atuação dos investigadores. Neste sentido, é fundamental encontrar um equilíbrio entre a necessidade de realizar investigações eficientes e a proteção dos direitos e privacidade das pessoas investigadas, por forma a tentar minimizar ao máximo o impacto nos direitos fundamentais dos visados.[18]

3- BREVE RESENHA HISTÓRICA DA EVOLUÇÃO LEGISLATIVA NO QUE RESPEITA À INVESTIGAÇÃO CRIMINAL EM AMBIENTE DIGITAL

Nas palavras de Jorge Reis Novais (2010, p. 295):

> A protecção juridicamente garantida pelos direitos fundamentais evolui, neste sentido, à medida da própria evolução e aperfeiçoamento das instituições de Estado de Direito. Começou, no Estado liberal, por se resumir a uma defesa contra a actuação ilegal da Administração; desenvolveu-se, nos primórdios do Estado social de Direito, através da consagração constitucional dos direitos sociais e através da garantia, também contra o legislador, de um núcleo essencial dos direitos fundamentais como valores, e prolonga-se, hoje, numa garantia plena contra quaisquer prejuízos da liberdade provocados pelo Estado.[19]

E, de acordo com Maria Lúcia Amaral (2012, p. 94), "(…) a unidade do ordenamento jurídico positivo é realizada, isto é, construída e reconstruída, tendo sempre a Constituição como ponto de partida e como ponto de chegada".[20]

Métodos proibidos de prova
1 - São nulas, não podendo ser utilizadas, as provas obtidas mediante tortura, coacção ou, em geral, ofensa da integridade física ou moral das pessoas.
2 - São ofensivas da integridade física ou moral das pessoas as provas obtidas, mesmo que com consentimento delas, mediante:
a) Perturbação da liberdade de vontade ou de decisão através de maus-tratos, ofensas corporais, administração de meios de qualquer natureza, hipnose ou utilização de meios cruéis ou enganosos;
b) Perturbação, por qualquer meio, da capacidade de memória ou de avaliação;
c) Utilização da força, fora dos casos e dos limites permitidos pela lei;
d) Ameaça com medida legalmente inadmissível e, bem assim, com denegação ou condicionamento da obtenção de benefício legalmente previsto;
e) Promessa de vantagem legalmente inadmissível, Cfr. https://dre.pt/dre/legislacao-consolidada/decreto-lei/1987-34570075 (consultado a 11/04/2023)

[18] Cfr. ASTORGA, Paula Celeste Moreira Cardoso (2014) - *Escutas telefónicas*, Coimbra, Universidade de Coimbra, p. 1.

[19] Cfr. NOVAIS Jorge Reis (2010) – *As restrições aos Direitos Fundamentais não expressamente autorizadas pela Constituição*, 2ª ed, Coimbra Editora, Coimbra, p. 295.

[20] Cfr. AMARAL, Maria Lúcia (2012) – *A Forma da República - Uma Introdução ao Estudo do Direito Constitucional*, Reimpressão, Coimbra, Coimbra Editora, Outubro, p. 94.

Neste sentido, com o avanço das novas tecnologias, o qual revolucionou diversos aspetos da vida e abriu um mundo de possibilidades e experiências antes inimagináveis, surgem também novos riscos e perigos no que respeita aos direitos fundamentais.[21] O avanço tecnológico tem transformado o mundo, trazendo consigo desafios e oportunidades. Neste sentido, o direito processual penal só poderá ser considerado eficaz, seguro e eficiente se estiver em conformidade com os direitos fundamentais e conseguir acompanhar as exigências do mundo tecnológico.

Neste sentido, conforme salienta Oliveira Ascensão (2001, p. 85), "a investigação criminal teve, necessariamente, que se adaptar à evolução da sociedade e das evoluções tecnológicas, criando mecanismos profissionais e modernos, afastando-se do amadorismo dos finais do séc. XX".[22]

O uso de tecnologias no âmbito da investigação penal permite agilizar procedimentos, conceder uma maior segurança às informações e proporcionar uma maior eficiência na busca da verdade material. No entanto, é essencial que exista uma compatibilização adequada entre essas inovações e os direitos fundamentais dos indivíduos, como o direito à privacidade e vida privada e à presunção de inocência.

Além disso, as novas exigências do mundo tecnológico requerem que os profissionais estejam atualizados e capacitados para lidar com questões relacionadas à cibersegurança, à proteção de dados e à utilização de provas digitais.

É necessário um equilíbrio entre a utilização das tecnologias no âmbito processual penal e a garantia dos direitos fundamentais, para que o sistema seja eficiente, justo e confiável e possa promover a segurança jurídica e o respeito aos princípios democráticos na era digital.

Posto isto, em termos de evolução histórica, podemos referir a revisão de 2007 do Código de Processo Penal, o qual veio estabelecer analogia entre o regime das escutas telefónicas e outras comunicações eletrónicas, como e-mails ou mensagens de texto (SMS).

[21] Cfr. LEITÃO, Maria Da Glória (2012) - *A Admissibilidade como meio de prova em processo disciplinar das mensagens de correio eletrónico enviadas e recebidas por trabalhador a partir de e na caixa de correio fornecida pela entidade empregadora*, Colóquio no STJ, Lisboa, 10 Outubro de 2012, p. 1, disp. *in* https://www.yumpu.com/pt/document/view/12858820/adv-maria-da-gloria-leitao-supremo-tribunal-de-justica (consultado a 23/04/2023)

[22] Cfr. ASCENSÃO, Oliveira (2001) – *Estudos sobre Direito da Internet e da Sociedade de Informação*, Coimbra, Almedina, p. 85

Na versão antes de 2007 o referido art.º 189.º apenas dispunha que "todos os requisitos e condições referidos nos artigos 187.º e 188.º são estabelecidos sob pena de nulidade".[23]

Com a Lei n.º 48/2007, de 29 de agosto, o art.º 189.º CPP veio estender o alcance do regime das escutas telefónicas, passando a dispor:

> 1 - O disposto nos artigos 187.º e 188.º é correspondentemente aplicável às conversações ou comunicações transmitidas por qualquer meio técnico diferente do telefone, designadamente correio eletrónico ou outras formas de transmissão de dados por via telemática, mesmo que se encontrem guardadas em suporte digital, e à interceção das comunicações entre presentes.
>
> 2 - A obtenção e junção aos autos de dados sobre a localização celular ou de registos da realização de conversações ou comunicações só podem ser ordenadas ou autorizadas, em qualquer fase do processo, por despacho do juiz, quanto a crimes previstos no n.º 1 do artigo 187.º e em relação às pessoas referidas no n.º 4 do mesmo artigo.[24]

Por via desta revisão legal, o regime das escutas telefónicas passou a aplicar-se também às conversas realizadas por meio de computadores ou outros sistemas com armazenamento digital. Assim, seja por meio de escutas telefónicas, SMS ou e-mails, o conteúdo dessas comunicações, ou seja, a conversa que possa indicar a prática de um crime, pode ser um elemento probatório relevante.

Um ano após a referida lei, tivemos a aprovação da Lei n.º 32/2008, de 17 de julho[25], a qual traspôs para a ordem jurídica interna a Diretiva n.º 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de março, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações.

Esta lei visou regular a conservação e a transmissão dos dados de tráfego e de localização relativos a pessoas singulares e a pessoas coletivas, bem como dos dados conexos necessários para identificar o assinante ou o utilizador registado, para fins de investigação, deteção e repressão de crimes graves por parte das autoridades competentes, transpondo para a ordem jurídica interna a Diretiva n.º 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de março, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas

[23] Cfr. :::DL n.º 78/87, de 17 de Fevereiro (pgdlisboa.pt) (consultado a 18/04/2023)
[24] Cfr. https://files.dre.pt/1s/2007/08/16600/0584405954.pdf (consultado a 20/04/2023)
[25] Cfr. Lei n.º 32/2008 | DR (diariodarepublica.pt) (consultado a 21/04/2023)

publicamente disponíveis ou de redes públicas de comunicações, e que alterou a Diretiva n.º 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de junho, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas.

Já em 2009 tivemos a aprovação da chamada Lei do Cibercrime (Lei n.º 109/2009, de 15 de setembro)[26], a qual transpôs para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de fevereiro, relativa a ataques contra sistemas de informação, e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa.

Esta lei veio estabelecer as disposições penais materiais e processuais, assim como as disposições relativas à cooperação internacional em matéria penal, relativas ao domínio do cibercrime e da recolha de prova em suporte eletrónico, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de fevereiro[27], relativa a ataques contra sistemas de informação, e adaptando o direito interno à Convenção sobre Cibercrime do Conselho da Europa.

Concretamente, a Lei do Cibercrime estabelece a previsão legal de crimes materiais, mas também de normas processuais que possibilitam a interceção de comunicações em casos relacionados a crimes previstos na própria lei ou cometidos por meio de sistemas informáticos quando previstos no art.º 187.º do Código de Processo Penal[28], cujo conteúdo e alcance analisaremos em pormenor mais à frente.

---

[26] Cfr. https://dre.pt/dre/detalhe/lei/109-2009-489693 (consultado a 04/05/2023)

[27] Cfr. https://op.europa.eu/en/publication-detail/-/publication/708d86d8-ab9a-4e18-9bda-ac37405a3185/language-pt (consultado a 06/05/2023)

[28] Para mais fácil entendimento:
Artigo 187.º CPP
Admissibilidade de Escutas Telefónicas
1 - A interceção e a gravação de conversações ou comunicações telefónicas só podem ser autorizadas durante o inquérito, se houver razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter, por despacho fundamentado do juiz de instrução e mediante requerimento do Ministério Público, quanto a crimes:
a) Puníveis com pena de prisão superior, no seu máximo, a 3 anos;
b) Relativos ao tráfico de estupefacientes;
c) De detenção de arma proibida e de tráfico de armas;
d) De contrabando;
e) De injúria, de ameaça, de coação, de devassa da vida privada e perturbação da paz e do sossego, quando cometidos através de telefone;
f) De ameaça com prática de crime ou de abuso e simulação de sinais de perigo; ou
g) De evasão, quando o arguido haja sido condenado por algum dos crimes previstos nas alíneas anteriores.
2 - A autorização a que alude o número anterior pode ser solicitada ao juiz dos lugares onde eventualmente se puder efetivar a conversação ou comunicação telefónica ou da sede da entidade competente para a investigação criminal, tratando-se dos seguintes crimes:
a) Terrorismo, criminalidade violenta ou altamente organizada;
b) Sequestro, rapto e tomada de reféns;

De acordo com a referida Lei do Cibercrime, a autorização para a interceção e registo de transmissões de dados informáticos apenas poderá ocorrer durante o inquérito, mediante requerimento do Ministério Público e por despacho fundamentado do juiz de instrução, se existirem razões para acreditar que a referida diligência é indispensável para descobrir a verdade ou se a prova for difícil ou impossível de obter de outra forma.

Em termos concretos, a interceção pode visar o registo do conteúdo das comunicações ou apenas a obtenção e registo de dados de tráfego, consoante a necessidade da investigação, devendo o despacho do juiz especificar o âmbito dessa interceção.

c) Contra a identidade cultural e integridade pessoal, previstos no título iii do livro ii do Código Penal e previstos na Lei Penal Relativa às Violações do Direito Internacional Humanitário;
d) Contra a segurança do Estado previstos no capítulo i do título v do livro ii do Código Penal;
e) Falsificação de moeda ou títulos equiparados a moeda prevista nos artigos 262.º, 264.º, na parte em que remete para o artigo 262.º, e 267.º, na parte em que remete para os artigos 262.º e 264.º do Código Penal, bem como contrafação de cartões ou outros dispositivos de pagamento e uso de cartões ou outros dispositivos de pagamento contrafeitos, previstos no artigo 3.º-A e no n.º 3 do artigo 3.º-B da Lei n.º 109/2009, de 15 de setembro;
f) Abrangidos por convenção sobre segurança da navegação aérea ou marítima.
3 - Nos casos previstos no número anterior, a autorização é levada, no prazo máximo de setenta e duas horas, ao conhecimento do juiz do processo, a quem cabe praticar os actos jurisdicionais subsequentes.
4 - A interceção e a gravação previstas nos números anteriores só podem ser autorizadas, independentemente da titularidade do meio de comunicação utilizado, contra:
a) Suspeito ou arguido;
b) Pessoa que sirva de intermediário, relativamente à qual haja fundadas razões para crer que recebe ou transmite mensagens destinadas ou provenientes de suspeito ou arguido; ou
c) Vítima de crime, mediante o respectivo consentimento, efectivo ou presumido.
5 - É proibida a intercepção e a gravação de conversações ou comunicações entre o arguido e o seu defensor, salvo se o juiz tiver fundadas razões para crer que elas constituem objecto ou elemento de crime.
6 - A intercepção e a gravação de conversações ou comunicações são autorizadas pelo prazo máximo de três meses, renovável por períodos sujeitos ao mesmo limite, desde que se verifiquem os respectivos requisitos de admissibilidade.
7 - Sem prejuízo do disposto no artigo 248.º, a gravação de conversações ou comunicações só pode ser utilizada em outro processo, em curso ou a instaurar, se tiver resultado de intercepção de meio de comunicação utilizado por pessoa referida no n.º 4 e na medida em que for indispensável à prova de crime previsto no n.º 1.
8 - Nos casos previstos no número anterior, os suportes técnicos das conversações ou comunicações e os despachos que fundamentaram as respectivas intercepções são juntos, mediante despacho do juiz, ao processo em que devam ser usados como meio de prova, sendo extraídas, se necessário, cópias para o efeito.

CAPÍTULO II- *MALWARE* - CONCEITO E MODALIDADES

1- DISTINÇÃO DE FIGURAS AFINS

No âmbito das novas tecnologias de informação e comunicação, é comum depararmo-nos com diversos conceitos cuja semelhança fonética leva a muitas confusões conceptuais.

Entre esses termos, podemos destacar o *malware* (cujo conteúdo e alcance abordaremos em pormenor adiante), *software*, *hardware*, *middleware* e diferentes tipos de *softwares*, como *freeware*, *shareware*, *crippleware* e *demoware*.

Começando pelo termo *malware*, verificamos que o seu significado é resultado da junção dos termos "malicioso" e "*software*".[29]

Ora, o *malware* é um tipo de programa de computador desenvolvido com a intenção de causar danos, explorar vulnerabilidades ou obter acesso não autorizado a sistemas e informações pessoais, ou seja, é um programa criado com intenções maliciosas, pelo que, deve ser evitado para proteger a segurança dos sistemas.

Já o conceito de *software* consubstancia um termo amplo que engloba os programas de computador, aplicações e instruções eletrónicas que permitem que um dispositivo informático realize tarefas específicas. Em concreto, existem dois tipos principais de *software*: o *software* de sistema e o *software* de aplicação. O primeiro, enquanto sistema operacional, controla e gere os recursos do computador, enquanto o segundo (*software* de aplicação), pode atuar como processador de texto e navegadores da *web*, sendo projetado para realizar tarefas específicas para os utilizadores.[30]

Paralelamente, ao contrário do *software*, o *hardware* reporta-se aos componentes físicos de um computador ou dispositivo eletrónico e inclui componentes como processadores, memória, placas-mãe, discos rígidos, monitores, teclados ou rato. O

[29] Cfr. RAMALHO, David Silva (2015) – *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, *Dissertação de Mestrado em Direito, Especialidade de Ciências Jurídico-Criminais, Lisboa, Faculdade de Direito da Universidade de Lisboa, p. 201.*
30 Cfr. HUMPHREY, Watts (1989) – Managing the Software Process. Addison Wesley, p. 17.

hardware é a parte tangível e física do sistema informático, sendo essencial para o funcionamento dos *softwares.*[31]

O *middleware* é um tipo de *software* que atua como uma camada intermédia entre o sistema operativo e o *software* de aplicação, facilitando a comunicação e a integração entre diferentes componentes de *software* e *hardware*. Neste sentido, o *middleware* é projetado para simplificar o desenvolvimento de aplicativos e melhorar a interoperabilidade entre sistemas heterogéneos.[32]

Paralelamente ao já referido, podemos ainda enunciar vários tipos de concretos *software*.

Temos o *freeware*, o qual se reporta a *softwares* que são disponibilizados gratuitamente para uso pessoal e que, geralmente, podem ser distribuídos sem restrições, não obstante serem protegidos por direitos de autor, pelo que, a sua distribuição comercial sem autorização é proibida[33].

Paralelamente, temos o *shareware*, que é um tipo de *software* que distribuído gratuitamente para uso experimental por um período limitado. Por recurso ao *shareware*, os utilizadores podem experimentar o *software* antes de decidir se desejam adquirir a sua versão completa, geralmente mediante pagamento de um valor. Por conseguinte, o *shareware* incentiva os utilizadores a testarem o *software* antes da compra.[34]

Por seu turno, o *crippleware* é um tipo de *software* que oferece uma versão gratuita ou de avaliação com recursos limitados. A sua intenção é fornecer acesso a apenas alguns conteúdos do *software*, pelo que, apresenta funcionalidades restritas ou desativadas. A ideia do recurso ao *crippleware* é que os utilizadores se sintam incentivados a comprar a versão completa para desbloquear todos os recursos.[35]

Por último, cumpre ainda fazer uma breve referência ao *demoware*, que é um *software* que oferece uma versão de demonstração de um produto ou serviço, sendo usado para

---

[31] Cfr. KUTSCHER, Vladimir; MARTINS, Thiago Weber; OLBORT, Johannes; ANDERL, Reiner (2021) – *Concept for Interaction of Hardware Simulation and Embedded Software in a Digital Twin Based Test Environment*, Procedia CIRP, Volume 104, 2021, pp. 999 a 1004.
[32] Cfr. LIM, K. Y. H., ZHENG, P., e CHEN, C.-H. (2020) – *A state-of-the-art survey of Digital Twin: techniques, engineering product lifecycle management and business innovation perspectives*. Journal of Intelligent Manufacturing, 31(6), pp. 1313 a 1337.
[33] Cfr. LEE, Y. e TAN, Y. (2008) – *Making Money with Free Software? Sampling Implications of Software Market*. Entrepreneurship & Law eJournal.
[34] Cfr. SWOBODA, W., GÖTTLER, M., ZINNHOBLER, K. e HASFORD, J. (2001) – *Putting the Pieces Together: Using "Off-The-Shelf" Software to Safely Transfer Medical Data*. Methods of Information in Medicine, 40, pp. 236 a 240.
[35] Cfr. https://www.collinsdictionary.com/dictionary/english/crippleware (consultado a 5/04/2023).

apresentar as capacidades do *software*, possibilitando que os utilizadores testem as suas funcionalidades (não obstante algumas limitações) antes de tomar uma decisão final de aquisição.[36]

2- O CONCEITO DE *MALWARE*

A fim de conseguirmos obter uma visão o mais aprofundada e abrangente possível do assunto que pretendemos abordar, é crucial que dediquemos um capítulo à apreciação de conceitos técnicos.

Ora, conforme nos refere John Aycock, *malware* é um tipo de *software* malicioso, sendo o seu conceito usado para descrever programas de computador maliciosos criados com a intenção de prejudicar, danificar ou explorar ilegitimamente sistemas e dispositivos eletrónicos.[37]

Nas palavras de Bosworth, Kabay e Whyne (2014, p. 272), o *malware* é entendido como "um *software* projetado para danificar ou controlar computadores ou redes de computadores, ou roubar informações confidenciais do utilizador sem o seu conhecimento ou consentimento".[38]

Procurando clarificar definitivamente o conceito de *malware*, David Silva Ramalho (2015, p. 201 e 202) define o mesmo como:

> Um conjunto de instruções executadas no computador que levam o sistema a fazer algo que um atacante quer que ele faça". Neste sentido, para o referido autor, estamos perante "um programa simples ou autorreplicativo que discretamente se instala num sistema de processamento de dados sem o conhecimento ou consentimento do utilizador, com vista a colocar em perigo a confidencialidade dos dados, a integridade dos dados e a disponibilidade do sistema ou para assegurar que o utilizador seja incriminado por um crime informático.[39]

[36] Cfr. https://www.yourdictionary.com/demoware (consultado a 5/04/2023).
[37] Cfr. AYCOCK, John (2006) – *Computer Viruses and Malware*, Advances in Information Security 22, pp. 6 a 12.
[38] Cfr. BOSWORTH, Seymour; KABAY, M. E.; WHYNE, Eric (2014) – *Computer Security Handbook*. 6th ed. Hoboken, NJ: John Wiley & Sons, Inc., p. 272.
[39] Cfr. RAMALHO, David Silva (2015) – *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, Dissertação de Mestrado em Direito, Especialidade de Ciências Jurídico-Criminais, Lisboa, Faculdade de Direito da Universidade de Lisboa, pp. 201 e 202.

Já Paulo Pinto de Albuquerque utiliza o conceito de busca *online* para analisar o conceito de *malware*, salientando que o mesmo se refere ao ato de infiltração eletrónica em sistemas informáticos usando *softwares* maliciosos, como os denominados Cavalos de Troia, tendo como objetivo permitir que a pessoa em causa obtenha acesso, em tempo real ou posteriormente, às informações que estão a ser ou foram previamente inseridas nesse sistema.[40]

Por seu turno, Manuel de Andrade afirma que a busca *online*, não sendo um conceito fechado/imutável, é um conceito amplo que se refere às atividades de interferência nos sistemas informáticos por meio da *internet*, como observação, pesquisa, cópia, vigilância e outras ações relacionadas à obtenção de dados presentes no sistema em questão.[41]

No mundo digital, é possível utilizar técnicas de *hacking*[42] para obter acesso não autorizado a sistemas informáticos e a busca *online* é uma dessas técnicas, na qual os invasores utilizam *software* malicioso, como Cavalos de Troia, para se infiltrar nos sistemas alvo.

Ora, um Cavalo de Troia é um tipo de *malware* que se disfarça como um programa legítimo, enganando os utilizadores, levando-os a fazer o seu *download* ou a executá-lo e, uma vez que o Cavalo de Troia é ativado no sistema, permite ao invasor acesso remoto e controlo do computador afetado.[43] Ao realizar a busca *online*, o invasor pode monitorizar em tempo real a atividade ou recuperar posteriormente as informações que são inseridas no sistema comprometido, podendo ter acesso a senhas, mensagens, dados pessoais e outras informações confidenciais.[44]

Esta prática consubstancia uma violação séria da privacidade e da segurança de dados, sendo por isso ilegal e amplamente condenada em todo o mundo. Neste sentido, empresas e cidadãos devem adotar medidas de segurança robustas para protegerem os seus sistemas contra tais ameaças e garantir a privacidade e integridade das informações armazenadas nos seus computadores. Além disso, é essencial estar ciente

[40] Cfr. ALBUQUERQUE, Paulo Pinto de (2008) – *Comentário do Código de Processo Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem*, 2.ª ed., Lisboa, Universidade Católica Editora, p. 502.
[41] Cfr. ANDRADE, Manuel da Costa (2009) – *Bruscamente no Verão passado, a reforma do Código de Processo Penal*, Coimbra Editora, p. 166.
[42] Cfr. https://www.kaspersky.com.br/resource-center/definitions/what-is-hacking (consultado a 21/01/2023).
[43] Cfr. JIN, C., WANG, X., & TAN, H. (2010) – *Dynamic Attack Tree and Its Applications on Trojan Horse Detection*. Second International Conference on Multimedia and Information Technology, 1, pp. 56 a 59;
[44] Cfr. HODKINSON, Alan (2020) – *Fundamental British Values. International Review of Qualitative Research*, 13, pp. 23 a 40.

dos perigos existentes no mundo *online* e tomar precauções para evitar a infiltração de *software* malicioso nos seus sistemas.

Concretamente, o *malware* pode ser desenvolvido para realizar uma variedade de atividades indesejáveis pelos utilizadores legítimos, como roubar informações pessoais, causar danos aos dados, controlar dispositivos remotamente, espiar atividades do utilizador, interromper o funcionamento normal dos sistemas, exibir anúncios indesejados ou até mesmo extorquir dinheiro dos utilizadores.[45]

O *malware* pode ser distribuído de diversas maneiras, incluindo *downloads* de *sites* não confiáveis, anexos de e-mails maliciosos, mensagens instantâneas infetadas, *links* enganosos e até mesmo através de dispositivos de armazenamento removíveis. Paralelamente, cumpre referir que, à medida que a tecnologia se desenvolve, os criadores de *malware* também se tornam mais sofisticados, utilizando técnicas como engenharia social e exploração de vulnerabilidades para infetar os sistemas.

Para conseguir criar proteção adequada contra o *malware*, é essencial adotar medidas de segurança, como manter o sistema operacional e os aplicativos atualizados, utilizar um programa antivírus confiável, evitar clicar em *links* suspeitos ou proceder ao *download* arquivos de fontes não confiáveis, bem como, estar atento a possíveis sinais de infeção, como lentidão do sistema, comportamento estranho ou perda de dados. A consciencialização e a realização de boas práticas segurança cibernética são fundamentais para prevenir a infeção por *malware* e para proteger a privacidade e a integridade dos sistemas e dispositivos.[46]

No que respeita às modalidades, podemos afirmar que existem vários tipos de *malware*, incluindo Cavalos de Troia, *logic bombs*, *spyware*, *keyloggers* e *screen loggers*, *rootkits*, vírus, *worms*, *blended threats* e *bots*, aspetos que analisaremos em seguida.

[45] Cfr. LIGH, Michael; ADAIR, Steven; HARTSTEIN, Blake; RICHARD, Matthew (2010) – *Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code*. 1st ed. Indianapolis: Wiley Publishing, Inc.
[46] Cfr. SCHWARZ, M., WEISER, S., GRUSS, D., MAURICE, C. e MANGARD, S. (2020) – *Malware Guard Extension: abusing Intel SGX to conceal cache attacks*. Cybersecurity, 3, pp. 1 a 20.

3- MODALIDADES E MECANISMOS DE UTILIZAÇÃO DE *MALWARE*

Conforme já se aflorou, o *malware* representa uma ameaça séria e bastante perigosa para a segurança dos sistemas informáticos, podendo causar danos significativos nos mesmos. Em concreto, como já se referiu atrás, estamos perante uma forma de *software* malicioso desenvolvido para ser possível a infiltração e o comprometimento de sistemas de computador, com o intuito de roubar informações, danificar arquivos, espionar atividades ou até mesmo tomar controle remoto.

Esta ferramenta maligna é usada por criminosos cibernéticos numa variedade de formas, representando uma violação de privacidade e segurança, podendo resultar em perdas financeiras, roubo de identidade e interrupção de serviços essenciais, pelo que, conforme salienta Sergio Toral, é fundamental estar alerta e consciente dos riscos para adotar medidas preventivas para proteger-se contra essa ameaça persistente.[47]

3.1- CAVALOS DE TROIA

Para entendermos o que são os Cavalos de Troia no âmbito do *malware*, é necessário saber o que foi a história do Cavalo de Troia.

A história do Cavalo de Troia é um dos episódios mais famosos da mitologia grega, sendo narrado na épica obra de Homero, a Ilíada, o que ocorre durante a Guerra de Troia, quando os gregos e os troianos estavam envolvidos num conflito prolongado. Após dez anos de cerco, os gregos estavam desesperados para conquistar a cidade de Troia, sabendo que não o conseguiriam numa guerra "mano a mano".[48]

Assim, os gregos conceberam um plano engenhoso. Construíram um enorme cavalo de madeira oco, o "Cavalo de Troia", e esconderam um grupo de guerreiros gregos no seu interior. Depois de concluído, os gregos fingiram retirar-se, deixando o cavalo como um presente para os troianos. Ora, o engano tinha como objetivo fazer os troianos acreditarem que os gregos haviam desistido da guerra. No entanto, um soldado grego permaneceu próximo às muralhas da cidade e enganou os troianos, dizendo que o cavalo era um presente para agradar aos deuses.[49]

---

[47] Cfr. TORAL, Sergio (2009) – *Estudo comparativo de técnicas antimalware*, Revista Iberoamericana de Tecnologías del Aprendizaje 4.3, pp. 26 a 31.
[48] Cfr. https://www.infopedia.pt/apoio/artigos/$o-cavalo-de-troia (consultado a 05/02/2023).
[49] *Id*.

Intrigados e vendo-o como um sinal de vitória, os troianos decidiram levar o cavalo para dentro das muralhas de Troia. No meio da noite, quando todos estavam desprevenidos e celebrando a aparente vitória, os guerreiros gregos saíram do cavalo, abriram as portas da cidade para o exército grego, que havia voltado secretamente, e iniciaram um ataque surpresa. A cidade de Troia foi invadida e destruída, encerrando assim a guerra. Neste sentido, o Cavalo de Troia simboliza a astúcia e a traição, dado que, os troianos pagaram um preço alto pela sua ingenuidade e confiança na aparência benigna do presente.

Os Cavalos de Troia, também conhecidos como *trojans*, são um tipo insidioso de *malware*, os quais foram batizados com este nome devido à famosa história do Cavalo de Troia na mitologia grega. Assim como o lendário cavalo de madeira que escondia soldados gregos, os Cavalos de Troia enganam os utilizadores ao se disfarçarem como arquivos ou programas legítimos, levando-os a abrir as portas para a infeção.

Os Cavalos de Troia são projetados para executar ações maliciosas sem o conhecimento ou consentimento do utilizador, podendo roubar informações pessoais, como senhas, números de cartões de crédito e dados bancários, fornecendo o seu acesso a criminosos cibernéticos. Além disso, os Cavalos de Troia podem fornecer acesso remoto ao sistema comprometido, permitindo que os invasores controlem o computador da vítima para realizar atividades prejudiciais.[50]

Os Cavalos de Troia podem disseminar-se por várias formas, como anexos de *e-mail*, *downloads* de *sites* não confiáveis ou até mesmo através de dispositivos USB infetados, sendo altamente versáteis e podendo assumir diferentes formas, como programas aparentemente inofensivos, atualizações falsas do *software* ou até mesmo jogos populares. Em suma, podemos dizer que os Cavalos de Troia são um tipo de *software* malicioso que se faz passar por um programa confiável, enganando os utilizadores para que procedam à sua utilização e/ou *download*.

