Daniel de Lima Ferreira

O MONITORAMENTO ONLINE COMO MÉTODO OCULTO DE INVESTIGAÇÃO NOS ORDENAMENTOS BRASILEIRO E PORTUGUÊS: UMA PROPOSTA DE SISTEMATIZAÇÃO A PARTIR DA NORMA ALEMÃ.

DISSERTAÇÃO DE MESTRADO EM DIREITO E CIÊNCIA JURÍDICA

LISBOA, 2023.

FACULDADE DE DIREITO
Universidade de Lisboa

Daniel de Lima Ferreira

O MONITORAMENTO ONLINE COMO MÉTODO OCULTO DE INVESTIGAÇÃO NOS ORDENAMENTOS BRASILEIRO E PORTUGUÊS: UMA PROPOSTA DE SISTEMATIZAÇÃO A PARTIR DA NORMA ALEMÃ.

DISSERTAÇÃO DE MESTRADO EM DIREITO E CIÊNCIA JURÍDICA

Orientador:
Professor Doutor Paulo de Sousa Mendes

LISBOA, 2023.

AGRADECIMENTOS

Agradeço a oportunidade de acesso ao estudo e educação aos meus pais que sempre me guiaram pelo melhor caminho. Sem dúvidas, são os maiores responsáveis por quem me tornei, e sem os quais nada seria possível.

Ao Professor Doutor Paulo de Sousa Mendes, meu agradecimento pelo conhecimento transmitido e pelas críticas construtivas.

Meu muito obrigada a todos que foram responsáveis, direta e indiretamente, pela minha construção para chegar até aqui. Ninguém constrói nada sozinho.

RESUMO

Com base nos avanços tecnológicos da atualidade e nas mudanças que eles têm causado no Direito Processual Penal, assim como no aumento da criminalidade, este trabalho tem como objetivo estudar os métodos ocultos de investigação criminal em ambiente digital, suas características, consequências, limites (e a falta destes). Isso se deve ao fato de que os sistemas de informática se tornaram uma fonte rica de provas para diversos tipos de crimes. Considerando as particularidades e desafios envolvidos na obtenção de provas digitais, o Estado, responsável por acompanhar a evolução tecnológica e equiparar-se para combater os crimes cometidos em ambiente digital, passou a utilizar métodos ocultos de investigação criminal como uma ferramenta, como é o caso do *malware*. O uso de *malware* visa auxiliar nas investigações de crimes digitais mais graves e permitir um maior alcance na coleta de documentos necessários para a persecução penal. Contudo, da observação do tema, constatou-se que tal método investigativo, ainda, não tem previsão legal expressa no ordenamento jurídico português e brasileiro (mesmo já existindo em outros países), além disso, quando usado para coleta de prova em tempo real (monitoramento *online*), observa-se restrições mais severas aos direitos fundamentais dos indivíduos investigados, quando comparado a um simples acesso sigiloso ao dispositivo informático, bem como a outros métodos ocultos de investigação. Chega-se a conclusão de que é necessário criar um sistema abrangente e uniforme para regular esse método nos ordenamentos jurídicos português e brasileiro. Tal sistema visa estabelecer diretrizes claras, procedimentos e garantias processuais para garantir um equilíbrio adequado entre a eficácia das investigações criminais e a proteção dos direitos fundamentais dos cidadãos envolvidos. Para tanto, esta dissertação se utiliza do estudo das leis que regulam o tema em outros países e sugere, como base especialmente, na legislação alemã, uma sistematização normativa sobre o tema no Brasil e em Portugal.

Palavras-chave: *malware*; prova digital; métodos ocultos de investigação criminal; monitoramento *online*; direitos fundamentais.

ABSTRACT

Based on current technological advances and the changes they have caused in Criminal Procedural Law, as well as the increase in crime, this work aims to study the hidden methods of criminal investigation in a digital environment, their characteristics, consequences, limits (and the lack of these). This is due to the fact that computer systems have become a rich source of evidence for various types of crimes. Considering the particularities and challenges involved in obtaining digital evidence, the State, responsible for keeping up with technological evolution and equipping itself to fight crimes committed in a digital environment, began to use hidden methods of criminal investigation as a tool, as is the case from the malware. The use of malware aims to assist in the investigation of more serious digital crimes and allow a greater reach in the collection of documents necessary for criminal prosecution. However, from the observation of the theme, it was found that such an investigative method still does not have an express legal provision in the Portuguese and Brazilian legal systems (even though it already exists in other countries), in addition, when used to collect evidence in real time (online monitoring), there are more severe restrictions on the fundamental rights of the investigated individuals, when compared to simple confidential access to the computer device, as well as other hidden methods of investigation. It is concluded that it is necessary to create a comprehensive and uniform system to regulate this method in Portuguese and Brazilian legal systems. Such a system aims to establish clear guidelines, procedures and procedural guarantees to ensure an adequate balance between the effectiveness of criminal investigations and the protection of the fundamental rights of the citizens involved. Therefore, this dissertation uses the study of the laws that regulate the subject in other countries and suggests, as a basis especially in German legislation, a normative systematization on the subject in Brazil and Portugal.

Keywords: *malware; digital proof; hidden methods of criminal investigation; online monitoring; fundamental rights.*

ÍNDICE

INTRODUÇÃO

As rápidas e significativas inovações tecnológicas e científicas das últimas décadas são indiscutíveis, o que resulta na transformação de todos os aspectos da vida pessoal e comunitária, afetando diretamente os indivíduos e as suas interações interpessoais. Estas mudanças alcançam todos os âmbitos da vida humana, e não seria diferente em relação ao Direito, o qual é um espelho que reflete a cultura, problemas e aspectos sociais inerentes aos indivíduos em determinada época e local. Mais especificamente, o sistema de justiça penal, por espelhar o Estado e seus diversos conflitos sociais, deve acompanhar as mudanças que ocorrem nas condições socioeconômicas, políticas e culturais da comunidade, tanto no que se refere ao fenômeno criminal quanto à dinâmica processual.

De um lado, a tecnologia possibilitou o surgimento de novos tipos de crimes, enquanto os delitos tradicionais passaram a ocorrer, não apenas no mundo físico/material, mas também no mundo digital. De outro lado, os métodos tradicionais de obtenção de provas foram se tornando insuficientes no que concerne a detecção de crimes, a apreensão de provas e às características próprias das provas digitais que são imateriais e voláteis. Dessa forma, o Estado passou a necessitar de técnicas inovadoras para a investigação criminal, o que contribuiu para a introdução de novos elementos e fatores, como métodos ocultos mais intrusivos.

A utilização de ferramentas digitais por criminosos está em constante crescimento. Como resultado, os ataques cibernéticos estão mais frequentes e sofisticados, utilizando, inclusive, *softwares* maliciosos avançados, como é o caso do *malware*. Tal método também é utilizado pelo Estado como ferramenta de investigação criminal. É exatamente neste contexto que surge o tema a ser tratado neste trabalho: o monitoramento *online* como método oculto de investigação nos ordenamentos brasileiro e português: uma proposta de sistematização a partir da norma alemã.

No presente trabalho será abordado as características do malware, enquanto método oculto de investigação criminal, analisando-se com ênfase, o seu aspecto de monitoramento *online*. Não será objeto de estudo, a utilização de outras ferramenta ou aplicações que também possibilitam o monitoramento em tempo real de indivíduos em investigações criminais. A utilização de técnica do monitoramento *online* será apreciada, enquanto meio de obtenção de prova em processo criminal, razão pela qual, excluir-se-á o uso dessa metodologia para fins de prevenção criminal e combate a atos de terrorismo. É dizer, o trabalho se voltará a apreciar as características do *malware* e a sua relação com direito fundamentais, para ao final propor, a

partir da norma habilitante alemã, proposta de sistematização para os ordenamentos brasileiro e português que, ainda, não preveem expressamente o *malware* em suas respectivas legislações.

Assim, abordagem será organizada em três capítulos. O primeiro se refere a relação entre a sociedade de informação e os crimes digitais, cada vez mais comuns devido ao avanço tecnológico e ao fenômeno da globalização. Nesse contexto, surge a investigação criminal em ambiente eletrônico-digital e as evidências digitais resultantes dela, caracterizadas por serem informações probatórias armazenadas em sistemas informáticos. Atualmente, esse tipo de prova é essencial para o processo penal, sendo indispensável para esclarecer e fundamentar as investigações.

Tendo em vista a dificuldade de obtenção de provas no ambiente digital, ocasionadas pelo uso de medidas anonimizadoras pelos criminosos, surge a necessidade do Estado se valer das mesmas técnicas investigativas, substituindo-se os métodos clássicos de obtenção de provas.

Assim surge o *malware* estatal, um *software* malicioso que é utilizado para acessar e apreender dados, de forma imperceptível ao investigado. Tal método oculto ocasiona uma intrusão indevida na vida dos investigados, e até de terceiros ao seu redor, pois é utilizado sem o seu conhecimento ou consentimento, até mesmo através de monitoramento *online*, com acesso, em tempo real, a informações referentes aos dispositivos. Devido a estas características, o malware, enquanto método oculto, acaba por se tornar uma poderosa ferramenta estatal frente aos indivíduos, com potencial risco de devassas e arbitrariedades no que concerne a seus direitos e garantias constitucionais, especialmente no contexto de um Estado Democrático de Direito. Nesse cenário, ocorre um conflito entre o interesse público de buscar a justiça e a eficiência nas investigações criminais, e o interesse público de proteger os direitos fundamentais relacionados. De um lado, temos a segurança pública, enquanto do outro, estão a privacidade e a liberdade individual.

Nessa senda, para haver a admissibilidade do uso do *malware* numa investigação criminal, é necessário estabelecer os pilares para a sua atuação prática.

Outros ordenamentos, como o espanhol, italiano e alemão, acompanharam mais de perto toda essa transformação tecnológica e editaram leis em sentido formal que preveem o *malware* como método típico de investigação criminal, o regulamentando e estabelecendo seus requisitos e limites. O segundo capítulo desta dissertação traz, justamente, o estudo sobre a normatização do *malware* como método de investigação criminal na legislação espanhola, italiana e alemã, especialmente nesta última, onde se aborda de forma mais aprofundada a

previsão legal e tratamento alemão ao tema em comento, que servirá de parâmetro para, mais adiante, ser proposta uma sugestão de normatização legal nos ordenamentos português e brasileiro, os quais, apenas, utilizam o *malware* como métodos ocultos como meio atípico de investigação.

Por fim, o último capítulo do presente trabalho elabora uma análise acerca das consequências do uso, de forma atípica, dos métodos de investigação ocultos, em nosso caso o *malware*, ou seja, sem uma legislação expressa que o regulamente. Trata sobre a potencial capacidade deste uso gerar invasão e, irretratável devassa, na vida dos indivíduos, ferindo gravemente princípios constitucionais para um devido processo penal, justo e imparcial, bem como agredindo os direitos e garantias fundamentais, como da reserva de lei e de juiz, proporcionalidade e subsidiariedade, os quais estão consagrados na Carta Maior e são base de todo o ordenamento jurídico de um Estado de Direito.

São trazidos à baila também, os direitos fundamentais à privacidade, inviolabilidade do domicílio, autodeterminação informativa e proteção de dados, bem como o direito a não se auto incriminar. Dessa maneira, traz toda uma argumentação fundada em regras, princípios e direitos constitucionais, para defender que não é possível o uso do *malware* como método atípico de investigação criminal, sob pena de se proporcionar um direito processual penal arbitrário e irresponsável. Ademais, justifica a necessidade de uma legislação expressa no ordenamento brasileiro e português sobre o *malware*, regulando todas as suas funcionalidades, uma vez que, após a sua instalação no dispositivo alvo, este método oculto propicia, não apenas um único acesso ao dispositivo, mas também o monitoramento em tempo real das atividades do visado.

Assim, tendo-se em vista a norma alemã, referido trabalho visa trazer à tona a reflexão acerca de um método de investigação que em muito pode ajudar na resolução da criminalidade e dos conflitos sociais, no entanto, caso não utilizado da forma devida, pode se tornar uma arma contra os próprios cidadãos de um Estado Democrático.

I. CIBERCRIME E PROVA DIGITAL: DESAFIOS E POSSIBILIDADES

A inovação em sentido *lato* consubstancia-se no desenvolvimento de novas formas de produzir, aplicar e distribuir o conhecimento, dito de outro modo, o conhecimento não é só fator, como também produto do processo de inovação.[1]

Frisa-se que a inovação pode ocorrer em diversos campos do conhecimento, não por outra razão, chega-se a várias tipologias de inovação, tais como inovação jurídica, inovação econômica, inovação legislativa, e especificadamente a tratada no presente trabalho, a inovação tecnológica. Nesta senda, vislumbra-se que a inovação tecnológica consiste na produção, aplicação e distribuição de novas tecnologias, tendo como efeito precípuo a penetração de tais tecnologias nas diversas atividades praticadas na sociedade, influenciando de modo demasiado os setores econômicos e sociais.[2]

Tal inovação na contemporaneidade não é concebida apenas para atingir uma finalidade específica dentro do contexto social, não possuindo a tecnologia apenas um sentido utilitarista e instrumental, ao contrário, há um perfil dinâmico da tecnologia, a qual tem por escopo o progresso da sociedade como um todo.[3] Nesta senda, a inovação passa a ser então um dos principais mecanismos para o desenvolvimento social, econômico e cultural de uma população, já que essa eleva o patamar dos conhecimentos gerados e utilizados pelos indivíduos, oferecendo um constante estímulo de aprendizagem e mudança.[4]

Não por outra razão, que em âmbito internacional e nacional passa-se a incentivar a elaboração de legislações que tratem a inovação como um fato que é imprescindível de regulação jurídica e de políticas públicas para a sua promoção.[5]

Tem-se que o forte estímulo a inovação atrelado ao seu caráter essencialmente dinâmico, fez emergir a denominada sociedade de informação, a qual conferiu novos contornos as relações sociais.[6]

---

1 MACIEL, Maria Lucia. Ciência, tecnologia e inovação: ideias sobre o papel das ciências sociais no desenvolvimento. In: **Revista Parcerias Estratégicas**, v.10, n° 21, 2005, p. 34.

2 RODOTÀ, Stefano. **A vida na sociedade de vigilância: a privacidade hoje**. Rio de Janeiro: Renovar, 2008, p. 41.

3 DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006, p. 42.

4 WERTHEIN, J. A sociedade da informação e seus desafios. In: **Ciência da Informação**, v. 29, n° 2, 2000, p. 75.

5 KRUGLIANSKAS, Isak; MATIAS-PEREIRA, José. Um enfoque sobre a Lei de Inovação Tecnológica do Brasil. In: **Revista de Administração Pública**, vol. 39, n° 5, 2005, p. 1011-1029.

6 CASTELLS, Manuel. **A Sociedade em rede,** vol. 1. 8ª ed. rev. e ampl. Tradução: Roneide Venâncio Majer. São Paulo: Editora paz e terra, 2005, p. 17.

Nesta nova sociedade, as comunicações interpessoais tornaram-se mais céleres e os indivíduos que a compõe, por meio das novas tecnologias, conseguem armazenar mais dados e informações, de forma a estender a capacidade de memorização. Neste sentido, destaca-se que "as novas tecnologias, baseadas na eletrônica e na informática devem ser, sempre sob um mesmo aspecto, consideradas como extensões materiais da nossa capacidade de memorizar."[7]

É impossível atualmente imaginar nossa sociedade sem a utilização da *internet* e dessas novas tecnologias, que modificaram radicalmente a forma na qual as pessoas se organizam e interagem. Não mais subsistindo a possibilidade de se pensar nas relações interpessoais sem a utilização de aparatos tecnológicos, como por exemplo, *ipad*, *notebook*, *smartphones*, entre outros.[8]

Assim, por sociedade de informação, ou sociedade em rede, entende-se por uma estrutura social baseada e operada por tecnologias de comunicação e de informação, as quais por sua vez, são fundadas na microtecnologia e nas redes digitais de computadores, que geram, processam e distribuem informação do conhecimento acumulado nessas redes.

Tal sociedade estruturada em inovações tecnológicas promoveu alterações em todo o cenário social, modificando significativamente sistemas econômicos, políticos e jurídicos, introduzindo no Direito Penal novos interesses e bens jurídicos merecedores de proteção estatal.

No âmbito do Processo Penal não foi diferente, ao passo que a sociedade de informação trouxe para os criminosos facilidades para o cometimento de crimes, trouxe para os órgãos de persecução criminal novas formas de investigação e produção de prova para combater a dita criminalidade informática ou virtual.

Desta forma, o presente capítulo busca demonstrar as características e nuances desta sociedade, perpassando por conceitos como sociedade de informação, cibercrimes, prova digital, métodos ocultos de investigação e utilização de *malware* nas investigações criminais, tendo por foco principal analisar a questão do monitoramento *online* através de *malware* no âmbito das investigações criminais em ambiente digital.

1. SOCIEDADE DE INFORMAÇÃO E CIBERCRIMES

7 LYOTARD, Jean François. **O Inumano, considerações sobre o tempo**.2ª Ed: Editorial Estampa, 1997, p, 52.

[8] CASTELLS, Manuel. **A Sociedade em rede,** vol. 1. 8ª ed. rev. e ampl. Tradução: Roneide Venâncio Majer. São Paulo: Editora paz e terra, 2005, p. 17-20.

A denominada sociedade de informação decorre, incontestavelmente, do fenômeno da globalização ou processos de globalização, que representa uma modificação de paradigma, no qual questões econômicas, políticas e sociais passam a ser questões de ordem internacional, controladas conjuntamente por diversos Estados. [9] Essa mudança de paradigma também é uma espécie de revolução tecnológica, baseada em tecnologias de informação e comunicação, que remodelam de modo acelerado a base material da sociedade.[10]

Castells enfatiza que o fator principal de caracterização da sociedade de informação não é a centralidade da informação, "mas a aplicação dessa informação para a geração de conhecimentos e de dispositivos de processamento-comunicação da informação, em um ciclo de realimentação cumulativo entre a inovação e seu uso". [11] Por conseguinte, a sociedade informacional, é marcada essencialmente: a. pela velocidade, pois tudo está ocorrendo em um ritmo mais acelerado do que antes; b. pela amplitude e profundidade, já que há uma gama de mudanças radicais ocorrendo simultaneamente; c. pela transformação completa de sistemas inteiros, tais como, jurídicos, sociais e econômicos. [12] Havendo uma prevalência da economia sobre a política, da velocidade sobre a lentidão, do virtual sobre o tangível, além da mercantilização de bens imateriais, a exemplo do conhecimento, que passa a ser fator de produção.[13] Neste ponto, destaca-se que essa sociedade recebe ainda a alcunha de sociedade dos serviços, tendo como fonte basilar do mercado econômico a produção de serviços e de bens imateriais.[14]

Neste sentido, o direito como um todo resta também impactado, como assevera Manuela Lima e Sebastião Costa:

> À luz das aludidas premissas, as implicações da Sociedade do Conhecimento no direito podem ser delineadas sistematicamente da seguinte forma: (a.) os novos parâmetros fáticos para aplicação do direito já posto, exigindo sua readequação; (b.) a existência de fatos que passam a ter relevância jurídica pelo avanço técnico-científico; (c.) a necessidade da tomada de decisão jurídica em um cenário de incerteza

[9] FACCHINI NETO, Eugênio. Reflexões histórico- evolutivas sobre a constitucionalização do direito privado, In: SARLET, Ingo Wolfgang (org). **Constituição, Direitos Fundamentais e Direito Privado**. Porto Alegre: Liv. Do Advogado, 2003, p. 10.
[10] CASTELLS, Manuel. **A sociedade em rede**. Tradução por Roneide Venancio Majer. 8. ed. rev. e ampl. vol. 1. São Paulo: Paz e Terra, 2005, p. 50.
[11] Idem, p. 67.
[12] SCHWAB, Klaus. **A quarta revolução industrial**. Tradução Daniel Moreira Miranda - São Paulo: Edipro, 2016, p. 42.
[13] DE MASI, Domenico. **O futuro chegou.** Tradução Marcelo Costa Sievens. 1. ed. Rio de Janeiro: Casa da Palavra, 2014, p. 541.
[14] RODOTÀ, Stefano. **A vida na sociedade de vigilância**: a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 92.