De acordo com Jonathan Clough, a caraterística que mais diferencia os Cavalos de Troia de outros tipos de *malware* é o facto de que os mesmos se espalham principalmente através da interação social, ou seja, os utilizadores precisam interagir com o Cavalo de Troia, seja por via do *download* ou por via da sua execução, para o mesmo se propagar e causar danos.[51]

[50] Cfr. FRANZ, Marcel (2007) – *Containing the Ultimate Trojan Horse*. IEEE Security & Privacy, p. 5.
[51] Cfr. CLOUGH, Jonathan (2015) – *Principles of Cybercrime*, Cambridge, Cambridge University Press, (2.ª ed., 2015), p. 33.

A prevenção contra Cavalos de Troia envolve a adoção de boas práticas de segurança cibernética, pelo que, é essencial manter o sistema operacional e o *software* atualizados, utilizar uma solução antivírus, evitar abrir anexos de *e-mails* suspeitos ou clicar em *links* desconhecidos. Além disso, é recomendável realizar verificações regulares no sistema em busca de *malware* e tomar cuidado ao baixar *softwares* de fontes que possam ser consideradas duvidosas.

3.2- LOGIC BOMBS

Paralelamente aos Cavalos de Troia, temos as chamadas *logic bombs* ou bombas de lógica.

Ora, uma *logic bomb* – ou bomba lógica – é um tipo de *malware* que é projetado para ser ativado num determinado momento ou quando certas condições se verificam.[52] As *logic bombs* são frequentemente usadas por indivíduos com conhecimento avançado de programação que têm acesso privilegiado aos sistemas ou redes que desejam atacar. No entanto, diferentemente de outros tipos de *malware*, que têm como objetivo principal a invasão de sistemas ou a obtenção de informações confidenciais, as *logic bombs* são projetadas para causar danos específicos num sistema de computador ou rede.[53]

A ideia por trás de uma *logic bomb* é simples: um programador mal-intencionado insere um trecho de código num concreto *software* ou sistema, o qual permanece inativo até que uma condição pré-determinada seja satisfeita. Tal condição pode ser uma data específica, um evento ou até mesmo uma sequência de ações executadas pelo utilizador e, desta forma, quando a condição é cumprida, a *logic bomb* é ativada e causa algum tipo de dano. Assim, verificamos que capacidade de uma *logic bomb* em permanecer inativa e não ser detetada por um longo período é, precisamente, uma das características mais perigosas desse tipo de *malware.*[54]

Por outro lado, uma das características interessantes das *logic bombs* é que as mesmas podem ser programadas para se autodestruírem após serem ativadas, dificultando a

[52] Cfr. RAMALHO, David (2013) – *O uso de malware como meio de obtenção de prova em processo penal*, Revista de Concorrência e Regulação, número 16, ano IV, outubro/dezembro de 2013, p. 203.
[53] Cfr. FRATANTONIO, Y.; BIANCHI, A.; ROBERTSON, W., KIRDA, E.; KRÜGEL, C. e VIGNA, G. (2016) – *TriggerScope: Towards Detecting Logic Bombs in Android Applications*. 2016 IEEE Symposium on Security and Privacy (SP), pp. 377 a 396.
[54] Cfr. FILIOL, Eric (2005) – *Computer viruses: from theory to applications*, Springer, p.120.

identificação e análise do *malware*, o que pode tornar o processo de deteção e remoção da *logic bomb* um desafio especialmente complexo e moroso para os especialistas em segurança.

No que respeita aos danos causados por uma *logic bomb*, os mesmos podem variar de intensidade, dependendo da intenção do programador.

Em concreto, podemos referir alguns exemplos de danos como a exclusão de arquivos importantes, a corrupção de dados, o "*shutdown*" de sistemas críticos ou até mesmo a destruição completa de um sistema.[55]

Por todo o exposto, verificamos que, para proteger de forma cabal os sistemas e redes contra *logic bombs*, é essencial implementar medidas robustas de segurança cibernética, incluindo a implementação de *firewalls*, sistemas de deteção de intrusão, atualizações regulares de *software* e ainda a adoção de boas práticas de segurança, como a restrição de acesso privilegiado e a realização de verificações regulares em código e sistemas de verificação de comportamentos anormais.

3.3- SPYWARE

Paralelamente aos dois casos acima referidos, temos o *spyware*.

Ora, conforme nos refere Jonathan Clough, o *spyware* é um tipo de *software* malicioso bem conhecido dos utilizadores em geral, o qual é projetado para obter informações sobre um utilizador ou sistema, sem o seu consentimento, pelo que, é uma ameaça de segurança cibernética que pode ser muito invasiva e prejudicial.[56]

O objetivo principal do *spyware* é espiar as atividades do utilizador, como navegação na *web*, histórico de digitação, informações pessoais e até mesmo capturas de tela, enviando tais informações para terceiros sem o conhecimento do utilizador.[57]

Uma das principais formas de infeção por *spyware* é através da realização *downloads* de *softwares* gratuitos, especialmente de fontes não confiáveis.[58] Neste sentido, muitas

[55] *Id*.
[56] Cfr. CLOUGH, Jonathan (2015) – *Principles of Cybercrime*, Cambridge, Cambridge University Press, p. 34. (2.ª ed., 2015), p. 36.
[57] Cfr. ERBSCHLEO, Michael (2005) – *Trojans, Worms and Spyware – A Computer Security Professional's* Guide to Malicious Code, Elsevier Butterworth–Heinemann, p.22.
[58] Cfr. BOLDT, Martin (2010) – Privacy-Invasive Software, Blekinge Institute of Technology, p. 75.

vezes, os utilizadores são induzidos a instalar um programa legítimo, mas, sem o seu conhecimento, o *spyware* também é instalado de forma simultânea quando o utilizador faz "*next*", "*next*", praticamente de olhos fechados durante o processo de *download*. Além disso, o *spyware* pode ser difundido por meio de *links* maliciosos em *e-mails*, *sites* comprometidos ou anúncios fraudulentos.

Uma vez instalado no sistema, o *spyware* atua de forma oculta, obtendo informações e monitorizando as atividades do utilizador, podendo registar *passwords*, informações bancárias, números de cartões de crédito ou qualquer outra informação pessoal que seja digitada no computador, sendo que tais informações podem ser usadas para cometer fraudes financeiras, roubo de identidade, chantagem ou para quaisquer outros fins maliciosos.[59]

Por outro lado, o *spyware* também pode afetar o desempenho do sistema, tornando-o lento e instável, o que ocorre porque o *software* malicioso consome recursos do sistema, como memória e processamento, para executar suas atividades furtivas. Além disso, o *spyware* pode exibir anúncios indesejados, redirecionar o navegador para sites maliciosos ou alterar as configurações do sistema sem a permissão do utilizador.

Assim, à semelhança do que já foi ferido a propósito das *logic bombs*, para lograr obter proteção cabal contra o *spyware*, é importante adotar medidas de segurança cibernética adequadas, como a realização de atualizações frequentes do *software*, incluindo do sistema operacional, navegadores, antivírus, ferramentas anti *spyware*, as quais fornecem correções de segurança essenciais para evitar vulnerabilidades exploradas pelo *spyware.*[60]

Paralelamente, é necessário ter especial cuidado com *downloads* e *links* suspeitos, evitando proceder ao *download* de programas de fontes não confiáveis e ter cuidado ao clicar em *links* desconhecidos ou suspeitos em *e-mails*, mensagens instantâneas ou em determinados *sites*.

3.4- KEYLOGGERS E SCREEN LOGGER

Ademais, temos os chamados *keyloggers* e *screen loggers*.

[59] Cfr. FILIOL, Eric (2005) – Computer viruses: from theory to applications, Springer, p. 75.
[60] Cfr. BOLDT, Martin (2010) – *Privacy-Invasive Software*, Blekinge Institute of Technology, p. 75.

De acordo com Sergio Toral, os *keyloggers* e *screen loggers* são tipos de *malware* projetados para capturar informações confidenciais, como *password*s, informações de *login* e outras atividades digitadas pelo utilizador num concreto dispositivo, os quais, apesar de terem propósitos semelhantes às modalidades de *malware* já referidas, distinguem-se pela forma como operam e nas informações que coletam.[61]

Keylogger é um programa malicioso que regista todas as teclas digitadas pelo utilizador num dispositivo. Em seguida, as informações são enviadas para o invasor, o qual as pode usar para obter acesso a contas pessoais, informações financeiras e outros dados confidenciais.[62]

Assim, os *keyloggers* podem ser implementados a nível de *software*, em que são executados como um programa oculto no sistema operacional, ou até mesmo em nível de *hardware*, em que um dispositivo físico é conectado ao computador para capturar as teclas digitadas.[63]

Os *keyloggers* podem ser distribuídos de várias maneiras, como anexos de *e-mail* maliciosos, *downloads* infetados ou através de vulnerabilidades de segurança exploradas e, à semelhança do *spyware*, uma vez instalado no dispositivo, o *keylogger* opera em segundo plano, registando silenciosamente todas as teclas digitadas pelo utilizador, o qual poderá utilizar as informações de forma criminosa, comprometendo a segurança do utilizador.

Paralelamente aos *keyloggers*, temos os *screen loggers*.

Ora, os *screen loggers* são um tipo de *malware* que captura imagens da tela do dispositivo e registam todas as atividades visuais, incluindo as telas de *login*, *sites* visitados, conversas e qualquer outra informação exibida no monitor. Assim como os *keyloggers*, os *screen loggers* são usados para obter informações confidenciais e são distribuídos de maneira semelhante, por meio de *downloads* maliciosos, *links* comprometidos ou exploração de vulnerabilidades.[64]

Conforme nos alerta Eric Filiol, os *screen loggers* podem ser particularmente perigosos, dado que podem capturar informações visuais sensíveis, como detalhes de pagamento,

[61] Cfr. TORAL, Sergio (2009) – *Estudio comparativo de técnicas antimalware*, Revista Iberoamericana de Tecnologías del Aprendizaje 4.3, pp. 26 a 31.
[62] Cfr. WAZID, M., SHARMA, R., KATAL, A., GOUDAR, R., BHAKUNI, P., & TYAGI, A. (2013) – *Implementation and Embellishment of Prevention of Keylogger Spyware Attacks*, pp. 262 a 271.
[63] Cfr. FILIOL, Eric (2005) – *Computer viruses: from theory to applications*, Springer, p. 328.
[64] Cfr. TORAL, Sergio (2009) – *Estudio comparativo de técnicas antimalware*, Revista Iberoamericana de Tecnologías del Aprendizaje 4.3, pp. 26 a 31.

documentos confidenciais ou imagens pessoais[65]. Não é difícil entender esta afirmação. Basta imaginar o perigo público que é alguém obter cópia de um vídeo íntimo de um primeiro-ministro com a sua esposa, feito de forma totalmente consentida e totalmente legal, mas para ser visto apenas pelos próprios.

Neste sentido, as informações obtidas podem ser usadas para chantagem, roubo de identidade ou outros crimes cibernéticos.

Por conseguinte, é necessário investir em proteção contra *keyloggers* e *screen loggers*, sendo importante adotar práticas de segurança cibernética adequadas, à semelhança do já referido atrás, com a realização de atualizações de *software* frequentes, ter cuidado com *downloads* e *links* suspeitos e, paralelamente, recorrendo ao uso de ferramentas anti *keylogger.*[66]

3.5- ROOTKITS

Conforme já fomos referindo, no mundo cada vez mais interconectado e dependente da tecnologia, surgem diversas ameaças que procuram explorar vulnerabilidades para obter acesso não autorizado a sistemas.

Entre essas ameaças, os *rootkits* destacam-se como um dos mecanismos mais perigosos e pérfidos. É que, um *rootkit* é um tipo de *software* malicioso projetado para ocultar a presença de um invasor num sistema comprometido. São chamados de *rootkits* porque geralmente obtêm acesso privilegiado ao nível de "*root*" em sistemas *Unix-like* ou "*Administrator*" no caso do *Windows*, o que lhes permite controlar completamente o sistema e ocultar as suas atividades.[67]

No que respeita às funcionalidades, os *rootkits* têm a capacidade de esconder processos, arquivos e conexões de rede, manipular dados em tempo real e até mesmo modificar o *kernel* do sistema operacional, possibilitando que os invasores permaneçam despercebidos e mantenham o controlo contínuo do sistema comprometido.[68]

---

[65] Cfr. FILIOL, Eric (2005) – *Computer viruses: from theory to applications*, Springer, p. 328.
[66] Cfr. TORAL, Sergio (2009) – *Estudio comparativo de técnicas antimalware*, Revista Iberoamericana de Tecnologías del Aprendizaje 4.3, pp. 26 a 31.
[67] Cfr. ERESHEIM, S., LUH, R., e SCHRITTWIESER, S. (2017) – *The Evolution of Process Hiding Techniques in Malware - Current Threats and Possible Countermeasures*. J. Inf. Process., 25, pp. 866 a 874.
[68] Cfr. BRENNER, Susan (2007) – *At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare*, Journal of Criminal Law and Criminology, volume 97, Tomo 2, p. 380.

Em concreto, os *rootkits* comprometem a segurança ao fornecerem acesso privilegiado a um invasor, permitindo que este execute ações maliciosas sem deteção por parte do utilizador, levando a que possam ser roubadas informações confidenciais, como senhas e dados bancários, bem como, ser espionadas atividades do utilizador e ainda distribuir *malware* adicional, criando uma *backdoor* para acesso futuro ou até mesmo transformar um dispositivo em parte de uma *botnet.*[69]

Um dos principais aspetos distintivos dos *rootkits* é que a sua deteção e remoção podem ser um desafio especialmente complicado, dado que estes são projetados precisamente para serem furtivos e difíceis de detetar.[70]

Uma vez mais, é necessário tomar medidas de segurança adequadas, como manter o sistema atualizado, utilizar soluções de segurança confiáveis e praticar uma navegação segura é essencial para qualquer pessoa se proteger contra os *rootkits*.

3.6- VÍRUS

Paralelamente aos aspetos já referidos, cumpre agora analisar os (universalmente conhecidos) vírus informáticos.

Os vírus informáticos são programas maliciosos criados para infetar computadores e dispositivos eletrónicos, os quais causam uma série de problemas e danos aos sistemas, uma vez que se espalham silenciosamente pela *internet*, comprometendo a segurança e a privacidade dos utilizadores. Com o avanço da tecnologia, estes evoluíram e tornaram-se cada vez mais sofisticados, representando um desafio constante para a segurança cibernética.[71]

Em concreto, os vírus informáticos são concebidos com o propósito de se infiltrar nos sistemas sem serem detetados, aproveitando vulnerabilidades e explorando falhas de segurança. Após a infeção do sistema, o vírus pode executar uma série de ações prejudiciais, como roubar informações confidenciais, corromper dados, desativar

[69] *Id*.
[70] Cfr. RAMALHO, David (2013) – *O uso de malware como meio de obtenção de prova em processo penal*, Revista de Concorrência e Regulação, número 16, ano IV, outubro/dezembro de 2013, p. 204.
[71] Cfr. BROWN, David (1992) – *An introduction to computer viroses*, p. 4, Disp. *in* https://www.osti.gov/servlets/purl/5608409 (consultado a 14/03/2023).

programas e até mesmo tornar o dispositivo totalmente inutilizável causando danos irreparáveis no disco rígido.

No que respeita às nuances dos vírus, podemos afirmar que existem diversos tipos de vírus informáticos, cada um com características e comportamentos específicos.

O vírus de computador clássico é um programa que se anexa a outros arquivos e se replica quando esses arquivos são executados. Esta técnica permite que o vírus se espalhe e infete outros sistemas, causando danos e interrompendo o funcionamento normal dos computadores. Os vírus podem ter diferentes objetivos, como destruir dados, roubar informações pessoais, controlar o sistema ou simplesmente causar problemas. No que respeita aos tipos de vírus, com o avanço da tecnologia e das medidas de segurança, os mesmos têm evoluído para formas mais sofisticadas, como *malware*, *ransomware*[72] e *spyware* (já analisado), tornando-se uma preocupação constante para os utilizadores de computador.

3.7- *WORMS*

Ainda dentro do *malware*, temos os *worms*.

Ora, de acordo com Susan Brenner, os *worms*, também conhecidos como vermes de computador, são uma categoria específica de *malware* que se espalha rapidamente através de redes de computadores, explorando vulnerabilidades nos sistemas. No entanto, diferentemente dos vírus clássicos, que dependem da interação do utilizador para se propagarem, os *worms* são capazes de se replicar e se espalhar automaticamente, sem a necessidade de interação humana.[73]

[72] O r*ansomware* é um tipo de *malware* que é projetado para bloquear o acesso a sistemas, dispositivos ou arquivos, exigindo o pagamento de um resgate (*ransom*) para restaurar o acesso ou evitar a divulgação de informações confidenciais.
Em concreto, o *ransomware* funciona por via da infeção do sistema-alvo por meio de diversos métodos, como anexos de *e-mail* maliciosos, *links* de *download* comprometidos ou explorando vulnerabilidades em *software* desatualizado e, uma vez dentro do sistema, o *ransomware* criptografa arquivos e exibe uma mensagem de resgate ao utilizador, geralmente em forma de *pop-up* ou arquivo de texto, instruindo-o sobre como pagar para obter uma chave de desbloquear o acesso.
No que concerne aos diferentes tipos de *ransomware*, podemos referir o *ransomware* bloqueador, que impede o acesso ao sistema ou a determinados arquivos ou o *ransomware* de criptografia, que criptografa os arquivos, tornando-os inacessíveis. Além disso, o ransomware evoluiu para variantes mais sofisticadas, como o *ransomware* duplo-extorsão, que além de criptografar arquivos, ameaça também divulgar informações confidenciais caso o resgate não seja pago, Cfr. GAZET, A. (2010) – *Comparative analysis of various ransomware virii*. Journal in Computer Virology, 6, pp. 77 a 90.
[73] Cfr. BRENNER, Susan (2012) – *Cybercrime and the law, challenges, issues, and outcomes*, Boston, Northeastern University Press, p. 37.

Os *worms* são projetados para explorar falhas de segurança em sistemas operacionais e *softwares*, aproveitando-se de vulnerabilidades previamente desconhecidas ou não corrigidas, dado que, uma vez que um *worm* infecta um dispositivo, pode-se espalhar para outros computadores e dispositivos conectados à mesma rede, criando uma cadeia de infeção, sendo capaz de se propagar de maneira rápida e eficiente, explorando portas de rede abertas, enviando cópias de si mesmos por *e-mail*, mensagens instantâneas ou até mesmo através de unidades USB infetadas[74]. Além disso, os *worms* podem explorar falhas em sistemas de compartilhamento de arquivos, servidores *web* e outros serviços de rede, facilitando a sua propagação.[75]

Após a instalação de um *worm* num dispositivo, o mesmo pode executar uma série de atividades maliciosas, incluindo a criação de portas dos fundos, permitindo que *hackers* acedam ao sistema comprometido de forma remota, obtendo informações pessoais ou confidenciais, roubando *passwords*, destruindo arquivos.[76]

Os *worms* representam uma ameaça significativa para a segurança cibernética, dado que se podem espalhar rapidamente e causar danos em grande escala, pelo que, uma vez mais, a prevenção é fundamental para evitar infeções por *worms*, sendo necessário manter os sistemas operacionais e os *softwares* atualizados, utilizar programas antivírus e *firewall*, além de implementar medidas de segurança em redes, como segmentação e controle de acesso.[77]

3.8- BLENDED THREATS

Conforme referimos a propósito de outras modalidades de *malware*, os cibercriminosos têm evoluído cada vez mais e têm-se tornar cada vez mais sofisticados e criativos nas suas abordagens, utilizando táticas avançadas para atingir seus objetivos nefastos. Ora, entre essas táticas, destacam-se as *blended threats*, ou ameaças combinadas, as quais combinam diferentes métodos e vetores de ataque, aproveitando-se de várias vulnerabilidades para obter resultados devastadores.

[74] Cfr. https://www.wired.co.uk/article/ransomware-viruses-trojans-worms (consultado a 06/03/2023).
[75] Cfr. CLOUGH, Jonathan (2015) – *Principles of Cybercrime*, Cambridge, Cambridge University Press, p. 34. (2.ª ed., 2015), p. 33.
[76] *Id*.
[77] Cfr. BRENNER, Susan (2007) – *At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare*, Journal of Criminal Law and Criminology, volume 97, Tomo 2, p. 381.

Em termos práticos, podemos afirmar que as *blended threats* são uma evolução natural dos ataques cibernéticos tradicionais, pois, conforme nos refere David Ramalho, ao combinarem diferentes técnicas como *malware*, engenharia social e exploração de vulnerabilidades, os criminosos criam um cenário altamente complexo e desafiador para as organizações e indivíduos que buscam se proteger, podendo tais ameaças se manifestar de diversas formas, desde ataques direcionados a instituições financeiras até campanhas de *phishing* sofisticadas.[78]

Um exemplo comum de *blended threat* é a utilização de *malware* em conjunto com técnicas de engenharia social em que, neste tipo de ataque, os criminosos enviam *e-mails* falsos ou mensagens em redes sociais, utilizando-se de técnicas de persuasão para convencer as vítimas a clicarem em *links* maliciosos ou baixarem arquivos infetados. Ao fazer isso, o *malware* é introduzido nos sistemas das vítimas, permitindo aos atacantes acesso não autorizado e a possibilidade de roubar informações confidenciais ou realizar outras atividades prejudiciais.[79]

Por conseguinte, combater as *blended threats* é um desafio constante para as empresas e indivíduos. A abordagem tradicional de segurança cibernética, baseada em medidas pontuais e isoladas, muitas vezes não é eficaz contra estas ameaças complexas, sendo necessário adotar uma abordagem mais abrangente, que inclua a implementação de soluções de segurança em várias camadas, a consciencialização dos utilizadores e a prática de boas políticas de segurança. Além disso, é essencial manter-se atualizado em relação às tendências e técnicas utilizadas pelos criminosos cibernéticos, pelo que, a partilha de informações e a colaboração entre organizações e especialistas em segurança também desempenham um papel fundamental na deteção e mitigação das *blended threats.*[80]

3.9- *BOTS*

Uma vez mais, em face do desenvolvimento tecnológico, temos o surgimento dos *bots*.

[78] Cfr. RAMALHO, David (2013) – O uso de malware como meio de obtenção de prova em processo penal, Revista de Concorrência e Regulação, número 16, ano IV, outubro/dezembro de 2013, p. 204.
79 Cfr. RAMALHO, David (2013) – O uso de malware como meio de obtenção de prova em processo penal, Revista de Concorrência e Regulação, número 16, ano IV, outubro/dezembro de 2013, p. 205.
80 Cfr. CHIEN, Eric e SZÖR, Péter (2002) – *Blended Attacks Exploits, Vulnerabilities and Buffer-Overflow Techniques in Computer Viruses*, Virus Bulletin, p. 32.

Na definição apresentada por David Ramalho, os *bots* são programas de computador automatizados que podem ser utilizados para fins benéficos, como automação de tarefas, mas também representam um perigo significativo quando empregados como *malware.*[81]

Na prática, verificamos que um *bot* é um programa desenvolvido para executar tarefas específicas de maneira autónoma e repetitiva, sendo amplamente utilizados em diversas áreas, como atendimento ao cliente, indexação de páginas da *web* ou até mesmo em jogos *online*.

No entanto, quando utilizados como *malware*, podem causar danos significativos.

Um dos principais perigos dos *bots* maliciosos é a sua capacidade de se espalhar rapidamente pela *internet*, uma vez que, após infetar um sistema, um *bot* pode se auto-replicar e se espalhar para outros dispositivos, formando uma rede de *bots* conhecida como *botnet*, a qual pode ser controlada remotamente por *hackers*, que as utilizam para realizar ataques em grande escala, como ataques de negação de serviço (DDoS), envio de *spam* ou até mesmo roubo de informações pessoais e financeiras.[82]

Além disso, os *bots* podem ser programados para realizar atividades fraudulentas, como fraudes em publicidade *online*, manipulação de mercado financeiro ou disseminação de desinformação, pois, com a capacidade de automatizar tarefas repetitivas em grande escala, os *bots* maliciosos podem explorar vulnerabilidades nos sistemas de segurança e prejudicar empresas, governos e indivíduos.[83]

Outro aspeto perigoso é a evolução e sofisticação dos *bots*, pois muitos já são capazes de imitar comportamentos humanos, como interagir em redes sociais, enviar mensagens personalizadas e até mesmo passar despercebidos em testes de Captcha[84], o que dificulta a deteção e a remoção desses programas maliciosos, tornando-os ainda mais perigosos.

[81] Cfr. RAMALHO, David (2013) – *O uso de malware como meio de obtenção de prova em processo penal*, Revista de Concorrência e Regulação, número 16, ano IV, outubro/dezembro de 2013, p. 205.
[82] Cfr. https://www.akamai.com/pt/glossary/what-is-application-layer-ddos-attack (consultado a 18/03/2023).
[83] Cfr. CLOUGH, Jonathan (2015) – *Principles of Cybercrime*, Cambridge, Cambridge University Press, p. 34. (2.ª ed., 2015), p. 35.
[84] Cfr. CAPTCHA, que significa "Completely Automated Public Turing Test to Tell Computers and Humans Apart", é um tipo de desafio ou teste projetado para distinguir humanos de *bots*. – Ex. uma série de imagens em que o usuário deve selecionar as imagens que correspondem a uma determinada descrição.

3.10- MODO DE INSTALAÇÃO

Conforme se referiu sobremaneira, o avanço da tecnologia trouxe consigo uma ameaça virtual que assombra utilizadores e empresas: o *malware*.

Este tipo de *software* malicioso pode causar danos graves aos sistemas informáticos, roubar informações confidenciais e comprometer a privacidade dos indivíduos.

Os *hackers* procuram encontrar cada vez mais maneiras engenhosas de infetar computadores com *malware*. Para tal, recorrem a diversos procedimentos como enviar anexos de *e-mail* e *links* maliciosos. Neste sentido, os e-mails de *phishing* são enviados em massa, com mensagens falsas que parecem legítimas e os anexos maliciosos podem conter *malware*, e os *links* redirecionam os utilizadores para sites falsos, que instalam silenciosamente o *software* malicioso.

Paralelamente, podem recorrer à criação de produtos informáticos "mascarados", fazendo com que o utilizador pense que está a proceder ao *download* de um produto perfeitamente genuíno e, no final de contas, ao baixar arquivos, programas ou jogos de fontes não confiáveis, os utilizadores correm o risco de instalar *malware* sem o seu conhecimento.[85]

Noutro âmbito, procedem à exploração de vulnerabilidades em *software*s e sistemas operacionais e, quando encontram uma brecha, desenvolvem códigos maliciosos que exploram tais falhas para infetar os computadores desprotegidos.

Podem também recorrer ao chamado "*malvertising*", ou seja, à distribuição de *malware* através de anúncios *online*. Os *hackers* exploram redes de publicidade para exibir anúncios infetados em *sites* populares e, ao clicar nesses anúncios, o utilizador é redirecionado para páginas que realizam a instalação silenciosa do *malware.*[86]

Outro mecanismo de instalação passa por dispositivos externos infetados como *pendrives* ou discos rígidos externo, os quais, uma vez conectados a um computador procedem à instalação automática do *malware*, podendo mesmo espalhar-se para outros dispositivos.

[85] Cfr. CLOUGH, Jonathan (2015) – *Principles of Cybercrime*, Cambridge, Cambridge University Press, p. 34. (2.ª ed., 2015), p. 35.
[86] Cfr. https://ostec.blog/noticias/malvertising/ (consultado a 16/03/2023).

CAPÍTULO III- DIREITOS E PRINCÍPIOS FUNDAMENTAIS SUBJACENTES À ATUAÇÃO DO *MALWARE*

1- DIREITOS FUNDAMENTAIS E OUTROS PRINCÍPIOS CONSTITUCIONAIS COLOCADOS EM CAUSA PELO *MALWARE*

De acordo com Vieira de Andrade (1976, p. 15):

> Aquilo a que se chama ou a que é lícito chamar direitos fundamentais pode afinal ser considerado por diversas perspetivas. De facto, os direitos fundamentais tanto podem ser vistos enquanto direitos naturais de todos os homens, independentemente dos tempos e dos lugares-perspetiva filosófica ou jusnaturalista; como podem ser referidos aos direitos mais importantes das pessoas, num determinado tempo e lugar, isto é, num Estado concreto ou numa comunidade de Estados-perspetiva estadual ou constitucional; como ainda podem ser considerados direitos essenciais das pessoas num certo tempo, em todos os lugares ou, pelo menos, em grandes regiões do mundo-perspetiva universalista ou internacionalista[87].

E, nas palavras de Jorge Reis Novais (2010, p. 295):

> A proteção juridicamente garantida pelos direitos fundamentais evolui, neste sentido, à medida da própria evolução e aperfeiçoamento das instituições de Estado de Direito. Começou, no Estado liberal, por se resumir a uma defesa contra a actuação ilegal da Administração; desenvolveu-se, nos primórdios do Estado social de Direito, através da consagração constitucional dos direitos sociais e através da garantia, também contra o legislador, de um núcleo essencial dos direitos fundamentais como valores, e prolonga-se, hoje, numa garantia plena contra quaisquer prejuízos da liberdade provocados pelo Estado[88].

Ora, os direitos fundamentais são a base de uma sociedade justa e democrática, e são o mecanismo de garante da proteção e o respeito aos direitos mais básicos dos cidadãos. No entanto, num mundo cada vez mais interligado, tais direitos podem ser colocados em causa por ameaças digitais, de que o *malware* é exemplo.

Conforme já referimos, o *malware*, ou *software* malicioso, é um programa de computador desenvolvido com o intuito de causar danos, roubar informações ou obter acesso não autorizado a sistemas, pelo que, o mesmo pode comprometer diversos

[87] Cfr. ANDRADE José Carlos Vieira de (2012) – *Os Direitos Fundamentais na Constituição Portuguesa de 1976*, 5ª ed., Almedina, Coimbra, p. 15.
[88] Cfr. NOVAIS Jorge Reis (2010) – *As restrições aos Direitos Fundamentais não expressamente autorizadas pela Constituição*, 2ª ed, Coimbra Editora, Coimbra, p. 295.

princípios constitucionais, trazendo consequências significativas para a segurança e privacidade dos indivíduos.

Neste sentido, um dos direitos fundamentais frequentemente afetados pelo *malware* é o direito à privacidade. Com o aumento da digitalização e a crescente dependência de dispositivos eletrónicos, torna-se mais fácil para os cibercriminosos acederem a informações pessoais e colocar em perigo dados sensíveis, como informações bancárias, dados de identificação e registos médicos, concretizando roubos de informação, fraudes, invasões de privacidade e até mesmo casos de coação e extorsão.