> e risco, bem como; (d.) a elaboração de normas jurídicas gradativamente vem sendo condicionada para atender os interesses de uma inovação guiada pela economia.[15]

Assim sendo, fica evidente que com o avanço da tecnologia e a consequente evolução da sociedade, novos bens jurídicos surgiram, e com eles a necessidade de serem tutelados. Neste cenário, aponta-se a segurança informática como bem jurídico merecedor de tutela penal nas sociedades modernas.[16]

De acordo com Sydow, o supracitado bem jurídico compreende a confidencialidade dos dados e dos sistemas, a integridade dos dados e dos sistemas, bem como a disponibilidade dos dados e dos sistemas. Sendo a confidencialidade o direito de apenas o titular daquele dado ou sistema ter acesso ao conteúdo daquele dado ou sistema, já a integridade é o direito do titular de não ver aquele dado ou sistema modificado sem a sua anuência (autorização). E por fim, a disponibilidade corresponde ao direito daquele titular de poder acessar livremente aquele dado ou sistema, mesmo que este seja íntegro e sigiloso.[17]

Neste sentido, destaca-se a Convenção de Budapeste sobre Cibercrime de 2001, concebendo que os cibercrimes são infrações contra a confidencialidade, integridade e disponibilidade dos dados e sistemas informáticos, tais como: acesso ilegítimo a dados, interferência em dados e sistemas, entre outros; ou podem ser infrações relacionadas com computadores, como a falsidade informática, a burla informática e afins; ou ser infrações relacionadas com o conteúdo, como o típico exemplo de pornografia infantil; ou ser infrações relacionadas ao direito do autor e conexos.[18]

Observa-se, pois, no âmbito do Direito Penal, esta nova modalidade da prática de delitos, qual seja, os cibercrimes. Tem-se, que são dispostos em gerações, sendo a primeira delas caracterizada pela utilização dos computadores no estágio preparatório do crime, como forma de obter comunicação; informações de cunho preparatório. A segunda geração é marcada pelo cometimento de crimes por meio da rede, mas, que a prática criminosa perdura fora dela. A terceira geração, que consiste nos cibercrimes próprios, são produtos do meio cibernético e tecnológico e somente perpetrados no ciberespaço.[19]

---

[15] LIMA, Manuela Ithamar; DA COSTA, Sebastião Mendes. Direito, inovação e ciência: possibilidades e desafios da sociedade do conhecimento. In: **Revista Jurídica Eletrônica da UFPI**, v. 6, n. 01,2011, p. 173.
[16] SYDOW, Spencer Toth. **Curso de Direito Penal Informático**. Salvador: Editora JusPodivm, 2020, p. 157
[17] Idem, pg. 159-160.
[18] CONSELHO DA EUROPA**. Explanatory Report to the Convention on Cybercrime. 2001**. Disponível em < CETS 210 - Explanatory Report to the Council of Europe Convention on preventing and combating violence against women and domestic violence (coe.int) >. Acesso em: 20/06/2022.
[19] FRANÇA, Leandro Ayres. Cibercriminologias**. In: Criminologias alternativas.** Organizado por Pat Carlen e Leandro Ayres França. Porto Alegre: Canal Ciências Criminais, 2017, p. 231-239.

A bem da verdade é que atualmente quase todos os delitos podem ter a lógica informática permeando sua execução. Assim, faz-se importante diferenciar os crimes informáticos próprios dos impróprios, conforme as lições de Sydow. Nas palavras do autor retromencionado, delitos informáticos impróprios são aqueles em que a tecnologia é usada apenas como ferramenta para a prática delitiva, de modo que a ação criminosa poderia ser perpetrada normalmente sem o apoio dos mecanismos informáticos. Por outro lado, crimes informáticos próprios são aquelas condutas que objetivam atingir dados ou sistemas informáticos, sendo exemplo o delito de invasão ou intrusão de dispositivos informáticos, conduta esta tipificada em diversas ordens jurídicas, por meio das mais diversas nomenclaturas.[20]

Em se tratando de Processo Penal, a Convenção de Budapeste sobre Cibercrime traz diversas medidas para o combate eficaz à criminalidade informática-digital. Dentre elas, destaca-se a interceptação de conteúdos, a busca e apreensão de dados informáticos, medidas de injunção para divulgação de dados que estejam na posse de um fornecedor de serviço em rede, por exemplo. Além de medidas com regras de cooperação internacional para persecução criminal envolvendo cibercrimes.[21]

Exemplifica-se, ainda, o avanço tecnológico e o recurso as novas tecnologias em matéria de investigação criminal, através das lições abaixo:

> Basta imaginar o caso do polícia que se depara com a constatação de que um criminoso utilizou seu computador para cometer vários crimes. Numa investigação de homicídio poderá encontrar-se informação importante num computador portátil onde constam vários e-mails ou um plano para arquitetar o rapto de uma pessoa que, efetivamente, viria a ser assassinada. Talvez, ainda, o nosso detective se encontre a investigar um abuso de confiança fiscal e necessite aceder aos registros informáticos que o investigado guarda no seu computador. Também numa investigação por tráfico de droga se afigura necessário analisar o computador do chefe da "gang" para, desse jeito, conseguir uma maior operatividade do combate a tal crime. Em todos estes casos, verifica-se que a informação probatória imprescindível se encontra armazenada ou contida em sistemas ou redes informáticos ou em equipamentos eletrônico-digitais de armazenamento. [22]

[20] SYDOW, Spencer Toth. **Delitos informáticos próprios**: uma abordagem sob a perspectiva vitimológica, 2009. Dissertação de Mestrado. Faculdade de Direito do Largo São Francisco: Universidade de São Paulo, p. 75.
[21] CONSELHO DA EUROPA**. Explanatory Report to the Convention on Cybercrime. 2001**. Disponível em < CETS 210 - Explanatory Report to the Council of Europe Convention on preventing and combating violence against women and domestic violence (coe.int) >. Acesso em: 20/06/2022.
[22] RODRIGUES, Benjamim Silva, **Da Prova Penal**, Tomo IV – Da Prova - Electrónico - Digital e da Criminalidade Informático-Digital (Contributo Para a Fundamentação de um Modelo Dinâmico-Reversivo de Ciência Forense Digital em sede de Investigação da Cyber-Criminalidade Informático-Digital e à Luz do Novíssimo Regime da Lei do Cibercrime Portuguesa), 1°. Edição, Rei dos Livros, 2011, p. 29.

Diante disso, tem-se que a maior dificuldade presente entre o trinômio, Sociedade de Informação, Processo Penal e Tecnologia, é adequar as normas processuais penais aos novos contornos tecnológicos oriundos da Sociedade da informação, a fim de que cibercrimes possam ser eficazmente combatidos e a prova digital devidamente colhida com a máxima eficiência.

2. PROVA DIGITAL E SUA AMEAÇA AO PROCESSO PENAL DEMOCRÁTICO.

A prova digital, ou na nomenclatura norte-americana, evidência digital, foi definida pelo *Standard Working Group on Digital Evidência* (SWGDE) como qualquer informação de valor probatório que é armazenada ou transmitida em formato digital. Outra definição proposta pela *International Organization of Computer Evidência* (IOCE) é a prova digital sendo a informação armazenada ou transmitida em forma binária que pode ser invocada em tribunal.Mas, em geral, prova digital, para fins de Direito Penal, pode ser aquela definida como quaisquer dados armazenados ou transmitidos usando um computador que apoiam ou refutam uma teoria de como ocorreu um crime ou que abordam elementos críticos do crime, como intenção ou álibi.[23]

Tem-se que, é bem verdade, que conceituar e caracterizar prova digital é algo complexo, tendo em vista que, uma prova não é relevante ou irrelevante em si mesma, devendo guardar relação com os fatos, por isso, a conceituação e caracterização de prova é algo dinâmico, pois, depende das circunstâncias concretas de cada caso, para a partir disso definir seus efeitos processuais e concluir se é admissível ou não.[24]

Há, portanto, diversas conceituações sobre prova digital, mas o presente trabalho se alinha a algumas proposições, quais sejam. A primeira delas é que prova digital não é sinônimo de prova eletrônica, sendo essa última, gênero da que prova digital é espécie. Explica-se. Prova eletrônica é qualquer informação de valor probatório produzida ou processada por meios eletrônicos, englobando a prova digital ou aquelas em formato analógico, como, por exemplo, documentos digitalizáveis.[25] A prova digital, por sua vez, é mais amplamente vinculada a

---

[23] CASEY, Eoghan. **Digital evidence and computer crime: forensic Science, computers and the internet**. Third Edition. Waltham: Elsevier, 2011, p. 07.
[24] VÁZQUEZ-ROJAS, Carmen. Sobre la cientificidad de la prueba científica en el proceso judicial. **Anuario de psicología jurídica**, v. 24, n. 1, p. 65-73, 2014.
[25] DELGADO MARTIN, Joaquin. **La prueba electronica en el proceso penal.** Diario La Ley, Nº 8167, Sección Doctrina, 10 Oct. 2013, Año XXXIV, Editorial La Ley. p, 1.

informática, embora associada também a tecnologia, não por outra razão, há quem prefira denominar provas eletrônico- digitais.[26]

A segunda proposição é que a definição de prova digital perpassa por saber identificar suas características, quais sejam a imaterialidade, volatilidade e fragilidade. A imaterialidade consiste no fato de que para a prova digital se tornar perceptível é imprescindível um suporte tecnológico.[27] A volatilidade baseia-se na facilidade de desaparecimento da prova digital, o que está intimamente relacionada à sua fragilidade, pois, há uma probabilidade alta de contaminação e desvirtuamento dos dados que se busca coletar.[28]

No tocante a aquisição da prova digital, essa pode ser por meio da investigação *offline*, ou seja, apreensão do equipamento eletrônico, ou por meio da investigação por meio da busca remota[29], o certo é que a despeito de como serão coletadas, "somente servirão de *fontes de prova digital* quando houver a possibilidade de, a partir da aquisição por acesso remoto, se comprovar a confiabilidade e integralidade da prova."[30]

Ademais, note-se que para a coleta da fonte de prova digital é imprescindível que o investigador tenha conhecimentos específicos em Ciência Forense Digital, tendo por certo, que é importante conhecimentos técnicos e conhecimentos acerca dos objetivos da investigação.[31]

A grande problemática da prova digital, se não observado o procedimento correto, é a sua aptidão para violar direitos fundamentais como da privacidade, intimidade e proteção de dados, bem como, ir contra a garantia processual penal da cadeia de custódia da prova. Isso porque há uma certa confiança infundada em sistema informáticos, de modo que a denominada busca da verdade por meio da prova digital, subtrai as possibilidades de se questionar ou refutar uma dita verdade, tendo em vista a evidência científica gerada pela prova digital.[32]

Observa-se, pois, que os próprios métodos ocultos de investigação, devem eles mesmos serem questionados e não se depositar uma confiança cega nas provas obtidas por eles

---

[26] RAMALHO, David Silva. **Métodos ocultos de investigação criminal em ambiente digital.** Coimbra: Almedina, 2017. p, 101.
[27] Idem, p. 104.
[28] Idem, p. 104.
[29] DELGADO MARTIN, Joaquin. **La prueba electronica en el proceso penal.** Diario La Ley, Nº 8167, Sección Doctrina, 10 Oct. 2013, Año XXXIV, Editorial La Ley, p, 3.
[30] MENDES, Carlos Hélder. **Malware do estado e processo penal: a proteção de dados informáticos face à infiltração por software na investigação criminal**. 2018. Dissertação de Mestrado. Pontifícia Universidade Católica do Rio Grande do Sul, p. 109.
[31] RAMALHO, David Silva. **Métodos ocultos de investigação criminal em ambiente digital.** Coimbra: Editora Almedina, 2017. p, 103.
[32] PRADO, Geraldo. **Prova penal e sistema de controles epistêmicos.** 1 ed. São Paulo: Marcial Pons, 2014, p. 73.

através de suporte tecnológico, visto que, bastaria um descuido por parte de quem manuseia os aparatos tecnológicos, para se contaminar toda uma prova.[33]

> As técnicas de captação de som, imagem e até de captura de outros elementos originalmente produzidos em meio digital não estão imunes à corrupção em termos metodológicos. Muito menos há isenção de risco de manipulação do produto obtido por meios dos métodos ocultos de investigação.[34]

Sobre a temática, a doutrina considera que a contaminação da prova digital pode se dar por duas maneiras distintas, a primeiro seria pelo contato físico inapropriado ao suporte informático e a segunda por meio do contágio digital, ou seja, uma alteração no conteúdo da prova digital, tais como a alteração dos dados informáticos, sendo por isso tão importante a observância da denominada cadeia de custódia da prova.[35]

O instituto da cadeia de custódia busca garantir o devido processo penal, com a observância de direitos e garantias fundamentais, como a ampla defesa, o contraditório e a licitude da prova. Nesta senda, "A cadeia de custódia abarca todo o caminho que deve ser percorrido pela prova até sua exata análise e escorreita inserção no processo, sendo que qualquer interferência durante o trâmite processual pode resultar na sua imprestabilidade".[36]

Assim sendo, a cadeia de custódia é uma sucessão de eventos interligados, que protege a integridade da fonte probatória e da própria prova até o finalizar do caso e julgamento do mérito processual.[37] Desse modo, para garantir a fiabilidade da prova digital é necessário que durante a curetagem do vestígio, se tenha o devido cuidado na sua coleta, manipulação e transporte. A inobservância pode repercutir diretamente no direito constitucional, no devido processo legal e em todos os meios e recursos associados a ele, como a garantia de ampla defesa, contraditório e igualdade de armas. Esses direitos têm como objetivo propiciar ao acusado as condições necessárias para se defender dos abusos das autoridades estatais.[38]

Nesse sentido, como dito, a cadeia de custódia consiste numa espécie de documentação dos vestígios resultantes dos crimes, havendo uma patente associação com o instituto das provas, já que é com a cadeia de custódia que se verá os fatos como realmente

---

[33] Idem, p. 74.
[34] Idem, p. 74.
[35]MARSHALL, Angus. **Digital forensics: digital evidence in Criminal Investigation.** Wiley-Blackwell. 2008. p, 41.
[36] DE MENEZES, Isabela Aparecida; BORRI, Luiz Antonio; SOARES, Rafael Junior. A quebra da cadeia de custódia da prova e seus desdobramentos no processo penal brasileiro. In: **Revista brasileira de direito processual penal**, v. 4, n. 1, 2018, p. 281.
[37] Idem, p. 281-282
[38] Idem, p. 284.

foram ou são, em uma natureza cronológica. Este caminho, portanto, deve ser todo percorrido por meio legal, sob pena de qualquer interferência interna ou externa, resultar na ilicitude e/ou desuso da prova que foi obtida de maneira dissonante.

Ocorre que os elementos de prova digital são transmitidos e manuseados em linguagem não natural, mas digital e, assim, ainda que os dados digitais possam ser diretamente percebidos por quem está em contato com eles, eles não possuem materialidade, o que dificulta a conservação da cadeia de custódia. Por essa razão, *National Institute for Standard and Technology* (NIST) distingue quatro fases para a coleta de prova digital:[39]

> Durante a coleta, os dados relacionados a um evento específico são identificados, rotulados, registrados e coletados, e sua integridade é preservada. Na segunda fase, de exame, ferramentas e técnicas forenses adequadas aos tipos de dados que foram coletados são executados para identificar e extrair as informações relevantes dos dados coletados, protegendo sua integridade. O exame pode usar uma combinação de ferramentas automatizadas e processos manuais. A próxima fase, a análise, envolve a análise dos resultados do exame para obter informações úteis que abordem as questões que foram o ímpeto para a realização da coleta e do exame. A fase final envolve relatar os resultados da análise, que podem incluir a descrição das ações executadas e recomendar melhorias para políticas, diretrizes, procedimentos, ferramentas e outros aspectos do processo forense.[40]

Nesse cenário, para que a prova digital possa ser utilizável no processo judicial é necessário:

> (i) individualizar o suporte informático que contém o dado digital útil à investigação; (ii) obter o dado digital através de técnica de interceptação, no caso de fluxo de comunicação, ou mediante o sequestro e cópia ou espelhamento do suporte em que está registrado o arquivo de dados; (iii) conservar os dados digitais obtidos e copiados em local seguro e adequado; (iv) realizar a análise dos dados obtidos – examinando exclusivamente a cópia do suporte informático – que sejam relevantes para o objeto da investigação; (v) mediante a produção de prova pericial e eventuais esclarecimentos verbais dos peritos em audiência.[41]

Por conseguinte, nota-se que o fato de a prova digital ser pautada na cientificidade, não garante a confiabilidade do conhecimento apresentado como tal, pois uma coisa é identificar as ciências e outra é o grau de confiabilidade e validade das afirmações científicas. Por essa razão, com vistas a garantia de um processo penal democrático e pautado nos direitos e garantias fundamentais, é necessário adotar *standards* de utilização dessa prova digital.

---

[39] BADARÓ, Gustavo Henrique. Os standards metodológicos de produção na prova digital e a importância da cadeia de custódia. In: **Boletim IBCCRIM**, ano, v. 29, p. 7-9, 2021.
[40] Idem.
[41] VACIAGO, Giuseppe. **Digital Evidence**. I mezzi di ricerca della prova digitale nel procedimento penale e le garanzie dell'indagato. Torino: Giappichelli, 2012.

3. OS MÉTODOS OCULTOS DE INVESTIGAÇÃO.

Nas sociedades contemporâneas, marcadas pela clara tendência de supressão de direitos, constantemente a tortura e atos que violam direitos fundamentais são normalizados em nome do combate ao crime, sendo o Direito Penal utilizado pelas autoridades como instrumento para perseguir e punir os indivíduos considerados inimigos públicos do Estado.[42] Nestas sociedades, como ensina Ferrajoli, caracterizadas pela adoção do sistema estatal-disciplinar, tem-se cada vez mais uma redução das liberdades individuais para fins preventivos, com o Estado se utilizando de aparatos tecnológicos, como, por exemplo, de câmeras de vigilância, para exercer o controle da população.[43]

Diante desse cenário de combate ao crime, em particular o crime organizado e o terrorismo, é que se coloca o tema dos métodos ocultos de investigação, que surgiu no direito norte-americano e representa não só o avanço tecnológico das medidas de persecução penal, mas também uma ideia de "*war on terrorismo*".[44]

A crescente necessidade na utilização dos métodos ocultos de investigação deu-se em razão do progresso tecnológico e como forma de resposta ao aumento da criminalidade econômico-financeira e das ameaças terroristas, que exigiram dos órgãos de polícia criminal uma resposta mais combativa, a fim de garantir efetividade às investigações.[45]

Conforme aduz Andrade:

> de um lado, a progressão – expressa na emergência e triunfo de novos direitos fundamentais ou de novas dimensões dos direitos preexistentes – é espontânea, contínua e automática, apenas dependendo da consciência jurídica, ás mãos da doutrina e da jurisprudência (constitucionais). Diferentemente, do outro lado, o caminho – sc. a consagração de novos meios de obtenção de provas resultantes do aproveitamento das possibilidades de intervenção e intromissão oferecidas pelas realizações técnico-científicas – faz-se de forma descontinua e derivada, ao ritmo das sucessivas e localizadas intervenções do legislador.[46]

---

[42] DI GIORGI, Alessandro; PRADO, Geraldo. Mesa 3: O processo penal das formações sociais do capitalismo pós-industrial e globalizado e o retorno à prevalência da confissão – da subsistiência da tortura aos novos meios invasivos de busca de prova e à pena negociad**a.** *In:* KARAM, Maria Lúcia (Org.). **Globalização, sistema penal e ameaças ao Estado Democrático de Direito.** Rio de Janeiro: Editora Lumen Juris. 2005. p, 135 – 152.

[43] FERRAJOLI, Luigi. **Derecho y Razon: teoría del garantismo penal.** Madrid: Editorial Trotta, 1995. p, 338 389.

[44] ANDRADE, Manuel da Costa. "**Bruscamente no verão passado", a reforma do Código de Processo Penal.** Coimbra**:** Coimbra Editora, 2009. p, 105.

[45] CAIRES, João Gouveia de. "Métodos ocultos de criminalidade econômico-financeira: entre a (a)tipicidade e a cumulação. In: **Revista Julgar**, n° 38, (maio/agosto), 2019, p.50-52.

[46] ANDRADE, Manuel da Costa. "**Bruscamente no verão passado", a reforma do Código de Processo Penal.** Coimbra**:** Coimbra Editora, 2009. p, 148.

A "legitimação material e formal-procedimental"[47] destas metodologias investigativas pode ser observada através de diversas ordens jurídicas, que há bastante tempo estipulam em suas legislações e utilizam das supracitadas técnicas ocultas em suas investigações, como exemplo, cita-se as conhecidas medidas de interceptações telefônicas e a figura do agente encoberto.