Para Jorge Miranda e Rui Medeiros, o direito à intimidade e à privacidade é um dos direitos com maior importância prática[89].

Podemos afirmar que o *malware* também pode violar o direito à intimidade, à privacidade e à liberdade de expressão, dado que o mesmo pode ser usado para censurar ou monitorizar a atividade *online* dos indivíduos, restringindo assim a sua capacidade de se expressar sem medo de represálias.

Outro princípio constitucional ameaçado pelo *malware* é o direito à segurança. O art.º 27.º, n.º 1 da CRP estabelece que todos têm direito à liberdade e à segurança[90]. Ora, por maioria de razão, os cidadãos têm o direito de se sentirem seguros também no seu ambiente digital, seja ao realizar transações *online*, seja ao utilizar serviços eletrónicos ou simplesmente a navegar na *internet*. O *malware* pode comprometer a segurança dos sistemas, tornando os dispositivos vulneráveis a ataques e possibilitando a infiltração de *hackers* e criminosos cibernéticos.

Por outro lado, a igualdade de acesso à informação também é um princípio constitucional que pode ser prejudicado pelo *malware*. A *internet* é uma ferramenta poderosa que permite o acesso rápido e amplo a uma variedade de informações, no entanto, o *malware* pode infetar *sites*, bloquear conteúdo ou disseminar desinformação, restringindo assim o acesso igualitário e confiável às informações, dado que nem todos conseguem ter acesso aos mesmos mecanismos de proteção tecnológica contra ameaças mais evoluídas.

Diante dessas ameaças, é fundamental que as autoridades e os cidadãos adotem medidas de proteção com a implementação de leis e regulamentos eficazes para punir

[89] Cfr. MIRANDA, Jorge e MEDEIROS, Rui (2005) – Constituição Portuguesa Anotada, tomo I, 2.ª ed., Coimbra, Coimbra Editora, p. 290.
90 Cfr. https://www.parlamento.pt/Legislacao/Documents/constpt2005.pdf (consultado a 17/04/2023).

os responsáveis pelo desenvolvimento e disseminação de *malware*. Além disso, é necessário investir em sistemas de segurança robustos e em programas educacionais para conscientizar as pessoas sobre os riscos e ensiná-las a adotarem boas práticas de segurança digital.

1.1- DIREITO À RESERVA DA INTIMIDADE DA VIDA PRIVADA

O direito à reserva da intimidade da vida privada é um direito fundamental dos cidadãos, o qual visa proteger a esfera pessoal e íntima das pessoas contra intromissões indesejadas na sua vivência quotidiana, a qual está intrinsecamente ligada à dignidade humana, ao respeito à individualidade e à autonomia das pessoas.

Devido à sua importância, o direito à reserva da intimidade da vida privada tem expressa previsão constitucional no art.º 26.º, n.º 1 da Constituição da República Portuguesa, o qual estabelece que "A todos são reconhecidos os direitos à identidade pessoal, ao desenvolvimento da personalidade, à capacidade civil, à cidadania, ao bom nome e reputação, à imagem, à palavra, à reserva da intimidade da vida privada e familiar e à proteção legal contra quaisquer formas de discriminação".[91]

Ademais, também a lei ordinária o prevê, o com o art.º 80.º do Código Civil a conferir proteção ao nível dos direitos de personalidade, consagrando que "Todos devem guardar reserva quanto à intimidade da vida privada de outrem".[92]

Ora, de acordo com Ingo Sarlet (2001, p. 50) a dignidade da pessoa humana pode ser definida como:

> A qualidade intrínseca e distintiva de cada ser humano que o faz merecedor do mesmo respeito e consideração por parte do Estado e da comunidade, implicando, neste sentido, um complexo de direitos e deveres fundamentais que assegurem a pessoa tanto contra todo e qualquer ato de cunho degradante e desumano, como venham a lhe garantir as condições existenciais mínimas para uma vida saudável, além de propiciar e promover a sua participação ativa e corresponsável nos destinos da própria existência e da vida em comunhão com os demais seres humanos.[93]

[91] Cfr. https://www.parlamento.pt/Legislacao/Documents/constpt2005.pdf (consultado a 23/10/2023).
[92] Cfr. https://dre.pt/dre/legislacao-consolidada/decreto-lei/1966-34509075 (consultado a 25/10/2023).
[93] Cfr. SARLET, Ingo (2001) – *Dignidade da Pessoa Humana e Direitos Fundamentais na Constituição Federal de 1988*, p. 50.

Paralelamente, Gomes Canotilho e Vital Moreira (2007, p. 198) enunciam três dimensões essenciais da dignidade da pessoa humana:

> 1- A dignidade da pessoa humana como dimensão intrínseca do homem; 2- A dignidade da pessoa humana como reconhecimento recíproco; 3- A dignidade da pessoa humana como valor.[94]

Assim, o princípio da dignidade da pessoa humana e, por inerência, o direito à reserva da intimidade da vida privada abrange uma ampla gama de aspetos, desde a privacidade física até à proteção de informações pessoais sensíveis, o que significa que as pessoas têm o direito de decidir sobre a sua própria vida privada, o que inclui a escolha de como e com quem compartilhar informações pessoais, bem como o direito de controlar o acesso a seus espaços pessoais, como a residência.

Neste sentido, cumpre referir o Acórdão do Supremo Tribunal de Justiça de 23/09/2004[95], que, analisando o impacto concreto dos direitos de personalidade no quotidiano dos cidadãos, nos refere:

> 1 - O direito à imagem e direito à reserva sobre a intimidade da vida privada, enquanto direitos fundamentais de personalidade, são inatos, inalienáveis, irrenunciáveis e absolutos, no sentido de que se impõem, por definição, ao respeito de todas as pessoas.
>
> 2 - O que se passa no interior da residência de cada pessoa e na área, privada, que a circunda, integra o núcleo duro da reserva da intimidade da vida privada legalmente protegida..[96]

Isto posto, em ambiente digital, o direito à reserva da intimidade da vida privada tornou-se ainda mais relevante, pois com a ascensão das tecnologias de informação e comunicação, é cada vez mais fácil para terceiros invadirem a privacidade das pessoas.

---

[94] Cfr. CANOTILHO, Gomes e MOREIRA, Vital (2007) – *Constituição da República Portuguesa Anotada*. Vol. I, p. 198.

[95] Disp. *in* http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/e4428a4a669f03088025705a0052bf9f?OpenDocument&Highlight=0,05A945%20 (consultado a 19/10/2023).

[96] "3 - A publicação numa revista pertencente à ré de uma reportagem fotográfica legendada divulgando, sem consentimento do autor, uma visita por ele feita na companhia da mulher à residência familiar então em fase de construção na cidade de Madrid, integra a violação simultânea dos seus direitos à imagem e à reserva da intimidade da vida privada.
4 - A ilicitude desta conduta não é afastada, nem pelo facto de o autor ser uma pessoa de grande notoriedade, adquirida graças à sua condição de futebolista profissional mundialmente reconhecido (figura pública), nem pela circunstância de as fotografias mostrarem apenas a entrada da casa e de esta se encontrar em fase de construção.
5 - O direito da liberdade de imprensa tem como limite intransponível, entre outros, a salvaguarda do direito à reserva da intimidade da vida privada e à imagem dos cidadãos.
6 - De igual modo, também a invocação do direito de informar consagrado no art.º 37º, nº 1, da Constituição não legitima a conduta do lesante se não houver qualquer conexão entre as imagens ou factos divulgados pertencentes ao foro privado do lesado e a actividade profissional por ele desempenhada que originou a sua notoriedade pública." Cfr http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/e4428a4a669f03088025705a0052bf9f?OpenDocument&Highlight=0,05A945%20 (consultado a 19/10/2023).

Assim, questões relacionadas à proteção de dados pessoais, vigilância eletrónica e exposição não consentida na *internet* têm colocado em evidência a importância de se estabelecerem salvaguardas efetivas para garantir a privacidade dos indivíduos.

Por conseguinte, os Estados democráticos têm o dever de proteger e promover o direito à reserva da intimidade da vida privada, estabelecendo legislações claras e eficientes, sendo ainda essencial que exista uma atuação robusta por parte das autoridades competentes para fiscalizar e punir eventuais violações desse direito.

Além do papel do Estado, cada indivíduo também tem a responsabilidade de respeitar a privacidade alheia. O exercício da liberdade de expressão, por exemplo, deve estar sujeito a limites quando se trata de divulgar informações pessoais de terceiros sem o seu consentimento, sendo por isso importante a promoção de uma cultura de respeito à privacidade, onde as pessoas sejam conscientes dos limites éticos e legais ao compartilharem informações alheias.

Neste sentido nos refere o Acórdão do Tribunal da Relação do Porto de 11/04/2019, o qual afirma que:

> (…) III - O direito à reserva sobre a intimidade da vida privada, enquanto direito fundamental de personalidade, caracteriza-se juridicamente como inato, inalienável, irrenunciável e absoluto, no sentido de que se impõe, por definição, ao respeito de todas as pessoas.
>
> IV - A esta luz, a reserva juscivilística envolverá, designadamente, a proibição de introdução não autorizada em casa alheia, a proibição de observação às ocultas do domicílio de outrem e das pessoas que nele se encontrem, bem como a proibição de captação fotográfica ou por qualquer outro meio de imagens da residência de cada qual, e na área, privada, que a circunda (logradouro, jardim, parque, etc. (…)".[97]

No entanto e, no que ao presente estudo mais nos importa, é importante lembrar que o direito à reserva da intimidade da vida privada, apesar de ser um direito e absoluto no que respeita à sua titularidade, o mesmo pode ser limitado em determinadas circunstâncias, designadamente no âmbito da investigação de crimes ou na proteção da segurança nacional, sendo necessário equilibrar os direitos individuais com o interesse coletivo, a fim de garantir uma sociedade justa e segura.

O direito à reserva da intimidade da vida privada é uma salvaguarda crucial para garantir a liberdade individual e a proteção da dignidade humana, sendo a consubstanciação de

[97] Cfr. http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/d7c7bbf9d0de6091802583fa003bb587?OpenDocument (consultado a 22/10/2023).

um princípio que reconhece o direito das pessoas de controlar e manter sua esfera íntima longe de intrusões indesejadas. Este direito abrange diversos aspetos da vida privada, incluindo a privacidade do lar, das comunicações pessoais, das atividades pessoais e das informações sensíveis e envolve também a proteção da imagem, da honra e da reputação das pessoas, assim como o direito de decidir como e com quem compartilhar essas informações.

No contexto atual, em que vivemos numa sociedade globalizada, altamente conectada e digitalizada, a proteção da intimidade da vida privada tornou-se ainda mais desafiadora, com os problemas de fuga de dados pessoais, a vigilância pela polícia ou ainda a disseminação não autorizada de informações na *internet*, são todos aspetos que representam ameaças significativas à privacidade individual.

Por conseguinte, é crucial que os Estados aprovem leis e regulamentos (ex.: Regulamento Geral de Proteção de Dados (RGPD[98])) que protejam efetivamente o direito à reserva da intimidade da vida privada, protejam os dados pessoais, a transparência no uso de informações, o consentimento informado e a segurança da informação. Além disso, é necessário que os governos adotem medidas adequadas para garantir o cumprimento dessas leis e a proteção dos direitos individuais, o que implica investir em recursos e tecnologias para fortalecer a segurança cibernética, promover a consciencialização da importância da privacidade e realizar ações de fiscalização e responsabilização em casos de violações.

Sem prejuízo de todo o exposto, cumpre reiterar que é necessário encontrar um equilíbrio entre o direito à reserva da intimidade da vida privada e outros interesses legítimos, como a segurança pública e a prevenção de crimes, dado que em certas circunstâncias, pode ser necessário restringir temporariamente esse direito para proteger o bem-estar coletivo, no entanto, tais restrições devem ser estritamente necessárias, proporcionais e estar sujeitas a um controlo adequado.

1.2- DIREITO À PALAVRA

O direito à palavra é um dos pilares fundamentais da democracia e o garante da liberdade de expressão e da participação ativa dos cidadãos na tomada de decisões

[98] Cfr. https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679 (consultado a 26/10/2023).

políticas e sociais, o qual assegura que todos tenham a oportunidade de expressar as suas opiniões, compartilhar ideias e contribuir para o debate público em condições de igualdade.

Ora, apesar de o mesmo ter nascido do direito à reserva da intimidade, de acordo com João Gouveia de Caires, o direito à palavra deve hoje ser considerado um direito completamente autónomo[99].

A liberdade de expressão é um dos direitos humanos mais universalmente reconhecido, consagrado em documentos internacionais como a Declaração Universal dos Direitos Humanos (DUDH), a qual no seu art.º 19.º dispõe que:

> Todo o indivíduo tem direito à liberdade de opinião e de expressão, o que implica o direito de não ser inquietado pelas suas opiniões e o de procurar, receber e difundir, sem consideração de fronteiras, informações e ideias por qualquer meio de expressão.[100]

ou ainda a Convenção Europeia de Direitos Humanos (CEDH), que estabelece no seu art.º 10.º, n.º 1 que:

> Qualquer pessoa tem direito à liberdade de expressão. Este direito compreende a liberdade de opinião e a liberdade de receber ou de transmitir informações ou ideias sem que possa haver ingerência de quaisquer autoridades públicas e sem considerações de fronteiras. O presente artigo não impede que os Estados submetam as empresas de radiodifusão, de cinematografia ou de televisão a um regime de autorização previa.[101]

Assim, a liberdade de expressão abrange não apenas a liberdade de falar, mas também a liberdade de procurar, receber e compartilhar informações e ideias de qualquer natureza, sem interferência ou censura governamental.

1.3- DIREITO À IMAGEM

Paralelamente ao que referimos, no mundo moderno, global, onde a tecnologia avançada e a conectividade digital estão cada vez mais presentes, o direito à imagem é também um direito de grande relevância, sendo também um pilar fundamental da proteção individual e abrange uma ampla gama de situações e contextos.

[99] Cfr. CAIRES, João Gouveia de (2014) – *O registo de som e imagem e as escutas ambientais*, *in* Direito da Investigação Criminal e da Prova, coord. Maria Fernanda Palma *et al*., Coimbra, Almedina, p. 276.
[100] Cfr. https://www.ohchr.org/sites/default/files/UDHR/Documents/UDHR_Translations/por.pdf (consultado a 21/10/2023).
[101] Cfr. https://www.echr.coe.int/documents/d/echr/convention_por (consultado a 21/10/2023).

O direito à imagem é o direito de uma pessoa controlar o uso e a divulgação da sua própria imagem, cabendo apenas ao seu titular o direito de utilizar pessoalmente a sua imagem e decidir quem a poderá utilizar, reproduzir ou divulgar, mediante o seu consentimento prévio. Aqui se incluem não apenas fotografias e vídeos, mas também desenhos, caricaturas e outras representações visuais.

Uma vez mais, também o direito à imagem tem expressa previsão constitucional no já referido art.º 26.º, n.º 1 da Constituição da República Portuguesa, o qual estabelece que:

> A todos são reconhecidos os direitos à identidade pessoal, ao desenvolvimento da personalidade, à capacidade civil, à cidadania, ao bom nome e reputação, à imagem, à palavra, à reserva da intimidade da vida privada e familiar e à proteção legal contra quaisquer formas de discriminação.[102]

Também a lei ordinária o prevê enquanto direito de personalidade, com o art.º 79.º, n.º 1 do Código Civil a prever que "o retrato de uma pessoa não pode ser exposto, reproduzido ou lançado no comércio sem o consentimento dela; depois da morte da pessoa retratada, a autorização compete às pessoas designadas no n.º 2 do artigo 71.º, segundo a ordem nele indicada".[103]

Uma das principais razões para a existência desse direito é a proteção da privacidade e da dignidade humana, pois cada indivíduo tem o direito de manter o controlo sobre a sua própria imagem e decidir quando e como ela será exposta ao público.

À semelhança do que sucede com a liberdade de expressão, também no contexto digital o direito à imagem enfrenta novos desafios, uma vez que, com a proliferação das redes sociais e a partilha instantânea de fotos e vídeos, tornou-se mais fácil do que nunca violar esse direito. Ora, a disseminação rápida e global de imagens pode levar a danos irreparáveis à reputação e à vida pessoal das pessoas.

No entanto, é importante ressaltar que, uma vez mais, também o direito à imagem não é absoluto, existindo situações em que o interesse público pode justificar a divulgação de imagens sem consentimento, como por exemplo no âmbito de investigação criminal.

Tal desiderato vem sendo confirmado pela jurisprudência, onde o direito à imagem é derrogado pela necessidade de recolher prova em inquéritos criminais, citando nesse sentido, o Tribunal da Relação do Porto, por acórdão proferido em 2021 que preconiza:

[102] Cfr. https://www.parlamento.pt/Legislacao/Documents/constpt2005.pdf (consultado a 23/04/2023).
[103] Cfr. https://www.codigocivil.pt/ (consultado a 01/10/2023).

> A imagem captada, em local público, por factos ocorridos em via pública, do suposto autor do crime por um lado não constitui nenhuma violação do "núcleo duro da sua vida privada", nem do seu direito à imagem, não sendo necessário o seu consentimento para essa gravação, tal como decorre do art.º 79º, nº 2, do CC (estando a filmagem do suspeito justificada por exigências de justiça) e, por outro lado, aquela conduta do particular que fez a filmagem de imagens em local público não constitui a prática do crime de "gravações e fotografias ilícitas p. e p. no art.º 199º, nº 2, do CP, nem tão pouco integra a prática de qualquer ilícito culposo segundo o ordenamento jurídico, mesmo considerado este globalmente.
>
> Não sendo ilícita, nos termos da lei penal, essa filmagem de imagens em local público, feita por particular, nas circunstâncias acima descritas, também a reprodução mecânica dessa filmagem (através da junção ao processo, quer do CD contendo a dita gravação de imagens, quer da reprodução em papel de imagens dela retiradas) é permitida, tal como decorre do art.º 176º n.º 1 do CPP.[104]

1.4- DIREITO À INVIOLABILIDADE DO DOMICÍLIO

De acordo com António Costa Pinto, Luís de Sousa e Pedro Magalhães (2013, p. 29):

> O Estado de direito é uma figura jurídica, circunscrita a uma comunidade politicamente constituída num contexto espacial e temporal, na qual os detentores do poder se encontram sujeitos à Constituição e às leis promulgadas, onde existe uma separação efetiva de poderes e o respeito pelos direitos, liberdades e garantias fundamentais dos cidadãos. Os limites e as regras para o exercício do poder estatal (onde se inscrevem as chamadas «garantias fundamentais») encontram-se consignados numa constituição democraticamente aceite, ainda que não necessariamente referendada.[105]

Conforme nos refere Uadi Bullos, num Estado constitucional, a Constituição é a lei das leis por excelência[106].

Neste sentido, o art.º 2.º da Constituição da República Portuguesa estabelece que a República Portuguesa é um Estado de Direito Democrático, baseado na soberania popular, no pluralismo de expressão e organização política democráticas, no respeito e na garantia de efetivação dos direitos e liberdades fundamentais e na separação e

---

[104] Crf. https://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/3f8bcf4415c27b52802587ed0065d1cf?OpenDocument&Highlight=0,RGPD, (consultado em 12/01/2024). Ainda com tal entendimento: https://www.dgsi.pt/jtrc.nsf/8fe0e606d8f56b22802576c0005637dc/4bd77bb02c09e75b80257f6800512c33?OpenDocument (consultado em 12/01/2024).

[105] Cfr. PINTO, António Costa, SOUSA, Luís de, e MAGALHÃES, Pedro (2013) A Qualidade da Democracia em Portugal: a visão dos Cidadãos, 1ª ed., Lisboa, Imprensa de Ciências Sociais, p. 29, disp. em https://repositorio.ul.pt/bitstream/10451/22839/1/ICS_ACPinto_PMagalhaes_Qualidade_LEN.pdf (consultado a 05/09/2023).

[106] Cfr. BULLOS, Uadi Lammêgo (2011) – *Curso de Direito Constitucional*. 6. ed., rev. São Paulo: Saraiva, p. 64.

interdependência de poderes, visando a realização da democracia económica, social e cultural e o aprofundamento da democracia participativa.[107]

Ora, num Estado de Direito Democrático, o direito à inviolabilidade do domicílio representa a concretização de um princípio que é considerado como um dos pilares fundamentais da liberdade individual, o qual assegura que a residência de uma pessoa é um espaço protegido, onde ela tem o direito de se sentir segura, livre de intervenções arbitrárias ou ilegais por parte do Estado ou de terceiros.

Assim, o art.º 34.º, n.º 1 CRP, estabelece que "O domicílio e o sigilo da correspondência e dos outros meios de comunicação privada são invioláveis".[108]

O conceito de inviolabilidade do domicílio remonta a tempos antigos e está intimamente ligado à proteção da privacidade e da intimidade do indivíduo, à noção de que cada pessoa tem o direito de ter um espaço pessoal sagrado, onde possa exercer a sua autonomia e exercer as suas atividades livremente, aspetos fundamentais para uma sociedade democrática e que respeita os direitos e liberdades individuais de todos os seus cidadãos.

Assim, ao garantir a inviolabilidade do domicílio, o Estado reconhece que o lar é o refúgio do indivíduo, onde o mesmo se pode resguardar da pressão social, descansar, reunir-se com a sua família e exercer a sua liberdade de pensamento, religião e expressão, sendo nesse ambiente que a personalidade do indivíduo se desenvolve e se fortalece, aspetos essenciais para que uma pessoa se sinta segura e protegida dentro dos seus próprios limites. A inviolabilidade do domicílio é especialmente relevante quando se considera o contexto de sociedades democráticas, onde a liberdade e o respeito aos direitos individuais são valores essenciais, motivo pelo qual a garantia desse direito contribui para o fortalecimento do Estado de Direito e para a consolidação de uma sociedade justa e igualitária.

Além disso, a inviolabilidade do domicílio desempenha um papel importante na preservação da intimidade e da vida familiar, pois é dentro de casa que as pessoas se podem sentir à vontade para partilhar momentos e experiências com os seus entes queridos, estabelecer laços afetivos e fortalecer o núcleo familiar, motivo pelo qual a proteção desse espaço é essencial para o desenvolvimento saudável das relações interpessoais e para o florescimento das pessoas como seres sociais.

[107] Cfr. https://www.parlamento.pt/Legislacao/Documents/constpt2005.pdf (consultado a 13/09/2023).
[108] *Id*.

Paralelamente ao exposto, cumpre referir que, embora o domicílio seja inviolável, a proteção da privacidade não se limita apenas aos muros de uma residência, pois com os avanços tecnológicos, a esfera privada expandiu-se para o ambiente virtual, e o direito à privacidade deve ser garantido também nesse contexto.

Neste sentido, Gomes Canotilho e Vital Moreira (2007, p. 541) afirmam que:

> O domicílio não é violado somente quando se entra na morada de alguém sem o seu consentimento [pois também] modernos meios técnicos possibilitam a invasão e devassa do domicílio mediante meios eletrónicos, que, além disso, permitem também a devassa das conversas e da vida privada dos moradores. A inviolabilidade do domicílio é seguramente incompatível com tais mecanismos.[109]

Assim, é crucial considerar a evolução da tecnologia e o impacto que a mesma tem na proteção da inviolabilidade do domicílio. Com o avanço das técnicas de vigilância e a crescente digitalização da vida quotidiana, emergem novos desafios no que diz respeito à privacidade e à proteção do domicílio, sendo necessário, portanto, que o acervo legal seja atualizado e adaptado para enfrentar tais desafios, garantindo a proteção dos direitos individuais também no ambiente virtual.

Neste sentido, a intercetação de comunicações, a vigilância em massa e a obtenção indiscriminada de dados são questões que exigem a atenção do legislador, levantam também questões éticas e fundamentais para a preservação da liberdade individual, pelo que requerem também a proteção adequada dos direitos individuais.

Não obstante todo o exposto, o direito à inviolabilidade do domicílio não é absoluto, existindo situações em que o Estado pode teoricamente violar esse direito, desde que haja justificação legítima e a observância de procedimentos adequados (o que tornam a pretensa violação lícita). Neste sentido, a invasão do domicílio físico ou virtual pode ocorrer mediante mandado judicial, quando há suspeita de prática de certos crimes ou ameaça à segurança pública. No entanto, a intervenção estatal é limitada legalmente e deve ser proporcional à finalidade pretendida e justificada, sempre respeitando a dignidade e os direitos fundamentais dos ocupantes da residência.

Rege quanto a este aspeto o art.º 32, n.º 8 da CRP, o qual nos refere que “São nulas todas as provas obtidas mediante tortura, coação, ofensa da integridade física ou moral

[109] Cfr. CANOTILHO, Gomes e MOREIRA, Vital (2007) – *Constituição da República Portuguesa Anotada*, 4.ª edição revista, volume I, Coimbra, Coimbra Editora, p. 541.

da pessoa, abusiva intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações".[110]

O art.º 34.º, n.º 1 da CRP especifica o domicílio e o sigilo da correspondência e dos outros meios de comunicação privada são invioláveis.

Sem prejuízo do exposto, o n.º 2 do referido artigo estabelece que a entrada no domicílio dos cidadãos contra a sua vontade só pode ser ordenada pela autoridade judicial competente, nos casos e segundo as formas previstos na lei.

Por seu turno, o n.º 3 coloca limites, dispondo que ninguém pode entrar durante a noite no domicílio de qualquer pessoa sem o seu consentimento, salvo em situação de flagrante delito ou mediante autorização judicial em casos de criminalidade especialmente violenta ou altamente organizada, incluindo o terrorismo e o tráfico de pessoas, de armas e de estupefacientes, nos termos previstos na lei.

E, por último, igualando o conceito de domicílio físico ao de domicílio virtual, o n.º 4 do referido art.º 34.º da CRP estabelece que é proibida toda a ingerência das autoridades públicas na correspondência, nas telecomunicações e nos demais meios de comunicação, salvos os casos previstos na lei em matéria de processo criminal.[111]

1.5- DIREITO AO SEGREDO DAS COMUNICAÇÕES

Paralelamente aos aspetos já referidos, temos o direito ao segredo das comunicações.

O direito ao segredo das comunicações é um princípio fundamental para a preservação da privacidade, da liberdade de expressão e do exercício pleno dos direitos individuais, o qual assegura que as comunicações realizadas por meio de correspondência via postal, telefónica, mensagens eletrónicas e outras formas de comunicação sejam protegidas contra interferências arbitrárias por parte do Estado ou de terceiros. Assim, o direito ao segredo das comunicações é um dos pilares fundamentais da proteção da privacidade e da liberdade individual dos cidadãos.

A importância do direito ao segredo das comunicações assenta no facto de que as comunicações privadas desempenham um papel central na vida quotidiana das

[110] Cfr. https://www.parlamento.pt/Legislacao/Documents/constpt2005.pdf (consultado a 14/09/2023).
[111] *Id*.

pessoas, seja por meio de telefonemas, mensagens de texto, e-mails ou aplicações de mensagens instantâneas, as pessoas têm o direito de expressar as suas opiniões, compartilhar informações pessoais e comunicar livremente com quem quiserem.[112]

Por conseguinte, a importância do direito ao segredo das comunicações reside fundamentalmente no facto de que as pessoas têm o direito de comunicar livremente, sem medo de serem espiadas, censuradas ou alvo de perseguições injustificadas, sendo tal direito essencial para o funcionamento de uma sociedade democrática e para o exercício efetivo da liberdade de expressão e do direito à informação.

Assim, a proteção do segredo das comunicações tem como base a ideia de que os indivíduos têm o direito de controlar a divulgação e o acesso às suas comunicações privadas, pelo que, este direito é garantido não apenas para proteger a privacidade individual, mas também para preservar a liberdade de expressão e a diversidade de opiniões na sociedade. Por conseguinte, também aqui tem aplicação o n.º 4 do art.º 34.º da CRP, o qual estabelece que é proibida toda a ingerência das autoridades públicas na correspondência, nas telecomunicações e nos demais meios de comunicação, salvos os casos previstos na lei em matéria de processo criminal.[113]

É que, apenas quando as pessoas se sentem seguras para se comunicar livremente, as mesmas estão livres para compartilhar ideias, expressar as suas opiniões e participar ativamente do debate público.

Uma vez mais, o avanço da tecnologia e das comunicações digitais trouxe novos desafios para a proteção do direito ao segredo das comunicações, dado que, a facilidade de acesso e armazenamento de informações digitais torna a privacidade das comunicações mais vulnerável a ameaças, como a intercetação ilegal, o acesso não autorizado aos dados pessoais ou a fuga de dados de que são exemplo os casos futebol *leaks*[114] ou vaticano *leaks*[115]*.*

Diante disto, é fundamental que as leis e regulamentações sejam permanentemente atualizadas e adaptadas para garantir a proteção adequada das comunicações digitais em cada momento. Além disso, o direito ao segredo das comunicações também se estende à proteção das fontes jornalísticas, permitindo que jornalistas e profissionais dos media possam exercer o seu papel de investigar, informar e trazer à tona questões

[112] Cfr. CONTE, Christiany Pegorari e FIORILLO, Celso Antonio Pacheco (2015) – *Crimes no Meio Digital*, Editora Saraiva, p.160.
[113] *Id*.
[114] Cfr. https://sicnoticias.pt/especiais/football-leaks (consultado a 20/09/2023)
[115] Cfr. https://www.bbc.com/news/world-europe-34703293 (consultado a 22/09/2023).

de interesse público sem medo de represálias ou perseguições. Neste sentido, tem aplicação o art.º 11.º, n.º 1 do Estatuto do Jornalista, o qual nos refere que "Sem prejuízo do disposto na lei processual penal, os jornalistas não são obrigados a revelar as suas fontes de informação, não sendo o seu silêncio passível de qualquer sanção, directa ou indirecta".[116]

No entanto, assim como o direito à inviolabilidade do domicílio, o direito ao segredo das comunicações não é absoluto e pode sofrer limitações em certas circunstâncias, designadamente, em casos de investigação criminal, motivo pelo qual a intercetação de comunicações pode ser autorizada mediante ordem judicial, desde que haja fundamentos legítimos e respeito aos princípios da proporcionalidade e da necessidade.