Ocorre que apesar de estarem previstos expressamente em vários diplomas legais de vários países, os métodos ocultos de investigação carecem de uma teoria geral e centralidade normativa nas ordens jurídicas de Brasil e Portugal. Em Portugal, a título exemplificativo, menciona-se que as escutas telefônicas estão previstas no Código de Processo Penal, enquanto a figura do agente encoberto está disciplinada em legislação extravagante, havendo ainda a Lei n° 109/2009 - Lei do Cibercrime – que regula alguns métodos ocultos manuseados em ambiente digital. O que demonstra a falta de "unidade sistêmica" das normas sobre métodos ocultos de investigação, sendo verdadeiras "ilhas processuais" as legislações portuguesas que tratam da referida temática, conforme adverte Ramalho.[48]

Em contraposição aos métodos tradicionais de obtenção de prova, que são executados de forma transparente – às claras - com a ciência do suspeito (arguido), os métodos ocultos de investigação são caracterizados pelo seu caráter oculto e dissimulado. Nas palavras de Andrade, os métodos ocultos de investigação "representam uma intromissão nos processos de ação, interação e comunicação das pessoas concretamente visadas, sem que estas tenham conhecimento do fato nem dele se apercebam."[49]

Ainda, segundo o autor retromencionado, "De forma simplificada e reducionista, os meios ocultos de investigação levam as pessoas atingidas – normalmente o suspeito – a 'ditar', inconscientemente, para o processo, 'confissões' não esclarecidas nem livres."[50] Isso porque a pessoa investigada não tem a noção da realização da ação e dá continuidade às suas atividades diárias, sem qualquer desconfiança da realização de uma investigação criminal contra si.

---

[47] ANDRADE, Manuel da Costa. Métodos Ocultos de Investigação (*plädoyer* para uma teoria geral). In: **Que futuro para o direito processual penal? Simpósio em homenagem a Jorge de Figueiredo Dias, por ocasião dos 20 anos do Código de Processo Penal Português**. Coimbra: Coimbra Editora, 2009, p. 532.
[48] RAMALHO, David Silva. **Métodos ocultos de investigação criminal em ambiente digital.** Coimbra: Editora Almedina, 2017, p. 211-212.
[49] ANDRADE, Manuel da Costa. "**Bruscamente no verão passado", a reforma do Código de Processo Penal.** Coimbra Editora, 2009. p, 105.
[50] Idem, p. 106.

Valente, por sua vez, entende que a clandestinidade dos métodos ocultos de investigação traz um cerceamento na liberdade de pensamento, decisão e ação do investigado.[51] Segundo Costa, o investigado sem saber da existência de técnica investigativa contra si "age espontaneamente, 'inocentemente', entregando informações e provas aos investigadores ou praticando atos ilícitos ou tendencialmente ilícitos, comportamentos esses que não assumiria se tivesse conhecimento do engano."[52]

Assim sendo, percebe-se que o secretismo inerente ao uso de tais técnicas, ocasiona implicações no plano processual penal, especificadamente no direito a recusar testemunho, bem como no direito ao silêncio (*nemo tenetur se ipsum acusare*).[53] Pois as pessoas investigadas e as que com elas interagem se expõe e prestam declarações auto incriminatórias que não prestariam se soubessem que estavam sendo observadas.

Acerca do princípio do *nemo tenetur*, Giacomolli afirma que este possui guarida em diversas Constituições e Convenções Internacionais e abarca, desde o direito a ficar em silêncio ao direito de não colaborar com as investigações ou produzir elementos de prova contra si mesmo, de modo a conservar o "estado de inocência" do investigado, bem como sua "expectativa de privacidade".[54] Assim, em última instância, o uso de técnicas ocultas investigativas viola, também, o princípio da presunção de inocência.

Nesse caminhar, destaca-se que as metodologias investigativas ocultas conferem um maior valor a fase preliminar (de investigação) em detrimento daquilo que é produzido em juízo, sob o crivo da ampla defesa e do contraditório. Nesse sentido, Campos afirma que a utilização dos métodos ocultos "reflete num 'desarmar' da função do juiz em prol do MP e dos OPC.[55] Andrade, por sua vez, assevera:

> o centro de gravidade das decisões tende a deslocar-se do julgamento (público) para os resultados das investigações ocultas. Se o julgamento tende a transformar-se num ritual externo, a figura e a função do juiz ficam cada vez mais desarmadas e debilitadas em benefício do Ministério Público e, sobretudo, da polícia. Enquanto isso, também

[51] VALENTE, Manuel M. Guedes. **Os meios ocultos de investigação.** 21º Seminário Internacional de Ciências Criminais. São Paulo: IBCCRIM, 2015. p, 28.
[52] COSTA, Eduardo Maia, Acções Encobertas (Alguns Problemas, Algumas Sugestões). In: **Estudos em Memória do Conselheiro Artur Maurício**, Coimbra Editora, 2014, p. 357.
[53] ANDRADE, Manuel da Costa. "**Bruscamente no verão passado", a reforma do Código de Processo Penal.** Coimbra Editora, 2009. p, 106.
[54] GIACOMOLLI, Nereu. **O Devido Processo Penal: Abordagem conforme a Constituição Federal e o Pacto de São José da Costa Rica.** 2ª ed. rev. e ampl. São Paulo: Atlas, 2015. p, 207-211.
[55] CAMPOS, Juliana Filipa Sousa. **O malware como meio de obtenção de prova em processo penal: a investigação oculta em ambiente digital – (monografias).** Coimbra: Almedina, 2021, p. 50.

> o arguido vê minado o seu estatuto de sujeito processual, aproximando-se progressivamente de um mero objeto do processo.[56]

Indo mais além, Andrade também destaca que a ausência de conhecimento acerca da medida faz com que o investigado perca sua capacidade de reação, impossibilitando-o de, eventualmente, se voltar contra possível ilegalidade e exercer o contraditório em face do método oculto utilizado.[57]

Os métodos ocultos de investigação criminal também levantam questões jurídicas significativas no plano material, tendo em vista os direitos fundamentais e bens jurídicos dos indivíduos que são alvo de investigações e das pessoas com que esses indivíduos interagem. Algumas das grandes questões desses métodos concentram-se na inviolabilidade de domicílio, das telecomunicações e da correspondência, no direito à imagem, direito ao silêncio, sendo todos esses direitos fundamentais inerentes ao investigado (arguido).[58]

Há uma linha tênue entre o uso dos métodos ocultos de investigação criminal e o cerceamento da liberdade individual, linha essa que deve ser observada com muita cautela. Além dos direitos fundamentais estarem garantidos constitucionalmente, é necessário existir respeito ao princípio da proporcionalidade e da proibição do excesso, pois não é permitido que o âmbito de aplicação de um método oculto de investigação extrapole para além daquele campo em que foi, inicialmente, considerado necessário.[59] Por isso, é crucial que os métodos ocultos de investigação sejam devidamente estabelecido por lei que os regulamente com a máximo de rigor possível, especificando como e em que hipóteses os direitos fundamentais do investigado podem ser flexibilizados em favor dos interesses da justiça. Deve-se sempre ter a comprovação de que a medida mais gravosa é necessária e proporcional ao caso concreto.[60]

Consoante Figueiredo Dias:

> Tanto o legislador, como o aplicador do processo penal têm de ter clara consciência de que, sempre que se alargue ou estreite a consistência de um direito fundamental processualmente relevante, estar-se-á inversamente a estreitar ou alargar a consistência de direitos fundamentais conflitantes, seja de direitos do próprio Estado, de instituições, de corporações ou das vítimas reais e potenciais, que atuam no

[56] ANDRADE, Manuel da Costa. **"Bruscamente no Verão Passado**", a reforma do Código de Processo Penal. Observações críticas sobre uma Lei que podia ter sido diferente, Coimbra: Coimbra Editora, 2009, p.107.
[57] Idem.
[58] RIBOLI, Eduardo Bolsoni. Eu sei o que vocês fizeram no verão passado: o uso de software de espionagem como meio de obtenção de prova penal. In: **Revista Brasileira de Ciências Criminais**, São Paulo, v. 27, n. 156, jun. 2019, p. 94.
[59] Idem, p. 94.
[60] MENDES, Paulo de Sousa. O processo penal entre a eficácia e as garantias. In: PALMA, Maria Fernanda; DIAS, Augusto Silva; MENDES, Paulo de Sousa; ALMEIDA, Carlota (Coords.). **Direito da Investigação Criminal e da Prova**. Coimbra: Almedina, 2014, p. 77.

> processo penal ou sofrem, direta ou indiretamente, as suas consequências. Por isso, a correta solução de um questionado problema processual penal tem como suposto decisivo que o aplicador leve previamente a cabo uma operação de ponderação das valorações conflituantes, para se decidir em princípio em favor de valoração que deva reputar-se preferível, por dominante.[61]

Neste enquadramento, é imprescindível que em face de uma iminente violação de direito fundamental, por conta do emprego de método oculto de investigação, haja o uso da ponderação e proporcionalidade, além da demonstração da acentuada necessidade de uso do meio em questão. É essencial que outros recursos tenham se esgotado para que este seja usado.

As técnicas investigativas para obtenção de provas penais não podem exceder, sem parâmetros legais, a esfera das liberdades individuais, pois isso pode levar à normalização da violação aos direitos fundamentais. Conforme Di Giorgi, se for autorizada uma repressão penal indiscriminada, pode-se ir chegar a um estado de guerra, no qual através da representação de um inimigo público, normaliza-se atos restritivos e violentos, a exemplo da tortura, destoando-se, desse modo, dos princípios democráticos. Fazendo uma comparação entre uma guerra bélica e o inimigo que se combate na criminalidade comum, o retromencionado autor ressalta a importância de conservar e respeitar os preceitos fundamentais.[62] Por isso importa a não violação de valores fundamentais, para que não haja a desvirtuação do objetivo principal do uso dos meios ocultos de investigação.

A perda do objeto em face de uma tentativa de combate à criminalidade pelo uso de métodos invasivos, e até arbitrários, os quais violam direitos fundamentais, incontestavelmente, pelo exercício do poder, é criticada. Giacomolli expõe que a aplicação de qualquer método investigativo deve possuir conexão com a Constituição, mas afirma também que existem novas práticas investigatórias, as quais não possuem elo com o aparato constitucional. Esse desapreço aos direitos fundamentais, segundo o autor, promove, ainda mais, a violência e não produz proveito eficaz à investigação, ocasionando na perda do objetivo acima mencionado.[63]

Por isso, Silva afirma que mesmo no pior dos confrontos face a criminalidade, o Estado Democrático de Direito não pode ser colocado em dúvida, devendo ser observado o

---

[61] DIAS, Jorge de Figueiredo**.** Revisitação de algumas ideias-mestras da teoria das proibições de prova em processo penal (Também à luz da jurisprudência constitucional portuguesa). In: **Revista de Legislação e de Jurisprudência**, Coimbra, A. 146, n. 4000, p. 3-16, 2016, p. 9.

[62] DI GIORGI, Alessandro; PRADO, Geraldo. Mesa 3: O processo penal das formações sociais do capitalismo pós-industrial e globalizado e o retorno à prevalência da confissão – da subsistiência da tortura aos novos meios invasivos de busca de prova e à pena negociada**.** *In:* KARAM, Maria Lúcia (Org.). **Globalização, sistema penal e ameaças ao Estado Democrático de Direito.** Rio de Janeiro: Editora Lumen Juris. 2005. p, 135 – 152.

[63] GIACOMOLLI, Nereu José. **A fase preliminar do processo penal: crises, misérias e novas metodologias investigatórias**. Editora Lumen Juris, 2011, p. 15.

apreço aos princípios e valores constitucionais e individuais. A violação dos direitos mínimos e individuais acarreta numa autoincriminação involuntária compulsória pelo Estado, a qual faz referência a períodos de repressão. O Estado Democrático de Direito não pode ser colocado em questão a fim de que se resolva a todo custo uma situação penal.[64]

O que ocorre, agora, é um comportamento ativo estatal com o intuito investigativo, não sendo mais uma instituição que espera que o investigado oferte informações, mas sim adiantando tal processo. Essa inversão de papéis, reverbera numa invasão da privacidade e da violação à autodeterminação informativa, conforme Andrade.[65]

Outrossim, os meios ocultos deturpam totalmente o funcionamento processual penal e o seguimento ao devido processo legal. No meio digital, conforme assevera Valente, tais métodos se mostram, ainda mais, lesivos e com alto potencial de ocasionar danos aos direitos, liberdades e garantias fundamentais.[66] Esse potencial dano de lesionar direitos fundamentais, como a privacidade, advindo das novas ferramentas tecnológicas, também é criticado por Chirino Sanchez, que em suas lições destaca a atual facilidade das investigações criminais em aceder aos dados pessoais dos investigados, minorando as garantias processuais. Segundo ele, o uso de tecnologias cada vez mais sofisticadas, com o interesse de buscar a verdade a qualquer preço, ocasiona uma crise no processo penal e gera um debate sobre a função do Estado de Direito nas sociedades atuais.[67]

A busca da verdade material a qualquer preço, resgata sistemas políticos autoritários e estruturas inquisitórias, em que se admite a tortura para obtenção de confissões auto incriminatórias. A violação de garantias processuais e direitos fundamentais é a marca desses sistemas pautados pela racionalidade eficientista, os quais desprezam a condição de sujeito processual do investigado.[68] Assim, a verdade a ser alcançada no processo penal é a aquela objetiva, obtida respeitando-se as formalidades legais e o devido processo legal.[69]

---

[64] SILVA, Germano Marques da. **Meios processuais expeditos no combate ao crime organizado (a democracia em perigo?).** Lisboa: Lusíada. Direito, nº 3. 2005, p, 73.

[65] ANDRADE, Manuel da Costa. Métodos Ocultos de Investigação (plädoyer para uma teoria geral). In*:* **Que futuro para o direito processual penal? Simpósio em homenagem a Jorge de Figueiredo Dias, por ocasião dos 20 anos do Código de Processo Penal Português**, (coord. Mário Ferreira Monte entre outros), Coimbra: Coimbra Editora, 2009, p. 536-538.

[66] VALENTE, Manuel Monteiro Guedes. O Reforço dos Princípios Constitucionais na Obtenção de Prova no Mundo Digital. Corpus Delicti — **Revista de Direito de Polícia Judiciária**, Brasília, v. 2, n. 3, p. 11-25, 2018, p. 15.

[67] CHIRINO SANCHEZ, Alfredo. Las tecnologias de la informacion y el processo penal: análisis de uns crisisanunciada.**Revista de ciências penales de Costa Rica.** Rep. Fed. de Alemania 6 (1982): 275. p, 46.

[68] LOPES JR., Aury. O problema da "verdade" no processo penal**.** *In:* GRINOVER, Ada Pellegrini, *et all.* **Verdade e prova no processo penal: Estudos em homenagem ao professor Michele Taruffo**. 1 ed. Brasília, DF: Gazeta Jurídica,2016. p, 67- 68.

[69] HASSEMER, Winfried. **Fundamentos del derecho penal**, trad. de Arroyo Zapatero y Muñoz Conde, Barcelona: Bosch, 1984, p. 190.

Por essas razões, faz-se necessário entender os limites dos meios ocultos investigativos, a fim de que não se perca o objetivo, como já mencionado, e para que não haja uma desumanização dentro de casos criminais. Pois não vale a pena cercear direitos e princípios constitucionais, com o intuito de solucionar situações que, também, violam o ordenamento jurídico.

4. AS MEDIDAS ANTIFORENSES E O RECURSO AO *MALWARE*

Nos últimos anos, tem-se testemunhado uma progressão significativa de ferramentas tecnológicas, o que tem causado impacto substancial na rotina e no comportamento, tanto da população em geral como das estruturas jurídicas, como evidenciado no tópico anterior, quando tratou-se dos métodos ocultos de investigação criminal.

O certo é que essa transformação impulsionada por dispositivos como celulares, computadores, *tablets*, *ipads* e programas digitais tem a capacidade de auxiliar nossa perspectiva de mundo, além de facilitar nossas tarefas diárias. Se mostra impossível, atualmente, associar a prática de qualquer ato, sem haver o auxílio de novas tecnologias, sem a participação de artifícios virtuais, de modo que, somente se percebe o grau de avanço tecnológico, assim como a submissão existente, na ausência dos meios e da ação em si, ainda que temporária.[70]

A sociedade moderna ou informatizada é marcada pelo grande número de tarefas que são realizadas *online*, sejam elas no âmbito profissional ou pessoal, bem como pela conectividade entre as pessoas e pela quantidade de informações que ficam armazenadas na rede.[71] Nesse sentido, destaca-se que a revolução ocasionada pelo uso da *internet* trouxe significativas mudanças nas formas como as pessoas se comunicam, tendo sido os postais substituídos pelo uso de *e-mails* e pela comunicação em tempo real, através do uso de aplicações de mensagens instantâneas, por exemplo.[72]

O desenvolvimento do corpo social também causou implicações no Direito Penal, uma vez que com o avanço tecnológico, novas modalidades delitivas surgiram e os crimes

[70] MENDES, Carlos Hélder. **Malware do estado e processo penal: a proteção de dados informáticos face à infiltração por software na investigação criminal**. 2018. Dissertação de Mestrado. Pontifícia Universidade Católica do Rio Grande do Sul, p. 15-16.
[71] RAMOS MÉNDEZ, Franciso. **Enjuiciamento Criminal: Duodécima lectura constitucional**. Barcelona: Atelier Libros Jurídicos, 2018. p.272.
[72] ORTIZ PRADILLO, Juan Carlos. "Hacking" legal al servicio de la investigación criminal: nuevos instrumentos para la investigación y prueba de la delincuencia informática**.** In: Castrillo, Eduardo de Urbano. **Delincuencia informática: tiempos de cautela y amparo.** Editora Aranzadi, 2012. p, 178.

tradicionais, por sua vez, passaram a ser cometidos com o apoio de aparatos tecnológicos, havendo uma modernização do *modus operandi* dos crimes já existentes, dificultando, assim, as ações de combate do aparelho estatal.[73]

Se por um lado as novas tecnologias possibilitaram aos criminosos "informatizar" as práticas delitivas, transportando os crimes para o ambiente digital, por outro, permitiu a estes mesmos criminosos utilizarem de certas técnicas ou medidas para ocultar a prática das condutas delitivas cometidas na *internet*.

Neste panorama é que se introduz o tema das medidas antiforenses, que são instrumentos ou programas informáticos utilizados pelos agentes da prática de crimes em ambiente digital, com a finalidade de ocultar os "rastros digitais" da prática delitiva, evitando que os investigadores tenham acesso a dados informáticos com valor probatório.[74] Em contraposição a Ciência Forense Digital, que tem por escopo garantir a confiabilidade da prova digital, as medidas antiforenses visam colocar em dúvida a fidedignidade da referida prova.[75] Partindo deste panorama, Harris conceitua as medidas antiforenses como sendo técnicas adotadas pelos agentes da prática de crimes, para tornar inútil ou indisponível a prova a ser utilizada perante um tribunal.[76] No mesmo sentido, Campos aduz que as medidas antiforenses "comprometem a disponibilidade da prova digital (dados informáticos), uma vez que tendem a esconder a sua existência, mas também afetam a sua utilização em tribunal, pois podem destruir ou colocar em causa a sua integridade."[77]

Nessa esteira, aponta-se que há uma multiplicidade de medidas que podem ser adotadas para obstruir a investigação criminal em ambiente digital. Sendo as mais comuns, aquelas que viabilizam a comunicação de forma anônima, o uso de *e-mails* falsos e a encriptação de dados.[78]

Assim, como não existe unanimidade acerca do conceito e de quais seriam todas as medidas antiforenses atualmente existentes, serão realizados, apenas, breves apontamentos

---

[73] Idem, p. 179.
[74] RAMALHO, David Silva. **Métodos ocultos de investigação criminal em ambiente digital.** Editora Almedina, 2017, p. 152.
[75] CRIADO POVEDA, Miguel Ángel. **Delitos em la red: cibercrimen, ciberdelitos, ciberseguidad, ciberespionage y ciberterrorismo**. Madrid: Fragua, 2015, p.147.
[76] HARRIS, Ryan. **Arriving at an anti-forensics consensus: Examining how to define and control the antiforensic sproblem, Digital Investigation - The international Journal of Digital Forensics & Incident** Response, Vol. 03 – Suplemento, 2006, p. 45.
[77] CAMPOS, Juliana Filipa Sousa. **O malware como meio de obtenção de prova em processo penal: a investigação oculta em ambiente digital – (monografias).** Coimbra: Almedina, 2021, p. 38.
[78] GERCKE, Marco. **Understanding Cybercrime: A Guide for Developing Countries**. Geneva: International Telecommunication Union, 2011, p. 142-144.

acerca das medidas que trazem mais dificuldade para a obtenção da prova pelos órgãos de persecução criminal.

Nesta perspectiva, Ramalho destaca os programas anonimizadores, como uma das espécies de medidas antiforenses mais utilizadas, já que garantem o anonimato dos criminosos em suas atuações por meio da *internet*. Nas palavras do autor, os instrumentos anonimizadores "visam impedir que o investigador criminal consiga associar uma certa conduta *online* ao seu autor."[79]

Dentre os programas anonimizadores, chama-se atenção ao *Tor*, que nada mais é do que um *software* programado para ocultar a origem – identidade - do utilizador, conferindo-lhe anonimato e privacidade na *internet*. Sendo tal programa frequentemente usado pelos criminosos para aceder a *Dark Web.*[80] Neste diapasão, Ramalho conceitua a *Dark Web* como uma área profunda da *internet* acessível apenas por meio da instalação de determinados programas dedicados a ocultar a identidade do utilizador. Segundo o autor, tal parcela da *internet* é um ambiente propício para "cibercriminalidade", em razão da navegação ser "livre, tendencialmente anônima, cifrada e potencialmente indetectável."[81]

Ainda de acordo com o autor retromencionado, por meio do *Tor*, surgiram vários *websites* na *Dark Web* destinados a todo tipo de criminalidade, merecendo destaque o conhecido caso denominado de *The Skil Road*, em que o FBI conseguiu descortinar um volumoso mercado negro de drogas *online*, no qual os agentes criminosos aproveitavam-se da anonimização da *Dark Web* e da *bitcoin* – moeda virtual em que se permite ocultar a identidade do proprietário durante a transação – para a vendar drogas na *internet*. Além disso, acrescenta-se que nesta parcela da *internet*, opera-se enorme venda e exposição de pornografia infantil.[82]

Para além do recurso aos programas anonimizadores, os agentes da prática de crimes em ambiente digital, nas ocasiões em que há o prévio conhecimento de que seus sistemas informáticos serão alvo de perícia, também se utilizam de técnicas para apagar ou esconder seus dados informáticos. Nestas situações, eles instalam programas informáticos capazes de adulterar ou modificar a prova digital, de modo a frustrar a investigação criminal.[83]

---

[79] RAMALHO, David Silva. **Métodos ocultos de investigação criminal em ambiente digital.** Editora Almedina, 2017, p. 153.
[80] CAMPOS, Juliana Filipa Sousa. **O malware como meio de obtenção de prova em processo penal: a investigação oculta em ambiente digital – (monografias).** Coimbra: Almedina, 2021, p. 40.
[81] RAMALHO, David Silva. A investigação Criminal na Dark Web. In: **Revista de Concorrência & Regulação**, ano IV, N° 16, (outubro/dezembro), 2013, p. 385.
[82] Idem, p. 392-393.
[83] Idem, p. 174.

No mais, destaca-se a encriptação, que além de ser uma medida encontrada em várias tecnologias e serviços – a exemplo do aplicativo de mensagem instantânea *WhatsApp* que utiliza a denominada encriptação de "ponta a ponta" -, também é utilizada pelos criminosos para proteger dados informáticos do acesso não autorizado ou de eventual modificação por parte de terceiros.[84]

Assim, por se tratar de programa de fácil instalação – e muitas vezes gratuito -, que protege uma infinidade de dados, a referida técnica acaba sendo muito utilizada pelos criminosos em ambiente digital.[85] Principalmente nas comunicações via protocolo IP (*Voice Over Internet Protocol -VoIP*) ou por meio de aplicativos de mensagem instantânea, vez que, nestas hipóteses, as conversas ficam indisponíveis para o servidor, tendo acesso ao conteúdo delas, apenas, o receptor, não podendo ser, portanto, desencriptadas. Situação desinteressante para os criminosos e oposta a que ocorre com as comunicações telefônicas através do *Global System for Mobile Communications - GSM*, pois aqui os prestadores de serviço possuem a chave da desencriptação e podem disponibilizar o conteúdo da comunicação para os órgãos de investigação, desde que haja requerimento e posterior autorização judicial.[86]

As dificuldades trazidas pela encriptação podem ser observadas no caso do direito norte-americano, *United States v. Nicodemo S. Scarfo*, que é um caso de relevância por ser o primeiro que se tem notícia acerca do uso do *malware*. É considerado, por muitos, o marco inicial no uso desta técnica oculta investigativa em sede de persecução criminal.

Trata-se de um caso ocorrido em janeiro de 1999, em que o FBI investigava um mafioso americano suspeito de envolvimento em jogos ilegais. Na oportunidade, utilizando-se de mandado de busca e apreensão, o FBI apreendeu o computador do suspeito, entretanto, não obteve êxito em acessar as informações e dados armazenados no referido dispositivo informático, uma vez que os arquivos estavam encriptados. Assim, com a finalidade de descobrir a senha (chave) da encriptação e aceder ao conteúdo dos arquivos até então protegidos, o FBI, por meio de nova autorização judicial, instalou presencialmente, no referido computador, o *malware* denominado de *keylogger*, que é um software espião que registra tudo que é digitado no teclado pelo utilizador. Assim, meses após a obtenção da senha de acesso aos

[84] CAMPOS, Juliana Filipa Sousa. **O malware como meio de obtenção de prova em processo penal: a investigação oculta em ambiente digital – (monografias).** Coimbra: Almedina, 2021, p. 38.
[85] GERCKE, Marco. **Understanding Cybercrime: A Guide for Developing Countries**. Geneva: International Telecommunication Union, 2011, p. 146.
[86] CAMPOS, Juliana Filipa Sousa. **O malware como meio de obtenção de prova em processo penal: a investigação oculta em ambiente digital – (monografias).** Coimbra: Almedina, 2021, p. 38-39.

ficheiros, foram recolhidas as provas, para ao final ser *Nicodemo S. Scarfo* acusado e condenado criminalmente. [87]

Posteriormente a este primeiro caso, tornou-se cristalina a necessidade de utilização de medidas tecnológicas nas investigações criminais. Nesta perspectiva, em 2001, o FBI desenvolveu um *software* mais evoluído denominado de *Magic Lantern*, que assim como o seu antecessor, registrava tudo o que era digitado no teclado pelo utilizador, com a diferença que podia ser instalado tanto presencialmente como remotamente, via *internet*, diferindo neste ponto do *keylogger*, na versão do caso anteriormente citado.[88]

Ao tratar das características do *Magic Lantern*, Ramalho aduz que o referido *malware* "podia ser instalado, quer através de abertura, no computador visado, de anexos em mensagens de correio eletrônico enviadas para o suspeito, quer por via da exploração de vulnerabilidades nos sistemas operativos instalados no sistema informático em causa."[89] Além disso, o retromencionado autor informou que o *Magic Lantern* com o progresso tecnológico foi substituído por um *malware* mais poderoso, denominado de *Computer and Internet Protocol Address Verifier – CIPAV* que podia captar, por exemplo, a localização e o IP do computador visado, bem como o sistema operacional em uso, e até mesmo o histórico do último site visitado, entre outras funções.[90]

Outra ofensiva do FBI ocorreu no ano de 2013, no Estado do Texas, nos Estados Unidos. Na ocasião, com a finalidade de recolher prova da prática de suposto crime de fraude em bancos federais, planejou-se aceder, via *malware* por envio de *e-mail*, a um computador de origem desconhecida, utilizado por sujeito não identificado e sem localização certa. O único elemento informativo que se tinha disponível era que pessoas suspeitas teriam conseguido acesso ilícito à conta de *e-mail* da vítima, utilizando-a posteriormente para acessar a conta bancária e praticar atos de fraude. Assim, com a informação de que os criminosos ainda acessavam o *e-mail* em questão, o FBI requereu a instalação de *malware* nos computadores dos

[87] ESTADOS UNIDOS DA AMERICA, **ESTADOS UNIDOS, v. Nicodemo S. SCARFO, et al.** Ação Criminal No. 00-404 (NHP). 180 F. Supp. 2d 572 (2001). Tribunal Distrital dos Estados Unidos, D. New Jersey**.** 26 de dezembro de 2001. Disponível em: https://law.justia.com/cases/federal/district-courts/FSupp2/180/572/2475159/. Acesso em outubro de 2022.
[88] CARRELL, Nathan E. **Spying on the mob: United Sta Tes v. Scarfo - a constitutional analysis**. JOURNAL OF LAW, TECHNOLOGY & POLICY. Vol. 2002. p, 194.
[89] RAMALHO, David Silva. **Métodos ocultos de investigação criminal em ambiente digital.** Editora Almedina, 2017, p. 325.
[90] RAMALHO, David Silva. **Métodos ocultos de investigação criminal em ambiente digital.** Editora Almedina, 2017, p. 326.

suspeitos para, dentre outras coisas, conseguir identificar, localizar e capturar as imagens deles. Ocasião em que teve o seu pleito negado.[91]

De acordo com o *decisum*, em linhas gerais, o desconhecimento da localização do computador utilizado trouxe problemas relacionados à competência jurisdicional do Estado do Texas. Além disso, não havia garantias que, apenas, o mínimo de dados seria coletado e que somente os alvos pretendidos seriam atingidos com a medida.[92] Nesse mesmo sentido, ao comentar sobre o caso, Ramalho afirmou que o envio de *malware* por *e-mail* possibilita que outras pessoas não envolvidas e que tenham acesso ao *e-mail* em pauta, sejam atingidas e instalem o *malware* em seus dispositivos. Acrescenta ainda que a funcionalidade de ativação da câmera caracteriza vídeovigilância, o que requer a observância de uma série de requisitos.[93]

Assim, fica evidente que o recurso ao *malware* surge em oposição as técnicas antiforenses, uma vez que a adoção de tais técnicas pelos criminosos tornou, ainda mais difícil, a recolha da prova criminal em ambiente digital, fazendo com que os órgãos de persecução penal tenham que utilizar métodos mais intrusivos para garantir o resultado útil das investigações.

Portanto, o deslocamento das investigações criminais para o ambiente digital e a larga utilização de medidas para ocultar a prática de crimes na *internet* são as razões que justificam a utilização do *malware* pelos Estados, que tiverem que substituir os tradicionais métodos investigativos pelas novas ferramentas tecnológicas, dotando a investigação criminal dos mesmos instrumentos utilizados pelos agentes da prática de cibercrimes."[94] Tal como um *hacker*, também o Estado pode intrometer-se num computador alheio e verificar o que lá está."[95]

5. *MALWARE*: CARACTERÍSTICAS E FUNCIONALIDADES

Tem-se por evidente que os novos meios tecnológicos trouxeram significativas mudanças no âmbito das investigações criminais, não apenas por modernizarem as ações

[91] ESTADOS UNIDOS. **United States District Court Southern District Of Texas Houston Division**. *In re warrant to search a target computer at premises unknown*. CASE NO. H-13-234M. Document 3 Filed in TXSD on 04/22/13. Disponível em: http://pt.scribd.com/doc/137842124/texas-order-denying-warrant. Acesso em outubro de 2022.
[92] Idem.
[93] RAMALHO, David Silva. **Métodos ocultos de investigação criminal em ambiente digital.** Editora Almedina, 2017, p. 328.
[94] CAMPOS, Juliana Filipa Sousa. **O malware como meio de obtenção de prova em processo penal: a investigação oculta em ambiente digital – (monografias).** Coimbra: Almedina, 2021, p. 25.
[95] CORREIA, João Conde. Prova digital: as leis que temos e a lei que devíamos ter. In: **Revista do Ministério Público**, ano 35, n° 139 (julho/setembro), 2014, p. 42.

policiais, mas, principalmente, por trazerem mais eficiência na coleta da prova criminal. A mudança de paradigma é cristalina, uma vez que estas novas metodologias possuem uma maior eficácia na coleta da prova, trazendo uma maior qualidade para as investigações criminais, ao passo que apresentam questionáveis restrições aos direitos fundamentais do investigado.[96]

Por se tratar de um programa altamente tecnológico e eficaz, usa-se o *malware* para atacar os sistemas de segurança internos dos dispositivos, como os antivírus presentes nos dispositivos informáticos, bem como para desencriptar as mensagens que não são acessíveis através da interceptação telefônica comum.[97]

Destaca-se, pois, que alguns *malwares* - que usualmente são utilizados pelos agentes da prática de crimes, ou pelos órgãos de investigação criminal – também podem ser utilizados para outros fins – para além da resolução de casos penais -, a exemplo do *spyware*, que é um *malware* corriqueiramente manuseado para coletar informações sobre o padrão de comportamento dos usuários na *internet*, bem como para apresentação de anúncios publicitários por meio de *pop up* na *web*.[98]

Assim, por ser impossível, atualmente, afastar as novas ferramentas tecnológicas da vida das pessoas e da resolução dos casos penais, tem-se como objetivo no presente tópico traçar as principais características e funcionalidades inerentes ao uso do *malware*, enquanto metodologia oculta de investigação, a fim de que posteriormente sejam estabelecidos critérios para sua utilização, evitando, assim, o seu generalizado, massivo e irrestrito uso nas investigações criminais.

A metodologia *malware*, assim como o denominado *hacking*, se assemelham por serem métodos ocultos intrusivos, executadas à distância, com a alta capacidade de monitorar as atividades do investigado, a partir da ativação da câmera, microfone e GPS do seu dispositivo informático. Por outro lado, apesar das similitudes, a infiltração por *malware* – que é o objeto de estudo do nosso trabalho – não se confunde com o *hacking*, pois enquanto este se trata de um acesso remoto não autorizado, vinculado à utilização de *internet*, o primeiro se trata de um

[96] ORTIZ PRADILLO, Juan Carlos. "Hacking" legal al servicio de la investigación criminal: nuevos instrumentos para la investigación y prueba de la delincuencia informática**.** In: Castrillo, Eduardo de Urbano. **Delincuencia informática: tiempos de cautela y amparo.** Editora Aranzadi, 2012. p, 185.
[97] TORRE, Marco. **Il captatore informático: nuove tecnologie investigative e rispetto delle regole processuali.** Giufrré Editore, 2017, p. 18.
[98] RIBEIRO, Gustavo Alves Magalhães; CORDEIRO, Pedro Ivo Rodrigues Velloso; FUMACH, Débora Moretti. O malware como meio de obtenção de prova e a sua implementação no ordenamento jurídico brasileiro. In: **Revista Brasileira de Direito Processual Penal**, vol. 8, n. 3, (set./dez), 2022, p.1468.

software malicioso instalado em determinado sistema ou dispositivo informático, possuindo uma maior capacidade na recolha de provas por um maior período.[99]

Em outras palavras, enquanto no *hacking* um agente físico (investigador) atua remotamente para obter acesso a um dispositivo informático, no *malware* a invasão ao dispositivo informático ocorre por meio de um *software* auto programado para ativar determinadas funcionalidades do dispositivo alvo, sem a necessária presença de um agente físico, diferindo, assim, do *hacking*.

A nomenclatura *malware* possui origem na "conjugação do adjetivo *malicius* e do substantivo *software*". Em termos simples, *malware* é um *software* criado para infiltração em dispositivos informativos alheios, com o fim de danificá-los ou coletar informações.[100] De outro modo, define-se *malware* como:

> 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.[101]

Ademais, o *malware* também pode ser conceituado como um programa:

> que se aproveita de uma vulnerabilidade existente no sistema informático e, em alguns casos, do próprio utilizador. Por sua vez, este é instalado, in *loco* ou remotamente (via *internet*), no sistema informático do visado, sem o conhecimento e consentimento esclarecido daquele. Uma vez instalado, o programa pode levar a cabo um conjunto de tarefas ou funcionalidades, em função daquilo que o atacante (*in casu* os OPC e/ou AJ) pretendem que ele faça, possibilitando a recolha de informação interna ao sistema informático (dados armazenados, não armazenados ou a ser produzidos em tempo real), quer de informação externa. Por fim, segue-se a possibilidade de envio desses dados para os OPC e/ou AJ.[102]

Partindo da premissa de que o *malware* se trata de uma intrusão não autorizada no dispositivo ou sistema informático do investigado, através da instalação de um *software* malicioso, alguns temas merecem ser levantados. O primeiro diz respeito ao modo de

---

[99] RAMALHO, David Silva. **Métodos ocultos de investigação criminal em ambiente digital.** Editora Almedina, 2017, p. 313-314

[100] BATISTA, Lydie Jorge Batista. **O malware como meio de obtenção de prova em processo penal**. 2018. Dissertação (Mestrado em Direito) Faculdade de Direito da Universidade de Lisboa, Lisboa, 2018, p. 25-26.

[101] RAMALHO, David Silva. O uso de malware como meio de obtenção de prova em processo penal. In: **Revista de Concorrência e Regulação**, número 16, ano IV (outubro/dezembro), 2013, p. 201-202.

[102] CAMPOS, Juliana Filipa Sousa. **O malware como meio de obtenção de prova em processo penal: a investigação oculta em ambiente digital – (monografias).** Coimbra: Almedina, 2021, p. 25.

instalação. De acordo com Batista, o *malware* pode ser instalado de três formas: "(1) via suporte removível; (2) via *web browser*; e (3) via *download* voluntário".[103]

De acordo com a autora retromencionada, a instalação via suporte removível (*pen drive*, por exemplo) possui uma vantagem em relação aos outros modelos, pois garante que apenas o investigado será infectado. Assim, diferentemente do que ocorre com as instalações por meio de *download* voluntário e acesso a página da *web*, em que terceiros também podem ser expostos a essa técnica maliciosa, na instalação local por suporte removível, infecta-se apenas e exatamente o dispositivo informático do investigado.[104]

Sobre o assunto, Ramalho pontua ser mais comum a instalação de *malware* de forma remota, contudo, assevera que o uso do *malware* não se restringe à *internet*, uma vez que a instalação deste também pode ocorrer localmente, por meio de suportes removíveis (*pen drives*, CDs, DVDs etc.).[105] Por sua vez, Velasco Nunez destaca duas possibilidades de instalação de *malware*, quais sejam, via correio eletrônico e por acesso a página da *web* infectada. Segundo ele, enquanto nesta hipótese a instalação atinge alvo indeterminado, podendo, inclusive, acertar terceiros não suspeitos, naquela o *malware* atinge tão somente suspeito certo e determinado.[106]

Tem-se, assim, que a instalação de *malware* de modo local é a forma que possui o menor potencial lesivo de atingir a privacidade e a intimidade de terceiros não envolvidos com a prática delitiva. E em se tratando da instalação remota, que é a mais usual, haja vista estarmos inseridos em uma sociedade tecnológica, o envio do *malware* por correio eletrônico parece ser a opção mais segura, apesar de não garantir com total certeza que só investigado acessará o *e-mail* e fará o *download* involuntário do arquivo infectado, pois o e-mail pode ser clonado ou acessado em dispositivos informáticos diferentes, por diferentes pessoas. Assim, ainda que as formas de instalação por correio eletrônico – com *download* involuntário de ficheiro infectado – e via pen drive – sejam menos nocivas em relação à hipótese de infecção de página da *web*, não se desconsidera a lesividade daquelas em relação ao investigado.

O segundo tema relaciona-se a integridade do elemento de prova obtido via *malware*. De acordo com Ribeiro, Cordeiro e Fumach, a operacionalização de diversas

---

[103] BATISTA, Lydie Jorge Batista. **O malware como meio de obtenção de prova em processo penal**. 2018. Dissertação (Mestrado em Direito) Faculdade de Direito da Universidade de Lisboa, Lisboa, 2018, p. 30.
[104] Idem, p.30-31.
[105] RAMALHO, David Silva. **Métodos ocultos de investigação criminal em ambiente digital.** Editora Almedina, 2017, p. 315.
[106] VELASCO NUÑEZ, Eloy. Limites a las investigaciones y a la prueba en el proceso penal. In: **Delitos tecnológicos: definición, investigación, y prueba en el proceso penal.** Madrid: Editorial Jurídica Sepín, 2016, p. 35.

funcionalidades pode gerar dúvidas acerca da integridade da prova a ser colhida.107A dúvida sobre a possibilidade de o *malware* alterar ou corromper os arquivos do dispositivo informático alvo, também é levantada por Mendes, que aduz ser dever dos órgãos de investigação criminal comprovar a confiabilidade dos elementos probatórios colhidos através de *malware*. Segundo ele, as autoridades devem demonstrar que não houve alteração das fontes de prova no momento da introdução do *malware* e que a cadeia de custódia da prova digital fora preservada.[108]

O terceiro tema que merece destaque refere-se as funcionalidades que cada tipo de *malware* pode desempenhar após sua instalação no dispositivo alvo. De acordo com Campos, o *malware* tem a capacidade de recolher "prova interna (dados armazenados, não armazenados ou produzidos em tempo real) e/ou prova externa ao sistema informático, quando aquele comporte a ativação do *hardware*".[109]

Já Torre destaca que o *malware* pode realizar de maneira dissimulada a atividade de vigilância em tempo real, incluindo o acesso a geolocalização do dispositivo móvel, ao áudio, vídeo, funções de microfone e câmeras, fluxo de dados e comunicações, do investigado.[110] Tem-se, desse modo, que a depender de sua espécie, o *malware* poderá realizar diversas funções, tendo a capacidade de recolher tanto os dados armazenados no dispositivo informático, como também os dados produzidos em tempo real, podendo, inclusive, ativar a câmera do dispositivo alvo.