Ora, quanto a este aspeto, podemos já referir que tem aplicação (para além do Código de Processo Penal e das normas relativas às escutas telefónicas) o art.º 18.º, n.º 1 da Lei do Cibercrime[117], o qual estabelece que é admissível o recurso à interceção de comunicações em processos relativos a crimes:

> a) Previstos na presente lei; ou
>
> b) Cometidos por meio de um sistema informático ou em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico, quando tais crimes se encontrem previstos no artigo 187.º do Código de Processo Penal[118] [119].

Neste sentido, o Acórdão do Tribunal da Relação de Lisboa de 10/12/1991[120] debate a questão, afirmando que:

> I - O princípio da inviolabilidade da correspondência e das telecomunicações, consagrado no art. 34, n. 1 da Constituição, tem carácter absoluto, não admitindo a lei qualquer outra exceção, sendo por isso ilícitas as violações que não tenham sido

[116] Cfr. https://www.clubedejornalistas.pt/?page_id=120 (consultado a 22/09/2023).
[117] Cfr. https://guiadoinvestidor.dre.pt/PDF.aspx?Idioma=1&DecretoLeiId=25 (consultado a 29/09/2023).
[118] Cfr. https://guiadoinvestidor.dre.pt/PDF.aspx?Idioma=1&DecretoLeiId=25 (consultado a 29/09/2023).
[119] Para mais fácil entendimento:
Artigo 187.º CPP
Admissibilidade
1 - A interceção e a gravação de conversações ou comunicações telefónicas só podem ser autorizadas durante o inquérito, se houver razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter, por despacho fundamentado do juiz de instrução e mediante requerimento do Ministério Público, quanto a crimes:
a) Puníveis com pena de prisão superior, no seu máximo, a 3 anos;
b) Relativos ao tráfico de estupefacientes;
c) De detenção de arma proibida e de tráfico de armas;
d) De contrabando;
e) De injúria, de ameaça, de coação, de devassa da vida privada e perturbação da paz e do sossego, quando cometidos através de telefone;
f) De ameaça com prática de crime ou de abuso e simulação de sinais de perigo; ou
g) De evasão, quando o arguido haja sido condenado por algum dos crimes previstos nas alíneas anteriores.
[120] Cfr. http://www.dgsi.pt/jtrl.nsf/-/09444CCE314CEAA88025680300046A2B (consultado a 29/09/2023).

> autorizadas para fins de investigação criminal, nos termos da lei, ou autorizadas com o consentimento dos visados;
>
> II - O arguido ao intrometer-se, deliberada, livre e conscientemente na escuta da comunicação telefónica entre o assistente e um seu colega de trabalho, sem autorização de qualquer deles, cometeu o crime p. e p. pelo art. 128, n. 2, do CP.[121]

Ou seja, verificamos assim que, uma vez mais, estamos perante um direito absoluto, no sentido em que todos os cidadãos são titulares de direitos devendo estes ser respeitados por todos. Porém, em determinados casos esse direito pode ceder em face das exigências de investigação criminal.

1.6- DIREITO À AUTODETERMINAÇÃO INFORMACIONAL

O direito à autodeterminação informacional é um princípio que diz respeito ao controlo que os indivíduos têm sobre os seus dados pessoais e a forma como são obtidos, armazenados, utilizados e partilhados por terceiros, especialmente por entidades governamentais e empresas.[122]

Este direito reconhece a importância da privacidade e da liberdade individual na era da informação, uma vez que, à medida que vivemos em uma sociedade cada vez mais digitalizada, as nossas informações pessoais são obtidas e processadas de diversas maneiras e, desde dados básicos, como nome, endereço e número de telefone, até informações mais sensíveis, como histórico médico, preferências políticas e dados biométricos, estamos constantemente expostos a um fluxo crescente de informações pessoais.[123]

Assim, a autodeterminação informacional afirma que cada pessoa tem o direito de controlar essas informações e decidir como as mesmas são utilizadas, incluindo o direito de saber quais dados que podem ser obtidos pelas autoridades, o propósito dessa obtenção de dados, com quem esses dados são partilhados e ainda a possibilidade de consentir ou recusar o uso das suas informações pessoais.[124]

---

[121] Cfr. http://www.dgsi.pt/jtrl.nsf/-/09444CCE314CEAA88025680300046A2B (consultado a 29/09/2023).
[122] Neste sentido, o instrumento fundamental é o já referido Regulamento Geral de Proteção de Dados.
[123] A título de exemplo, podemos referir a Lei n.º 68/2021, de 26 de Agosto, a qual aprovou os princípios gerais em matéria de dados abertos e transpõe para a ordem jurídica interna a Diretiva (UE) 2019/1024 do Parlamento Europeu e do Conselho, de 20 de junho de 2019, relativa aos dados abertos e à reutilização de informação do setor público, alterando a Lei n.º 26/2016, de 22 de Agosto, Cfr. https://files.dre.pt/1s/2021/08/16600/0000200035.pdf (consultado a 09/09/2023).
[124] Cfr. PINHEIRO, Alexandre Sousa (2015) – *Privacy e proteção de dados: a construção dogmática do direito à identidade informacional*, Lisboa, pp. 695 e ss.

Este direito tem como base a ideia de que os dados pessoais pertencem ao indivíduo e que o seu controlo é essencial para a proteção da privacidade e da liberdade individual. Por conseguinte, a autodeterminação informacional procura evitar a instrumentalização dos indivíduos por meio do uso indiscriminado e abusivo de seus dados, garantindo que as pessoas possam exercer a sua autonomia e tomar decisões informadas sobre o compartilhamento e o uso de suas informações pessoais.

No entanto, o direito à autodeterminação informacional enfrenta desafios significativos na prática, dado que os termos de uso e as políticas de privacidade são complexos e de difícil compreensão, tornando difícil para os indivíduos exercerem efetivamente o seu controlo sobre os seus dados pessoais. Além disso, a obtenção e a partilha indiscriminada de dados por parte de empresas e governos levantam preocupações sobre a proteção da privacidade e o uso indevido das informações pessoais.[125]

Conforme nos refere Guilherme da Fonseca Teixeira (2018, p. 21):

> É possível identificar no direito à proteção de dados pessoais um recorte dogmático ou âmbito de tutela autónomo que, mais do que procurar garantir uma tutela dos dados pessoais dos cidadãos, consoante a maior ou menor proximidade das informações em causa com a esfera íntima, privada ou individual/social do sujeito (máxime, ao núcleo íntimo da pessoa), procura conferir ao titular dos dados o poder de manter na sua disponibilidade a gestão dos mesmos, configurando-se como o direito do indivíduo a controlar a obtenção, detenção, tratamento e transmissão de dados pessoais, autorizando a sua recolha, armazenamento, e utilização, conhecendo onde estão armazenados, a identidade dos responsáveis pelo seu tratamento e quais as suas finalidades, acedendo aos mesmos ou inclusivamente exigindo a sua alteração, retificação ou eliminação (habeas data)".[126]

Diante desses desafios, várias legislações e regulamentos têm sido implementados para fortalecer o direito à autodeterminação informacional. Por exemplo, o já referido Regulamento Geral de Proteção de Dados na União Europeia e outras leis de proteção de dados em diferentes países estabelecem regras mais rigorosas para o tratamento de dados pessoais, exigindo maior transparência, consentimento informado e direitos de acesso e exclusão dos dados.

Além disso, a consciencialização sobre a importância da proteção da privacidade e do controle sobre os dados pessoais tem aumentado, impulsionando movimentos e

[125] Cfr. PINHEIRO, Alexandre Sousa (2015) – *Privacy e proteção de dados: a construção dogmática do direito à identidade informacional*, Lisboa, pp. 695 e ss.
[126] Cfr. TEIXEIRA, Guilherme da Fonseca (2018) – *Identidade e autodeterminação informacional no novo Regulamento Geral de Proteção de Dados: a inevitável privatização dos deveres estaduais de proteção*, VOLUME II \ n.º 1 \ janeiro 2018, p. 21.

iniciativas para promover a educação digital, a adoção de práticas de privacidade e a consciencialização sobre os direitos individuais no ambiente digital.

O direito à autodeterminação informacional está intimamente ligado à proteção da privacidade e da liberdade individual na era digital, pelo que, este direito reconhece que cada pessoa tem o poder de controlar suas próprias informações pessoais e decide como elas são obtidas, utilizadas e divulgadas. Num mundo cada vez mais conectado, os nossos dados pessoais são coletados e processados em diversas situações, como ao realizar transações *online*, utilizar redes sociais, fazer compras ou até mesmo ao navegar na *internet*. Assim, o direito à autodeterminação informacional visa garantir que as pessoas tenham o poder de tomar decisões informadas sobre suas informações pessoais e que essas decisões sejam respeitadas.[127]

Um dos pilares desse direito é o princípio do consentimento informado, o que significa que as pessoas devem receber informações claras e compreensíveis sobre como as suas informações pessoais serão utilizadas antes de fornecê-las. O consentimento deve ser livre, específico, informado e revogável a qualquer momento e, ao exercer o seu direito à autodeterminação informacional, as pessoas podem decidir se desejam compartilhar suas informações pessoais e com quem desejam compartilhá-las.[128]

Além disso, o direito à autodeterminação informacional inclui o direito de aceder e retificar os seus próprios dados pessoais, o que significa que as pessoas têm o direito de solicitar acesso aos dados que foram obtidos e de corrigir qualquer informação imprecisa ou desatualizada, sendo esta transparência e controlo sobre as informações pessoais fundamentais para garantir a precisão e a integridade dos dados.

No entanto, é importante destacar que o direito à autodeterminação informacional não é absoluto[129] e existem situações em que a obtenção e o processamento de dados pessoais são necessários, como para fins de segurança pública, saúde pública ou interesse legítimo. No entanto, mesmo nessas circunstâncias, é fundamental que a obtenção e o uso dos dados sejam limitados, proporcionais e protegidos por medidas de segurança adequadas.

---

[127] Cfr. PINHEIRO, Alexandre Sousa (2015) – *Privacy e proteção de dados: a construção dogmática do direito à identidade informacional*, Lisboa, pp. 695 e ss.

[128] *Id*.

[129] Um exemplo bastante recente de ponderação dos interesses em confronto reporta-se ao chamado Acórdão dos Metadados, o Acórdão n.º 268/2022 do Tribunal Constitucional, disp. em https://www.tribunalconstitucional.pt/tc/acordaos/20220268.html (consultado a 26/09/2023), onde declara a inconstitucionalidade, com força obrigatória geral, de várias normas constantes da Lei n.º 32/2008, de 17 de julho, por violação de disposições consagradas na CRP.

1.7- DIREITO À INTEGRIDADE E CONFIDENCIALIDADE DOS SISTEMAS INFORMÁTICOS

Associado aos direitos atrás referidos, temos o direito à integridade e confidencialidade dos sistemas informáticos, o qual representa a concretização de um princípio que visa proteger a segurança e a privacidade das informações armazenadas e processadas em sistemas informáticos e reconhece a importância de manter a integridade dos sistemas e garantir a confidencialidade das informações neles contidas.

A integridade dos sistemas é essencial para assegurar a confiabilidade das informações armazenadas e para evitar danos e prejuízos decorrentes de violações de segurança. Em concreto, a integridade dos sistemas informáticos reporta-se à proteção contra alterações não autorizadas ou manipulações indevidas nos sistemas de informação, o que envolve medidas de segurança para evitar acessos não autorizados, garantir a autenticidade dos dados e prevenir a corrupção dos sistemas, direito que, de acordo com Fabiano Menke, é mesmo qualificado como um verdadeiro novo direito fundamental.[130]

Já a confidencialidade dos sistemas informáticos diz respeito à proteção dos dados e das informações contra acessos não autorizados, o que implica a implementação de medidas de segurança, como criptografia e autenticação, para garantir que apenas pessoas autorizadas possam aceder e visualizar as informações. Neste sentido, a confidencialidade é fundamental para proteger a privacidade das pessoas e salvaguardar informações sensíveis.[131]

O direito à integridade e confidencialidade dos sistemas informáticos abrange tanto sistemas de uso pessoal, como computadores e dispositivos móveis, quanto sistemas utilizados por organizações e empresas, sendo essencial que as partes envolvidas adotem medidas adequadas de segurança da informação para proteger os sistemas contra ameaças, como *malware*, ataques cibernéticos e invasões.[132]

---

[130] Cfr. MENKE, Fabiano (2019) – *A proteção de dados e o direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão*, RJLB, Ano 5 (2019), nº 1, p. 783.
[131] Cfr. ERD, Rainer (2008) – *Bundesverfassungsgericht versus Politik*, Kritische Justiz, pp. 118-133.
[132] Cfr. LIMBERGER, Têmis (2007) – *O direito à intimidade na era da informática*, Porto Alegre: Livraria do Advogado.

Além disso, o direito à integridade e confidencialidade dos sistemas informáticos também está relacionado ao princípio da responsabilidade. Os responsáveis pela gestão e administração dos sistemas têm a obrigação de garantir que as medidas adequadas sejam implementadas para proteger a integridade e confidencialidade dos dados, o que envolve a manutenção de sistemas atualizados, a implementação de políticas de segurança, a realização de auditorias e a resposta efetiva a incidentes de segurança.[133]

O direito à integridade e confidencialidade dos sistemas informáticos é especialmente relevante na era da tecnologia e da informação, em que a dependência de sistemas informáticos é amplamente disseminada e a perda de integridade dos sistemas ou a violação da confidencialidade das informações pode ter impactos tremendos tanto a nível económico quanto social e tanto em termos financeiros como na privacidade e na confiança das pessoas afetadas.

Uma vez mais, cumpre referir que este direito não é absoluto no sentido de prevalecer sempre e em qualquer situação, podendo o mesmo ser colocado em causa em situações de estrita necessidade, designadamente em termos de investigação criminal.

1.8- PRINCÍPIO DA PROPORCIONALIDADE

Associado a todos os direitos e princípios atrás enunciados, temos o princípio da proporcionalidade, que é um dos pilares fundamentais do Direito e da Justiça, que visa equilibrar e harmonizar interesses conflitantes numa sociedade democrática, sendo uma ferramenta essencial para avaliar e controlar a atuação dos poderes do Estado, garantindo que as suas ações sejam proporcionais aos objetivos pretendidos e respeitem os direitos individuais dos cidadãos.

De acordo com Vitalino Canas (1994, p. 1), estamos mesmo perante um verdadeiro

> (…) Princípio geral de direito, constitucionalmente consagrado, conformador dos atos do poder público e, em certa medida, de entidades privadas, de acordo com o qual a limitação instrumental de bens, interesses ou valores subjetivamente radicáveis se deve revelar idónea e necessária para atingir os fins legítimos concretos que cada um

[133] Cfr. ERD, Rainer (2008) – *Bundesverfassungsgericht versus Politik*, Kritische Justiz, pp. 118-133.

> daqueles atos visam, bem como axiologicamente tolerável quando confrontada com esses fins.[134]

A ideia central do princípio da proporcionalidade é a de que qualquer intervenção do Estado, seja ela legislativa, executiva ou judicial, deve ser proporcional aos fins que se visa alcançar, o que significa que, ao tomar uma decisão ou implementar uma política pública, o Estado deve considerar cuidadosamente se os meios utilizados são adequados, necessários e proporcionais aos objetivos pretendidos.

Em termos concretos, a proporcionalidade pode ser compreendida em três dimensões principais: a adequação, a necessidade e a proporcionalidade em sentido estrito.

Além disso, o princípio da proporcionalidade também está relacionado com o respeito pelos direitos fundamentais e à proteção da dignidade humana, o que quer dizer que qualquer restrição aos direitos individuais deve ser justificada e proporcionada, de forma a preservar a essência desses direitos e garantir que as pessoas sejam tratadas de forma justa e igualitária.

O princípio da proporcionalidade no âmbito da investigação criminal é uma ferramenta essencial para equilibrar os interesses do Estado na busca pela verdade e a proteção dos direitos fundamentais dos indivíduos envolvidos no processo de investigação, uma vez que se aplica tanto às ações das autoridades policiais quanto às decisões dos tribunais ao avaliar a legalidade e a legitimidade das medidas adotadas durante a investigação.

Neste sentido, as medidas adotadas durante a investigação criminal devem ser proporcionais aos direitos em causa, garantindo que a dignidade e a integridade dos indivíduos sejam preservadas, o que abrange a proteção contra tratamentos cruéis, desumanos ou degradantes, o direito à privacidade e à inviolabilidade domiciliaria, bem como o direito de não autoincriminação.[135] Assim, é importante destacar que o princípio da proporcionalidade não impede que sejam adotadas medidas restritivas de direitos durante a investigação, desde que sejam devidamente fundamentadas e necessárias para alcançar os objetivos legítimos do processo penal e que, para além disso, têm de

[134] Cfr. CANAS, Vitalino (1994) – *Proporcionalidade (Princípio da)* - Separata do vol. VI do Dicionário Jurídico da Administração Pública, p. 1.
[135] Cfr. ONETO, Isabel (2005) - *O agente infiltrado: contributo para a compreensão do regime jurídico das acções encobertas*. Coimbra: Coimbra Editora, p.187.

ser proporcionais à gravidade do crime e à necessidade de proteção dos interesses públicos, respeitando os direitos fundamentais dos investigados.[136]

Procurando resumir o alcance do princípio da proporcionalidade (também referido como proibição do excesso), podemos apresentar a versão simplificada de Jorge Miranda, para o qual, sempre se terá que ter em conta que o "Direito é proporção"[137], motivo pelo qual terá sempre que existir um justo equilíbrio das medidas, em respeito por um concreto dever de moderação e de proibição do excesso.

1.8.1 - O PRINCÍPIO DA ADEQUAÇÃO OU DA IDONEIDADE

O princípio da adequação, também conhecido como princípio da idoneidade, é um baluarte do Estado de Direito e visa assegurar que as medidas adotadas pelo Estado sejam adequadas e eficazes para alcançar os objetivos pretendidos, garantindo a efetividade das ações e a proteção dos direitos individuais dos cidadãos.

De acordo com Isabel Oneto (2005, p. 187) a vertente do princípio da adequação traduz-se "na exigência de que os meios utilizados sejam aptos a atingir os fins (…) pelo que a adequação do meio é indissociável da sua necessidade, pois que o meio poderá ser adequado, mas desnecessário".[138]

Assim, o princípio da adequação exige que a medida utilizada seja apropriada para atingir o fim desejado, o que significa que o meio escolhido deve ser capaz de produzir os resultados esperados, levando em consideração as características do caso concreto e as circunstâncias envolvidas.

Por outro lado, a adequação também está relacionada à relação causa-efeito entre a medida adotada e o objetivo pretendido, sendo necessário que exista uma conexão lógica entre ambos, de forma que a medida possa contribuir de maneira efetiva para a realização do propósito almejado. Por exemplo, se o objetivo é reduzir a taxa de criminalidade, é necessário avaliar se uma determinada política de segurança pública é de facto capaz de impactar positivamente na diminuição dos índices de criminalidade.

---

[136] Neste sentido, *vide* BRITO, Miguel Teixeira de (2020) – *Modelos de Emergência no Direito Constitucional*, Revista e-Pública Vol. 7 No. 1, abril 2020, p. 8.
[137] Cfr. MIRANDA, Jorge (2012) – *Manual de Direito Constitucional*, Tomo IV (Direitos Fundamentais), 5.ª ed., Coimbra Editora, Coimbra, p. 302.
[138] Cfr. ONETO, Isabel (2005) - *O agente infiltrado: contributo para a compreensão do regime jurídico das acções encobertas*. Coimbra: Coimbra Editora, p.187.

Além disso, o princípio da adequação envolve a análise da eficácia da medida adotada, sendo necessário verificar se ela é capaz de produzir os efeitos desejados de maneira efetiva, levando em consideração os recursos disponíveis e as circunstâncias práticas.[139]

No entanto, é importante ressaltar que o princípio da adequação deve ser aplicado em conjunto com outros princípios e valores jurídicos, como a proporcionalidade e a legalidade. Uma medida adequada não é suficiente por si só, também deve ser proporcional aos fins pretendidos e estar de acordo com os limites estabelecidos pela lei. Além disso, a escolha da medida mais adequada deve ser feita levando em consideração a proteção dos direitos fundamentais e o respeito à dignidade humana.[140]

A aplicação correta do princípio da adequação é fundamental para garantir a eficácia das ações do Estado, evitando medidas arbitrárias ou desnecessárias e contribui para o fortalecimento do Estado de Direito, assegurando que as decisões e políticas públicas sejam fundamentadas em critérios objetivos e racionalmente justificáveis. Além disso, ao exigir a adequação das medidas adotadas, o princípio da adequação contribui para a proteção dos direitos individuais e para a promoção de uma sociedade mais justa e equitativa.

Por este motivo, Gomes Canotilho (1974, p. 270) afirma que de ver realizado o chamado teste da adequação ou idoneidade enquanto "relação de adequação medida-fim"[141], sendo necessário ponderar se, em cada caso concreto, a medida aplicada será efetivamente apta ao fim a que se destina.

O princípio da adequação, também conhecido como princípio da idoneidade, desempenha, assim, um papel crucial na avaliação das medidas adotadas pelo Estado em diversas áreas, como legislação, administração pública e políticas públicas e visa garantir que as ações do Estado sejam adequadas e eficazes para alcançar seus objetivos, evitando medidas desnecessárias ou ineficientes.

[139] Cfr. ONETO, Isabel (2005) - *O agente infiltrado: contributo para a compreensão do regime jurídico das acções encobertas*. Coimbra: Coimbra Editora, p.187.
[140] Neste sentido, qualquer medida terá que respeitar o disposto no art.º 1.º da CRP, o qual nos refere que "Portugal é uma República soberana, baseada na dignidade da pessoa humana e na vontade popular e empenhada na construção de uma sociedade livre, justa e solidária", Cfr. https://www.parlamento.pt/Legislacao/Documents/constpt2005.pdf (consultado a 26/09/2023).
[141] Cfr. CANOTILHO, Gomes (1974) – *O problema da responsabilidade do Estado por actos lícitos*, p. 270.

Assim, a adequação diz respeito à relação entre o meio utilizado e o objetivo a ser alcançado, sendo preciso verificar se a medida adotada é apropriada e eficaz para atingir o fim pretendido.

Com vista a entendermos o alcance prático, a título de exemplo de aplicação concreta da vertente da adequação, embora seja quanto à aplicação de medidas de coação, podemos referir o Acórdão do Tribunal da Relação do Porto de 27/10/2010, o qual nos refere que:

> I - Na aplicação de medidas de coacção e de garantia patrimonial, o princípio da adequação (art. 193.º, n.º 1, I parte, do CPP) comporta uma formulação positiva, relacionada com a eficácia que se obtém através da medida; e uma vertente garantística, que se reconduz ao princípio da subsidiariedade, nos termos do qual a aplicação de cada uma das medidas só se justifica quando todos os outros meios se revelam ineficazes para tutelar os interesses subjacentes.
>
> II - O princípio da proporcionalidade (art. 193.º, n.º 1, II parte) assenta em dois vetores: um ligado à gravidade do crime e outro à previsibilidade da sanção.
>
> III - No caso particular da prisão preventiva, o princípio da proporcionalidade tem a função negativa de limitar a aplicação da medida aos casos em que a pena final previsível seja de prisão efectiva, aspecto cuja avaliação por vezes passa em claro.[142]

1.8.2 - O PRINCÍPIO DA NECESSIDADE

O princípio da necessidade, enquanto corolário do princípio da proporcionalidade, é um conceito que permeia diversas áreas do conhecimento humano e está profundamente enraizado nas bases da sobrevivência, da justiça e do bem-estar social, tratando-se de uma ideia fundamental que reconhece a importância de utilizar apenas os recursos essenciais para alcançar determinado fim, evitando o desperdício e privilegiando a eficiência.

No âmbito legal, o princípio da necessidade é aplicado como um critério para a restrição de direitos fundamentais, quando existe uma situação excecional que exige a proteção de outros valores igualmente importantes. Neste sentido, o Estado pode restringir temporariamente alguns direitos individuais em prol do bem comum, desde que tal restrição seja necessária, proporcional e devidamente fundamentada.

[142] Disp. *in* http://www.dgsi.pt/jtrp.nsf/-/B34AD90C1A686669802577E3003ECE30 (consultado a 26/09/2023).

Para entendermos o alcance do princípio da proporcionalidade na sua vertente da necessidade (mas também nas suas outras vertentes), cumpre apreciar o Acórdão do Supremo Tribunal de Justiça de 31/03/2011.[143]

> (…) sob o prisma do princípio da proporcionalidade importa distinguir os requisitos da idoneidade, necessidade e da proporcionalidade em sentido estrito. Estas três exigências são requisitos intrínsecos de toda a medida processual restritiva de direitos fundamentais e exigíveis, tanto no momento da sua previsão pelo legislador, como na sua aplicação prática.
>
> VIII - O respeito pelo princípio da idoneidade exige que as limitações dos direitos fundamentais antecipadas pela lei estejam adaptadas aos fins legítimos a que se dirigem e que as mesmas sejam adequadas à prossecução das finalidades em função da sua adequação quantitativa e qualitativa e de seu espaço de aplicação subjetivo. Significa o exposto que o juízo sobre a idoneidade não se esgota na comprovação da aptidão abstrata de uma medida determinada para conseguir determinado objetivo, nem na adequação objetiva da mesma, tendo em consideração as circunstâncias concretas, mas também requer o respeito pelo princípio da idoneidade a forma concreta e ajustada como é aplicada a medida para que não se persiga uma finalidade diferente da antecipada pela lei.
>
> IX - Pela aplicação do princípio da necessidade a entidade vocacionada para aplicar a medida conformada pelo mesmo princípio deve eleger, entre aquelas medidas que são igualmente aptas para o objetivo pretendido que aquela é menos prejudicial para os direitos dos cidadãos.
>
> X -Por último, o uso do princípio da proporcionalidade em sentido estrito implica que se verifique se o sacrifício dos direitos individuais sujeitos à sua aplicação consagra uma relação razoável ou proporcional com a importância do objetivo que se pretende atingir.
>
> XI - O processo penal é um campo fundamental para tal exercício e, nessa sequência, as medidas restritivas de direitos, ou seja a limitação ao *jus libertatis* de cada um de nós terá a sua justificação numa tarefa que é exercida em nome de toda a comunidade no exercício de um *jus puniendi*, que não é mais do que uma defesa de bens jurídicos indispensáveis à vida em sociedade. O mesmo princípio da proporcionalidade constitui, conjuntamente com os pressupostos materiais de previsão constitucional expressa, fundamento de restrições ao exercício de direitos, liberdades e garantias com foro constitucional.[144]

Um exemplo concreto deste princípio é observado claramente em períodos de crise, como ocorreu durante a pandemia global da COVID-19 que levou a que tivessem que ser adotadas medidas de restrição à circulação de pessoas, visando conter a propagação do vírus e evitar o colapso dos sistemas de saúde. Embora essas medidas

[143] Disp. *in* http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/4d6e3c6c9e4bf7f6802578d900305716?OpenDocument (consultado a 09/10/2023).

[144] Disp. *in* http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/4d6e3c6c9e4bf7f6802578d900305716?OpenDocument (consultado a 09/10/2023).

tenham impactado negativamente em diversos direitos individuais, a sua adoção foi considerada necessária para garantir a saúde pública e preservar vidas.[145]

A necessidade está relacionada à existência de alternativas menos restritivas de direitos que possam alcançar o mesmo objetivo, o que significa que, se existirem medidas menos invasivas ou que causem menos restrições aos direitos individuais, o Estado deve preferir essas alternativas. Esta é uma forma de evitar o uso desnecessário ou excessivo do poder, garantindo que as restrições impostas sejam realmente indispensáveis.

Neste sentido, nas palavras de Gomes Canotilho, o princípio da proporcionalidade tem a sua base no conceito de necessidade e na concreta e específica necessidade de limitação das medidas prejudiciais ao mínimo necessário para que possa ser atingido determinado fim, tendo assim o cidadão direito a suportar a menor desvantagem possível[146].

A título de exemplo, podemos referir o campo da ecologia, em que a preservação da biodiversidade e dos ecossistemas também se baseia no princípio da necessidade, reconhecendo-se que a utilização excessiva dos recursos naturais e a destruição dos habitats têm consequências negativas para o equilíbrio ecológico, comprometendo a sobrevivência não apenas de espécies individuais, mas de todo o planeta. Assim, a adoção de práticas sustentáveis e a consciencialização sobre a importância da preservação são fundamentais para garantir a sobrevivência das gerações futuras.

Também no contexto social o princípio da necessidade pode ser aplicado para reduzir as desigualdades e promover a justiça, uma vez que, reconhecer as necessidades básicas de todos os indivíduos e garantir que elas sejam atendidas, é uma premissa para uma sociedade mais equitativa, o que implica em garantir o acesso à educação, saúde, moradia digna, alimentação adequada e outros direitos fundamentais, de modo que cada pessoa possa ter condições mínimas para viver com dignidade.

Já no âmbito relacionado especificamente com o nosso tema, o da investigação criminal, o princípio da necessidade desempenha um papel fundamental para que a busca pela verdade se concilie com a garantia dos direitos fundamentais dos indivíduos envolvidos e implica que as medidas adotadas durante uma investigação sejam estritamente

[145] Cfr. BRITO, Miguel Teixeira de (2020) – *Modelos de Emergência no Direito Constitucional*, Revista e-Pública Vol. 7 No. 1, abril 2020, p. 8
[146] Cfr. CANOTILHO, Gomes (2018) – *Direito Constitucional e Teoria da Constituição*, Almedina, Coimbra, p. 270.

necessárias e proporcionais aos objetivos buscados, evitando-se excessos e abusos por parte das autoridades.

Ao aplicar o princípio da necessidade em investigações criminais, é essencial que as autoridades atuem de forma criteriosa e fundamentada, levando em consideração a gravidade do delito, o risco para a sociedade e a preservação dos direitos individuais, o que significa que as medidas de investigação, como a intercetação telefónica, a quebra de sigilo bancário, a busca e apreensão, entre outras, devem ser justificadas pela necessidade concreta de se obter provas relevantes para o caso em questão.

Assim, o princípio da necessidade também está ligado à proporcionalidade das medidas adotadas, enquanto seu próprio corolário, o que significa que as restrições impostas durante a investigação devem ser proporcionais ao fim pretendido, evitando-se medidas excessivas ou desproporcionais que possam prejudicar a dignidade e os direitos dos investigados.