Para além das questões relacionadas com a instalação, integridade da prova e funcionalidades, vale pontuar que são vários os tipos de *malware* existentes, possuindo cada um deles suas características próprias e especificidades. Campos distingue cada um dos tipos atendendo a dois critérios. O primeiro é o da instalação, pois existem *malwares* que dependem da interação do utilizador para sua instalação e outros não. Já o segundo critério para distinção, segundo a autora, é o das funcionalidades, uma vez que cada *malware* pode apresentar funções distintas.

Assim, como não há um rol taxativo de espécies de *malware*, até porque o constante avanço da tecnologia permite que novos *softwares* sejam desenvolvidos em curto espaço de

107 RIBEIRO, Gustavo Alves Magalhães; CORDEIRO, Pedro Ivo Rodrigues Velloso; FUMACH, Débora Moretti. O malware como meio de obtenção de prova e a sua implementação no ordenamento jurídico brasileiro. In: **Revista Brasileira de Direito Processual Penal**, vol. 8, n. 3, (set./dez), 2022, p.1470.

108 MENDES, Carlos Hélder. **Malware do estado e processo penal: a proteção de dados informáticos face à infiltração por software na investigação criminal**. 2018. Dissertação de Mestrado. Pontifícia Universidade Católica do Rio Grande do Sul, p. 133.

109 CAMPOS, Juliana Filipa Sousa. **O malware como meio de obtenção de prova em processo penal: a investigação oculta em ambiente digital – (monografias).** Coimbra: Almedina, 2021, p. 21.

110 TORRE, Marco. **Il captatore informático: nuove tecnologie investigative e rispetto delle regole processuali.** Giufrré Editore, 2017, p. 18.

tempo, a presente exposição irá, apenas, apontar, a título exemplificativo, as principais características do *worm* e do cavalo de troia (*trojan horse*). A escolha se deu por estes dois, primeiro porque são *malwares* que se distinguem entre si pela necessidade ou não do utilizador para sua instalação, segundo porque o *trojan horse* é o *malware* mais popular do mundo, principalmente, depois de ter sido utilizado em uma investigação criminal relacionada a atos terroristas, ocorrida na Alemanha, no ano de 2006.[111]

Assim como o cavalo de troia, o *worm* é um programa capaz de se autorreplicar. No entanto, diferindo daquele, este tem a capacidade de se espalhar sem depender de um sistema hospedeiro ou da interação do utilizador. Os *worms* utilizam da rede para enviar cópias de si mesmo para outros sistemas na rede, explorando vulnerabilidades ou configurações incorretas de softwares presentes no sistema de computação. Seu principal propósito é infectar os sistemas, danificar os dados e comprometer a funcionalidade geral do próprio sistema em si.[112]

Por sua vez, cavalo de troia é um *malware* que carece de interação para ser instalado, possuindo aspecto inofensivo, de modo que o utilizador o instala pensando se tratar de arquivo legítimo. Outra característica sua é a capacidade de interferir no dispositivo alvo, através da monitorização das atividades do utilizador. A sua instalação no dispositivo alvo, por sua vez, decorre "da abertura de um anexo ao *e-mail*, do *download* ou execução de um ficheiro (v.g. uma imagem) de um *website*".[113]

A lesividade do cavalo de troia é evidenciada por meio de sua funcionalidade, uma vez que após sua instalação, o invasor ganha acesso a um amplo conjunto de dados do usuário, que vão desde as informações de *login* em páginas restritas (como *webmails* e redes sociais) até a obtenção de dados confidenciais, como as senhas de cartões de crédito. Além disso, o invasor tem a capacidade de causar danos ao sistema do utilizador (visado), implantando outros tipos de *malwares.*[114]

No que tange ao termo em si, importa destacar que são várias as designações para *malware* nas mais diversas ordens jurídicas, quais sejam, "*government hacking*"; "*policeware*"; "*hacking legal*"; "*online durchsuchung*" (Alemanha); "*captatore informático*" (Itália);

[111] Para maiores informações sobre o caso, acessar: https://www.hrr-strafrecht.de/hrr/1/06/1-bgs-184-2006.php Acesso em: 05/08/2022.
[112] BATISTA, Lydie Jorge Batista. **O malware como meio de obtenção de prova em processo penal**. 2018. Dissertação (Mestrado em Direito) Faculdade de Direito da Universidade de Lisboa, Lisboa, 2018, p. 29-30.
[113] CAMPOS, Juliana Filipa Sousa. **O malware como meio de obtenção de prova em processo penal: a investigação oculta em ambiente digital – (monografias).** Coimbra: Almedina, 2021, p. 33.
[114] BATISTA, Lydie Jorge Batista. **O malware como meio de obtenção de prova em processo penal**. 2018. Dissertação (Mestrado em Direito) Faculdade de Direito da Universidade de Lisboa, Lisboa, 2018, p. 27.

"*registros remotos*" (Espanha); "buscas *online*" (Portugal). No Brasil, ainda não existe debate doutrinário acerca da nomenclatura mais adequada para conceituar o supracitado método oculto de investigação. Em Portugal, o termo "buscas *online*" é utilizado para se referir a *malware* e recebe críticas por parte de alguma doutrina. Entende-se, em linhas gerais, que a referida nomenclatura não abrange todas as possíveis funcionalidades do *malware* e que a adoção do termo *online* induz a pensar que o *malware* só pode ser instalado de forma *online*, o que não é verdade, como já exposto.

Ramalho acertadamente critica o termo "busca *online*" para se referir a *malware*, uma vez que este não necessariamente pressupõe "ligação à internet", podendo ser instalado localmente, de maneira *offline*. Além disso, segundo o autor, a busca é apenas uma das várias funcionalidades inerentes a instalação da referida metodologia, que é bem mais intrusiva e não se confunde com a busca domiciliária.[115]

Este aspecto intrusivo do *malware*, pode ser observado com o seu uso, uma vez que a partir de sua instalação muitos dados são apreendidos de maneira desnecessária, de forma a violar frontalmente vários direitos fundamentais. Assim, o ideal seria que, no futuro, tal meio de obtenção de prova fosse automatizado para captar provas específicas e determinadas, durante um período pré-estabelecido, definido antes de sua execução. Isto tornaria tal mecanismo ainda mais indispensável para a investigação criminal, tendo em vista também o seu baixo custo.[116]

[115] RAMALHO, David Silva. **Métodos ocultos de investigação criminal em ambiente digital.** Editora Almedina, 2017, p. 315-316.
[116] SALT, Marcos. **Nuevos desafios de la evidencia digital: acceso transfornterizo y técnicas de acesso remeto a datos informáticos**. 1ª ed. Buenos Aires: Ad-hoc, 2017, p. 67-68.

II. EXPERIÊNCIA ALEMÃ COM A UTILIZAÇÃO DE *MALWARE*

O termo *malware*, como já disposto no capítulo anterior, "se refere a um conjunto específico de *softwares* que, instalados de modo oculto em um equipamento ou sistema informático, permitem a um terceiro não usuário o acesso às informações e dados neles contidos". Há um paradoxo a ser resolvido, pois, se por um lado o *malware* gera um ganho de eficiência no âmbito investigativo, por outro, enseja restrições controversas a direitos e garantias fundamentais do cidadão.[117] Os direitos fundamentais de proteção à não autoincriminação, à privacidade, à autodeterminação informativa e ao domicílio, são os que especialmente são colocados por vezes em ameaça pela referida metodologia investigativa.

Assim sendo, evidencia-se que a utilização de *malwares* em investigações criminais está cada vez mais se tornando comum em diferentes partes do mundo, com alguns países já prevendo de forma expressa em suas legislações o recurso ao *malware* enquanto método oculto de obtenção de prova.

Nesta senda, o presente capítulo, busca fazer uma análise de experiências internacionais sobre a temática. Para tanto, se enfatiza na experiência alemã, sendo essa pioneira sobre o tema, fazendo uma retomada das principais decisões e normativas acerca do *malware*, para então, desaguar em outras experiências, tais como, a espanhola e a italiana.

1. A DECISÃO DO *BUNDESGERICHTSHOF* DE 2007

O avanço tecnológico trouxe consigo diversas mudanças na forma como o indivíduo se relaciona com o mundo e com as informações, em que, perante o aumento da quantidade de dados compartilhados digitalmente, a privacidade tornou-se uma preocupação constante para a sociedade moderna.

Assim sendo, foram desenvolvidos marcos normativos e jurisprudenciais acerca da garantia da confidencialidade e integridade dos sistemas informáticos, com o objetivo de proteção de direitos fundamentais, principalmente os de personalidade.[118]

---

[117] RIBEIRO, Gustavo Alves Magalhães; CORDEIRO, Pedro Ivo Rodrigues Velloso; FUMACH, Débora Moretti. O malware como meio de obtenção de prova e a sua implementação no ordenamento jurídico brasileiro. **Revista Brasileira de Direito Processual Penal**, v. 8, p, 2022, p. 1465.

[118] ENDERS, Christoph. **The Right to have Rights**: The concept of human dignity in German Basic Law. Revista de Estudos Constitucionais, Hermenêutica e Teoria do Direito. 2018. Disponível em: <https://dialnet.unirioja.es/descarga/articulo/5007582.pdf>. Acesso em: 03 mai. 2023. p. 2.

A primeira legislação no mundo a respeito do tema foi implementada em 1970 pelo Estado alemão de *Hessen*, enquanto em 1977 o parlamento alemão aprovou a Lei Federal de Proteção de Dados (*Bundesdatenschutzgesetz*). Contudo, o ponto mais alto do reconhecimento da proteção de dados se deu com a decisão do Tribunal Constitucional Federal alemão a respeito do censo demográfico de 1983 (*Volkszählungsurteil*), que estabeleceu o direito fundamental à autodeterminação informativa (*Grundrecht auf informationelle Selbstbestimmung*).[119]

A discussão girou em torno da Lei do censo populacional, julgada em 1983, em virtude, da preocupação que se propagou na população em que fosse criado um Estado ultra informado, que fizesse uma utilização secundária dos dados colhidos dos cidadãos. Na oportunidade, o Tribunal Constitucional Federal Alemão julgou improcedente a Lei do censo, consagrando o direito à autodeterminação informativa, como o direito dos indivíduos "decidirem por si próprios, quando e dentro de quais limites seus dados pessoais podem ser utilizados."[120]

Essa decisão do Tribunal Constitucional Federal alemão foi um marco importante no reconhecimento da importância da proteção de dados pessoais e do direito à privacidade na era digital. O tribunal afirmou que os indivíduos têm o direito de decidir quando, como e em que medida seus dados pessoais são coletados, armazenados, processados e utilizados por terceiros, incluindo o Estado.[121]

Desde então, muitos países e organizações internacionais têm adotado leis e regulamentos para proteger a privacidade e a segurança dos dados pessoais, inspirados nesse modelo alemão. Entretanto, o direito teve que se adaptar para garantir o direito fundamental à proteção de dados privados, ao passo que, desde 1983, houve um rápido desenvolvimento das tecnologias da informação, principalmente em termos de digitalização, miniaturização, rede e infraestrutura de serviços, e, residindo na *internet* o fenômeno mais evidente deste desenvolvimento, pois, não é mais necessário depender de computadores volumosos, caros e relativamente lentos, com armazenamento limitado, como no passado.[122]

---

[119] MENKE, Fabiano. **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 2019. Disponível em: <https://www.cidp.pt/revistas/rjlb/2019/1/2019_01_0781_0809.pdf>. Acesso em: 30 abr. 2023. p. 782.

[120] DE LA CUEVA, Pablo Lucas Murillo. La construcción del derecho a la autodeterminación informativa. **Revista de Estudios Políticos** (Nueva Época), n. 104, p. 35-60, abr./jun. 1999.

[121] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

[122] HOFFMANN-RIEM, Wolfgang. **Innovaciones en la Jurisprudencia del Tribunal Constitucional Alemán, a Propósito de la Garantía de los Derechos Fundamentales en Respuesta a los Cambios que Conducen a la Sociedad de la Información**. Direito Público, 12(64). Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/2557. Acesso em: 03 mai. 2023. p. 48.

Neste contexto de desenvolvimento tecnológico acelerado, a proteção de dados pessoais se tornou um assunto de ainda maior importância, uma vez que a facilidade de coleta, processamento e compartilhamento de informações se ampliou consideravelmente. Isso trouxe novos desafios e exigiu mudanças na legislação para garantir a proteção da privacidade das pessoas em relação ao uso de suas informações pessoais.

Qualquer pessoa hoje em dia pode ter acesso a computadores de alto desempenho a preços acessíveis, além de, dispositivos portáteis como *pen drives*, *laptops*, *tablets* e *smartphones* que permitem comunicação móvel e armazenamento de dados, e, ainda, ter acesso a capacidade de armazenamento na nuvem e a comunicação e armazenamento podem ocorrer por meio de redes globais.[123]

Foi reconhecido que muitos dispositivos utilizados diariamente pela maioria dos alemães contêm elementos de tecnologia da informação, como celulares, *BlackBerries* e até mesmo *MP3 players*, assim como, dispositivos como geladeiras inteligentes, torradeiras e até mesmo joias estão surgindo como próximas extensões.[124] Fica evidente, portanto, que na maioria dos aparelhos eletrônicos existe a possibilidade de armazenamento de dados, englobando um número cada vez maior de aparelhos a apresentarem proteção.

Neste ínterim, o Tribunal também constatou que a importância cultural e social desses aparelhos, em particular os computadores pessoais, evoluiu de modo significativo devido ao fato de que eles podem ser usados para uma ampla variedade de funções, incluindo a administração e arquivamento de assuntos pessoais e comerciais, bem como em inúmeros aplicativos de entretenimento para atividades de lazer.[125]

O desenvolvimento contínuo dessas tecnologias tem um impacto significativo na sociedade, especialmente em relação à proteção de dados privados e à garantia da confidencialidade e integridade dos sistemas de tecnologia da informação. Com a disseminação dessas tecnologias, há uma maior probabilidade de violações de direitos fundamentais dos usuários, como o direito à privacidade.

Essa rápida evolução tecnológica apresenta desafios ao sistema jurídico, que deve garantir a proteção dos direitos fundamentais dos usuários, bem como proteger a sociedade em

---

[123] Idem, p. 48.

[124] ABEL, W; SCHAFER, B. **The German Constitutional Court on the Right in Confidentiality and Integrity of Information Technology Systems**. in V Madhuri (ed.), Hacking: A Legal Quandary. Icfai University Press. Disponível em: https://www.pure.ed.ac.uk/ws/portalfiles/portal/15050731/The_German_Constitutional_Court_on_the_Right_in_Confidentiality_and_Integrity_of_Information_Technology_Systems.pdf. Acesso em: Acesso em: 03 mai. 2023. p. 117.

[125] Idem, p. 117.

geral. É importante garantir que as leis e regulamentos correspondam às mudanças tecnológicas e sociais, bem como, a proteção de dados privados deve ser uma prioridade, pois a exposição de dados pessoais pode resultar em prejuízos financeiros, de reputação e outros danos.

Assim sendo, observa-se que as primeiras notícias de tentativas de uso dos *softwares* de espionagem com finalidade investigativa na Alemanha datam de 2006, tendo sido o Tribunal Federal de Justiça Alemão (*Bundesgerichtshof, "BGH"*) instado a se manifestar no ano seguinte sobre o tema. Na ocasião, em 2007, foi decidido pela referida Corte que não havia base legal no Código de Processo Penal Alemão (*Strafprozessordnung, StPO*) para autorizar a realização de "buscas *online*" em sistemas informáticos através do recurso ao *malware*.[126]

Baseando-se no direito à autodeterminação informativa, o Tribunal Federal de Justiça Alemão concluiu que não havia fundamento legal para a invasão de computadores e que uma analogia também não seria possível. Para tanto, argumentou "que o acesso aos dados armazenados no computador dos investigados seria uma severa intervenção ao direito fundamental à autodeterminação informacional."[127]

O Tribunal rechaçou qualquer tentativa de fundamentar a invasão de computadores em um combinado de normas, considerando que uma intervenção tão séria como essa e com reflexos nos direitos de personalidade e liberdade, deveria ser amparada em norma específica, para ter compatibilidade constitucional. Conceber de modo contrário seria o mesmo que violador o princípio da proporcionalidade e seria uma intervenção injustificável a direitos fundamentais. Em outros termos, entendeu-se que toda intervenção estatal em direitos fundamentais precisa ser regulamentada em lei e que a aplicação da proporcionalidade ao caso concreto não acontece em substituição a previsão legal, mas em momento posterior. De modo que a lei restritiva de direitos fundamentais é que é proporcional e não a intervenção sem norma autorizadora específica.[128]

Além desses argumentos, a Corte destacou que não caberia qualquer legitimação do *malware* nos regimes das buscas em locais físicos, das interceptações e da vigilância acústica domiciliar, visto que se trata de métodos ocultos com especificidades distintas em relação à dita infiltração *online*.[129] Veja-se:

---

[126] RIBOLI, Eduardo Bolsoni. "Eu sei o que vocês fizeram no verão passado": o uso de software de espionagem como meio de obtenção de prova penal. **Revista Brasileira de Ciências Criminais**, São Paulo, v. 27, n. 156, p. 91-139, jun. 2019, p. 98.

[127] GRECO, Luís; GLEIZER, Orlandino. A infiltração online no processo penal–Notícia sobre a experiência alemã. **Revista Brasileira de Direito Processual Penal**, v. 5, n. 3, p. 1483-1518, 2019, p. 1488.

[128] Idem, p. 1489.

[129] Idem, p. 1489.

> A norma de autorização para buscas domiciliares (§ 102 StPO) – um método de investigação físico, e não virtual – não autorizaria a medida, já que a busca em objetos físicos se baseia no princípio da publicidade: o investigado deve ser notificado e tem o direito de acompanhar a medida de busca em seu domicílio (§ 106 Abs. 1 Satz 2 StPO). Tampouco as normas que autorizam intervenções ocultas alcançariam a medida. A norma que autoriza o monitoramento de telecomunicações (§ 100a StPO) também não poderia ser aplicada ao caso: ainda que, durante a devassa nos dispositivos informáticos, possivelmente dados e procedimentos de telecomunicação sejam tangenciados, o objetivo central da medida seria a coleta abrangente de todas as informações armazenadas nos dispositivos, não necessariamente derivadas de telecomunicações. De vigilância acústica domiciliar (§ 100c StPO) tampouco se trataria. Por fim, a cláusula geral para investigações do Ministério Público e da Polícia (§ 161 StPO) não abrangeria uma intervenção tão severa em direito fundamental. [130]

Note-se, por conseguinte, que o Tribunal Federal de Justiça Alemão foi e tem sido um importante protagonista na defesa do direito à proteção de dados privados para garantia dos direitos fundamentais na sociedade da informação, de modo a se adaptar às mudanças tecnológicas para garantir a proteção da privacidade dos indivíduos como garantia à proteção de dados privados para a construção de uma sociedade democrática, tendo evoluído em termos de jurisprudência e marco normativo.

2. A DECISÃO DO *BVERFG* PELA INCONSTITUCIONALIDADE DA LEI DA RENÂNIA DO NORTE-VESTFÁLIA E A CRIAÇÃO DO DIREITO FUNDAMENTAL À GARANTIA DA CONFIABILIDADE E INTEGRIDADE DE SISTEMAS INFORMÁTICOS.

Inicialmente, antes de adentrar especificamente ao tema do presente tópico, devem ser colocadas algumas considerações sobre o direito de inteligência, que pode ser concatenado no acesso a informações sigilosas, que são coletadas por agências de inteligências governamentais, e, até mesmo empresas privadas a depender da sua função social. Prontamente, a definição de tal concepção é complexa, de modo a abranger tanto a proteção de informações sensíveis e segurança dos cidadãos, quanto a necessidade de transparência e responsabilização governamental.[131]

O acesso a informações de inteligência são fundamentais para a proteção da sociedade e da segurança nacional, como, por exemplo, nos casos de atentados terroristas ou

[130] Idem, p. 1489.
[131] TOGIAS, Stavros. **The right in confidentiality and integrity of information technology systems according to the german federal constitutional court**: 'old wine in new bottles'?, 2010. Disponível em: https://conferences.ionio.gr/isil2010/download.php?f=papers/togias_stavros_full.pdf. Acesso em: 03 mai. 2023. p. 1.

ataques a escolas, do mesmo modo que serve para assegurar interesses do próprio Estado. É importante destacar que não se deve confundir o interesse do Estado no direito de inteligência para prevenir ataques de qualquer natureza e garantir seus interesses com a violação à privacidade para obtenção em massa de dados, como assim foi protagonizado pelos Estados Unidos no caso *Edward Snowden*.[132]

Diante desses sucessivos avanços tecnológicos que proporcionam cada vez mais capacidade de coleta de dados em larga escala, é essencial que se estabeleçam limites claros e garantias de proteção à privacidade dos indivíduos. A necessidade de segurança do Estado não pode justificar a violação indiscriminada dos direitos individuais.

É preciso buscar um equilíbrio entre a proteção da segurança nacional e a salvaguarda dos direitos fundamentais, como a privacidade e intimidade, tudo isso diante do constante aprimoramento de *softwares* e *hardwares*, que podem apresentar um alto índice, ou não, de proteção ao usuário, a depender dos seus conhecimentos técnicos.

As ferramentas de criptografia, por também acompanharem essas evoluções tecnológicas, podem acobertar melhor os meios de comunicação utilizados por criminosos, de modo a dificultar sua identificação, localidade e suas informações em geral. Enquanto isso, as agências de aplicação da lei estão enfrentando o risco de serem abandonadas na detecção de crimes devido ao rápido progresso da tecnologia da informação e aos novos padrões cada vez mais sofisticados de conspiração e técnicas de redes criminosas.[133]

As agências de inteligência têm um papel crucial na proteção dos interesses do Estado e na prevenção de ameaças à segurança nacional, e é através deste direito de inteligência que as referidas agências têm a permissão para coletar informações relevantes para cumprir sua missão. Entretanto, é importante lembrar que esse direito deve ser exercido dentro dos limites da lei e sem violar os direitos fundamentais dos cidadãos, de modo a assegurar equilíbrio entre a necessidade de coletar informações e a proteção dos direitos individuais, apresentado um desafio constante para as agências de inteligência e para a sociedade como um todo.

O Serviço Federal de Inteligência da Alemanha (BND) é um dos três órgãos federais responsáveis pela inteligência estrangeira civil e militar do país, juntamente com o

---

[132] PILATI, José Isaac; OLIVIO, Mikhail Vieira Cancelier. **Um novo olhar sobre o direito à privacidade**: caso Snowden e pós-modernidade jurídica. Seqüência (Florianópolis), n. 69, p. 281-300, dez. 2014. Disponível em: https://www.scielo.br/j/seq/a/BKdjxJFTbXNPwJnnP4hk8kF/?format=pdf&lang=pt. Acesso em: 30 abr. 2023. P. 283.

[133] TOGIAS, Stavros. **The right in confidentiality and integrity of information technology systems according to the german federal constitutional court**: 'old wine in new bottles'?, 2010. Disponível em: https://conferences.ionio.gr/isil2010/download.php?f=papers/togias_stavros_full.pdf. Acesso em: 03 mai. 2023. p. 1.

Escritório Federal para a Proteção da Constituição (*Bundesamt für Verfassungsschutz*) e o Serviço de Contrainteligência do Exército (*Militärischer Abschirmdienst*)[134]. O BND desempenha um papel importante na cooperação com serviços de inteligência estrangeiros, trocando informações e coordenando esforços de segurança.

Essa cooperação é fundamental para a segurança nacional da Alemanha e para a prevenção de ameaças internacionais.[135] Um ponto a ser observado é que o direito de inteligência pode ser utilizado pelas agências de inteligência para violar direitos humanos e liberdades individuais nacional e internacionalmente. Isso só levanta preocupações crescentes diante dos repetidos abusos cometidos pelas agências governamentais, que se justificam em nome da proteção dos cidadãos e da sociedade em meio a uma guerra global e silenciosa entre as nações.

O direito de inteligência está intrinsecamente ligado com a coleta e análise de dados de inteligência, que podem ser utilizados para prevenir crimes além de, agregar em vantagem militar, econômica e avanços tecnológicos em favor de determinada instituição ou nação. Entretanto, também, podem ser utilizados para fins de espionagem e violação de privacidade em vários níveis, justificados pelo discurso de proteção à segurança nacional.[136]

Uma inovação do sistema jurídico deve acontecer e acompanhar as mudanças tecnologias que se apresentam perante a sociedade, e, mesmo diante das lacunas que se apresentem, pode o poder judiciário seguir diretrizes apresentadas pelo legislador como referência para a solução dos casos concretos diante das novas perspectivas que possam surgir perante a constante modificação social e tecnológica vigente.[137]

Com os métodos cada vez mais engenhosos de comunicação, é evidente a tensão contínua para se ter acesso a informações sensíveis ou pessoais em detrimento da garantia de direitos fundamentais, bem como, para mantê-las em segredo perante o público em geral. Se torna crucial, portanto, que o legislador desenvolva uma norma que apresente finalidade

---

[134] KAPPLER, Katrin. **Consequences of the German Constitutional Court's Ruling on Germany's Foreign Intelligence Service**: The Importance of Human Rights in the Cooperation of Intelligence Services. German Law Journal, 2022, p. 173–185. Disponível em: <https://doi.org/10.1017/glj.2022.12>. Acesso em: 03 mai. 2023. p. 174.

[135] Idem, p. 175.

[136] PILATI, José Isaac; OLIVIO, Mikhail Vieira Cancelier. **Um novo olhar sobre o direito à privacidade: caso Snowden e pós-modernidade jurídica**. Seqüência (Florianópolis), n. 69, p. 281-300, dez. 2014. Disponível em: https://www.scielo.br/j/seq/a/BKdjxJFTbXNPwJnnP4hk8kF/?format=pdf&lang=pt. Acesso em: 30 abr. 2023. p. 282.

[137] HOFFMANN-RIEM, Wolfgang. **Innovaciones en la Jurisprudencia del Tribunal Constitucional Alemán, a Propósito de la Garantía de los Derechos Fundamentales en Respuesta a los Cambios que Conducen a la Sociedad de la Información**. Direito Público, 12(64). Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/2557. Acesso em: 03 mai. 2023. p. 41.

específica para regulamentação de acesso aos dados, abrangendo as hipóteses que autorizam a visualização de informações mesmo diante dos avanços tecnológicos.[138]

Mas, tal tarefa não é tão simplória, pois circunda envolta do direito de inteligência uma linha tênue entre a segurança nacional e a privacidade dos cidadãos, e, já observamos que o acesso sem controle a informações privadas e pessoais pode agregar em violação massiva de direitos fundamentais.

É visível que a proteção dos direitos humanos e liberdades individuais deve ser levada em consideração sempre que se tratar dos aspectos do direito de inteligência, nessa toada, deve existir algum instrumento de regulamentação e fiscalização das agências de inteligência, para que se possa garantir que as informações sejam coletadas de um modo legal e ético.

Assim, o acesso às informações de inteligência deve ser limitado a indivíduos e organizações que apresentem autorização legal para conhecer de tais dados, bem como, o uso desses dados deve ocorrer para fins específicos. E, é seguindo esse raciocínio que a Alemanha apresenta uma enorme experiência acerca da proteção da privacidade, que apesar de ser considerada uma parte fundamental do direito de inteligência, especialmente no contexto da era digital, não comporta violações, como se passará a demonstrar.

Destarte, de forma paralela à decisão do *BGH* de 2007, o estado alemão de Renânia do Norte-Vestfália, inseriu em sua Lei de Proteção à Constituição de 2006 (*Verfassungsschutzgesetz*), dispositivo legal (§5.2) que autorizava a medida de infiltração *online* (*malware*) em sistemas informáticos pelos serviços de inteligência, para fins de desempenho de suas atividades de prevenção, em especial no combate ao terrorismo. Em linhas gerais, tal dispositivo viabilizava a espionagem, o monitoramento e o controle dos sistemas informáticos alvos, sob a condição de que à coleta de informações se limitassem a situações em que houvesse suspeita de ameaça à ordem democrática ou à segurança interna da nação.[139]

Destaca-se que na Alemanha o Serviço de Proteção à Constituição desempenha a atividade de inteligência estatal, de modo preventivo. Diferindo dos órgãos de persecução criminal, que agem em investigações criminais, de forma repressiva, após a realização da conduta ilícita, com a finalidade de elucidar o fato e punir os infratores.[140]Assim, tem-se que a

[138] Idem, p. 41.
[139] RIBOLI, Eduardo Bolsoni. "Eu sei o que vocês fizeram no verão passado": o uso de software de espionagem como meio de obtenção de prova penal. **Revista Brasileira de Ciências Criminais**, São Paulo, v. 27, n. 156, p. 91-139, jun. 2019, p. 100.
[140] GRECO, Luís; GLEIZER, Orlandino. A infiltração online no processo penal–Notícia sobre a experiência alemã. **Revista Brasileira de Direito Processual Penal**, v. 5, n. 3, p. 1483-1518, 2019, p. 1490.

referida alteração legislativa, introduzindo a possibilidade de infiltração *online*, não se referia ao processo penal, mas sim ao direito de inteligência.

Ocorre que em 2008, a referida legislação foi submetida ao crivo do Tribunal Constitucional Alemão (*BVerfG*) para análise da legalidade do dispositivo que autorizava a infiltração *online* na ordem interna. A discussão sobre o tema, contudo, havia iniciado em 2006 após o indeferimento do pedido de um promotor do Ministério Público que pleiteva acessar secretamente o computador de um suspeito de estar envolvido com o terrorismo. [141]

Na ocasião, foi argumentado perante a *BGH* que seria possível fazer uso de *malware* para acessar à distância computadores e dispositivos móveis com base nos dispositivos do Código de Processo Penal Alemão (*Strafprozessordnung- StPO*), que autorizam buscas físicas, e que por analogia serviriam para fundamentar o pedido de busca em computadores.[142]

No referido caso, o que estava em jogo era o acesso secreto a um sistema de informação, também compreendido por invasão técnica, o que se diferencia do monitoramento da *internet*, pois, neste se visualiza as comunicações em *sites* e fóruns abertos, ao passo que o pretendido era o acesso a um sistema informático através de uma infiltração que pode ocorrer por meio da exploração da segurança computacional do suspeito ou instalação de um programa espião.[143]

Nesse sentido, o que se almejava era utilizar do aparato estatal, por meio das suas agências de inteligência, para adentrar no sistema computacional do suspeito com fundamento baseado na analogia aos pedidos de busca em instalações físicas, o que certamente iria ensejar na violação da transparência governamental em relação ao direito de inteligência justamente pela ausência de autorização normativa, dentre a violação de outros direitos.[144]

No caso, foi adotado o *malware* denominado de cavalo de troia (*trojan horse*), que tem a vantagem de ser instalado clandestinamente e disfarçado como algo inofensivo, o que leva o suspeito a instalar involuntariamente, isso significa que essas tecnologias exigem a cooperação involuntária do alvo, assim como suas contrapartes criminosas[145].

---

[141] ABEL, W; SCHAFER, B. **The German Constitutional Court on the Right in Confidentiality and Integrity of Information Technology Systems**. in V Madhuri (ed.), Hacking: A Legal Quandary. Icfai University Press. Disponível em: https://www.pure.ed.ac.uk/ws/portalfiles/portal/15050731/The_German_Constitutional_Court_on_the_Right_in_Confidentiality_and_Integrity_of_Information_Technology_Systems.pdf. Acesso em: Acesso em: 03 mai. 2023. p. 107- 108.

[142] Idem, p. 108.

[143] Idem, p. 108.

[144] Idem, p. 108.

[145] Idem, p. 109.

Caso a infiltração obtenha êxito, esse método apresenta benefícios consideráveis para as autoridades de investigação em relação às técnicas tradicionais de investigação e, por ser realizada sem o conhecimento do suspeito, a pessoa não tem ciência de que está sob a mira da polícia, diferentemente do que ocorre em uma busca domiciliar comum.[146]

Assim sendo, ao apreciar o caso, em 2008, a Corte Constitucional alemã (*BVerfG*) reconheceu um novo direito fundamental, qual seja, o da confidencialidade e integridade dos sistemas informáticos. O referido entendimento teve por premissa inicial o fato de que os direitos fundamentais que asseguram a inviolabilidade do domicílio e das telecomunicações não possuem suficiência e pertinência para resguardar o indivíduo contra o acesso aos seus sistemas informáticos. [147]

No *decisum*, ficou destacado que para o enfrentamento dos novos riscos ao livre desenvolvimento da personalidade advindos da era tecnológica, relacionados ao uso de computadores e sistemas informáticos, seria necessário o desenvolvimento de um novo direito fundamental, derivado do "direito geral da personalidade". Ademais, ressaltou-se que o direito atingido, no presente caso, não era o de autodeterminação informacional, visto que o campo de abrangência da infiltração *online* não se limita aos dados privados do usuário, sendo bem mais amplo. [148]

A Corte ressaltou que, para a maioria das pessoas, o uso da *internet* é fundamental em suas vidas e é uma forma importante de desenvolver e expressar sua personalidade, entretanto, a dependência crescente de dispositivos conectados à rede também apresenta novos riscos ao desenvolvimento pessoal dos indivíduos, de modo que, os dados pessoais armazenados nos próprios dispositivos, os usuários também deixam dados e informações relacionados ao seu comportamento em servidores e intermediários.[149]

Concluiu-se que a proteção dos direitos fundamentais não estava adequada diante dos avanços tecnológicos, sociais e econômicos, e que era necessária uma nova abordagem

---

[146] Idem, p. 109.
[147] GRECO, Luís; GLEIZER, Orlandino. **A infiltração online no processo penal** – Notícia sobre a experiência alemã. In: Revista Brasileira de Direito Processual Penal, Porto Alegre, vol. 5, n. 3, p. 1483-1518, set./dez. 2019, p. 1491-1492. Dispónivel em: https://doi.org/10.22197/rbdpp.v5i3.278. Acesso em: 03 mai 2023.
[148] Idem, p. 1492-1493
[149] ABEL, W; SCHAFER, B. **The German Constitutional Court on the Right in Confidentiality and Integrity of Information Technology Systems**. in V Madhuri (ed.), Hacking: A Legal Quandary. Icfai University Press. Disponível em: https://www.pure.ed.ac.uk/ws/portalfiles/portal/15050731/The_German_Constitutional_Court_on_the_Right_in_Confidentiality_and_Integrity_of_Information_Technology_Systems.pdf. Acesso em: Acesso em: 03 mai. 2023. p. 117.

jurídica para a proteção aos direitos à personalidade, como garantia de liberdade, que precisava ser levada em consideração à luz das novas possibilidades tecnológicas.[150]

O Tribunal Constitucional, desse modo, não criou um direito, mas desenvolveu o direito constitucional existente para enfrentar as mudanças tecnológicas e sociais, criando uma nova concepção do direito geral de personalidade.[151]

Portanto, ficou estabelecido que o direito fundamental à proteção da privacidade, intimidade e autodeterminação informativa não se limita apenas à proteção de dados pessoais em si, mas também abrange a proteção dos sistemas técnicos que os armazenam e processam.[152] Isso significa que o Estado e outros agentes não podem violar a integridade e a confidencialidade desses sistemas sem uma justificativa legítima e sem os devidos procedimentos legais e técnicos. Essa decisão tem implicações importantes para o desenvolvimento da tecnologia da informação e para a proteção dos direitos fundamentais na era digital, pois reconhece a importância dos sistemas técnicos como parte integrante da esfera de privacidade e proteção de dados dos indivíduos.

Dessa maneira, a decisão da Corte alemã, que declarou a invalidade do §5.2 da Lei sobre a Proteção da Constituição na Renânia do Norte-Vestefália por contrariar a Constituição, evidenciou a insuficiência do conjunto de direitos existentes para garantir a proteção dos direitos constitucionais dos cidadãos diante da possibilidade de restrição de liberdades decorrente da utilização das buscas remotas em computadores.[153]

O reconhecimento do direito fundamental à garantia da confidencialidade e integridade dos sistemas informativos, assegura os sistemas informáticos de intromissões indesejadas que não eram garantidas por outros direitos fundamentais, como a confidencialidade das correspondências, correios e telecomunicações. Além disso, é uma atualização necessária da proteção da personalidade diante da realidade tecnológica atual do século XXI, destacando o Tribunal Constitucional Federal a importância que os sistemas

---

[150] HOFFMANN-RIEM, Wolfgang. **Innovaciones en la Jurisprudencia del Tribunal Constitucional Alemán, a Propósito de la Garantía de los Derechos Fundamentales en Respuesta a los Cambios que Conducen a la Sociedad de la Información**. Direito Público, 12(64). Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/2557. Acesso em: 03 mai. 2023. p. 52

[151] Idem,. p. 52.

[152] MENKE, Fabiano. **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 2019. Disponível em: <https://www.cidp.pt/revistas/rjlb/2019/1/2019_01_0781_0809.pdf>. Acesso em: 30 abr. 2023. p.782.

[153] ABEL, W; SCHAFER, B. **The German Constitutional Court on the Right in Confidentiality and Integrity of Information Technology Systems**. in V Madhuri (ed.), Hacking: A Legal Quandary. Icfai University Press. Disponível em: https://www.pure.ed.ac.uk/ws/portalfiles/portal/15050731/The_German_Constitutional_Court_on_the_Right_in_Confidentiality_and_Integrity_of_Information_Technology_Systems.pdf. Acesso em: Acesso em: 03 mai. 2023. p. 110.

informáticos adquiriram na formação da personalidade do indivíduo nos últimos anos, algo que não era previsto anteriormente.[154]

Assim, faz-se importante que os sistemas de tecnologia da informação sejam projetados de forma a garantir a confidencialidade e integridade dos dados. E isso se dá em decorrência da capacidade de que a autoridade investigadora tem de coletar dados criptografados de forma não criptografada, já que é possível acessar os dados enquanto o usuário os digita, ademais, é possível obter senhas e outras informações sobre o padrão de uso do suspeito, o que dificilmente seria alcançado com métodos de investigação tradicionais.[155]

O Tribunal Constitucional alemão enfatizou que confiar apenas no cumprimento dos princípios do estado de direito não é suficiente e que a precisão e a seriedade da declaração de conformidade devem ser verificadas pelo BND. Se houver dúvidas sobre o cumprimento do estado de direito, a transmissão de dados não deve ser permitida[156].

Por conseguinte, observa-se que o Tribunal Constitucional Federal não estabeleceu o direito à garantia da confidencialidade e integridade dos sistemas técnico-informacionais de forma absoluta, permitindo intervenções para fins preventivos e persecução criminal, desde que respeitados requisitos específicos.[157]

Sendo um destes requisitos a "prognóstico de perigo" (*Gefahrenprognose*), que se caracteriza pela presença de uma probabilidade suficiente de que, em um futuro próximo e determinado, sem a intervenção do Estado, danos sejam causados a bens protegidos pela norma por meio de certas pessoas, e, para determinar o perigo concreto, três fatores são considerados: 1) as particularidades do caso em questão; 2) a proximidade temporal da transformação do perigo em dano efetivo; e 3) a conexão entre determinadas pessoas individuais como causadoras do dano iminente.[158]

---

[154] MENKE, Fabiano. **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 2019. Disponível em: <https://www.cidp.pt/revistas/rjlb/2019/1/2019_01_0781_0809.pdf>. Acesso em: 30 abr. 2023 p. 795.

[155] ABEL, W; SCHAFER, B. **The German Constitutional Court on the Right in Confidentiality and Integrity of Information Technology Systems**. in V Madhuri (ed.), Hacking: A Legal Quandary. Icfai University Press. Disponível em: https://www.pure.ed.ac.uk/ws/portalfiles/portal/15050731/The_German_Constitutional_Court_on_the_Right_in_Confidentiality_and_Integrity_of_Information_Technology_Systems.pdf. Acesso em: Acesso em: 03 mai. 2023. p. 109.

[156] KAPPLER, Katrin. **Consequences of the german constitutional court's ruling on germany's foreign intelligence service**: the importance of human rights in the cooperation of intelligence services. German Law Journal, 2022, p. 173–185. Disponível em: <https://doi.org/10.1017/glj.2022.12>. Acesso em: 03 mai. 2023. p. 12.