Ademais, o princípio da necessidade também se relaciona com a presunção de inocência, a qual representa um princípio fundamental do direito penal[147]. A investigação criminal deve ser direcionada a obter provas que permitam comprovar a culpa ou a inocência do suspeito, evitando-se, assim, a perseguição arbitrária ou a utilização de recursos desnecessários que possam comprometer a dignidade do indivíduo e sua reputação. Neste contexto, é importante que as autoridades encarregadas da investigação criminal adotem um enfoque baseado em evidências e busquem o equilíbrio entre a necessidade de coletar informações relevantes e a proteção dos direitos dos envolvidos, com a adoção de técnicas de investigação adequadas, respeito aos limites legais e a devida fundamentação de cada medida adotada são aspetos essenciais para assegurar a legitimidade e a efetividade do processo de investigação.

[147] Artigo 32.º da CRP
(Garantias de processo criminal)
1. O processo criminal assegura todas as garantias de defesa, incluindo o recurso.
2. Todo o arguido se presume inocente até ao trânsito em julgado da sentença de condenação, devendo ser julgado no mais curto prazo compatível com as garantias de defesa.

1.8.3 - O PRINCÍPIO DA PROPORCIONALIDADE EM SENTIDO ESTRITO

Por último, o terceiro corolário do princípio da proporcionalidade é a proporcionalidade em sentido estrito, o qual representa uma importante ferramenta utilizada no campo legal para avaliar a validade e a adequação das medidas adotadas pelo Estado.

De acordo com Manuel Monteiro Guedes Valente (2008, p. 64 e 65), a proporcionalidade em sentido estrito assenta numa concreta ponderação entre o meio e os fins desejados, sendo por isso necessário a verificação de "(…) uma proporcionalidade quanto às finalidades do processo *sub judice* – quer de prevenção quer de investigação criminal – e quanto à gravidade do crime em investigação ou a investigar".[148]

Assim, este princípio estabelece que as restrições impostas aos direitos individuais devem ser proporcionais aos objetivos, garantindo um equilíbrio entre o interesse público e a proteção dos direitos fundamentais.

O princípio da proporcionalidade em sentido restrito é frequentemente utilizado como um critério de controlo da atuação estatal, especialmente quando ocorre uma colisão entre direitos fundamentais, o que significa que, ao tomar uma medida que restrinja determinado direito, o Estado deve demonstrar que essa restrição é estritamente necessária e que não existem alternativas menos invasivas para alcançar o mesmo objetivo.

Tal princípio também está presente na ética, na política e na tomada de decisões em geral, visando garantir que as ações tomadas sejam equilibradas e justas, evitando medidas excessivas ou desproporcionais que possam causar mais danos do que benefícios. Na ética, o princípio da proporcionalidade em sentido estrito é utilizado para avaliar a moralidade de uma ação, exigindo que os benefícios alcançados por uma ação sejam proporcionais às possíveis consequências negativas que ela possa gerar. Dessa forma, é necessário ponderar cuidadosamente os interesses em jogo e buscar um equilíbrio justo na tomada de decisões éticas.

De acordo com Vitalino Canas, a proporcionalidade em sentido estrito é um microconceito dentro do macroconceito princípio da proporcionalidade[149]. Ora, na política, o princípio é fundamental para garantir a legitimidade das ações do Estado. Os

[148] Cfr. VALENTE, Manuel Monteiro Guedes (2008) **–** *Escutas telefónicas: Da excepcionalidade à vulgaridade*. 2.ª ed.. Coimbra: Almedina, pp. 64 e 65

[149] Cfr. CANAS, Vitalino (1998) — *O princípio da proibição do excesso na Constituição: arqueologia e aplicações*, in Perspectivas Constitucionais — Nos 20 Anos da Constituição de 1976 (org. Jorge Miranda), vol. II, Coimbra, Coimbra Editora, p.323-325.

Governos devem agir de forma proporcional, considerando o impacto das suas políticas sobre a população e assegurando que não haja excessos ou abusos de poder, pelo que, a proporcionalidade é um elemento central na manutenção do Estado de Direito e no respeito aos direitos fundamentais dos cidadãos.

No âmbito da tomada de decisões em geral, o princípio da proporcionalidade em sentido estrito é uma ferramenta valiosa para avaliar as opções disponíveis e escolher a melhor solução, incentiva uma análise cuidadosa dos custos e benefícios de cada alternativa, levando em consideração os diferentes interesses e valores envolvidos, pelo que, ao aplicar este princípio, se visa evitar decisões precipitadas ou desequilibradas, privilegiando a racionalidade e a justiça.

É importante ressaltar, no entanto, que a aplicação do princípio da proporcionalidade em sentido estrito requer uma análise cuidadosa e contextualizada, devendo ser consideradas as circunstâncias particulares de cada situação, levando-se em conta os valores, os direitos e os interesses envolvidos, motivo pelo qual não há fórmula única para aplicar esse princípio, pois cada caso demandará uma avaliação individualizada.

Por fim, a proporcionalidade em sentido estrito avalia se os benefícios obtidos com a medida adotada justificam as restrições impostas aos direitos individuais, ou seja, verifica-se se estamos perante uma solução que procura equilibrar os interesses em conflito, ponderando os custos e benefícios envolvidos, sendo importante que o Estado leve em consideração não apenas os efeitos imediatos da medida, mas também as suas consequências de longo prazo.

1.9 - MÉTODOS DE COMBATE À VIOLAÇÃO DOS DIREITOS E PRINCÍPIOS ENUNCIADOS

Conforme se referiu já, a investigação criminal desempenha um papel crucial na busca pela verdade e na manutenção da ordem social, podendo – mediante o cumprimento de diversos requisitos – violar teoricamente alguns direitos fundamentais dos cidadãos em causa.

É essencial que qualquer processo de investigação seja conduzido dentro dos limites legais, sob pena de ser ilícito e de violar os direitos fundamentais dos cidadãos, o que pode resultar em consequências graves, minando a credibilidade do sistema de justiça e prejudicando a confiança da população.

Assim, para combater essa violação, é necessário adotar métodos eficazes que promovam a justiça e preservem a integridade do processo de investigação.

Sobre esta matéria, António da Silva Henriques Gaspar esclarece-nos que a lei possui mecanismos de controlo da investigação, impondo, por um lado, a existência de inquérito e, por outro, a concreta delimitação dos factos a investigar, devendo o JIC realizar uma ponderação tendo em conta todas as probabilidades, ponderando se os concretos elementos de prova a obter poderiam ter surgido por outra via menos lesiva que não o recurso à escuta telefónica.[150]

Paralelamente ao exposto, é essencial investir na formação adequada dos agentes responsáveis pela investigação criminal. Os profissionais envolvidos devem ser devidamente treinados sobre os direitos fundamentais dos cidadãos e os limites legais que regem suas ações, incluindo conhecimento aprofundado sobre a Constituição, tratados internacionais e leis nacionais que garantem a proteção dos direitos humanos. Além disso, é importante enfatizar a importância da ética e do respeito aos princípios fundamentais durante todo o processo investigativo.

Por outro lado, a implementação dos referidos mecanismos de controlo e de supervisão é crucial para evitar abusos e violações dos direitos dos cidadãos, com a existência de entidades dotadas de poderes e recursos adequados para fiscalizar as atividades dos órgãos de investigação criminal, garantindo que estes atuem de acordo com a lei e respeitem os direitos fundamentais dos cidadãos.

Noutro âmbito, é importante fortalecer a transparência e a prestação de contas no processo de investigação criminal. A divulgação de informações relevantes para a sociedade, de forma responsável e respeitando o sigilo necessário, contribui para aumentar a confiança dos cidadãos no sistema. Além disso, a criação de canais de denúncia seguros e acessíveis, bem como a proteção efetiva dos denunciantes, são medidas importantes para garantir que violações dos direitos fundamentais sejam reportadas e investigadas adequadamente.

Por fim, a utilização de tecnologias avançadas pode ser uma aliada na prevenção de violações dos direitos fundamentais durante a investigação criminal. O uso das chamadas *bodycams*, por exemplo, pode fornecer registos objetivos das ações dos agentes de segurança no âmbito de concretas investigações criminais, evitando

[150] Cfr. GASPAR, António da Silva Henriques *et al*. (2016) – *Código de Processo Penal Comentado*, Coimbra: Almedina, 2.ª ed., p. 790.

possíveis abusos[151]. Além disso, o uso de técnicas de análise forense digital pode contribuir para a obtenção de provas de maneira mais eficaz, minimizando o risco de violações de direitos.

A violação dos direitos fundamentais dos cidadãos durante a investigação criminal é um problema sério que requer ações contundentes para combater e prevenir abusos. Nesse sentido, é essencial promover a consciencialização sobre os direitos individuais e assegurar que sejam respeitados em todas as etapas do processo de investigação criminal levado a cabo.

Por conseguinte, é importante estabelecer salvaguardas legais e institucionais que protejam os direitos dos cidadãos durante a investigação, o que inclui a garantia do acesso a um advogado desde o início do processo, o direito a um julgamento justo e a proibição de práticas abusivas, como a tortura e os tratamentos cruéis, desumanos ou degradantes.[152]

Para tal, as leis devem ser claras e aplicadas de maneira consistente para evitar interpretações arbitrárias que possam levar a violações dos direitos fundamentais. Adicionalmente, é fundamental promover uma cultura de respeito aos direitos fundamentais em todos os níveis da sociedade, com a consciencialização e a educação da população sobre seus direitos e a importância de respeitar os direitos dos outros. As organizações da sociedade civil desempenham um papel importante nesse sentido, ao monitorizar o cumprimento das normas legais e ao denunciar violações aos órgãos competentes.

---

[151] Cfr. https://www.publico.pt/2023/04/27/sociedade/noticia/psp-gnr-vao-receber-primeiras-2500-bodycams-novembro-2047715 (consultado a 10/10/2023).

[152] Artigo 20.º da CRP
(Acesso ao direito e tutela jurisdicional efetiva)
1. A todos é assegurado o acesso ao direito e aos tribunais para defesa dos seus direitos e interesses legalmente protegidos, não podendo a justiça ser denegada por insuficiência de meios económicos.
2. Todos têm direito, nos termos da lei, à informação e consulta jurídicas, ao patrocínio judiciário e a fazer-se acompanhar por advogado perante qualquer autoridade.
3. A lei define e assegura a adequada proteção do segredo de justiça.
4. Todos têm direito a que uma causa em que intervenham seja objeto de decisão em prazo razoável e mediante processo equitativo.
5. Para defesa dos direitos, liberdades e garantias pessoais, a lei assegura aos cidadãos procedimentos judiciais caracterizados pela celeridade e prioridade, de modo a obter tutela efetiva e em tempo útil contra ameaças ou violações desses direitos.

2 - OS PRINCÍPIOS DO PROCESSO PENAL COLOCADOS EM CAUSA PELO *MALWARE*

No sistema de justiça penal português vigora o modelo acusatório do processo que, contrariamente do que sucede no modelo inquisitório - onde o arguido se apresenta como culpado até prova em contrário, inclui um conjunto de princípios, a somar aos acima referidos, corolários de um Estado de Direito. Poderíamos citar outros, como o princípio de presunção de inocência ou o princípio de garantia de um processo justo e equitativo ainda assim, optámos por nos debruçar apenas sobre o princípio da legalidade da prova uma vez que assume elevada importância em face da atuação do meio de obtenção prova a que alude o presente relatório.

2.1-PRINCÍPIO DA LEGALIDADE DA PROVA

A somar aos diversos princípios já referidos, o princípio da legalidade da prova é um dos pilares fundamentais do sistema jurídico num estado de direito democrático, o qual estabelece que as provas apresentadas num processo judicial devem ser obtidas de acordo com as normas legais e respeitar os direitos individuais. Este princípio encontra-se plasmado, entre outros, no art.º 32.º, n.º 8 da CRP, o qual nos refere que "São nulas todas as provas obtidas mediante tortura, coação, ofensa da integridade física ou moral da pessoa, abusiva intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações"[153] e visa assegurar a validade e a legitimidade das evidências apresentadas, bem como a proteção dos direitos fundamentais dos envolvidos no processo.

Em termos simples, o princípio da legalidade da prova significa que não é permitido utilizar qualquer meio para obter provas, mas somente aqueles que estão previstos e autorizados por lei, o que implica desde logo que as autoridades devam seguir procedimentos legais adequados para obter, preservar e apresentar as provas durante uma investigação ou julgamento.

O respeito ao princípio da legalidade da prova é crucial para garantir um sistema de justiça justo e equitativo e assegurar que os direitos individuais sejam protegidos, prevenindo abusos e garantindo que as autoridades não ultrapassem os limites estabelecidos pela lei na obtenção de provas. Dessa forma, o princípio busca evitar a

[153] Cfr. https://www.parlamento.pt/Legislacao/Documents/constpt2005.pdf (consultado a 03/06/2023).

utilização de provas obtidas por meios ilícitos, como tortura, coação, invasão abusiva de privacidade ou violação de direitos constitucionais.

Além disso, o princípio da legalidade da prova também exige que as provas sejam admissíveis perante o sistema jurídico, o que significa que as provas devem ser obtidas de forma legal, por meio de métodos aceites pela legislação aplicável, sendo totalmente inadmissível o uso de provas obtidas de maneira ilegal, não podendo um arguido ser condenado com base nas mesmas desde logo pela violação do princípio da legalidade, mas também por violação do seu direito de defesa.

Neste sentido, cumpre referir o art.º 219.º, n.º 1 da Constituição da República Portuguesa, o qual dispõe que:

> Ao Ministério Público compete representar o Estado e defender os interesses que a lei determinar, bem como, com observância do disposto no número seguinte e nos termos da lei, participar na execução da política criminal definida pelos órgãos de soberania, exercer a ação penal orientada pelo princípio da legalidade e defender a legalidade democrática.[154]

No seguimento do já referido, a crescente utilização de tecnologias digitais tem transformado profundamente as áreas de investigação criminal e cibersegurança e, nesse contexto, o recurso ao *malware* como uma ferramenta para obtenção de provas tem gerado um debate acalorado sobre os limites legais e éticos dessa prática e sua compatibilidade com o princípio da legalidade.

No que concerne em específico ao princípio da legalidade, cumpre referir o art.º 125.º do Código de Processo Penal, o qual, em conformidade com a Constituição, estabelece que apenas são admissíveis as provas que não forem proibidas por lei.[155]

E, por seu turno, o art.º 2.º do Código de Processo Penal, no que respeita à legalidade do processo, estabelece que aplicação de penas e de medidas de segurança criminais apenas poderá ter lugar em conformidade com as disposições do próprio Código de Processo Penal.[156]

Ora, uso de *malware* em investigações pode comprometer seriamente a privacidade dos indivíduos envolvidos, dado que a instalação clandestina de *software* malicioso em

[154] Cfr. https://www.parlamento.pt/Legislacao/Documents/constpt2005.pdf (consultado a 04/06/2023).
[155] Cfr. https://dre.pt/dre/legislacao-consolidada/decreto-lei/1987-34570075 (consultado a 07/06/2023).
[156] *Id*.

dispositivos pessoais invade a esfera privada dos suspeitos e, em alguns casos, também afeta terceiros não relacionados ao crime investigado.

Por conseguinte, essa vigilância descontrolada levanta questões sobre o direito à privacidade e a proteção dos dados pessoais, colocando em risco a confiança no sistema de justiça.

Paralelamente, o uso do *malware* como meio de obtenção de provas pode levar a abusos e uso indiscriminado por parte das autoridades. Caso não exista uma estrutura clara e regulamentação adequada, existe o risco de o recurso ao *malware* se tornar uma prática rotineira e desproporcional, o que poderia levar a violações dos direitos individuais e à criminalização em massa, comprometendo o princípio da presunção de inocência.

Outro perigo relevante é a possibilidade de comprometimento da integridade das provas obtidas por meio do *malware*.

A natureza intrusiva e complexa dessa técnica pode levantar dúvidas sobre a autenticidade e a confiabilidade das provas, especialmente quando não há um controlo adequado da cadeia de comando. A manipulação inadvertida ou mal-intencionada das informações obtidas por meio do *malware* pode resultar na invalidação das provas e na deterioração da credibilidade do sistema de justiça.

Por todo o exposto, embora o recurso ao *malware* em investigações possa ser uma ferramenta poderosa para combater a criminalidade, é essencial considerar os perigos envolvidos, dado que a proteção da privacidade, a prevenção de abusos e a garantia da integridade das provas são questões fundamentais que não podem ser ignoradas.

Assim, é necessário estabelecer um equilíbrio cuidadoso entre a eficácia da investigação e o respeito pelos direitos individuais com a definição de diretrizes claras, a supervisão adequada e o desenvolvimento de tecnologias que respeitem os princípios legais a emergir como passos cruciais para mitigar os riscos e preservar a confiança no sistema de justiça. A busca pela justiça deve ser sempre guiada pela ética e pelo respeito aos direitos fundamentais de todos os envolvidos, mesmo num mundo cada vez mais digital e complexo.

Para entendermos a importância do princípio da legalidade aplicado à obtenção de provas, incluindo a interceção de informações, cumpre apreciar o Acórdão do Supremo Tribunal de Justiça de 10/11/2010[157], o qual nos afirma que:

> III - Como se sabe, o princípio da legalidade da prova, perfilhado pelo art. 125.º do CPP, considera "admissíveis as provas que não forem proibidas por lei" [e que] em processo penal não existe um verdadeiro ónus da prova em sentido formal; nele vigora o princípio da aquisição da prova ligado ao princípio da investigação, donde resulta que são boas as provas validamente trazidas ao processo, sem importar a sua origem, devendo o tribunal, em último caso, investigar e esclarecer os factos na procura da verdade material.
>
> IV - Perante as provas admissíveis, é dos princípios gerais da produção da prova que o tribunal ordena, oficiosamente ou a requerimento, a produção de todos os meios de prova cujo conhecimento se lhe afigure necessário à descoberta da verdade e à boa decisão da causa – art. 340.º, n.º 1, do CPP – sem prejuízo do contraditório (n.º 2 do preceito). Vigora, por outro lado, o princípio da livre apreciação da prova, conforme art. 127.º do CPP, que dispõe: Salvo quando a lei dispuser diferentemente, a prova é apreciada segundo as regras da experiência e a livre convicção da entidade competente.[158]

Neste sentido, o Código de Processo Penal estabelece uma série de proibições de prova aplicáveis no âmbito da interceção das comunicações telefónicas e eletrónicas., de entre as quais podemos destacar:

> A proibição de utilização de meios de prova obtidos com violação de direitos fundamentais, por meios fraudulentos, simulados ou que não correspondam à verdade (art.º 126.º CPP);
>
> A proibição de utilização de declarações obtidas através de tortura, coação, violência, ameaça ou outras formas de pressão psicológica (art.º 126.º CPP)[159];
>
> A proibição de utilização de provas que sejam obtidas através de escutas telefónicas ou outras formas de vigilância sem autorização judicial (art.º 187.º CPP);
>
> Ou ainda,
>
> A proibição de utilização de provas obtidas por intermédio de busca domiciliária ou pessoal que não respeite as formalidades legais e constitucionais (art.º 177.º CPP).[160]

[157] Cfr. http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/f26cbff0474ec694802570ae006223a2?OpenDocument (consultado a 15/06/2023).

[158] Cfr. http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/f26cbff0474ec694802570ae006223a2?OpenDocument (consultado a 15/06/2023).

[159] Cfr. https://dre.pt/dre/legislacao-consolidada/decreto-lei/1987-34570075-50512275 (consultado a 15/06/2023).

[160] Cfr. https://dre.pt/dre/legislacao-consolidada/decreto-lei/1987-34570075-50512275 (consultado a 15/06/2023).

CAPÍTULO IV- O *MALWARE* ENQUANTO MEIO OCULTO DE INVESTIGAÇÃO CRIMINAL

1- A UTILIZAÇÃO DE *MALWARE* NA LEI PORTUGUESA – ENQUADRAMENTO LEGAL

No seguimento do que fomos referindo nos capítulos anteriores, cumpre salientar que a evolução tecnológica – felizmente – não se aplica apenas aos criminosos. Neste sentido, as autoridades de investigação criminal também procuram atualizar os seus conhecimentos e métodos de investigação. Assim, nos últimos anos, o avanço tecnológico tem proporcionado diversas ferramentas para o combate ao crime.

No entanto, nem todas as vias evolutivas são isentas de críticas. Uma abordagem polémica é a possibilidade de as autoridades policiais utilizarem *malware* para recolher elementos probatórios em inquéritos. A referida prática levanta questões éticas, jurídicas e de privacidade, uma vez que o uso de *malware* para fins de investigação representa uma intrusão nos direitos fundamentais dos cidadãos, o que contradiz o preconizado constitucionalmente no art.º 32º n.º 8 da CRP.[161]

É necessário ponderar os diversos aspetos em confronto, por forma a encontrar um equilíbrio entre o respeito pelos direitos dos cidadãos e a necessidade de prevenção e repressão por parte do Estado.

Assim, como benefícios da utilização de *malware* pela polícia podemos referir uma maior facilidade na identificação e rastreamento de criminosos, dado que o uso de *malware* pode permitir às autoridades identificar e rastrear criminosos digitais que operam na *dark web* ou em outros espaços virtuais ocultos, o que poderá facilitar a prevenção de crimes graves e o desmantelamento de redes criminosas. Com recurso ao *malware* a polícia poderá infiltrar-se em organizações criminosas e obter informações valiosas, facilitando assim o desmantelamento dessas redes.

Na outra face da moeda está o desrespeito pelos direitos dos cidadãos em face de uma invasão flagrante da privacidade. O uso de *malware* pela polícia para aceder a dispositivos pessoais e obter informações, como vimos atrás, pode pôr em causa direitos fundamentais relativos à privacidade, colocando em risco a liberdade dos cidadãos. Paralelamente, podemos afirmar que tal prática poderá consubstanciar abuso

[161] Cfr. Constituição da República Portuguesa - CRP | DR (diariodarepublica.pt) (consultado em 13/03/2023)

de poder, ampliando a possibilidade de vigilância em massa e a criação de um Estado policial. Ademais, tal prática é perigosa, uma vez que o uso de *malware* também pode resultar em vulnerabilidades que poderão ser exploradas por hackers maliciosos, expondo informações confidenciais de inocentes.

Isto posto, cumpre referir que o regime processual penal e penal português é um regime bastante garantístico dos cidadãos e dos arguidos, pelo que, qualquer investigação e qualquer condenação em processo penal terão de respeitar escrupulosamente os princípios e normas plasmadas na lei portuguesa.[162]

Ora, nos termos em que se encontra presentemente formulada a lei portuguesa, consideramos que é proibido o uso de *malware* como forma de obtenção de prova, pois dessa forma são violados direitos de privacidade e proteção de dados dos indivíduos para lá do permitido. Como resultado, quaisquer provas obtidas através desse método devem ser consideradas proibidas (art.º 126.º, n.º 1 CPP).[163]

É este o resultado da nossa apreciação do art.º 126.º, n.º 1 do CPP, o qual dispõe que que são nulas, não podendo ser utilizadas, as provas obtidas mediante tortura, coação ou, em geral, ofensa da integridade física ou moral das pessoas.[164]

Por seu turno, o n.º 2 do referido artigo estabelece que são ofensivas da integridade física ou moral das pessoas as provas obtidas, mesmo que com consentimento delas, mediante:

> a) Perturbação da liberdade de vontade ou de decisão através de maus-tratos, ofensas corporais, administração de meios de qualquer natureza, hipnose ou utilização de meios cruéis ou enganosos;
>
> b) Perturbação, por qualquer meio, da capacidade de memória ou de avaliação;
>
> c) Utilização da força, fora dos casos e dos limites permitidos pela lei;
>
> d) Ameaça com medida legalmente inadmissível e, bem assim, com denegação ou condicionamento da obtenção de benefício legalmente previsto;

[162] Artigo 29.º da Constituição da República Portuguesa
(Aplicação da lei criminal)
1. Ninguém pode ser sentenciado criminalmente senão em virtude de lei anterior que declare punível a acção ou a omissão, nem sofrer medida de segurança cujos pressupostos não estejam fixados em lei anterior, Cfr. https://www.parlamento.pt/Legislacao/Documents/constpt2005.pdf (consultado a 15/03/2023)
[163] Cfr. https://dre.pt/dre/legislacao-consolidada/decreto-lei/1987-34570075-58539918 (consultado a 18/03/2023)
[164] Cfr. https://diariodarepublica.pt/dr/legislacao-consolidada/decreto-lei/1987-34570075 (consultado a 16/03/2023)

e) Promessa de vantagem legalmente inadmissível.[165]

E, concretamente, o n.º 3 do art.º 126.º CPP é taxativo ao prever que "ressalvados os casos previstos na lei, são igualmente nulas, não podendo ser utilizadas, as provas obtidas mediante intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações sem o consentimento do respetivo titular".[166]

Da análise do regime processual penal português, não olvidando o preconizado no já citado art.º 32º nº 8 da CRP - "São nulas todas as provas obtidas mediante tortura, coação, ofensa da integridade física ou moral da pessoa, abusiva intromissão na vida provada, no domicílio, na correspondência ou nas telecomunicações", não vislumbramos a possibilidade de recurso ao *malware* enquanto meio de obtenção de prova por se considerar que representa uma intromissão na vida privada abusiva, até porque não há qualquer previsão legal que possibilite a sua utilização, pelo que, à luz do princípio da legalidade este deve ser proibido.

Ora, a proibição do uso de *malware* como meio de obtenção de prova, dentro do ordenamento jurídico português, tem uma justificação clara: a proteção dos direitos fundamentais dos cidadãos, especialmente no que diz respeito à sua privacidade e proteção de dados.

Em Portugal, a lei reconhece a importância da proteção dos direitos de privacidade e proteção de dados dos indivíduos. O RGPD[167] da União Europeia estabelece regras rigorosas para o tratamento de informações pessoais e impõe penalidades severas para violações. O uso de *malware* para obter informações privadas sem o consentimento dos titulares desses dados está em claro conflito com essas normas.

Consequentemente, decorre do art.º 126.º Código de Processo Penal português que qualquer prova obtida através do uso de *malware* é considerada nula, pelo que, qualquer prova obtida com recurso ao malware não podem ser utilizadas no processo judicial como meio de prova da culpa de um indivíduo, visando-se assim proteger os direitos dos cidadãos e garantir que a justiça seja feita de acordo com os princípios estabelecidos.

---

[165] Cfr. https://diariodarepublica.pt/dr/legislacao-consolidada/decreto-lei/1987-34570075 (consultado a 16/03/2023)
[166] Id.
[167] Cfr. https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679 (consultado a 28/10/2023)

Em vez disso, de acordo com o regime atualmente vigente em Portugal, as autoridades apenas podem recorrer a métodos legais e éticos para a obtenção de provas, como a obtenção de mandados judiciais fundamentados, a cooperação com provedores de serviços de *internet* ou a utilização de técnicas de investigação legalmente autorizadas como escutas telefónicas ou análise de correspondência eletrónica. Ora, na nossa ótica, o *malware* não cabe nem nas escutas telefónicas, nem na correspondência eletrónica ou qualquer meio de obtenção de prova legalmente autorizado.

Não obstante, como adiante explicitaremos melhor, através da alteração e adaptação de alguns regimes jurídicos já em vigor que, sublinhe-se, exigem quase indícios claros de práticas de certos ilícitos, para além de contemplarem regras muito estritas, quiçá o *malware* não possa vir a ser encarado, futuramente, como meio de obtenção de prova, uma vez que poderá atuar de forma mais eficaz que os já conhecidos do nosso sistema penal. Claro está que tal meio de obtenção de prova terá de respeitar os princípios basilares desenvolvidos atrás, nomeadamente o da proporcionalidade, da necessidade e da adequação.

2 – A RELEVÂNCIA DO *MALWARE* NO SISTEMA PENAL

De acordo com o relatório anual sobre a situação de terrorismo na União Europeia de 2022 da Europol[168], foram registados 28 ataques (concluídos, falhados ou frustrados na UE). Verificaram-se 380 detenções de pessoas pelas autoridades de aplicação da lei dos Estados Membros da UE e por infrações relacionadas com o terrorismo. A maioria das detenções foi realizada na sequência de investigações sobre o terrorismo jhadista, em França (93), Espanha (46), Alemanha (30) e Bélgica (22). Os processos judiciais relativos a esse ano resultaram em 427 condenações e absolvições por infrações terroristas.

Fazendo uma análise comparativa, segundo o Relatório Anual de Segurança Interna[169] apresentado ao Conselho Superior de Segurança, relativo ao ano de 2022, "o número

[168] Disp. *in* https://www.europol.europa.eu/cms/sites/default/files/documents/Tesat_Report_2022_0.pdf (consultado a 07/11/2023)

[169] Documento público, da responsabilidade da Secretária-Geral do Sistema de Segurança Interna, divulgado no final do primeiro trimestre de cada ano, onde constam informações e dados sobre a criminalidade e a segurança pública em Portugal registados pelas Forças de Segurança no ano transato.

total de participações criminais registadas pelos OPC (…) foi de 343.845, mais 42.451 participações que em 2021, a que corresponde a variação de +14.1%".[170]

Ainda nesse documento vislumbramos que o número de participações que integram a criminalidade violenta e grave foi de 13 281, mais 1 667 que em 2021, a que corresponde uma variação de +14.4%.[171]

No que respeita a crimes informáticos, constata-se uma escalada substancial, designadamente o aumento de 723 casos comparativamente com o ano transato, o que equivale a uma percentagem de +48.3%.[172] Ainda neste âmbito, segundo o relatório de Cibersegurança em Portugal – Riscos e Conflitos 4ª Edição[173], publicado em junho de 2023, informam-nos que o ano de 2021 foi o ano com mais condenados por crimes relacionados com informática desde 2009, com 256 condenados, tendo havido um crescimento de 78% face ao ano de 2020.

Mas vejamos a criminalidade através de outros números. Segundo os relatórios estatísticos divulgados pela Direção Geral da Política de Justiça[174], durante o mesmo ano de 2022, à data de 31 de dezembro, foram constituídos e julgados em tribunais de primeira instância, em processo crime, 19 332[175] arguidos por crimes contra as pessoas - nos quais se insere com especial destaque o crime de homicídio. Desse número apresentado, encontram-se, à mesma data, 14 877[176] processos findos, com decisão transitada em julgado, sendo que apenas 8 688[177] arguidos foram condenados em processo crime por tribunais de primeira instância. Ademais, tanto o número de arguidos constituídos e apresentados em tribunal de primeira instância bem como o número de condenação são superiores ao registado no ano de 2021.