[157] MENKE, Fabiano. **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 2019. Disponível em: <https://www.cidp.pt/revistas/rjlb/2019/1/2019_01_0781_0809.pdf>. Acesso em: 30 abr. 2023. p. 801.

[158] Idem, p. 802.

Em outras palavras, não basta a existência lei restringindo o direito fundamental da confidencialidade e integridade de sistemas informáticos para situações específicas e pontuas, se fazendo necessário, ainda, a análise do caso concreto e a verificação da ameaça de perigo concreto ao bem jurídico para autorização da medida restritiva de direitos fundamentais.

Dessa forma, enaltece-se que o direito à confidencialidade e integridade dos sistemas informáticos, inclui a confidencialidade da própria comunicação, ou seja, a proteção contra o acesso por parte do Estado e terceiros, bem como, "a proteção contra a superação de obstáculos que protegem contra intrusões, bem como contra erros e manipulações."[159]

Para mais, observa-se que não há uma proteção autônoma do sistema informático, mas, apenas, na medida em que sua confidencialidade e integridade impliquem relevância para os direitos de personalidade, destarte.[160]

> A proteção de dados visada pela proteção do sistema informático estende-se também aos dados pessoais (dotados de relevância para a personalidade) armazenados na memória de trabalho e armazenados temporária ou permanentemente nos suportes de armazenamento do sistema (possivelmente apenas indiretamente)[161].

Diante desses sucessivos avanços tecnológicos que proporcionam cada vez mais capacidade de coleta de dados em larga escala, é essencial que se estabeleçam limites claros e garantias de proteção à privacidade dos indivíduos. A necessidade de segurança do Estado não pode justificar a violação indiscriminada dos direitos individuais.

É preciso buscar um equilíbrio entre a proteção da segurança nacional e a salvaguarda dos direitos fundamentais, como a privacidade e intimidade, tudo isso diante do constante aprimoramento de softwares e hardwares, que podem apresentar um alto índice, ou não, de proteção ao usuário, a depender dos seus conhecimentos técnicos.

O Tribunal Constitucional Federal Alemão estabelecer um novo direito fundamental de "tecnologia da informação" não é apenas uma questão de rotular antigos conceitos sob uma nova designação, mas ao contrário, representa uma resposta ampla e abrangente à necessidade de uma Lei de Informação para o século 21, abordando as preocupações de privacidade levantadas pelo rápido desenvolvimento tecnológico[162].

---

[159] HOFFMANN-RIEM, Wolfgang; RIBEIRO, Pedro Henrique. A proteção de direitos fundamentais da confidencialidade e da integridade de sistemas próprios de tecnologia da informação. **Revista de Direito Civil Contemporâneo-RDCC (Journal of Contemporary Private Law)**, v. 23, p. 329-365, 2020, p. 339.
[160] Idem, p. 339.
[161] Idem, p. 339.
[162] TOGIAS, Stavros. **The right in confidentiality and integrity of information technology systems according to the german federal constitutional court**: 'old wine in new bottles'?, 2010. Disponível em:

Também é importante que os indivíduos tenham acesso a informações claras e precisas sobre seus direitos em relação aos dados pessoais e sobre como esses dados são coletados e usados.

Ver-se-á que tal responsabilização pelo desafio de viabilizar o direito de inteligência é exclusiva do Estado, ao passo que, é de incumbência do legislativo, executivo e judiciário promover mudanças diante dos sucessivos avanços tecnológicos para zelar pela justiça, mas, resguardando sempre o bem comum e o interesse dos cidadãos.[163]

Ressalta-se a necessidade de medidas efetivas de proteção de dados pessoais e integridade dos sistemas de informação, bem como a importância da supervisão judicial adequada para garantir que essas medidas sejam aplicadas de forma justa e equilibrada, e que as medidas de segurança não comprometam a privacidade dos usuários, tampouco seu direito a personalidade.

3. DISPOSIÇÕES LEGAIS SOBRE *MALWARE* NO *StPO* (CÓDIGO DE PROCESSO PENAL ALEMÃO)

Após a decisão de 2008 do Tribunal Constitucional Alemão, que consagrou o direito fundamental à confidencialidade e integridade dos sistemas informáticos, estabelecendo preceitos para as intervenções estatais restritivas de direitos fundamentais, várias alterações ocorreram em diversas legislações no estado alemão, com a finalidade de adequa-las aos novos contornos constitucionais de proteção de dados e sistemas informáticos.

Em termos de metodologias investigativas, a alteração mais significativa ocorreu na BKAG (*Bundeskriminalamtgesetz*), que foi atualizada, trazendo novamente para o ordenmento jurídico alemão a possibilidade de utilização de *malware* para fins de combate ao terrorismo. Por meio do seu § 20k e seguintes, foram fixadas diretrizes para uso exepcional da referida tecnologia de infiltração em sistemas informáticos.[164]

Acontece que posteriormente a isso, no ano de 2011, o grupo ativista *Chaos*

https://conferences.ionio.gr/isil2010/download.php?f=papers/togias_stavros_full.pdf. Acesso em: 03 mai. 2023. p. 8.

[163] HOFFMANN-RIEM, Wolfgang. **Innovaciones en la Jurisprudencia del Tribunal Constitucional Alemán, a Propósito de la Garantía de los Derechos Fundamentales en Respuesta a los Cambios que Conducen a la Sociedad de la Información**. Direito Público, 12(64). Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/2557. Acesso em: 03 mai. 2023. p. 48.

[164] RIBOLI, Eduardo Bolsoni. "Eu sei o que vocês fizeram no verão passado": o uso de software de espionagem como meio de obtenção de prova penal. In: **Revista Brasileira de Ciências Criminais**, São Paulo, v. 27, n. 156, p. 91-139, jun. 2019, p. 100.

Computer Club (*CCC*) noticiou na mídia que a polícia alemã estaria utilizando indevidamente em suas investigações na *internet,* sem autorização judicial, uma espécie de cavalo de troia, com mais funcionalidades e maior potencial lesivo denominado de *Bundestrojaner*, que teria a capacidade, inclusive, de monitorar em tempo real as ativiades dos investigados na *internet*. Isso inclui gravação de chamadas, capturas de senhas, ativação da *webcam* e microfone do visado.[165]

No ano de 2016, a *BKAG* foi submetida ao crivo do Tribunal Constitucional Alemão (*BVerfG*), tendo sido declarada a desconformidade do seu §20k e seguintes com os direitos fundamentais, visto que não atendiam ao princípio da proporcionalidade e não respeitavam o núcleo interno de proteção da vida privada. Assim, em 2017 a *BKAG* foi revisada, tendo sido introduzido o §49, que atualmente é o dispositivo legal que autoriza as "buscas *online*" para fins de prevenção e combate ao terrorismo na Alemanha.[166]

No que tange às investigações criminais, foi apenas em 2017 que o Código de Processo Penal alemão - *Strafprozessordnung* "*StPO*" passou a prever formalmente a possibilidade de infiltração *online* por *malware* em sistemas informáticos. Assim, apesar de se ter notícias de que eram realizadas "buscas *online*", em datas bem anteriores, em investigações criminais, a positivação em lei deste método oculto só se deu em momento posterior.

São quatro os dispositivos do *StPO* que tratam de *malware*. O primeiro é o §100b[167], que estabalece a famosa *online-durchsuchungs* ou "busca *online*". O segundo é o §100a, n° 1, parágrafo não numerado[168], que estabelece a *quellen-tku* ou "vigilância na fonte". O terceiro é o §100c[169] que trata da vigilância ambiental dentro do domicílio do suspeito. O

---

[165] Idem.

[166] Idem, p. 100-102.

[167] ALEMANHA. ***Strafprozessordnung* "*StPO*"**. §100b: Mesmo sem o conhecimento da pessoa em causa, podem ser utilizados meios técnicos para interferir com um sistema informático utilizado pela pessoa em causa e podem ser recolhidos dados a partir deste (pesquisa em linha) se: (1) Certos factos suscitam a suspeita de que um autor ou participante cometeu uma infracção penal particularmente grave referida no n.o 2 ou, nos casos em que a tentativa é punível, tentou cometê-la; (2) a infracção for particularmente grave em casos individuais, e (3) A investigação dos factos ou a determinação do paradeiro do arguido seriam, de outro modo, significativamente mais difíceis ou inúteis [tradução livre]. Disponível em: dejure.org/gesetze/StPO/100b.html. Acesso em: 15/03/2023.

[168]ALEMANHA. ***Strafprozessordnung* "*StPO*"**. §100a, n°1, p. não numerado: A vigilância e o registo das telecomunicações podem igualmente ser efetuados de modo a que sejam utilizados meios técnicos para interferir com os sistemas informáticos utilizados pelo interessado, se tal for necessário para permitir o controlo e o registo, nomeadamente sob forma não codificada. 3Em Os conteúdos e as circunstâncias da comunicação armazenada no sistema informático da pessoa em causa podem ser controlados e registados se puderem ter sido monitorizados e registados de forma cifrada durante o processo de transmissão em curso na rede pública de telecomunicações [tradução livre]. Disponível em: dejure.org/gesetze/StPO/100b.html. Acesso em: 15/03/2023.

[169] ALEMANHA. ***Strafprozessordnung* "*StPO*"**. §100c: Mesmo sem o conhecimento das pessoas em causa, a palavra não falada publicamente numa habitação pode ser interceptada e registada por meios técnicos se: 1) certos factos suscitam a suspeita de que alguém, na qualidade de autor ou participante, cometeu uma infracção penal

quarto e último dispositivo é o §100f[170] que trabalha a hipótese de vigilânca ambiental fora do domicílio.

Pela letra fria da lei, percebe-se que o ordenamento jurídico alemão trata das várias possibilidades de aplicabilidade do *malware* de forma espaçada e desarmônica, sem estabelecer um regime geral e próprio para a temática, proporcionando uma confusão com as demais categorias de medidas ocultas de investigação. Para além disso, destaca-se a imprecisão técnica do legislador alemão, que nos quatro dispositivos legais referentes à supracitada metodologia investigativa, utiliza-se do genérico termo "meios técnicos", ocasionando uma amplitude desnecessária ao conceito, de modo a possibilitar que outros *softwares* possam ser utilizados ao invés de, propriamente, o *malware*. Assim, tem-se que seria preferível a precisa adoção do termo *malware*.

Dito isto, o intuito do presente tópico não será, propriamente, percorrer por cada dispositivo legal, ou melhor, por cada medida oculta investigativa que autoriza o uso do *malware* na Alemanha, como também não se tem a intenção de analisar pormenorizadamente cada tipo penal em que o uso do *malware* é autorizado. Pelo contrário, a presente análise será voltada a verificar as principais características das normas habilitantes sobre o tema na ordem alemã, com ênfase na funcionalidade da *online-durchsuchungs* ou "busca *online*" (§100b), tanto pela sua capacidade de realizar verdadeiro monitoramento *online* do investigado, como também por ter sido intoduzida, diferentemente das demais funcionalidades, em dispositivo legal diverso das já conhecidas técnicas ocultas de interceptação de comunicações e escutas (captações) ambientais.

Diversas medidas investigativas no processo penal alemão estão condicionadas ao preenchimento do requisito da suspeita do fato para sua execução. Assim, a depender do nível de intrusão da medida e da fase processual em que a persecução criminal se encontra, diferentes graus são exigidos. São três os graus de suspeita, quais sejam, suspeita inicial,

particularmente grave referida no n.º 100 do artigo 2.º-B ou, nos casos em que a tentativa é punível, tentou cometê-la; 2) a infracção for particularmente grave, mesmo em casos individuais; 3) pode presumir-se, com base em elementos de facto, que a vigilância abrangerá declarações prestadas pelo arguido que sejam relevantes para a investigação dos factos ou para a determinação do paradeiro de um co-arguido, e 4) A investigação dos factos ou a determinação do paradeiro de um co-arguido seria, de outro modo, desproporcionadamente difícil ou inútil [tradução livre]. Disponível em: dejure.org/gesetze/StPO/100b.html. Acesso em: 15/03/2023.

[170] ALEMANHA. ***Strafprozessordnung* "*StPO*"**. §100f: Mesmo sem o conhecimento das pessoas em causa, a palavra não falada publicamente pode ser interceptada e gravada fora dos lares por meios técnicos se certos factos suscitarem a suspeita de que alguém cometeu uma infracção penal referida no n.º 100 do artigo 2.º-A, que também é grave em casos individuais, na qualidade de autor ou participante, ou tentou cometê-la nos casos em que a tentativa é punível, e a investigação dos factos do caso ou a determinação do paradeiro de um arguido seria, de outro modo, inútil ou significativamente mais difícil [tradução livre]. Disponível em: dejure.org/gesetze/StPO/100b.html. Acesso em: 15/03/2023.

suspeita forte e suspeita suficiente.[171]

Suspeita forte é aquela em que há grande probabilidade de que o imputado tenha praticado o crime, enquanto a suspeita suficiente é verificada ao término dos procedimentos investigatórios e impõe a propositura da denúncia. Já a suspeita inicial, como o próprio termo sugere, é aquela que apenas impõe o início das investigações, em razão da verificação da procedência dos elementos iniciais colhidos.[172]

No que tange à *online-durchsuchungs*, o item n°1 do §100b *StPO* não estabelece o nível de suspeita do fato que se exige para sua execução. Contudo, apesar de o legislador ter sido omisso e não ter delimitado o grau de suspeita exigido, o *BVerfG* se referindo à semelhante método oculto, entende que a suspeita precisa ser maior do que uma mera suspeita inicial, a fim de autorizar a medida investigativa. O *BGH*, por sua vez, é menos cauteloso e afirma a desnecessidade de uma suspeita forte ou suficiente, contentando-se com a suspeita simples.[173]

O certo é que meras suposições ou especulações não verificadas são insuficientes para legitimar a utilização de metodologias ocultas investigativas no processo penal alemão. Sendo necessária a existência de base fática sólida, apoiada em circunstâncias concretas, como depoimentos de testemunhas, observações ou outros indícios fáticos relacionados ao caso e, a suspeita deve estar embasada em circunstâncias que indiquem, em grau significante, o cometimento de um dos crimes constantes do catálogo de crimes. Sem tais elementos mínimos não haverá que se falar em aptidão da suspeita para autorização de medida oculta investigativa.[174]

Para além disso, destaca-se que a execução de qualquer medida oculta só será constitucionalmente legítima se for pautada pela existência de evidências concretas de um perigo iminente para um interesse legítimo de importância predominante, em que, interesses predominantes incluem a vida, a integridade física e a liberdade individual, bem como interesses públicos, tais como ameaças à existência do Estado ou à existência humana, como a funcionalidade de instalações essenciais de abastecimento.[175]

---

[171] GRECO, Luís; GLEIZER, Orlandino. **A infiltração online no processo penal** – Notícia sobre a experiência alemã. Revista Brasileira de Direito Processual Penal, Porto Alegre, vol. 5, n. 3, p. 1483-1518, set./dez. 2019. Disponível em: https://doi.org/10.22197/rbdpp.v5i3.278. Acesso em: 03 mai. 2023. p. 1498-1499.
[172] Idem, p. 1498-1499
[173] Idem, p. 1498-1499
[174] Idem. p. 1499-1500.
[175] TOGIAS, Stavros. **The right in confidentiality and integrity of information technology systems according to the german federal constitutional court**: 'old wine in new bottles'?, 2010. Disponível em: https://conferences.ionio.gr/isil2010/download.php?f=papers/togias_stavros_full.pdf. Acesso em: 03 mai. 2023. p. 10.

Assim, se por um lado, uma exigência menor de suspeita pode facilitar a autorização da *online-durchsuchungs* ou "busca *online*", permitindo que as autoridades tenham mais liberdade para investigar suspeitos. Por outro, pode aumentar o risco de abusos por parte das autoridades, especialmente se a suspeita não estiver fundamentada em fatos ou se basear em meros boatos ou suposições não verificadas.

Portanto, é importante que a autorização da *online-durchsuchungs* seja sempre acompanhada de medidas adequadas de controle e fiscalização, a fim de garantir que ela seja utilizada de forma proporcional e respeitando os direitos dos investigados.

Um outro requisito imprescindível é a necessidade de existir um catálogo de crimes, limitando, assim, os efeitos da investigação aos crimes previstos no catálogo, o qual funciona como norma autorizativa para a utilização do *malware*. Ademais, a seleção dos crimes constantes neste taxativo rol deve ser pautada por critérios de proporcionalidade, de modo que apenas crimes especialmente graves possam ser alvo de medidas tão invasivas.[176]

A existência de um catálogo restritivo ajuda a evitar abusos e a proteger os direitos fundamentais dos cidadãos. Ao mesmo tempo, ele também permite que a aplicação do *malware* seja efetiva em casos extremos. É importante destacar, no entanto, que a aplicação da referida metodologia deve ser feita com base em critérios objetivos e transparentes, a fim de garantir que não seja utilizada de forma arbitrária ou abusiva.

Assim, em relação à *online-durchsuchungs*, o legislador alemão no §100b, n° 2 *StPO*, estabeleceu um extenso rol de crimes, que abrange diversos tipos de delitos, como por exemplo, fraude informática, crimes de traição, de formação de organização criminosa, crimes contra a autodeterminação sexual, dentre outros.

Outra condição para autorização de infiltração *online* por *malware* consiste na gravidade do caso concreto, em que norma autorizativa, estabelecida pelo legislador, não apenas considerou a gravidade abstrata do crime, ou seja, se ele está incluído no catálogo de crimes especialmente graves, mas também a sua gravidade concreta.[177]

Outro pressuposto da autorização de infiltração *online* por *malware* consiste na necessidade de se avaliar a gravidade do caso em concreto, sendo dever não apenas do legislador estabelecer o rol de crimes suscetíveis de infiltração, com base na proporcionalidade,

[176] GRECO, Luís; GLEIZER, Orlandino. **A infiltração online no processo penal** – Notícia sobre a experiência alemã. Revista Brasileira de Direito Processual Penal, Porto Alegre, vol. 5, n. 3, p. 1483-1518, set./dez. 2019. Disponível em: https://doi.org/10.22197/rbdpp.v5i3.278. Acesso em: 03 mai. 2023. p. 1500.
[177] Idem, p. 1501.

mas também do julgador analisar as circunstâncias especiais do caso e avaliar se é proporcional aplicar a medida investigativa ao caso, tendo-se em vista as especificidades dele.[178]

Isso significa que a medida deve estar baseada nas circunstâncias específicas em que o crime ocorreu, e a exigência de gravidade abstrata é uma concretização do princípio da proporcionalidade, imposta ao legislador, a exigência de demonstração da gravidade concreta é o seu efeito em relação ao juiz.[179]

O quarto pressuposto é a subsidiariedade, compreendida pelo fato de que o *malware* só pode ser autorizado em casos em que a investigação dos fatos ou do local onde se encontre o afetado esteja impossibilitada ou fundamentalmente dificultada.[180]

Essa exigência tem por objetivo evitar que medidas excessivamente invasivas sejam adotadas quando existem outras menos invasivas disponíveis, como a busca e apreensão, logo, essa medida requer, portanto, um estado de necessidade probatório, em outras palavras, outras medidas devem ter sido esgotadas ou terem se mostrado ineficazes para obter a informação pretendida.[181]

Significa que essa técnica só pode ser utilizada quando as investigações convencionais se mostram ineficazes ou inviáveis para obter as informações necessárias para a resolução do caso. Isso significa que a infiltração online deve ser vista como uma medida excepcional, que só pode ser usada quando todas as outras alternativas se esgotaram.

Se apresenta ainda, como requisito, a proporcionalidade em sentido estrito, que pode ser entendida como a capacidade tanto do legislador quanto do executor da lei de verificar, antes e durante a execução da medida, se a intervenção é adequada em relação aos resultados pretendidos ou à culpabilidade do afetado[182]. É necessário que o monitoramento dos sistemas informáticos seja controlado de forma proporcional e utilizado, apenas, como última opção por órgãos investigativos, já que lei de *Nordrhein-Westfalen* foi considerada inconstitucional pelo Tribunal Constitucional Federal por não atender ao postulado da proporcionalidade em sentido estrito, o qual exige que a gravidade da intervenção a um direito seja ponderada em relação às razões pelas quais está ocorrendo, sem que haja uma desproporção insustentável.[183]

---

[178] Idem, p. 1501.
[179] Idem, p. 1501
[180] Idem, p. 1501
[181] Idem, p. 1502.
[182] GRECO, Luís; GLEIZER, Orlandino. **A infiltração online no processo penal** – Notícia sobre a experiência alemã. Revista Brasileira de Direito Processual Penal, Porto Alegre, vol. 5, n. 3, p. 1483-1518, set./dez. 2019. Disponível em: https://doi.org/10.22197/rbdpp.v5i3.278. Acesso em: 03 mai. 2023. p. 1502.
[183] MENKE, Fabiano. **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 2019. Disponível em: <https://www.cidp.pt/revistas/rjlb/2019/1/2019_01_0781_0809.pdf>. Acesso em: 30 abr. 2023. p. 802.