---

[170] Disp. in https://www.portugal.gov.pt/download-ficheiros/ficheiro.aspx?v=%3d%3dBQAAAB%2bLCAAAAAAABAAzNDazMAQAhxRa3gUAAAA%3d, p. 31 (consultado a 06/11/2023)
[171] Cfr. idem, p. 36 (consultado a 06/11/2023)
[172] Id. p. 64
[173] Disp. *in* https://www.cncs.gov.pt/docs/rel-riscosconflitos2023-obcibercncs.pdf, p. 18 (consultado em 06/11/2023)
[174] Disp. *in* https://estatisticas.justica.gov.pt/sites/siej/pt-pt/Paginas/Biblioteca-de-dados.aspx (consultado em 07/11/2023)
[175] Cfr. https://estatisticas.justica.gov.pt/sites/siej/pt-pt/Paginas/Arguidos-em-processos-crime-nos-tribunais-judiciais-de-1-instancia-.aspx - Arguidos em processos crime nos tribunais judiciais de 1ª instância. (consultado a 07/11/2023)
[176] Cfr. https://estatisticas.justica.gov.pt/sites/siej/pt-pt/Paginas/Processos-crime-em-fase-de-julgamento-findos-nos-tribunais-judiciais-de-1-instancia.aspx - Processos crime em fase de julgamento findos nos tribunais judiciais de 1ª instância. (consultado a 07/11/2023)
[177] Cfr. https://estatisticas.justica.gov.pt/sites/siej/pt-pt/Paginas/Condenados-em-processos-crime-nos-tribunais-judiciais-de-1-instancia.aspx - Condenados em processo crime nos tribunais judiciais de 1ª instância. (consultado a 07/11/2023)

Ora, é certo que nem todas as acusações deduzidas pelo Ministério Público se traduzem em condenações, podendo vir a resultar em absolvições todavia, este apenas profere despacho de acusação sempre que existam indícios suficientes da prática do crime, isto é, não haja dúvidas infundadas sobre o cometimento, por aquele agente, daquele ilícito – art.º 283º CPP.[178]

Nesta linha de raciocínio, cumpre questionar, o que realmente está a falhar ao sistema de justiça penal português. Sabendo que a prova se faz em sede de audiência de julgamento, conforme preconiza o art.º. 355º do CPP, e se o Ministério Público tinha a convicção que daquela acusação resultaria uma condenação parece-nos que daqui só podem resultar duas opções: ou as provas são insuficientes ou não foram reproduzidas em sede de audiência de discussão e julgamento.

Em nossa opinião, à qual daremos mais destaque no capítulo final, parece-nos que os meios de prova disponíveis no nosso ordenamento jurídico não se vislumbram adequados para certos tipos de crime e que, embora invasivo, o *malware* poderia ser uma forma de trazer aos autos provas concretas e mais precisas levando a uma consequente apreciação e decisão mais justa e adequada, não nos olvidando do princípio basilar do direito penal – *in dúbio pro réu*.

3 - ESCUTAS TELEFÓNICAS E LEI DO CIBERCRIME

No seguimento do que referimos no ponto anterior, a obtenção de prova desempenha um papel fundamental no sistema de justiça, sendo a via pela qual as autoridades conseguem reunir as provas necessárias para fazer prova do cometimento de ocorrências criminais e consequentemente o Ministério Público puder acusar em conformidade.

Não obstante estarmos perante um regime com elevadas garantias de proteção, a obtenção de prova terá, muitas vezes, de violar direitos fundamentais. No entanto, esta violação de direitos fundamentais não é ilícita, se for prevista pela lei e apresenta sustentação legal constitucional.

[178] Cfr. Código de Processo Penal - CPP | DR (diariodarepublica.pt) (consultado a 07/11/2023)

Entre os meios de obtenção de prova que, teoricamente, poderiam ser ilícitos por colidirem com direitos fundamentais, mas que, mediante o cumprimento de diversas condições, podem ser admissíveis, temos as escutas telefónicas.

Nas palavras de Costa Andrade (2009, p. 146), verificamos que a definição de telecomunicação abrange "todos os processos técnicos de recolha, processamento, tratamento, conservação e transmissão de dados, principalmente de dados correspondentes a palavras ou imagens ou nelas convertíveis".[179]

Conforme estabelece o art.º 187.º, n.º 1 do Código de Processo Penal, o conceito de escuta telefónica pode ser definido como a "interceção e a gravação de conversações ou comunicações telefónicas".[180]

Ainda nessa temática, surge o art.º 189º preconizando a extensão do regime das escutas telefónicas:

> Às conversações ou comunicações transmitidas por qualquer meio técnico diferente do telefone, designadamente correio electrónico ou outras formas de transmissão de dados por via telemática, mesmo que se encontrem guardadas em suporte digital, e à intercepção das comunicações entre presentes[181].

Paralelamente, analisando o art.º 2.º, alínea e), da Lei n.º 109/2009, de 15 de setembro – a denominada Lei do Cibercrime –, constatamos que o conceito de interceção é referido como o "ato destinado a captar informações contidas num sistema informático, através de dispositivos eletromagnéticos, acústicos, mecânicos ou outros".[182]

Assim, nos termos do regime processual penal português, as autoridades podem realizar a interceção e a gravação não apenas de conversas telefónicas, mas ainda de mensagens eletrónicas e ainda outros meios de comunicação para fins de investigação criminal. No entanto, tal não poderá ser realizado sem qualquer justificação, apenas pode ser levado a cabo mediante autorização judicial e somente em situações excecionais, consideradas essenciais para a investigação e prova da prática de uma conduta criminosa.

Por conseguinte, cumpre, desde logo, analisar o disposto no art.º 187.º do CPP.

---

[179] Cfr. ANDRADE, Manuel da Costa, *Bruscamente no Verão passado, a reforma do Código de Processo Penal,* Coimbra Editora, 2009, p.146
[180] Disp. *in* https://dre.pt/dre/legislacao-consolidada/decreto-lei/1987-34570075 (consultado a 17/10/2023).
[181] Cfr. Código de Processo Penal - CPP - Artigo 189.º | DR (diariodarepublica.pt) (consultado a 17/10/2023)
[182] Cfr. https://dre.pt/dre/legislacao-consolidada/lei/2009-128879174 (consultado a 17/10/2023).

O art.º 187.º, n.º 1 CPP prevê que a interceção e a gravação de conversações ou comunicações telefónicas somente podem ser autorizadas durante o inquérito, caso existam razões para crer que a diligência é fundamental para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter, sendo necessário existir despacho fundamentado do juiz de instrução e mediante requerimento do Ministério Público, quanto a crimes:

> a) Puníveis com pena de prisão superior, no seu máximo, a 3 anos;
>
> b) Relativos ao tráfico de estupefacientes;
>
> c) De detenção de arma proibida e de tráfico de armas;
>
> d) De contrabando;
>
> e) De injúria, de ameaça, de coação, de devassa da vida privada e perturbação da paz e do sossego, quando cometidos através de telefone;
>
> f) De ameaça com prática de crime ou de abuso e simulação de sinais de perigo; ou
>
> g) De evasão, quando o arguido haja sido condenado por algum dos crimes previstos nas alíneas anteriores[183] [184].

Portanto, observamos que a utilização de intercetações telefónicas só é permitida quando todos os outros métodos de investigação forem esgotados ou quando não se espera que nenhum outro seja eficaz.

Paralelamente ao exposto, a possibilidade de intervenção da investigação penal nas comunicações, incluindo *fax*, mensagem de voz, SMS, EMS e MMS, é também regulamentada pela Lei do Cibercrime, a qual regula a interceção de comunicações no quadro da investigação criminal.

Conforme nos refere Rui Cardoso (2018, p. 167 e 168):

> (…) os dados informáticos a que se aplica o artigo 17.º[185] [da lei do cibercrime] são dados armazenados que poderiam ter sido intercetados, em tempo real, através dos meios de obtenção de prova previstos noa artigos 187.º e 188.º do CPP (SMS, SEM e MMS) ou

[183] Cfr. https://dre.pt/dre/legislacao-consolidada/decreto-lei/1987-34570075 (consultado a 21/10/2023).
[184] Sem prejuízo de outras situações particulares, cujo conteúdo analisaremos em pormenor mais adiante.
[185] Art.º 17.º da Lei do Cibercrime:
Apreensão de correio eletrónico e registos de comunicações de natureza semelhante
Quando, no decurso de uma pesquisa informática ou outro acesso legítimo a um sistema informático, forem encontrados, armazenados nesse sistema informático ou noutro a que seja permitido o acesso legítimo a partir do primeiro, mensagens de correio eletrónico ou registos de comunicações de natureza semelhante, o juiz pode autorizar ou ordenar, por despacho, a apreensão daqueles que se afigurem ser de grande interesse para a descoberta da verdade ou para a prova, aplicando-se correspondentemente o regime da apreensão de correspondência previsto no Código de Processo Penal, Cfr. https://dre.pt/dre/legislacao-consolidada/lei/2009-128879174 (consultado a 21/10/2023).

> no artigo 18.º da LCC (e.g., mensagens de correio eletrónico e *instant messages*). Assim, quanto ao regime da destruição/devolução, sendo o artigo 17.º omisso e não oferecendo o artigo 179.º do CPP resposta satisfatória, parece-me que já hoje se deve aplicar o regime do artigo 188.º, n.ºs 6 e 12, deste código, ex vi do artigo 28.º da LCC. Sendo os dados da mesma natureza, deve o regime de conservação ser o mesmo.[186]

Ora, no mesmo sentido do que já foi referido para as escutas telefónicas, nos termos do disposto no art.º 18.º, n.º 2 da Lei do Cibercrime, verificamos que a interceção de outras comunicações somente pode ser autorizada pelo juiz de instrução, após requerimento do Ministério Público nesse sentido.

Assim, a interceção de comunicações prevista no art.º 18º da LCC apenas pode ser realizada relativamente a crimes:

> a) Previstos na lei do cibercrime;
>
> ou que sejam
>
> b) Cometidos por meio de um sistema informático ou em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico, quando tais crimes se encontrem previstos no art.º 187.º do Código de Processo Penal. [187]

3.1 – APLICAÇÃO DO REGIME JURÍDICO AO *MALWARE*

O regime jurídico das escutas telefónicas reporta-se à legislação que rege a utilização deste recurso em sede investigações criminais – respeitantes a ficheiros áudio.

As escutas telefónicas são uma forma de vigilância eletrónica na qual as comunicações telefónicas de uma pessoa são monitorizadas e gravadas por autoridades competentes, mediante mandado judicial, com o objetivo de obter provas em casos de crimes.

Assim, conforme verificámos, em determinadas situações, é possível às autoridades imiscuírem-se no conteúdo das comunicações dos cidadãos.

Ora, de acordo com o Dicionário Priberam da Língua Portuguesa, a palavra escuta significa "1. Acto de escutar; 2. Pessoa que escuta; 3. Lugar em que se escuta. 4. Gravação de uma conversa, feita geralmente de forma ilegal e sem o conhecimento dos

[186] Cfr. CARDOSO, Rui *–Apreensão de correio electrónico e registos de comunicações de natureza semelhante – artigo 17.º da Lei n.º 109/2009*, de 15.IX, *in* Revista do Ministério Público (2018), n.º 153, pp. 167 e 168.
[187] Cfr. https://dre.pt/dre/legislacao-consolidada/lei/2009-128879174 (consultado a 27/05/2023).

intervenientes (ex.: escuta telefónica); 5. [Antigo] Esculca)"[188] e a palavra telefónica significa "1. Relativo à telefonia ou ao telefone ou 2. Que implica uso do telefone".[189]

E, aplicando tais definições ao âmbito técnico-legal, Nuno Maurício e Catarina Iria afirmam que "[…] a escuta telefónica consubstancia-se na captação, por meio técnico, das comunicações estabelecidas entre uma pessoa (o escutado) e todos os demais, por princípio sem conhecimento de qualquer um dos interlocutores".[190]

Paralelamente, cumpre referir o disposto no art.º 187.º, n.º 1 do Código de Processo Penal, de acordo com o qual se define escuta telefónica como a "interceção e a gravação de conversações ou comunicações telefónicas"[191] e, analisando o disposto art.º 2.º, alínea e), da Lei n.º 109/2009, de 15 de setembro, Lei do Cibercrime, o conceito de interceção é apresentado como o "ato destinado a captar informações contidas num sistema informático, através de dispositivos eletromagnéticos, acústicos, mecânicos ou outros".[192]

Neste sentido, no que à captação de comunicações diz respeito, uma vez que através das escutas telefónicas também se obtém informações descontextualizadas no que à prática do crime diz respeito, poderá ponderar-se a possibilidade de legalizar o recurso ao *malware* por parte das autoridades policiais como via de investigação. Uma das possibilidades poderá passar pela expansão do regime previsto para as escutas telefónicas.

Se não vejamos: numa conversa telefónica podemos obter informações relevantes para a prática do crime, mas também podemos aceder a informações pessoais e confidenciais que não deveriam ser do conhecimento "público", uma vez que o orador desconhece que está a ser ouvido por determinado OPC. Da mesma forma, no *malware*, teríamos igualmente acesso a áudios não relevantes para os autos (os quais, à semelhança da prática já existente no atual sistema das interceções telefónicas, seriam desconsiderados) mas, mais que isso, acesso a áudios que nunca seriam produzidos através de uma chamada telefónica. Áudios que, por vezes, só no ato da consumação do crime se reproduzem.

[188] Cfr. https://dicionario.priberam.org/escuta (consultado a 24/06/2023).
[189] Cfr. https://dicionario.priberam.org/telef%C3%B3nica (consultado a 24/06/2023).
[190] Cfr. MAURÍCIO, Nuno; IRIA, Catarina (2006) - *As escutas telefónicas como meio de obtenção de prova - Necessidade de uma reforma legislativa ou suficiência de uma interpretação conforme?: Ponto de situação numa já vaexata quaestio! Polícia* e Justiça. Instituto Superior de Polícia Judiciária e Ciências Criminais. Loures: III Série, N.º 7 (Janeiro-Junho 2006), p. 93.
[191] Disp. *in* https://dre.pt/dre/legislacao-consolidada/decreto-lei/1987-34570075 (consultado a 27/06/2023).
[192] Cfr. https://dre.pt/dre/legislacao-consolidada/lei/2009-128879174 (consultado a 27/06/2023).

Concomitantemente, o mesmo se dirá no âmbito de dispositivos informáticos, sendo a interceção relativa a ficheiros áudios defendida de igual forma uma vez que o *malware*, contrariamente ao sistema atual das interceções, aplica-se não só em telemóveis, mas também em qualquer sistema informático, designadamente computadores.

No que ao âmbito de aplicação diz respeito, seja no respeitante às escutas telefónicas, como ao abrangido pelo art.º 189º do CPP, de acordo ambos os regimes atualmente em vigor, estes têm cumprimento pela previsão legal do art.º 187.º do CPP e nesse nos baseamos para atuação do *malware*, não olvidando o facto de se tratar de um método extremamente invasivo de direitos fundamentais.

Nessa conformidade, exigiria escrupulosamente os requisitos já invocados no atual regime, mormente na questão de ser "indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível[193]" de obter. Porque parece-nos que, se através deste meio não se consegue obter prova, de mais nenhum de irá certamente obter, a menos que seja refletida numa confissão.

4 – SISTEMAS DE VIDEOVIGILÂNCIA – LEI N.º 95/2021, DE 29 DE DEZEMBRO

O direito à imagem é um direito autónomo com proteção constitucional, a par de outros direitos de personalidade consagrados na Constituição da República Portuguesa – art.º 26º, abrangendo, entre outros, o direito da pessoa não ser fotografada nem filmada sem o seu consentimento e bem assim o direito à reserva da intimidade da vida privada e familiar.

O carácter inalienável e irrenunciável dos direitos de personalidade não impede, de facto, a sua limitação através do consentimento do lesado, admitindo-se, no art.º 81.º do Código Civil (CC), com carácter geral, a limitação voluntária dos direitos de personalidade.

[193] Cfr. Art. 187º CPP

O Parlamento Europeu e do Conselho adotaram a 24 de outubro de 1995 a Diretiva 95/46/CE[194] relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

Atualmente, vigora a Lei nº 95/2021, de 29 de dezembro que "regula a utilização e o acesso pelas forças e serviços de segurança e pela Autoridade Nacional de Emergência e Proteção Civil (ANEPC) a sistemas de videovigilância para captação, gravação e tratamento de imagem e som"[195], de acordo com as definições constantes do art.º 3º da Lei nº 59/2019, de 8 de Agosto, "que aprova as regras relativas ao tratamento de dados pessoais para efeitos de prevenção, deteção, investigação ou repressão de infrações penais ou de execução de sanções penais, transpondo a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, com as necessárias adaptações[196]."

Continuando a seguir de perto o exarado na lei invocada, a mesma aplica-se aos sistemas de videovigilância instalados ou utilizados no espaço público ou nos espaços privados de acesso público, quando devidamente autorizados para os fins que a mesma contempla, nos quais se encontram, entre outros: "a proteção da segurança das pessoas, animais e bens, em locais públicos ou de acesso público, e a prevenção da prática de factos qualificados pela lei como crimes, em locais em que exista razoável risco da sua ocorrência e; a prevenção de atos terroristas".[197]

Fruto da evolução tecnológica, pequenas câmaras de vídeo de fácil manuseamento permitem captar e gravar som e imagem com qualidade e precisão suficientes, possibilitando o seu ulterior aproveitamento, designadamente para efeitos probatórios. Tais imagens podem ser vistas em tempo real e de qualquer local, uma vez que se encontram ligadas a uma rede IP que assim o permite.

O recurso a estas novas tecnologias, designadamente a videovigilância, que assenta em preocupações e exigências securitárias, deve-se, desde logo, à necessidade de prevenir e reprimir de forma eficaz e eficiente fenómenos de criminalidade violenta e grave, atento o desenvolvimento das tecnológicas e o uso incessante da *internet*.

Desta forma, não se pode, portanto, questionar a importância da existência dos sistemas de videovigilância no combate à criminalidade e outros fins. Contudo, não nos olvidamos

[194] Disp. *in* Diretiva - 95/46 - EN - EUR-Lex (europa.eu) (consultado a 07/11/2023)
[195] Cfr. https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=3514&tabela=leis&ficha=1 (consultado a 07/11/2023)
[196] Idem – art. 2º Lei 95/2021, de 29 de dezembro
[197] Idem – art. 3º al. d) e e) Lei 95/2021, de 29 de dezembro

que este meio pode conduzir ao conflito, muitas vezes inevitável, entre o direito fundamental à segurança e os igualmente fundamentais direitos à liberdade, à reserva da intimidade da vida privada, à imagem e à palavra.

Todavia, é um sistema que, apesar das controversas doutrinárias e jurisprudenciais em torno do mesmo[198], ele encontra-se em vigor, podendo ser imagens e som recolhidos através de tal sistema e valorados em tribunal como meio de prova.

4.1 – APLICAÇÃO DO REGIME JURÍDICO AO *MALWARE*

As provas têm como função a demonstração da realidade dos factos[199], sendo certo que a obtenção de provas para determinados ilícitos é extremamente complexa de apurar, dificultando o trabalho dos OPC bem como da direção do inquérito, a qual cabe ao Ministério Público.

Assim, atenta a evolução tecnológica verificada ao longo dos tempos, impõe-se uma visão mais ampla, aliada à proporcionalidade, sobre futuros meios de obtenção de prova, mais eficazes.

O sistema abordado no ponto anterior abrange duas vertentes: áudio e visual. O recurso à videovigilância, instalado em qualquer dispositivo (câmaras de vigilância) permite-nos o acesso ao seu conteúdo tanto visual como auditivo, sendo por isso um método mais invasivo quando comparado com o sistema de escutas telefónicas.

Nessa ótica de ideias, existindo uma câmara de vigilância num estabelecimento comercial ou até numa via pública[200], esta poderá captar imagens descontextualizadas sem qualquer interesse para a prevenção e execução da segurança pública ou, no que

[198] Já é abundante a jurisprudência existente sobre a matéria da legalidade como meio de prova de imagens obtidas por sistemas de videovigilância instalados em espaços a que as pessoas podem aceder sem necessidade de autorização, ainda que sejam propriedade privada, como sejam habitações ou estabelecimentos comerciais, ainda que as imagens tenham sido obtidas sem conhecimento do visado (por não serem visíveis e por inexistência de aviso) e sem autorização/comunicação da Comissão Nacional de Proteção de Dados - CNPD.

Exemplo disso Acórdão proferido já em 2017, disponível em https://www.dgsi.pt/jtrc.nsf/8fe0e606d8f56b22802576c0005637dc/7c706750da1160bf802581a3003bfaf2 (consultado a 07/11/2023)

[199] Art. 341º do CC

[200] Exemplo disso é a cidade da Amadora, que toda ela tem sistemas de videovigilância

reporta ao presente projeto, sem qualquer interesse para a prevenção e obtenção de provas indiciárias de ilícitos criminais.

No que a captação de imagens e vídeo diz respeito, podemos ponderar o facto de as autoridades poderem utilizar técnicas de vigilância eletrónica, através da instalação de *malware* em dispositivos para monitorizar eventuais infratores e, por conseguinte, obter provas evidentes com acesso a imagens e vídeos, devendo tal prática requerer uma autorização judicial semelhante à exigida para as escutas telefónicas tradicionais.

Por outro lado, também podemos extrair deste método ficheiros auditivos, impondo-se uma distinção daquilo que se pretende. Isto é, na eventualidade de se considerar o *malware* enquanto meio de obtenção de prova, há que observar todas as exigências e formalismos legais já previstos nos atuais regimes, sublinhando-se sempre a patente da defesa de direitos fundamentais. E, poderíamos dividir a aplicação do *malware* consoante o seu objetivo for a obtenção de provas auditivas (ficheiros áudio captados tanto em escutas telefónicas como fora delas, na presença do aparelho eletrónico) e ao invés, for a obtenção de prova através de captação de imagens (fornecidas através da(s) câmara(s) do próprio aparelho).

Ora, se tais elementos de prova já existem e são legalmente admissíveis, o mesmo que poderá observar no âmbito de recurso ao *malware*, abrangendo os mesmos fundamentos para a sua utilização e, podendo ser delineado consoante a necessidade de fazer prova – auditiva ou visual.

É importante observar que as práticas de vigilância eletrónica e, por inerência, aqui incluindo o uso de *malware*, estão sujeitas a considerações legais e éticas complexas e podem variar significativamente entre os países, pelo que, será sempre essencial que as autoridades cumpram as leis e os padrões legais aplicáveis, garantindo a proteção dos direitos individuais, como a privacidade e a liberdade de expressão, devendo ser respeitados os princípios da legalidade e, bem assim, da proporcionalidade nas suas três vertentes atrás analisadas (necessidade, adequação e proporcionalidade em sentido estrito).

Assim, todos estes elementos coadjuvantes, conjugados entre si permitem dar lastro e verosimilhança ao facto de estamos perante um circunstancialismo bastante concludente no sentido em que efetivamente se verifica uma intromissão no meio da vida privada do agente “observado”, mas também uma essencialidade, não alcançável por qualquer outra via, de obtenção de provas atuais e eficazes, capazes de fundamentar a acusação de um cidadão.

5 – REGISTO DE VOZ E IMAGEM – LEI N.º 5/2002, DE 11 DE JANEIRO

A par do já supra exposto relativamente à obtenção prova, tanto através de escutas telefónicas como, sopesando, o sistema de videovigilância, surge a Lei n.º 5/2002, de 11 de janeiro que admite o registo de voz e imagem no combate à criminalidade organizada e económico-financeira:

> Artigo6.º
> Registo de voz e imagem
>
> 1 -É admissível, quando necessário para a investigação de crimes referidos no artigo 1º, o registo de voz e imagem, por qualquer meio, sem consentimento do visado.
>
> 2 – A produção destes registos depende de prévia autorização ou ordem do juíz, consoante os casos.
>
> 3 – São aplicáveis aos registos obtidos, com as necessárias adaptações, as formalidades previstas no artigo 188º do Código de Processo Penal.[201]

Tal regime depende de prévia autorização ou ordem do juiz e poderá ser utilizado na investigação dos seguintes ilícitos (art.º 1):

> Artigo1.º
> Âmbito de aplicação
>
> a) Tráfico de estupefacientes, nos termos dos artigos 21.º a 23.º e 28.º do Decreto-Lei n.º 15/93, de 22 de janeiro;
>
> b) Infrações terroristas, infrações relacionadas com um grupo terrorista, infrações relacionadas com atividades terroristas e financiamento do terrorismo;
>
> c) Tráfico de armas;
>
> d) Tráfico de influência;
>
> e) Recebimento indevido de vantagem;
>
> f) Corrupção ativa e passiva, incluindo a praticada nos setores público e privado e no comércio internacional, bem como na atividade desportiva;
>
> g) Peculato;

[201] Cfr. ::: Lei n.º 5/2002, de 11 de Janeiro (pgdlisboa.pt) (consultado em 13/11/2023)

> h) Participação económica em negócio;
>
> i) Branqueamento de capitais;
>
> j) Associação criminosa;
>
> l) Pornografia infantil e lenocínio de menores;
>
> m) Contrafação, uso e aquisição de cartões ou outros dispositivos de pagamento contrafeitos e respetivos atos preparatórios, aquisição de cartões ou outros dispositivos de pagamento obtidos mediante crime informático, dano relativo a programas ou outros dados informáticos e sabotagem informática, nos termos dos artigos 3.º-A, 3.º-B, 3.º-C, 3.º-D, 3.º-E, 4.º e 5.º da Lei n.º 109/2009, de 15 de setembro, e ainda o acesso ilegítimo a sistema informático, se tiver produzido um dos resultados previstos nas alíneas a) e b) do n.º 5 do artigo 6.º daquela lei, for realizado com recurso a um dos instrumentos referidos no n.º 2 do mesmo artigo, ou integrar uma das condutas aí tipificadas;
>
> n) Tráfico de pessoas;
>
> o) Contrafação de moeda e de títulos equiparados a moeda;
>
> p) Lenocínio;
>
> q) Contrabando;
>
> r) Tráfico e viciação de veículos furtados.
>
> 2 - O disposto na presente lei só é aplicável aos crimes previstos nas alíneas p) a r) do número anterior se o crime for praticado de forma organizada.
>
> 3 - O disposto nos capítulos ii e iii é ainda aplicável aos demais crimes referidos no n.º 1 do artigo 1.º da Lei n.º 36/94, de 29 de setembro.
>
> 4 - O disposto na secção ii do capítulo iv é ainda aplicável aos crimes previstos na Lei n.º 109/2009, de 15 de setembro, quando não abrangidos pela alínea m) do n.º 1 do presente artigo.[202]

Ao tornar admissível, quando necessário para a investigação dos crimes acima referidos, o registo de voz e de imagem, por qualquer meio sem consentimento do visado, ainda que mediante as formalidades previstas no art.º 188º do CPP, o legislador veio claramente criar um regime de exceção relativamente ao tratamento daqueles direitos que tanto se têm mencionado ao longo deste projeto, os quais constitucionalmente tutelados, constituindo uma restrição dos direitos fundamentais da imagem e da palavra.

De facto, se é permitida a obtenção de registo de voz e imagem por qualquer meio, a mesma engloba tanto registos telefónicos como conversas efetuadas fora do telefone

[202] Cfr. ::: Lei n.º 5/2002, de 11 de Janeiro (pgdlisboa.pt) (consultado a 13/11/2023)

como, por exemplo, conversas face-to-face ou similares, desde que com prévia autorização ou ordem do juiz.

Nesse âmbito, até no seio de imagens/vídeos recolhidos através dos sistemas de videovigilância, para investigação dos crimes de natureza acima referidos, não será óbice a captação de registos áudio.

Em suma, concluiu-se que a aplicação deste art.º 6º versa sobre a obtenção de qualquer tipo de imagem/vídeo e som, desde que relevante para a descoberta da verdade e a boa decisão da causa, em matéria de investigação no elenco de crimes citados, desde que previamente autorizado por juiz.

5.1. APLICAÇÃO DO REGIME JURÍDICO AO *MALWARE*

Neste subcapítulo reforçamos a ideia já plasmada aquando da abordagem aos sistemas de videovigilância em 4.1, pese embora o catálogo de crimes a que se destina possa divergir.

Se, por um lado, o sistema de videovigilância defende a sua prossecução, em traços gerais, para fins de proteção, circulação e segurança de pessoas, animais e bens, edifícios ou infraestruturas, atos terroristas ou, tão somente o controlo do tráfego rodoviário, este, por seu turno é menos abrangente, pretendendo combater a criminalidade organizada no catálogo de crimes que lhe está inerente.

Aqui chegados, constatamos que a execução da Lei n.º 5/2002 pode ser conseguida por duas vias: ou através de mecanismos de particulares (telefónicas, câmaras fotográficas e câmaras de filmar); ou através do sistema de videovigilância – porque são as legalmente previstas.

Equiparando tal raciocínio ao *malware*, este que visa a obtenção de prova através da recolha de imagens e áudios por via de sistemas informáticos ocultos, também se poderá aplicar, ainda que devidamente fundamentado e autorizado por entidade competente, a determinado tipo criminal.

6 – LOCALIZAÇÃO DE CELULAR

No que concerne à localização celular, norma prevista no art.º 252.º-A, n.º 1 do CPP, estamos perante um meio de prova já existente para o celular pelo que, com a aplicação do *malware* não suscitariam grandes questões, podendo vir a beneficiar-se pela localização deste, obtendo-se assim o local exato da consumação do ilícito ou outros indícios fundamentais, regendo-se o seu funcionamento pelo preconizado no artigo suprarreferido, podendo agora reportar a um celular ou qualquer outro tipo de dispositivo eletrónico/informático.

CAPÍTULO V- BREVES NOTAS AO DIREITO COMPARADO E JURISPRUDÊNCIA

1 – DIREITO COMPARADO

Conforme se foi referindo, as escutas telefónicas, o sistema de videovigilância e a investigação criminal em geral são matérias complexas que envolvem o equilíbrio entre a proteção dos direitos individuais e a necessidade de combater crimes, pelo que, a forma de abordar estes aspetos varia em diferentes sistemas jurídicos ao redor do mundo. Por conseguinte, o mesmo sucede relativamente à forma como os diversos países olham para a possibilidade de o *malware* ser utilizado como via de investigação.

Começando pelo direito alemão, verificamos que desde o ano de 2008 que o mesmo permite o recurso ao *malware* no âmbito de investigações criminais.

Efetivamente, a 25 de dezembro de 2008 foi aprovada a Lei sobre a defesa contra os perigos do terrorismo internacional pelo Serviço Federal de Polícia Criminal (*Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt*), qual introduziu no ordenamento jurídico alemão (reformando a *Bundeskriminalamtgesetz* [*BKA-Gesetz*]) a possibilidade de recurso ao *malware.*[203]

A Lei sobre a defesa contra os perigos do terrorismo internacional pelo Serviço Federal de Polícia Criminal possibilita o recurso ao *malware* quando existe risco para a vida, a integridade física ou a liberdade de um cidadão, a segurança nacional se encontre em perigo, ou tal seja necessário para prevenir o terrorismo internacional ou crimes graves (desde que cumprido o elenco plasmado no § 129a do StGB (§ 4a).

Sem prejuízo do exposto, cumpre referir que a citada lei dispõe que apenas é permitida a utilização do *malware* quando inexiste qualquer outro meio menos invasivo para chegar à mesma informação.

Por outro lado, conforme salienta Ortiz Pradillo, em Espanha, até 2015, o recurso ao *malware* não se encontrava legalmente consagrado, no entanto, a jurisprudência foi

[203] Cfr. https://dip.bundestag.de/vorgang/.../14447 (consultado a 10/05/2023)

permitindo a sua utilização, tendo tal facto conduzido a que o Tribunal Europeu dos Direitos Humanos condenasse o Estado espanhol.[204]

Assim, foi somente em 8 de dezembro de 2015 que entrou em vigor a nova *Ley de Enjuiciamiento Criminal*, a qual veio permitir de forma expressa o recurso ao *malware* com vista à investigação.[205]

Ora, o art.º 588.º *septies da Ley de Enjuiciamiento Criminal*, verificamos que o mesmo nos refere que:

> 1. El juez competente podrá autorizar la utilización de datos de identificación y códigos, así como la instalación de un software, que permitan, de forma remota y telemática, el examen a distancia y sin conocimiento de su titular o usuario del contenido de un ordenador, dispositivo electrónico, sistema informático, instrumento de almacenamiento masivo de datos informáticos o base de datos, siempre que persiga la investigación de alguno de los siguientes delitos:
>
> a) Delitos cometidos en el seno de organizaciones criminales.
>
> b) Delitos de terrorismo.
>
> c) Delitos cometidos contra menores o personas con capacidad modificada judicialmente.
>
> d) Delitos contra la Constitución, de traición y relativos a la defensa nacional.
>
> e) Delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación o servicio de comunicación.[206]

Por todo o exposto, verificamos que desde 2015 que a legislação espanhola possibilita, de forma expressa, o recurso ao *malware* como um meio válido para obtenção de provas, sendo possível autorizar a instalação de um *software* que permite aceder remotamente, sem conhecimento do indivíduo-alvo, ao conteúdo de um computador, dispositivo eletrónico, sistema informático, dispositivo de armazenamento em massa de dados ou qualquer base de dados.

No caso do direito italiano ainda não existe previsão legal expressa para a admissibilidade do uso do *malware* no âmbito da investigação criminal. No entanto, a jurisprudência tem aberto a possibilidade de utilização do *malware* como meio de obtenção de prova.

---

[204] Cfr. ORTIZ PRADILLO, Juan Carlos (2009) – *El Remote Forensic Software como Herramienta de Investigación contra el Terrorismo*, ENAC, número 4, Outubro de 2009, p. 3-4.
[205] Cfr. https://www.boe.es/buscar/doc.php?id=BOE-A-2015-10725 (consultado a 12/05/2023)
[206] Cfr. https://www.boe.es/buscar/doc.php?id=BOE-A-2015-10725 (consultado a 13/05/2023).

A título de exemplo, podemos referir o Acórdão do Supremo Tribunal de Cassação, divisão V, decisão número 24695, datado de 14 de outubro de 2009 ou ainda o Acórdão do Tribunal de Cassação, divisão VI, decisão número 254865, de 27 novembro.[207]

Concretamente, a posição assumida pelos tribunais italianos é a de que o recurso ao *malware* não se trata de verdadeira vigilância, mas antes de um mecanismo que visa a apreensão e cópia de documentos armazenados no disco rígido do computador do acusado e apenas após a apreensão dos diversos documentos, poderão as provas obtidas ser consideradas para efeitos de condenação.

Fora do universo europeu, podemos referir o caso do Brasil, o qual não admite a utilização do *malware* como meio de obtenção de prova. Neste sentido, Ribeiro, Cordeiro e Fumach (2021, p. 95) afirmam que:

> O uso de *malwares* em investigações criminais tem o potencial de comprometer direitos fundamentais constitucionalmente afirmados. No Brasil, por exemplo, os seus reflexos sobre a Constituição de 1988 podem ser identificados na afetação à intimidade, vida privada, honra e imagem do cidadão (art. 5º, X), à inviolabilidade do domicílio (art. 5º, XI) e ao sigilo das comunicações telemáticas (art. 5º, XII).[208]

Por último e em sentido completamente contrário ao caso brasileiro, cumpre fazer referência aos Estados Unidos da América, os quais admitem plenamente o recurso ao *malware* como via de investigação.

Em termos jurisprudenciais, podemos enunciar os casos Nicodemo S. Scarfo (1999) e Magic Latern (2001).[209]

Em 2001 o Governo americano desenvolveu uma *backdoor* (designada por *magic latern*) para fins de investigação criminal no FBI.[210]

Voltando aos conceitos atrás abordados, podemos qualificar a *magic lantern* como um *keylogger* que podia ser instalado de forma clandestina ou remota via *internet* no sistema informático do investigado.

---

[207] Cfr. VACIAGO, Giuseppe e RAMALHO, David Silva (2016) – *Online searches and online surveillance: the use of Trojans and other types of malware as means of obtaining evidence in criminal proceedings*, Digital Evidence and Electronic Signature Law Review, volume 13, novembro de 2016, p. 91.
[208] Cfr. RIBEIRO, Gustavo Alves Magalhães; CORDEIRO, Pedro Ivo Rodrigues Velloso; FUMACH, Débora Moretti (2021) – *O malware como meio de obtenção de prova e a sua implementação no ordenamento jurídico brasileiro*. Revista Brasileira de Direito Processual Penal jan./abr. 2021, v. 7, n. 1, p. 95.
[209] Cfr. POULSEN, Kevin (2007) – *FBI's Secret Spyware Tracks Down Teen Who Made Bomb Threats*, WIRED, 18-07-2007.
[210] Cfr. *Magic Lantern on back of Carnivore*, Computer Fraud & Security, volume 2002, tomo 1, janeiro de 2002, pp. 2-3.

Paralelamente, Kevin Poulsen enuncia ainda os casos do CIPAV (2007), Timberlinebombinfo (2007) e, mais recentemente, da Operação Torpedo (2011-2014).[211]

Antes de passar à análise de jurisprudência portuguesa relevante para o nosso tema, gostaríamos de referir que consideramos que o 11 de Setembro de 2001 nos Estados Unidos da América – Word Trace Center, o 11 de março de 2004 em Madrid ou já posterior, o 13 de novembro de 2015 em Paris – Ataque ao Bataclan, assim como o 22 de julho de 2011 na ilha de Utoya, na Noruega foram os pontos de viragem para uma alteração do panorama da sociedade atual, tendo havido uma alteração profunda no pensamento social, como na forma como se vive em sociedade.

A preocupação não partiu apenas dos Estados atingidos diretamente com os ataques terroristas, mas sim de toda a comunidade: desde os Estados Unidos da América aos Estados Membros da União Europeia.

A legislação sobre matérias tecnológicas, comércio eletrónico e telecomunicações tornou-se prioridade na União Europeia, após os sucessivos ataques terroristas. Nesse sentido e abreviadamente, expomos dois casos de jurisprudência.

2 – JURISPRUDÊNCIA

Iremos sinalizar abreviadamente dois casos de jurisprudência, que nos parecem relevantes para uma melhor compreensão do nosso tema. Apesar de o primeiro caso ser apenas para chamar a atenção para os possíveis perigos do *malware* para lá do processo penal.

[211] Cfr. POULSEN, Kevin (2007) – *FBI's Secret Spyware Tracks Down Teen Who Made Bomb Threats*, WIRED, 18-07-2007.

2.1- ACÓRDÃO DO SUPREMO TRIBUNAL DE JUSTIÇA DE 27/11/2019: A UTILIZAÇÃO DE *MALWARE* POR PRIVADOS E O DIREITO FUNDAMENTAL À RESERVA DA INTIMIDADE DA VIDA PRIVADA

No âmbito do Acórdão do Supremo Tribunal de Justiça de 27/11/2019 estava em causa uma situação em que, AA, consultor jurídico, intentou ação declarativa de condenação, sob a forma de processo comum, contra "BB, S.A.", pedindo que este fosse condenado:

> a) restituir ao Autor a quantia global de 218.863,38 €, acrescida de juros, contados desde o levantamento dos valores em causa;
>
> b) pagar ao Autor compensação pelos danos não patrimoniais sofridos, que liquida em 10.000,00 €.[212]

No que respeita aos fundamentos invocados, o Autor alegou que, após ter procedido à abertura de conta bancária na agência do Réu, transferiu para essa conta, em 08.07.2013, 1.500.000,00 €, com o objetivo de adquirir um imóvel, finalidade de que deu conhecimento ao seu gestor de conta.

Porém, com a frustração desse negócio, a conta bancária aberta junto do Réu ficou destinada a pequenos pagamentos do dia-a-dia da vida do Autor em Portugal, além da compra do imóvel que, de facto, se viria a concretizar posteriormente.

O Autor alegou que tinha confiança no Réu, e particularmente no seu gestor de conta, com quem conversava frequentemente, motivo pelo qual, devido às suas frequentes ausências de Portugal, o Réu conferiu-lhe a possibilidade de efetuar movimentos na sua conta bancária mediante instruções enviadas por *e-mail*.

Para tal, em 17.09.2013, Autor e o Réu celebraram acordo pelo qual passou a ser possível, ao primeiro, enviar por *e-mail* instruções quanto à execução das transações pelo Banco do Réu e tais instruções consistiam na realização de pagamentos, geralmente de valor inferior a 10.000,00 €, muito raramente em transferências pessoais, para outras contas bancárias, e mais raramente ainda para contas bancárias fora de Portugal.

Ao Réu cabia, na pessoa do seu gestor de conta, controlar e verificar os movimentos bancários, de forma diligente, alertando para eventuais anomalias, podendo mesmo bloquear pagamentos e /ou transferências.

---

[212] Cfr. http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/27962f73862f5520802584c00040134b?OpenDocument (consultado a 13/05/2023).

Isto posto, alegou o Autor que no dia 04.03.2014, foram ordenadas 2 transferências bancárias da sua conta: uma no valor de 57.000,00 €, e uma outra, no valor de 40.000 £ (cerca de 48.863,38 €), destinada ao "..., PLC", ..., ... (...) e em 11.03.2014, mais 2 transferências bancárias, cada uma no valor de 85.000,00 €.[213]

Porém, o Autor alegou que apesar de ordem para a realização destas operações ter sido enviada através do seu endereço de *e-mail*, as mesmas foram feitas à sua revelia, desconhecendo a identidade do emitente.

É neste sentido que o Autor alegou ter sido alvo de um ataque informático, o qual não se teria traduzido na simples apropriação de dados bancários do autor, posteriormente utilizados no relacionamento eletrónico com o banco do réu como se do autor se tratara, mas numa verdadeira manipulação dos ficheiros do computador do autor, com criação de documentos/ficheiros similares aos que o Autor anteriormente enviara, cópia da assinatura do autor, e posterior envio desses documentos/ficheiros, falsamente assinados, através do endereço eletrónico do autor.[214]

De acordo com o Autor, o *software* do seu computador terá sido atacado e invadido por um *malware* enviado por terceiro, que terá manipulado as informações armazenadas na máquina, gerando as instruções de transferência cuja autenticidade o mesmo impugnou em Tribunal.

De acordo com o Autor, tais instruções referiam-se a valores muito mais altos que os valores dos movimentos feitos na sua conta bancária e representavam operações sem relação com a finalidade previamente fixada à conta bancária e que, caso tivesse sido executada a ordem de transferência de 57.000,00 €, a conta ficaria a descoberto em cerca de 25.000,00 €.

Neste sentido, inclusive, a transferência de 57.000,00 € frustrou-se devido a uma irregularidade técnica, o que não sucedeu com as restantes três, sendo que as singularidades formais dessas ordens de transferência, designadamente quanto aos erros ortográficos e dactilográficos que apresentavam, deveriam ter alertado o Réu para a falta da sua autenticidade.

---

[213] Cfr. http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/27962f73862f5520802584c00040134b?OpenDocument (consultado a 02/11/2023).

[214] *Id*.

Por todo o exposto, o Autor alegou que viveu momentos de angústia com toda a situação e a perda do valor correspondente às transferências fraudulentas desarranjou toda a sua vida, sentindo-se frustrado por não poder confiar nos serviços bancários do Réu, tendo ainda sofrido outros danos na sua saúde.

Não obstante todo o exposto, o Tribunal, porém, considerou a ação improcedente, não porque não considerasse a argumentação válida, mas porque entendeu que o Autor não cumpriu, de forma suficiente, o ónus da prova, afirmando que:

> (…) não deixa de surpreender que, para demonstrar a ilegitimidade das instruções de transferência, o único meio de prova apresentado pelo autor se reconduza às declarações de parte por si prestadas, simplesmente afirmando ter o *software* do seu computador sido atacado e invadido por um *malware* enviado por terceiro, que teria manipulado as informações armazenadas na máquina, gerando as instruções de transferência cuja autenticidade impugna.[215]

Ora, dado que inexiste muita jurisprudência sobre a matéria, apesar de o presente Acórdão se reportar a processo civil e não a processo penal, entendemos que é bastante interessante para o tema em apreço, dado que podemos verificar na prática os perigos do recurso ao *malware*.

Da análise dos factos em causa, verificamos os riscos de um mundo globalizado e cada vez mais digital, podendo os perigos do cibercrime colocar em causa a confiança nas instituições.

No caso em apreço, fazendo fé na posição apresentada pelo Autor, verificamos que o seu direito fundamental à reserva da intimidade da vida privada e ao domicílio digital foi violado, o tráfego jurídico foi comprometido, tendo o seu computador sido infetado com *malware* por privados, prática que terá, alegadamente, possibilitado a realização das transferências com tremendo prejuízo para o mesmo.

Porém, conforme também já tivemos oportunidade de analisar, o regime processual português é bastante garantístico e é regido pelo princípio da presunção da inocência e do ónus da prova. Assim, é assustador verificar, na prática, os riscos que existem em virtude da cada vez maior criminalidade digital, dado que para quem pratica o ato, o mesmo fica de imediato consumado. Já para a vítima, a mesma terá de recorrer a

[215] Cfr. http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/27962f73862f5520802584c00040134b?OpenDocument (consultado a 14/05/2023).

tribunal, aguardar vários anos por decisões e recursos e, no final, poderá não conseguir provar que teve razão e, por conseguinte, ficar totalmente prejudicada.

2.2 - Acórdão do Tribunal Constitucional Federal alemão de 27 de fevereiro de 2008: a utilização de *malware* e o princípio da legalidade da prova, o direito fundamental à confidencialidade e integridade dos sistemas informáticos e o direito à inviolabilidade do domicílio

No âmbito do Acórdão do Tribunal Constitucional Federal alemão de 27 de fevereiro de 2008 estavam em causa três direitos fundamentais: (i) o direito à privacidade da correspondência, do correio e das telecomunicações, (ii) o direito à inviolabilidade do lar e ainda (iii) o direito à autodeterminação informacional.[216]

O Tribunal Constitucional Federal alemão começa por afirmar que o direito geral da personalidade abrange o direito fundamental à proteção da confidencialidade e integridade dos sistemas de tecnologia da informação.

Neste sentido, de acordo com o mesmo, a infiltração secreta num sistema de tecnologia da informação com o propósito de monitorizar o uso do sistema e extrair dados armazenados nos seus dispositivos de armazenamento apenas é permitida de acordo com a lei constitucional se houver indícios factuais de um perigo específico para um interesse jurídico excecionalmente significativo e, de acordo com o Tribunal Constitucional Federal alemão, interesses jurídicos excecionalmente significativos são a vida, integridade física e liberdade da pessoa ou interesses públicos de tal importância que uma ameaça a eles afetaria os fundamentos ou a existência do Estado, ou os fundamentos da existência humana.

Assim, entendeu o Tribunal que a medida pode ser justificada mesmo que ainda não possa ser estabelecida com probabilidade suficiente que o perigo se materializará num futuro próximo, desde que existam factos específicos indicando um perigo iminente para um interesse jurídico excecionalmente significativo no caso individual que possa ser atribuído a pessoas específicas.

[216] Cfr. https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2008/02/rs20080227_1bvr037007en.html (consultado a 04/11/2023).

Por conseguinte, a infiltração secreta num sistema de tecnologia da informação, em princípio, requer uma ordem judicial e a base legal que autoriza tal interferência deve incluir salvaguardas para proteger o núcleo da vida privada. Na medida em que a autorização legislativa se limite a medidas estatais de intercetação de conteúdos e circunstâncias de telecomunicações em rede de computadores em andamento, ou análise de dados assim obtidos, a interferência deve ser avaliada de acordo com a Lei Fundamental.

Assim, quando o Estado obtém conhecimento do conteúdo das comunicações na *internet* usando os meios técnicos normais previstos para esse fim, ocorre uma infração da Constituição apenas se a autoridade estatal relevante não recebeu permissão para fazê-lo e não cumpriu as condições estabelecidas atrás. Já quando o Estado obtém conhecimento de conteúdos de comunicação que são publicamente acessíveis na *internet* ou participa de processos de comunicação publicamente acessíveis, geralmente não interfere nos direitos fundamentais e já não será necessário observar as condições estabelecidas na lei com vista à proteção do direito á privacidade.

Em face do exposto, de acordo com a interpretação do douto Tribunal, verificamos que o direito fundamental à confidencialidade e integridade de sistemas informáticos deverá prevalecer face à utilização de *malware* como via de investigação, a não ser que se verifiquem as condições estabelecidas pela decisão do Tribunal Constitucional alemão que referimos atrás.[217]

Com base no exposto, de acordo com a interpretação do tribunal, observa-se que o direito fundamental à confidencialidade e integridade dos sistemas informáticos deve prevalecer sobre o uso de *malware* como meio de investigação, só podendo ser justificado em casos excecionais.

O direito à confidencialidade e integridade dos sistemas informáticos é essencial para proteger a privacidade e os dados pessoais dos indivíduos e apesar do avanço da tecnologia e a crescente dependência de sistemas de informação esse direito é ainda mais relevante nos dias atuais. Assim, os indivíduos confiam nos seus sistemas informáticos para armazenar informações confidenciais, realizar transações financeiras e comunicar-se de forma segura.

[217] Neste sentido, *vide* RAMALHO, David Silva (2015) – *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, Dissertação de Mestrado em Direito, Especialidade de Ciências Jurídico-Criminais, Lisboa, Faculdade de Direito da Universidade de Lisboa, p. 218.

É verdade que, em certas circunstâncias, como investigações criminais, surge a questão de equilibrar a proteção dos direitos individuais com a necessidade legítima de aplicação da lei. Porém, o uso de *malware* consiste na instalação de *software* malicioso num sistema informático sem o conhecimento ou consentimento do utilizador e apesar de poder ser uma ferramenta tentadora para obter acesso a informações relevantes em investigações, cumpre proceder à ponderação dos interesses em confronto e, de acordo com a interpretação do Tribunal Constitucional Federal alemão, o direito fundamental à confidencialidade e integridade de sistemas informáticos deverá prevalecer, salvo circunstâncias muito excecionais estabelecidas na Lei sobre a defesa contra os perigos do terrorismo internacional pelo Serviço Federal de Polícia Criminal e aceites pelo Tribunal Constitucional alemão.

CAPÍTULO VI – PROPOSTA DE REGIME JURÍDICO

1 - PROPOSTA FINAL DE REGIME JURÍDICO

Conforme fomos analisando, o advento da globalização, máxime, das novas tecnologias de informação e comunicação trouxe consigo inúmeras mudanças na forma como lidamos com questões de segurança e justiça.

Neste sentido, também no contexto das investigações policiais têm surgido novos mecanismos como as escutas telefónicas ou a pesquisa de dados informáticos, a intervenção do sistema de videovigilância, o acesso a SMS ou mensagens de correio eletrónico mediante requerimento do Ministério Público e despacho fundamentado do juiz de instrução.

Ora, a possibilidade de recorrer ao *malware* emergiu como uma possível ferramenta controversa, capaz de oferecer vantagens significativas, mas que também pode acarretar perigos potenciais.

Neste sentido, como vantagens, podemos enunciar a possibilidade de realizar uma investigação mais eficiente, dado que o *malware* pode ser usado para rastrear, monitorizar e obter dados de suspeitos em tempo real, acelerando o processo de investigação e permitindo aos OPC a obtenção de informações cruciais mais rapidamente, agilizando a tomada de decisões e possibilitando a prevenção de atividades criminosas em curso.

Por outro lado, pode permitir o acesso a informações ocultas, dado que algumas formas de *malware* possibilitam penetrar em sistemas e dispositivos que normalmente estariam inacessíveis para as autoridades, o que pode revelar evidências valiosas, como conversas criptografadas ou arquivos apagados, os quis seriam difíceis de obter por meios convencionais.

Acrescentamos ainda como vantagem a possibilidade de identificação de novos métodos criminosos, permitindo às entidades policiais acompanharem as últimas tendências em táticas criminosas e, ao entenderem melhor como os criminosos operam no mundo digital, a polícia tem a possibilidade de se preparar melhor para combater as ameaças emergentes.

Sem prejuízo do exposto, a eventual utilização do *malware* é indissociável dos riscos inerentes.

Em primeiro lugar, conforme já se referiu, o uso de *malware* em investigações pode levantar questões éticas e legais sobre a invasão de privacidade dos cidadãos, dado que, se não existirem salvaguardas adequadas e supervisão rigorosa, as ações das forças policiais podem prejudicar injustificadamente a privacidade de pessoas inocentes, violando os seus direitos fundamentais.

Por outro lado, caso não exista controlo adequado, o *malware* pode permitir o aceso a informação sensível por parte de agentes mal-intencionados dentro das forças policiais, o que poderá conduzir a abusos de poder e à manipulação de informações para fins ilegítimos, prejudicando a integridade do sistema judiciário e a confiança do público nas instituições.

Por todo o exposto, dado os riscos que acarreta, somos da opinião que uma eventual legalização do uso do *malware* em investigações criminais deve ser bem ponderada antes de ser formalizada na lei. Ademais, haverá desde logo que partir do art.º 26º da CRP que preconiza outros direitos pessoais do cidadão, nos quais se inclui o direito à imagem e à reserva da intimidade da vida privada e familiar.

No que concerne aos meios de prova, e ao artigo que os define, mormente o art.º 126º que reporta aos métodos proibidos de prova, haveria igualmente que considerar como incluído nos casos ressalvados por lei referidos logo no início deste número a utilização de *malware* que inevitavelmente se considera invasivo na vida privada e nas telecomunicações sem o consentimento do titular.

Tal implica, caso se pretenda avançar neste caminho, uma expansão dos regimes atualmente previstos na lei e abordados no Capítulo IV.

Assim, propomos uma divisão sistémica relativamente ao uso e às várias utilidades do *malware* quanto ao pretendido. Em crimes de menor gravidade, mas já com alguma complexidade e moldura penal superior, o sistema de interceções telefónicas talvez se afigure proporcional. No entanto, no que à criminalidade violenta e organizada diz respeito, estamos em crer que um meio mais sofisticado será essencial. Desta forma, sugerimos a utilização de um *malware*, de forma adequada e proporcional, isto é, como se referiu no capítulo IV, podendo optar pelo recurso ao mesmo a fim de obter apenas imagens e vídeo ou, por seu turno, obter ficheiros áudio.

Em casos extremos a utilização destas duas vertentes, com acesso ao dispositivo por inteiro, quando se demonstre ser a última *racio* para a descoberta da verdade material.

Quanto aos seus requisitos, teremos de estar perante um crime de catálogo que, como referimos atrás, faça parte da criminalidade violenta e organizada e relativamente à investigação do mesmo deverá existir requerimento do Ministério Público e, necessariamente, despacho do Juiz de Instrução, sob pena de nulidade.

Tal despacho deverá ser devidamente fundamentado e conter as exatas diretrizes a seguir pelos órgãos de polícia criminal nomeadamente se a utilização do *malware* servirá para fins de obtenção de imagens e vídeos ou para obtenção de ficheiros áudio ou para ambos, qual o crime em causa e a complexidade do caso que torna indispensável o recurso a este meio. Tal decisão será ainda do conhecimento do Ministério Público, para que este possa confirmar que a utilização do *malware* está a ser utilizada dentro dos cânones legais aplicáveis.

Sobre as informações obtidas sem qualquer relevo e de carácter pessoal e íntimo deverão ser automaticamente destruídas, como já está decretado nos vários regulamentos citados, nomeadamente art.º 4º nº 7[218] da Lei nº 95/2021, de 29 de setembro; art.º 188º nº 6[219] do CPP.

Isto posto, mais uma vez reiteramos que existem tremendos riscos nesta legalização, porém, tendo em conta crimes complexos como associação criminosa, terrorismo ou grandes esquemas de fraude fiscal, o recurso ao *malware* poderá eventualmente ser proporcional face aos riscos de continuação de atividade criminosa.

1.1 - CRIMES ABRANGIDOS

No que concerne aos crimes abrangidos pela possibilidade de recurso ao *malware* como via de investigação, e em face de tudo o que já se foi defendendo, entendemos ser de aplicar inevitavelmente aos crimes mais gravosos do nosso ordenamento jurídico,

[218] Cfr. "As imagens e os sons acidentalmente obtidos, em violação do disposto nos arts. 5º e 6º, devem ser destruídos de imediato pelo responsável pelo sistema.

[219] Cfr. Sem prejuízo do disposto no nº 7 do artigo anterior, o juiz determina a destruição imediata dos suportes técnicos e relatórios manifestamente estranhos ao processo: a) Que disserem respeito a gravações em que não intervenham pessoas referidas no nº 4 anterior; b) Que abranjam matérias cobertas pelo segredo profissional, de funcionário ou de Estado ou; c) Cuja divulgação possa afetar gravemente direitos, liberdades e garantias; ficando todos os intervenientes vinculados ao dever de segredo relativamente às conversações de que tenham tomado conhecimento.

atendendo, desde logo e com especial relevância aos conceitos explanados no art.º 1º do CPP: o terrorismo, a criminalidade violenta, criminalidade especialmente violenta e a criminalidade altamente organizada.

Aqui realçamos também os crimes abrangidos pela Lei n.º 5/2002, de 29 de dezembro, os quais elencámos no título 5 do capítulo V, que se inserem no âmbito da criminalidade organizada e económico-financeira, os quais nos parecem apresentar gravidade suficiente para ser ponderada a aplicação do referido mecanismo.

Dessa forma, aqui nos afastamos do previsto no art.º 187º nº 1 do CPP, uma vez que tal regime é demasiado abrangente no que tangue ao catálogo de crimes comparativamente com o aceitável no recurso ao *malware*, por tudo aquilo que vimos defendendo.

Cremos que, caso se pretenda ponderar a consagração legal do recurso ao *malware* como mecanismo legal de investigação, será essencial identificar escrupulosamente um catálogo de crimes, deixando assim de haver uma "cláusula aberta" tal como configura o art.º 187.º do CPP, o qual prevê a possibilidade de realizar escutas telefónicas relativamente a qualquer crime que seja punível com pena superior a 3 anos.

1.2 - PROCEDIMENTO E ÓRGÃOS RESPONSÁVEIS

No que respeita ao procedimento e órgãos responsáveis, somos da opinião de que o regime vigente para as escutas telefónicas poderá ser aplicável a uma possível consagração do *malware* como via de investigação.

Assim, nos termos do disposto art.º 187.º, n.º 1 CPP, o procedimento apenas seria passível de aplicar durante o inquérito e caso existam razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter.[220]

Paralelamente, os órgãos responsáveis seriam, em primeira instância, o Ministério Público, o qual teria de apresentar requerimento e, por seu turno, teria que existir despacho fundamentado do juiz de instrução.

[220] Cfr. https://dre.pt/dre/legislacao-consolidada/decreto-lei/1987-34570075 (consultado a 04/11/2023).

No requerimento e na decisão em causa, seria sempre necessário cumprir o princípio da legalidade da prova e, bem assim, o princípio da proporcionalidade, jamais podendo, em caso algum, o recurso ao *malware* ser a primeira via de investigação apenas numa lógica de facilitismo.

Ademais, terá de existir intervenção dos órgãos de polícia criminal[221], os quais irão executar a decisão do JIC nos precisos termos em que a mesma tenha sido estabelecida.

Em nosso entendimento, arriscamo-nos a apontar as entidades da Polícia Judiciária como os principais órgãos de polícia criminal a utilizar este meio de obtenção de prova, uma vez que estes se encarregam dos ilícitos mais gravosos como já acontece com as ações encobertas.

[221] Art.º 1.º, alínea c) do CPP:
Considera-se que são órgãos de polícia criminal todas as entidades e agentes policiais a quem caiba levar a cabo quaisquer actos ordenados por uma autoridade judiciária ou determinados pelo CPP, Cfr. https://dre.pt/dre/legislacao-consolidada/decreto-lei/1987-34570075 (consultado a 04-11-2023).

CONCLUSÕES

A possibilidade de recurso ao *malware* pelos órgãos de polícia criminal no âmbito das investigações criminais abrange uma série de aspetos importantes no contexto atual da segurança cibernética e do trabalho policial.

O *malware* foi desenvolvido como um *software* malicioso projetado para infiltrar, danificar ou controlar sistemas de computador, sendo uma ferramenta de grande perigo e causador de grandes transtornos na era digital.

Os perigos associados ao *malware* são evidentes.

Em primeiro lugar, o *malware* é usado por criminosos cibernéticos para roubar informações pessoais, financeiras e confidenciais de indivíduos e organizações, o que pode levar a consequências graves, como roubo de identidade, perdas financeiras e comprometimento da privacidade. Além disso, o *malware* pode causar danos significativos a sistemas de computador e redes e resultar na interrupção de serviços, perda de dados e custos substanciais para as vítimas.

Estas ameaças cibernéticas estão em constante evolução, sendo constantemente criadas novas modalidades de *malware*, pelo que, o combate ao mesmo exige medidas robustas de segurança para proteção efetiva.

No entanto, apesar da sua génese negativa, a verdade é que o *malware* apresenta potencial para ser utilizado legalmente pela polícia em investigações, dado que permite à mesma ter acesso a dados que, de outra forma, não conseguiria ou teria muito mais dificuldade em conseguir.

Assim, apesar desses perigos, a possibilidade de a polícia utilizar o *malware* em investigações levanta questões sobre o equilíbrio entre segurança e privacidade. Em certos casos, a utilização controlada e legal do *malware* poderá fornecer às autoridades acesso a evidências cruciais para investigações criminais quanto a criminalidade extremamente complexa e altamente organizada.

A título de exemplo, podemos referir que a capacidade de monitorizar comunicações criptografadas ou rastrear atividades online de suspeitos pode ser uma ferramenta valiosa na luta contra o terrorismo, tráfico de drogas e outros crimes graves, ou seja, numa lógica de legalidade de proporcionalidade, poderemos chegar à conclusão de que

os benefícios da utilização do *malware* pela polícia poderá ser superior aos riscos de continuação de atividade criminosa.

Uma das grandes vantagens potenciais do uso controlado do *malware* pela polícia é a possibilidade de prevenção e deteção de atividades criminosas, dado que, a capacidade de infiltrar e monitorizar sistemas comprometidos pode permitir que as autoridades identifiquem e impeçam ameaças antes de as mesmas se agravarem. Além disso, o uso de *malware* em investigações pode ajudar na obtenção de provas digitais, fornecendo dados essenciais para processos judiciais, os quais podem ser vitais para determinar a autoria de um crime e garantir a condenação justa dos culpados.

No entanto, caso se pretenda fazer o uso do *malware* pela polícia, o mesmo deverá ser devidamente regulamentado por estruturas legais claras, garantindo que os direitos individuais e a privacidade sejam protegidos.

Contudo, é importante reconhecer que o uso do *malware* pela polícia também pode levantar preocupações significativas.

Em primeiro lugar, a segurança e a integridade dos sistemas de computador podem ser comprometidas se o *malware* utilizado pela polícia cair nas mãos erradas. Além disso, a falta de controlo adequado sobre o uso do *malware* pode resultar em violações da privacidade dos cidadãos, bem como abusos por parte das autoridades, pelo que, é fundamental estabelecer salvaguardas rigorosas, supervisionar o uso do *malware* pela polícia e garantir a prestação de contas e transparência em relação às suas atividades.

A questão do uso do *malware* pela polícia em investigações requer um equilíbrio delicado entre segurança, privacidade e proteção dos direitos individuais. Embora o *malware* possa oferecer vantagens na prevenção e combate ao crime altamente organizado incluindo o cibernético, o seu uso deve ser limitado, regulamentado e monitorização de perto para evitar abusos e garantir a justiça. A colaboração entre especialistas em segurança cibernética, legisladores e órgãos policiais é essencial para desenvolver políticas e diretrizes que permitam o uso responsável do *malware* em investigações, enquanto se protege a privacidade e se preserva a confiança do público. A segurança cibernética e a aplicação da lei devem andar de mãos dadas para enfrentar os desafios cada vez maiores apresentados pelas ameaças digitais, encontrando um equilíbrio adequado que proteja a sociedade como um todo.

Por todo o exposto, somos da opinião de que, observando critérios rigorosos e formalismos essenciais, o *malware* poderá ser uma mais valia enquanto meio de

investigação sopesando o interesse no apuramento de factos com relevância criminal em contraposição com o direito à imagem e á privacidade, podendo concluir pela preponderância do primeiro em detrimento do outro, pois que este não fica beliscado de forma intolerável ou desproporcionada.

Desta forma, através de despacho fundamentado por magistrado Judicial de Instrução Criminal, com a concordância de magistrado do Ministério Público, devendo expressamente ser indicado o tipo de *malware* a utilizar, fazendo a distinção entre a captação de imagens, a modalidade de obtenção de áudio ou ambos, vislumbramos assim uma importante evolução na investigação criminal no que concerne aos meios de prova.

Tal mecanismo deverá, em nosso entendimento, ser operado por responsáveis pela investigação da criminalidade grave, indicando para o efeito especializados no seio da Polícia Judiciária – sendo do nosso conhecimento que o *malware* se encontra disponível no nosso país por estas mesmas entidades, contudo não está em prática uma vez que não é admitido no nosso sistema penal.

REFERÊNCIAS BIBLIOGRÁFICAS

ALBUQUERQUE, Paulo Pinto de (2008) – Comentário do Código de Processo Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem, 2.ª ed., Lisboa, Universidade Católica Editora

AMARAL, Maria Lúcia (2005) – A Forma da República – Uma Introdução ao estudo do Direito Constitucional, Coimbra, Coimbra Editora

AMARAL, Maria Lúcia (2012) – A Forma da República - Uma Introdução ao Estudo do Direito Constitucional, Reimpressão, Coimbra, Coimbra Editora

ANDRADE José Carlos Vieira de (2012) – Os Direitos Fundamentais na Constituição Portuguesa de 1976, 5ª ed., Coimbra, Almedina

ANDRADE, Manuel da Costa (2009) – Bruscamente no Verão Passado, a Reforma do Código de Processo Penal. Observações críticas sobre uma Lei que podia e devia ter sido diferente, Coimbra, Coimbra Editora

ASCENSÃO, Oliveira (2001) – Estudos sobre Direito da Internet e da Sociedade de Informação, Coimbra, Almedina

ASTORGA, Paula Celeste Moreira Cardoso (2014) - Escutas telefónicas, Coimbra, Universidade de Coimbra

AYCOCK, John (2006) – Computer Viruses and Malware, Advances in Information Security, Spinger

BOLDT, Martin (2010) – Privacy-Invasive Software, Blekinge Institute of Technology

BOSWORTH, Seymour; KABAY, M. E.; WHYNE, Eric (2014) – Computer Security Handbook. 6th ed. Hoboken, NJ: John Wiley & Sons, Inc.

BRAZ, José (2013) – Investigação Criminal: A organização, o método e a prova: os desafios da nova criminalidade. 3ª ed, Coimbra: Almedina

BRENNER, Susan (2007) – At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare, Journal of Criminal Law and Criminology, volume 97, Tomo 2, Northwestern University, Copyright (c)

BRITO, Miguel Teixeira de (2020) – Modelos de Emergência no Direito Constitucional, Revista e-Pública Vol. 7 No. 1, abril 2020

BROWN, David (1992) – An introduction to computer viroses, United States, Martin Marietta Energy Systems inc

BULLOS, Uadi Lammêgo (2011) – Curso de Direito Constitucional. 6. ed., rev. São Paulo: Saraiva

CABRAL, António do Passo (2009) – O contraditório como dever e a boa-fé processual objetiva, in Revista Baiana de Direito. v. 4. Salvador: Faculdade Baiana de Direito

CAIRES, João Gouveia de (2019) – Métodos Ocultos na Criminalidade Económico-Financeira: entre a (A)Tipicidade e a Cumulação, Revista Julgar n.º 38, Almedina

CAIRES, João Gouveia de (2014) – O registo de som e imagem e as escutas ambientais, in Direito da Investigação Criminal e da Prova, coord. Maria Fernanda Palma et al., Coimbra, Almedina

CANAS, Vitalino (1994) – Proporcionalidade (Princípio da) - Separata do vol. VI do Dicionário Jurídico da Administração Pública

CANAS, Vitalino (1998) — O princípio da proibição do excesso na Constituição: arqueologia e aplicações, in Perspectivas Constitucionais — Nos 20 Anos da Constituição de 1976 (org. Jorge Miranda), vol. II, Coimbra, Coimbra Editora

CANOTILHO, J. J. Gomes (1974) – O problema da responsabilidade do Estado por actos lícitos, Coimbra, Almedina

CANOTILHO, Gomes (2018) – Direito Constitucional e Teoria da Constituição, Coimbra, Almedina

CANOTILHO, Gomes e MOREIRA, Vital (2007) – Constituição da República Portuguesa Anotada, 4.ª edição revista, volume I, Coimbra, Coimbra Editora

CARDOSO, Rui –Apreensão de correio electrónico e registos de comunicações de natureza semelhante – artigo 17.º da Lei n.º 109/2009, de 15.IX, in Revista do Ministério Público, n.º 153

CHIEN, Eric e SZÖR, Péter (2002) – Blended Attacks Exploits, Vulnerabilities and Buffer-Overflow Techniques in Computer Viruses, Virus Bulletin

CLOUGH, Jonathan (2015) – Principles of Cybercrime, Cambridge, Cambridge University Press, p. 34. (2.ª ed., 2015)

CONTE, Christiany Pegorari e FIORILLO, Celso Antonio Pacheco (2015) – Crimes no Meio Digital, São Paulo, Editora Saraiva

COSTA, Eduardo Maia (2014) – Acções Encobertas (Alguns Problemas, Algumas Sugestões), Estudos em Memória do Conselheiro Artur Maurício, Coimbra, Coimbra Editora

ERBSCHLEO, Michael (2005) – Trojans, Worms and Spyware – A Computer Security Professional's Guide to Malicious Code, Elsevier Butterworth–Heinemann

ERD, Rainer (2008) – Bundesverfassungsgericht versus Politik, Kritische Justiz

ERESHEIM, S., LUH, R., e SCHRITTWIESER, S. (2017) – The Evolution of Process Hiding Techniques in Malware - Current Threats and Possible Countermeasures. J. Inf. Process., 25

FILIOL, Eric (2005) – Computer viruses: from theory to applications, Springer

FRANZ, Marcel (2007) – Containing the Ultimate Trojan Horse. IEEE Security & Privacy

FRATANTONIO, Y.; BIANCHI, A.; ROBERTSON, W., KIRDA, E.; KRÜGEL, C. e VIGNA, G. (2016) – TriggerScope: Towards Detecting Logic Bombs in Android Applications. Symposium on Security and Privacy (SP)

GASPAR, António da Silva Henriques et al. (2016) – Código de Processo Penal Comentado 2.ª ed., Coimbra, Almedina,

GAZET, A. (2010) – Comparative analysis of various ransomware virii. Journal in Computer Virology, 6

GONÇALVES, Fernando; ALVES, Manuel João; e VALENTE, Manuel Monteiro Guedes (2001) – Lei e Crime, Lei e Crime - O Agente Infiltrado Versus o Agente Provocador - Os Princípios do Processo Penal, Coimbra, Almedina

HODKINSON, Alan (2020) – Fundamental British Values. International Review of Qualitative Research

HUMPHREY, Watts (1989) – Managing the Software Process. Addison Wesley

INÁCIO, André (2016) – Tecnologias de Informação e Segurança Pública: Um Equilíbrio Instável, Revista Científica Sobre Cyberlaw, CIJC, Faculdade de Direito de Lisboa, n.º 1, janeiro 2016

JIN, C., WANG, X., & TAN, H. (2010) – Dynamic Attack Tree and Its Applications on Trojan Horse Detection. Second International Conference on Multimedia and Information Technology, 1

KUTSCHER, Vladimir; MARTINS, Thiago Weber; OLBORT, Johannes; ANDERL, Reiner (2021) – Concept for Interaction of Hardware Simulation and Embedded Software in a Digital Twin Based Test Environment, Procedia CIRP, Volume 104, 2021

LEE, Y. e TAN, Y. (2008) – Making Money with Free Software? Sampling Implications of Software Market. Entrepreneurship & Law eJournal.

LEITÃO, Maria Da Glória (2012) - A Admissibilidade como meio de prova em processo disciplinar das mensagens de correio eletrónico enviadas e recebidas por trabalhador a partir de e na caixa de correio fornecida pela entidade empregadora, Colóquio no STJ, Lisboa, 10 outubro de 2012

LIGH, Michael; ADAIR, Steven; HARTSTEIN, Blake; RICHARD, Matthew (2010) – Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code. 1st ed. Indianapolis: Wiley Publishing, Inc.

LIM, K. Y. H., ZHENG, P., e CHEN, C.-H. (2020) – A state-of-the-art survey of Digital Twin: techniques, engineering product lifecycle management and business innovation perspectives. Journal of Intelligent Manufacturing, 31(6)

LIMBERGER, Têmis (2007) – O direito à intimidade na era da informática, Porto Alegre: Livraria do Advogado.

Magic Lantern on back of Carnivore, Computer Fraud & Security, volume 2002, tomo 1, janeiro de 2002

MAURÍCIO, Nuno; IRIA, Catarina (2006) - As escutas telefónicas como meio de obtenção de prova - Necessidade de uma reforma legislativa ou suficiência de uma interpretação conforme?: Ponto de situação numa já vaexata quaestio! Polícia e Justiça. Instituto Superior de Polícia Judiciária e Ciências Criminais. Loures: III Série, N.º 7 (janeiro-junho 2006)

Medeiros, Armando (2017) – Os perigos da indiferença à verdade. Revista UNO, Vol. 27

MENKE, Fabiano (2019) – A proteção de dados e o direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão, RJLB, Ano 5 (2019), nº 1

MIRANDA, Jorge (2012) – Manual de Direito Constitucional, Tomo IV (Direitos Fundamentais), 5.ª ed., Coimbra, Coimbra Editora

MIRANDA, Jorge e MEDEIROS, Rui (2005) – Constituição Portuguesa Anotada, tomo I, 2.ª ed., Coimbra, Coimbra Editora

NOVAIS Jorge Reis (2010) – As restrições aos Direitos Fundamentais não expressamente autorizadas pela Constituição, 2ª ed, Coimbra, Coimbra Editora

ONETO, Isabel (2005) - O agente infiltrado: contributo para a compreensão do regime jurídico das acções encobertas, Coimbra, Coimbra Editora

ORTIZ PRADILLO, Juan Carlos (2009) – El Remote Forensic Software como Herramienta de Investigación contra el Terrorismo, ENAC, número 4, outubro de 2009

PINHEIRO, Alexandre Sousa (2015) – Privacy e proteção de dados: a construção dogmática do direito à identidade informacional, Lisboa, Faculdade de Direito da Universidade de Lisboa

POULSEN, Kevin (2007) – FBI's Secret Spyware Tracks Down Teen Who Made Bomb Threats, WIRED, 18-07-2007.

RAMALHO, David (2013) – O uso de malware como meio de obtenção de prova em processo penal, Revista de Concorrência e Regulação, número 16, ano IV, outubro/zezembro de 2013

RAMALHO, David Silva (2015) – Métodos Ocultos de Investigação Criminal em Ambiente Digital, Dissertação de Mestrado em Direito, Especialidade de Ciências Jurídico-Criminais, Lisboa, Faculdade de Direito da Universidade de Lisboa

RIBEIRO, Gustavo Alves Magalhães; CORDEIRO, Pedro Ivo Rodrigues Velloso; FUMACH, Débora Moretti (2021) – O malware como meio de obtenção de prova e a sua implementação no ordenamento jurídico brasileiro. Revista Brasileira de Direito Processual Penal, v. 7, n. 1, p. 95-120, jan./abr. 2021.

SANTOS, Cláudia Cruz (2001) – O Crime de Colarinho Branco, Coimbra, Stvdia Ivridica

SARLET, Ingo (2021) – Dignidade da Pessoa Humana e Direitos Fundamentais na Constituição Federal de 1988, 10ª Edição, Porto Alegre RS, Livraria do Advogado Editora

SCHWARZ, M., WEISER, S., GRUSS, D., MAURICE, C. e MANGARD, S. (2020) – Malware Guard Extension: abusing Intel SGX to conceal cache attacks. Cybersecurity

SWOBODA, W., GÖTTLER, M., ZINNHOBLER, K. e HASFORD, J. (2001) – Putting the Pieces Together: Using "Off-The-Shelf" Software to Safely Transfer Medical Data. Methods of Information in Medicine

TEIXEIRA, Carlos Adérito e GONÇALVES, Jorge (2007) – Direito Penal e Processual Penal (Tomo II), INA – Instituto Nacional de Administração

TEIXEIRA, Guilherme da Fonseca (2018) – Identidade e autodeterminação informacional no novo Regulamento Geral de Proteção de Dados: a inevitável privatização dos deveres estaduais de proteção, Volume II \ n.º 1 \ janeiro 2018

TORAL, Sergio (2009) – Estudio comparativo de técnicas antimalware, Revista Iberoamericana de Tecnologías del Aprendizaje 4.3

VACIAGO, Giuseppe e RAMALHO, David Silva (2016) – Online searches and online surveillance: the use of Trojans and other types of malware as means of obtaining evidence in criminal proceedings, Digital Evidence and Electronic Signature Law Review, volume 13, novembro de 2016

VALENTE, Manuel Monteiro Guedes (2008) – Escutas telefónicas: Da excepcionalidade à vulgaridade. 2.ª ed. Coimbra, Almedina

VALENTE, Manuel Monteiro Guedes (2017) - Contributos para um Direito Penal Supranacional, Ed. Abdul´s Angels, 2º ed.

VILELA, Alexandra (2000) – Considerações acerca da presunção de inocência em direito processual penal, Coimbra, Coimbra Editora

WAZID, M., SHARMA, R., KATAL, A., GOUDAR, R., BHAKUNI, P., & TYAGI, A. (2013) – Implementation and Embellishment of Prevention of Keylogger Spyware Attacks

WEBGRAFIA

Acórdão do Supremo Tribunal de Justiça, n.º 12693/16.2T8PRT.P1.S1, de 27 de novembro de 2019. Disponível em http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/27962f73862f5520802584c00040134b?OpenDocument

Acórdão do Supremo Tribunal de Justiça, n.º 257/10.9YRCBR.S1, de 31 de março de 2011. Disponível em http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/4d6e3c6c9e4bf7f6802578d900305716?OpenDocument

Acórdão do Supremo Tribunal de Justiça, n.º 05A945, de 23 de setembro de 2004. Disponível em http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/e4428a4a669f03088025705a0052bf9f?OpenDocument&Highlight=0,05A945%20

Acórdão do Supremo Tribunal de Justiça, n.º 05P1831, de 28 de setembro de 2005. Disponível em http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/f26cbff0474ec694802570ae006223a2?OpenDocument

Acórdão do Tribunal da Relação de Coimbra, n.º 63/07.8SAGRD.C1, de 17 de março de 2009. Disponível em http://www.dgsi.pt/jtrc.nsf/c3fb530030ea1c61802568d9005cd5bb/74fccccc257ebcfd8025758d00322252?OpenDocument

Acórdão do Tribunal da Relação de Coimbra, n.º 98/14.4TANZR-B.C1, de 11 de maio de 2016. Disponível em http://www.dgsi.pt/jtrc.nsf/c3fb530030ea1c61802568d9005cd5bb/bc35a4ef671c121980257fb5004cedfe?OpenDocument

Acórdão do Tribunal da Relação de Lisboa, n.º 0008445, de 10 de dezembro de 1991. Disponível em http://www.dgsi.pt/jtrl.nsf/-/09444CCE314CEAA88025680300046A2B

Acórdão do Tribunal da Relação de Lisboa, n.º 176/06.3TNLSB.L2-1, de 16 de fevereiro de 2016. Disponível em http://www.dgsi.pt/jtrl.nsf/-/F2DF5C9FEEF843ED80257FDF006B80CD

Acórdão do Tribunal da Relação de Lisboa, n.º 5011/2004-6, de 22 de setembro de 2005. Disponível em http://www.dgsi.pt/jtrl.nsf/e6e1f17fa82712ff80257583004e3ddc/aa9205a64a196c4d802572340050c772?OpenDocument

Acórdão do Tribunal da Relação do Porto, n.º 991/08.3PRPRT-B.P1, de 27 de outubro de 2010. Disponível em http://www.dgsi.pt/jtrp.nsf/-/B34AD90C1A686669802577E3003ECE30

Acórdão do Tribunal da Relação do Porto, n.º 24733/17.3T8PRT.P1, de 11 de abril de 2019. Disponível em http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/d7c7bbf9d0de6091802583fa003bb587?OpenDocument

Acórdão do Tribunal do Tribunal Constitucional, n.º 328/2020, de 25 de junho de 2020. Disponível em http://www.tribunalconstitucional.pt/tc/acordaos/20200328.htmlhttps://diariodarepublica.pt/dr/legislacao-consolidada/decreto-lei/1987-34570075

Aprova os princípios gerais em matéria de dados abertos e transpõe para a ordem jurídica interna a Diretiva (UE) 2019/1024 do Parlamento Europeu e do Conselho, de 20 de junho de 2019, relativa aos dados abertos e à reutilização de informação do setor público, alterando a Lei n.º 26/2016, de 22 de agosto, Lei nº 68/2021. Disponível em https://files.dre.pt/1s/2021/08/16600/0000200035.pdf

Acórdão do Tribunal do Tribunal Constitucional, n.º 268/2022. Disponível em https://www.tribunalconstitucional.pt/tc/acordaos/20220268.html

BROWN, David R., An Instroduction to Computer Viruses. (1992). U.S. Department of Energy. Disponível em https://www.osti.gov/servlets/purl/5608409

Constituição da República Portuguesa VII Revisão Constitucional (2005). Disponível em https://www.parlamento.pt/Legislacao/Documents/constpt2005.pdf

Código de Processo Penal, DL n.º 78/87, de 17 de fevereiro, Versão desatualizada – redação DL n.º 324/2003, de 27 de dezembro. Disponível em https://www.pgdlisboa.pt/leis/lei_print_articulado.php?tabela=lei_velhas&artigo_id=&nid=199&nversao=17&tabela=lei_velhas

Declaração Universal dos Direitos Humanos. Disponível em https://www.ohchr.org/sites/default/files/UDHR/Documents/UDHR_Translations/por.pdf

CAIRES, João Gouveia de, Métodos Ocultos na Criminalidade Económico-financeira entre a (A)Tipicidade e a Cumulação . Revista Julgar nº38 2019. Disponível em http://julgar.pt/wp-content/uploads/2019/05/JULGAR38-04-JC.pdf

Código da Execução das Penas e Medidas Privativas da Liberdade, Lei n.º 115/2009. Disponível em https://diariodarepublica.pt/dr/legislacao-consolidada/lei/2009-34515975

Código Civil, Decreto-Lei n.º 47344. Disponível em https://dre.pt/dre/legislacao-consolidada/decreto-lei/1966-34509075

Código Civil. Disponível em https://www.codigocivil.pt/

Código de Processo Penal – Capítulo II, Decreto Lei n.º 78/87. Disponível em https://dre.pt/dre/legislacao-consolidada/decreto-lei/1987-34570075-50512275

Conheça o malware que liga a sua webcam e microfone – e saiba como prevenir. Disponível em https://www.tecmundo.com.br/macos/110308-conheca-malware-liga-webcam-microfone-saiba-prevenir.htm

Como evitar a pornografia de vingança, Revista DecoProteste, publicada em 31 de maio de 2023. Disponível em https://www.deco.proteste.pt/familia-consumo/divorcio/noticias/como-evitar-pornografia-vinganca

Convenção Europeia dos Direitos do Homem. Disponível em https://www.echr.coe.int/documents/convention_por.pdf

Decreto do Presidente da República n.º 14-A/2020, de 18 de março. Disponível em https://files.dre.pt/1s/2020/03/05503/0000200004.pdf

Dicionário Priberam. Palavra "Escuta". Disponível em https://dicionario.priberam.org/escuta

Dicionário Priberam. Palavra "Telefónica". Disponível em https://dicionario.priberam.org/telef%C3%B3nica

Directiva 95/46/CE do Parlamento Europeu e do Conselho de 24 de Outubro de 1995. Disponível em: https://www.conjur.com.br/dl/diretiva-europeia.pdf

Dicionário Porto Editora. Significado da palavra "Inquisição". Disponível em https://www.infopedia.pt/apoio/artigos/$inquisicao

Dicionário Porto Editora. Significado da palavra "Cavalo de Troia". Disponível em https://www.infopedia.pt/apoio/artigos/$muro-de-berlimhttps://www.infopedia.pt/apoio/artigos/$o-cavalo-de-troia

Dicionário Porto Editora. Significado da palavra "Malware". Disponível em https://www.infopedia.pt/dicionarios/lingua-portuguesa/malware

European Union Terrorosm Situation and Trend Report 2022. Disponível em https://www.europol.europa.eu/cms/sites/default/files/documents/Tesat_Report_2022_0.pdf

Estatísticas da Justiça, - Condenados em processos crime nos tribunais judiciais de 1ª instância, última atualização em 31 de outubro de 2023. Disponível em https://estatisticas.justica.gov.pt/sites/siej/pt-pt/Paginas/Condenados-em-processos-crime-nos-tribunais-judiciais-de-1-instancia.aspx

Estatísticas da Justiça, - Arguidos em processos crime nos tribunais judiciais de 1ª instância, última atualização em 31 de outubro de 2023. Disponível em https://estatisticas.justica.gov.pt/sites/siej/pt-pt/Paginas/Arguidos-em-processos-crime-nos-tribunais-judiciais-de-1-instancia-.aspx

Estatísticas da Justiça, - Processos crime em fase de julgamento findos em tribunais judiciais de 1ª instância, última atualização em 31 de outubro de 2023. Disponível em

https://estatisticas.justica.gov.pt/sites/siej/pt-pt/Paginas/Processos-crime-em-fase-de-julgamento-findos-nos-tribunais-judiciais-de-1-instancia.aspx

Estatuto dos Jornalistas. Disponível em https://www.clubedejornalistas.pt/?page_id=120

English dictionary. Definition of "crippleware". Disponível em https://www.collinsdictionary.com/dictionary/english/crippleware

Globalization and new technologies: challenges to drug law enforcement in the twenty-first century (2001). Disponível em https://www.incb.org/documents/Publications/AnnualReports/Thematic_chapters/English/AR_2001_E_Chapter_I.pdf

Headnotes to the Judgment of the First Senate of 27 february 2008. Disponível em https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2008/02/rs20080227_1bvr037007en.html

Lei de Prevenção dos Perigos do Terrorismo Internacional pela Polícia Federal Criminal na Alemanha. Disponível em https://dip.bundestag.de/vorgang/.../14447

Lei n.º 109/2009, de 15 de setembro. Disponível em https://dre.pt/dre/detalhe/lei/109-2009-489693

Lei n.º 32/2008, de 17 de julho. Disponível em https://dre.pt/dre/detalhe/lei/32-2008-456812

Lei do Cibercrime, Lei n.º 109/2009. Disponível em https://dre.pt/dre/legislacao-consolidada/lei/2009-128879174

Lei n.º 109/2009 - Aprova a Lei do Cibercrime, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação, e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa. Disponível em https://guiadoinvestidor.dre.pt/PDF.aspx?Idioma=1&DecretoLeiId=25

Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimento de las garantias procesales y la regulación de las medidas de investigacíon tecnológica. Disponível em https://www.boe.es/buscar/doc.php?id=BOE-A-2015-10725

Legal Information Institute, Surveillance. Disponível em https://www.law.cornell.edu/wex/surveillance

O que é o malvertising? Disponível em https://ostec.blog/noticias/malvertising/

O que é um ataque de DDoS de camada de aplicação? Disponível em https://www.akamai.com/pt/glossary/what-is-application-layer-ddos-attack

O que é hacking? E como se prevenir. Disponível em https://www.kaspersky.com.br/resource-center/definitions/what-is-hacking

Pinto, António Costa, Sousa, Luís de, Magalhães, Pedro, A qualidade da democracia em Portugal, A visão dos Cidadãos (2013), Lisboa, Imprensa de Ciências Sociais. Disponível em https://repositorio.ul.pt/bitstream/10451/22839/1/ICS_ACPinto_PMagalhaes_Qualidade_LEN.pdf

PSP e GNR vão receber as primeiras 2500 bodycams em novembro - Artigo de Jornal "Público", publicado em 27 de abril de 2023. Disponível em https://www.publico.pt/2023/04/27/sociedade/noticia/psp-gnr-vao-receber-primeiras-2500-bodycams-novembro-2047715

Pacto Internacional Sobre os Direitos Civis e Políticos. Disponível em https://gddc.ministeriopublico.pt/sites/default/files/documentos/instrumentos/pacto_internacional_sobre_os_direitos_civis_e_politicos.pdf

Publication Office of the Europe Union, Decisão-Quadro 2005/222/JAI do Conselho, de 24 de fevereiro de 2005, relativa a ataques contra os sistemas de informação. Disponível em https://op.europa.eu/en/publication-detail/-/publication/708d86d8-ab9a-4e18-9bda-ac37405a3185/language-pt

Relatório Anual de Segurança Interna, Ano 2022. Disponível em https://www.portugal.gov.pt/download-ficheiros/ficheiro.aspx?v=%3d%3dBQAAAB%2bLCAAAAAAABAAzNDazMAQAhxRa3gUAAAA%3d

Relatório de Cibersegurança em Portugal, Riscos e Conflitos 4ª Ediçao. Disponível em https://www.cncs.gov.pt/docs/rel-riscosconflitos2023-obcibercncs.pdf

Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE. Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679

Sic Notícias – Football Leaks. Disponível em https://sicnoticias.pt/especiais/football-leaks

Vatican leaks: Two arrested in new scandal. Disponível em https://www.bbc.com/news/world-europe-34703293

Vírus InvisiMole controla webcam, microfone e faz print da tela. Disponível em https://www.techtudo.com.br/noticias/2018/08/virus-invisimole-controla-webcam-microfone-e-faz-print-da-tela-conheca.ghtml

Viruses, trojans, malware, worms - what's the difference? Disponível em https://www.wired.co.uk/article/ransomware-viruses-trojans-worms

15.ª alteração ao Código de Processo Penal, aprovado pelo Decreto -Lei n.º 78/87, de 17 de Fevereiro, Lei n.º 48/2007. Disponível em https://files.dre.pt/1s/2007/08/16600/0584405954.pdf