Em síntese, o Tribunal Constitucional Federal deixou claro que o direito à garantia da confidencialidade e integridade dos sistemas informáticos só pode ser imposta por meio de lei especial, que deve ser clara, precisa e proporcional. A reserva legal é um princípio fundamental, garantindo a segurança jurídica e a previsibilidade para os cidadãos.

O amplo monitoramento dos sistemas informáticos previsto na lei foi considerado pelo Tribunal como uma violação aos direitos fundamentais, sendo inconstitucional quando comparado ao interesse público de investigação, previsto na legislação.

Nesse sentido, é necessário considerar uma variedade de fatores, como a possibilidade de obtenção de informações não relacionadas ao caso em questão, ou um grande intervalo de tempo entre a ocorrência do fato e a implementação da medida, o que pode sugerir que o afetado não possui mais evidências relevantes em seu dispositivo eletrônico.[184]

E, por fim, se tem como pressuposto autorizador da infiltração *online,* a delimitação do possível afetado pela medida, uma vez que, apesar desta ser direcionada apenas ao investigado, ainda assim pode ser autorizada, caso exista a possibilidade de acesso inevitável a informações relacionadas a terceiros não envolvidos.[185]

Os sistemas informáticos contemporâneos dificilmente contêm informações exclusivamente do usuário principal, já que os sistemas informáticos de terceiros também podem ser alvo da medida, se forem utilizados pelo investigado (mesmo sem o consentimento do terceiro). No entanto, tal situação apenas ocorre se a execução da medida contra o investigado não for suficiente para esclarecer os fatos ou para localizar um co-investigado, logo, familiares, amigos, vizinhos e até mesmo a vítima do crime são exemplos de terceiros afetados.[186]

Outro exemplo de sistema informático de terceiros são os serviços de armazenamento em nuvem, que normalmente pertencem a empresas privadas, e a infiltração *online* de nuvens também levanta questões de cooperação jurídica internacional, já que esses sistemas privados são geralmente hospedados fisicamente em diferentes países.[187]

A infiltração por *malware* é uma medida investigatória que tem causado muita controvérsia nos últimos anos. Trata-se de uma técnica utilizada pelos órgãos de segurança

[184] GRECO, Luís; GLEIZER, Orlandino. **A infiltração online no processo penal** – Notícia sobre a experiência alemã. Revista Brasileira de Direito Processual Penal, Porto Alegre, vol. 5, n. 3, p. 1483-1518, set./dez. 2019. Disponível em: https://doi.org/10.22197/rbdpp.v5i3.278. Acesso em: 03 mai. 2023. p. 1502.
[185] Idem. p. 1503.
[186] Idem. p. 1503.
[187] Idem, p. 1503.

pública para monitorar o comportamento de suspeitos em ambientes virtuais, como redes sociais, aplicativos de mensagens e fóruns na internet.

A lei deve respeitar a proporcionalidade, que implica que as restrições aos direitos fundamentais devem ser necessárias e adequadas para atingir o objetivo visado, sem ir além do necessário e, isso significa que a intervenção nos sistemas técnico-informacionais deve ser a última opção, a fim de evitar que as medidas adotadas sejam excessivas ou desproporcionais em relação à finalidade pretendida.[188]

A clareza e a precisão normativas são igualmente importantes, pois a lei deve ser clara o suficiente para permitir que os indivíduos possam entender quais são as suas obrigações e quais são os seus direitos em relação à utilização dos sistemas técnico-informacionais.[189] A falta de clareza ou precisão na lei pode levar a interpretações equivocadas ou abusos por parte das autoridades responsáveis pela sua implementação.

Em geral, dados pessoais não devem ser coletados, a menos que sejam dados relevantes em termos legais. No entanto, para verificar ou falsificar essa relevância, eles devem ser coletados em primeiro lugar - em caso de suspeito.[190] E, se os dados pessoais coletados se mostrarem irrelevantes, eles devem ser excluídos imediatamente e, acima de tudo, não podem ser apresentados a um tribunal como evidência. Isso comprova que não existe uma área de privacidade absolutamente protegida. Somente dados absolutamente desinteressantes desfrutam de proteção absoluta.[191]

Essa técnica só pode ser autorizada em casos específicos, como quando outras medidas menos invasivas não são suficientes para a elucidação dos fatos. Além disso, é necessário que haja uma ordem judicial para que a infiltração por *malware* possa ser realizada, garantindo assim o respeito aos direitos fundamentais do cidadão.

Para evitar o uso abusivo da infiltração *online,* o aplicador da lei deve avaliar a proporcionalidade da medida antes e durante sua execução. Além disso, a medida só pode ser direcionada ao investigado, mas também pode ser autorizada se houver expectativa de obter informações de terceiros não-implicados. Devido à complexidade e aos riscos associados a essa

---

[188] MENKE, Fabiano. **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 2019. Disponível em: <https://www.cidp.pt/revistas/rjlb/2019/1/2019_01_0781_0809.pdf>. Acesso em: 30 abr. 2023. p. 798

[189] Idem, p. 798.

[190] ENDERS, Christoph. **The Right to have Rights**: The concept of human dignity in German Basic Law. Revista de Estudos Constitucionais, Hermenêutica e Teoria do Direito. 2018. Disponível em: <https://dialnet.unirioja.es/descarga/articulo/5007582.pdf>. Acesso em: 03 mai. 2023. p. 6.

[191] Idem, p. 6.

técnica, é fundamental que os agentes de segurança sejam capacitados e treinados para lidar com essas situações.

A infiltração *online* é uma medida investigatória que exige grande cuidado e responsabilidade por parte dos órgãos de segurança pública. É necessário que ela seja utilizada com parcimônia e somente em situações excepcionais, garantindo assim a preservação dos direitos fundamentais dos cidadãos.[192]

Tanto a polícia quanto as agências de inteligência devem atender aos requisitos que exigem evidências factuais de um perigo concreto para um bem jurídico de grande importância, esses bens jurídicos são principalmente a vida, a integridade física e a liberdade individual, bem como os de interesses público que, se ameaçados, afetam a base ou a continuidade da existência do Estado ou da vida humana.[193]

Por fim, é importante lembrar que a infiltração *online* é uma técnica que está em constante evolução, e que é necessário que as autoridades estejam sempre atualizadas e capacitadas para lidar com as novas tecnologias e estratégias utilizadas pelos suspeitos na *internet*.

4. A PREVISÃO DO *MALWARE* EM OUTROS ORDENAMENTOS: ESPANHA E ITÁLIA

Dando sequência ao proposto, neste tópico serão analisadas as experiências da Espanha e da Itália acerca do uso do *malware* nas suas investigações criminais. A opção por estes dois países se deu com base em suas localizações geográficas, no sistema jurídico adotado – *civil law* -, bem como pelo fato de a referida metodologia investigativa já ter sido positivada em seus ordenamentos jurídicos, assim como ocorre na Alemanha. Destaca-se, pois, que no presente tópico apenas breves apontamentos serão feitos, não sendo o escopo do presente esmiuçar todos os detalhes de aplicabilidade do *malware* nas referidas ordens jurídicas, assim como se fez preteritamente em relação ao ordenamento alemão.

---

[192] MENKE, Fabiano. **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 2019. Disponível em: <https://www.cidp.pt/revistas/rjlb/2019/1/2019_01_0781_0809.pdf>. Acesso em: 30 abr. 2023. p. 807.

[193] HORNUNG, G., SCHNABEL, C. **Data protection in Germany I**: The population census decision and the right to information self-determination. Computer Law & Security Report, vol. 25, número 1, 2009. Disponível em: https://www.unikassel.de/fb07/index.php?eID=dumpFile&t=f&f=566&token=982b30547e56fb9f2eb130a7b27c177d774c20e2. Acesso em: 30 abr. 2023. p. 5.

Na Espanha, o recurso ao *malware* é resultado da Lei Orgânica 13/2015, que introduziu no processo penal espanhol novas metodologias investigativas, estando o *malware* disposto nos termos do atual artigo 588 *septies a*[194], da *Ley de Enjuiciamiento Criminal*, sob o nome de "*registros remotos sobre equipos informáticos*".[195]

Antes disso, o uso do *malware* como meio de obtenção de provas em processos penais não era legalmente previsto na legislação espanhola. No entanto, ao longo dos anos, a jurisprudência começou a admitir seu uso com base nas regras das buscas tradicionais, especialmente, através da analogia em relação a lei das interceptações de comunicações eletrônicas, à luz da jurisprudência do Supremo Tribunal e do Tribunal Constitucional da Espanha.[196] Esse movimento levou o Tribunal Europeu dos Direitos Humanos (TEDH) a condenar o Estado espanhol, considerando que a utilização de *malware* violava os direitos fundamentais protegidos pela Convenção Europeia dos Direitos Humanos.[197]

A nova legislação supracitada incluiu um capítulo específico para tratar do *malware* e de formas semelhantes de investigação. Regulou tal prática detalhadamente, trazendo seus pressupostos, período de duração, requisitos, além de prever o dever de colaboração de terceiros (fornecedores de serviço).[198]

A utilização deste meio de obtenção de prova só poderá ser autorizada pelo juiz instrutor em casos específicos e mediante determinadas condições.[199]Assim, a decisão do juiz que autoriza o uso do *malware* como meio de acesso de prova deve conter especificações claras sobre os dispositivos técnicos que serão acessados, mencionar os dados que serão objeto de investigação, além de outros conteúdos digitais relevantes para o caso. Ademais, deve delimitar o âmbito no qual será realizada e a maneira de proceder, o *software* que será utilizado para acessar as informações, os agentes competentes que serão autorizados para a execução, o

---

[194] ESPANHA. **Ley de Enjuiciamento Criminal**. Art. 588 septies a: 1. O juiz competente pode autorizar a utilização de dados e códigos de identificação, bem como a instalação de programas informáticos que permitam, à distância e por telematicamente, o exame à distância e sem o conhecimento do seu proprietário ou utilizador do conteúdo de um computador, dispositivo eletrónico, sistema informático, instrumento de armazenamento em massa de dados informáticos ou base de dados, desde que prossiga a investigação de qualquer um dos seguinte (tradução livre) [...]. Disponível em: www.conceptosjuridicos.com/lecrim-articulo-588-septies-a/. Acesso em: 20/09/2022.

[195] NUÑEZ, Eloy Velasco, ADSL y **Troyanos: Intervención de sus datos y telecomunicaciones en la investigación penal**, La Ley Penal, nº 82, 2011, p. 24.

[196] Idem, p. 24.

[197] RAMALHO, David Silva. O uso de *malware* como meio de obtenção de prova em processo penal, In: **Revista de concorrência e regulação**, Lisboa, Ano 4, nº 16, 2013, p. 220-221.

[198] RAMALHO, David Silva, **Métodos ocultos de investigação criminal em ambiente digital**. Coimbra: Editora Almedina, 2017, p. 333-334.

[199] ESPANHA. **Ley Organica 13/2015**. Disponível em: http://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-10725. Acesso em: 20/09/2022.

catálogo de crimes que se submetem a este tratamento, bem como os elementos necessários para garantir a integridade, autenticidade e inacessibilidade dos dados acessados.[200]

Essas especificações são necessárias para delimitar o escopo da intervenção autorizada judicialmente. Ao indicar os sistemas, dispositivos e meios de processamento específico, bem como os dados ou conteúdos digitais relacionados à investigação, o despacho garante que a intervenção seja direcionada e proporcional à finalidade da investigação em curso, que, segundo a norma espanhola, não poderá ultrapassar três meses.[201]

Além do exposto, é importante mencionar o projeto feito pela Comissão Europeia e a *International Telecommunication Union*, no ano de 2008, referente a *Harmonization of ICT Policies, Legislation and Regulatory Procedures in the Caribbean* (HIPCAR), o qual tem como objetivo central uniformizar a legislação sobre tecnologia informacional de todos os países pertencentes ao CARICOM - Comunidades das Caraíbas. Deste projeto, surgiu uma minuciosa legislação sobre crime digital, chamada *Cybercrime/e-Crimes Model Policy Guidelines in Legislative Texts*, a qual prevê a utilização do *malware* na investigação criminal. A norma estabelece certos critérios que devem ser atendidos para o seu uso, tais como a indisponibilidade de outra forma de obtenção da prova, a obrigatoriedade de autorização prévia detalhada de um juiz e a necessidade de restrição da sua aplicação a casos específicos.[202]

No cenário Italiano, o método *malware* recebe o nome de *captatore informático* e encontra-se previsto no capítulo referente às interceptações de comunicação entre presentes, mais precisamente no art. 266, n° 2[203] e n° 2-*bis*[204] do *Codice de Procedura Penale*, tendo sido positivado no ordenamento jurídico italiano, após uma sequência de entendimentos jurisprudenciais divergentes sobre a matéria.

Pela sua localização topográfica na legislação, o recurso ao *malware* na Itália parece se limitar à recolha de prova externa ao dispositivo informático visado, funcionando como

---

[200] Idem.
[201] Idem.
[202] RAMALHO, David Silva. **Métodos ocultos de investigação criminal em ambiente digital.** Coimbra: Editora Almedina, 2017, p. 336.
[203] ITÁLIA. **Codice di Procedura Penale**. Art. 266, n° 2: Nos mesmos casos, é permitida a intercepção de comunicações entre os presentes, que pode igualmente ser efectuada através da inserção de um coletor informático num dispositivo electrónico portátil. No entanto, se ocorrerem nos locais indicados no artigo 614 do Código Penal, a interceptação só é permitida se houver motivos razoáveis para crer que a atividade criminosa está ocorrendo ali [tradução livre]. Disponível em: https://www.altalex.com/documents/news/2014/03/26/mezzi-di-ricerca-della-prova. Acesso em: 12/06/2022.
[204] ITÁLIA. **Codice di Procedura Penale**. Art. 266, n° 2-bis. Nos mesmos casos, é permitida a intercepção de comunicações entre os presentes, que pode igualmente ser efectuada através da inserção de um coletor informático num dispositivo electrónico portátil. No entanto, se ocorrerem nos locais indicados no artigo 614 do Código Penal, a interceptação só é permitida se houver motivos razoáveis para crer que a atividade criminosa está ocorrendo ali [tradução livre]. Disponível em: https://www.altalex.com/documents/news/2014/03/26/mezzi-di-ricerca-della-prova. Acesso em: 12/06/2022.

medida de interceptação ambiental. Não sendo admitida, portanto, a ativação das demais funcionalidades possíveis. Ademais, o referido método oculto, de acordo com a legislação italiana, só pode ser instalado em "dispositivos eletrônicos portáteis", excluindo-se a possibilidade de acesso remoto aos sistemas informáticos estáticos, a exemplo dos computadores.

Observa-se, pois, que o *malware* ou *captatore informático* na Itália tem usualidade bastante específica, havendo condições diferentes para o ingresso remoto no domicílio do visado, a depender do crime supostamente praticado por ele. O legislador italiano, preocupou-se com o direito fundamental à inviolabilidade domiciliar e fixou critérios diferentes para o recurso ao *malware*. Nos casos de terrorismo e criminalidade organizada, por exemplo, não se exige o requisito da "fundada suspeita" para utilização do mesmo. Diferentemente do que ocorre em outros tipos penais que também constam catalogados no rol de crimes suscetíveis de aplicação da referida metodologia.

Todavia, apesar de atualmente o uso do *captatore informático* na Itália ser restrito a hipótese de recolha de prova externa, vale salientar que no emblemático caso "*Virruso*" da Suprema Corte Italiana (*Corte Suprema di Cassazione*), datado de 2010, a referida metodologia investigativa foi utilizada como forma de monitoramento *online*, com o fim de recolher prova interna ao dispositivo informático do visado, o que não é mais possível de acordo com a sua atual regulamentação.

No caso em questão, o Ministério Público Italiano decretou a medida de busca e apreensão a ser realizada nos computadores da empresa responsável pelo fornecimento de água potável de *Villafrati*. Acontece que o *software* invasor utilizado tinha a habilidade de recolher todas as informações constantes dos sistemas informáticos infectados, tanto aquelas já armazenadas na memória, quanto aquelas produzidas em tempo real.[205]

Assim, após a realização da medida de busca e apreensão, fundamentada no art. 234 do Código de Processo Penal Italiano, e tendo-se em vista a devassa na vida privada dos investigados, as defesas se insurgiram alegando que a utilização do *malware* no mencionado caso deveria ter obedecido os tramites da norma sobre interceptação telefônica e telemática. Em outras palavras, pleiteou-se a inutilização dos elementos obtidos com a medida investigativa, sob a alegação de que o acompanhamento oculto e contínuo dos sistemas informáticos alvos se equipara a uma interceptação. De modo que o acesso remoto deveria ter sido precedido de

[205] ITALIA. **Cass. Pen. sez. V, 29 abril 2010, n. 16556**, Virruso. Disponível em: http://www.penale.it/stampa.asp?idpag=1228. Acesso em: 12/06/2022.

autorização judicial, contendo os procedimentos a serem observados, bem como o tempo de duração da medida.

Nessa esteira, na contramão das alegações defensivas, o Tribunal Italiano condenou os réus com base nas provas obtidas via acesso remoto aos dispositivos informáticos. O fundamento do *decisum* condenatório foi o de que o *software* espião não interveio no fluxo das comunicações, tendo ocorrido apenas uma captação unilateral dos elementos constantes nos sistemas alvos. Assim, a medida investigativa foi declarada legítima e as provas obtidas foram utilizadas na sentença, com base no art. 189 do Código de Processo Penal Italiano (*Codice de Procedura Penale*).

Posto isto, passaremos ao estudo do *malware* como método (a)típico na investigação criminal e suas consequências práticas.

III. DA (A)TIPICIDADE PROCESSUAL À PROPOSTA DE SISTEMATIZAÇÃO: MEDIDAS PARA UTILIZAÇÃO DO *MALWARE* NAS ORDENS JURÍDICAS DE BRASIL E PORTUGAL.

1. O USO *MALWARE* PODE SER ADMITIDO NO BRASIL E EM PORTUGAL ATRAVÉS DE ALGUM MEIO DE OBTENÇÃO DE PROVA JÁ REGULAMENTADO EM LEI?

De início, aponta-se que o ordenamento jurídico português não possui uma centralidade normativa em relação ao tema da prova digital, de modo que as medidas de obtenção de prova penal digital encontram-se espalhadas quer no Código de Processo Penal, quer em legislações extravagantes. São três os diplomas que versam sobre prova digital em Portugal, quais sejam, Código de Processo Penal, Lei n° 109/2009 (Lei do Cibercrime) e Lei n° 32/2008. Embora sejam muitos os diplomas legais existentes, nenhum deles faz referência expressa ao *malware*. Por outro lado, no Brasil, o que se observa é uma negligência procedimental referente ao tema da prova digital. Havendo apenas a Lei n° Lei nº 12.965 (Marco Civil da *Internet*), que estabelece regras para o uso da *internet* no país, bem como algumas leis extravagantes que trazem determinados métodos específicos de obtenção de prova penal no âmbito virtual. Não havendo assim como em Portugal, qualquer referência expressa ao *malware*.

Acontece que apesar de inexistir nas duas ordens jurídicas dispositivo legal específico prevendo o uso do *malware*, alguma doutrina brasileira e portuguesa, legitima sua utilização em proposições que se referem a outros métodos ocultos. Desta feita, neste tópico iremos verificar se o *malware* pode ser admitido no Brasil e em Portugal a partir de algum dos métodos ocultos já consagrados nas duas ordens jurídicas.

Inicialmente, é oportuno analisar a possibilidade de legitimação do *malware* no regime das buscas domiciliares à luz do que ocorre no Estados Unidos da América em que a supracitada metodologia investigativa é enquadrada no regime das buscas em lugares físicos. Aventa-se tal hipótese, uma vez que alguma doutrina portuguesa utiliza a nomenclatura "busca *online*" para se referir ao *malware*. Além disso, o questionamento também se justifica em razão de existirem similitudes entre as medidas de busca domiciliar e o *malware*, quais sejam, ambas objetivam encontrar elementos da prática delitiva e são realizadas com o fim de coletar provas que se encontram em lugares não acessíveis ao público.

No ordenamento brasileiro, a possibilidade de legitimação do *malware* nas disposições relativas às buscas domiciliares é rechaçada por Castro. Segundo o autor, o regime das buscas domiciliares não se confunde com o uso do *malware*, pois enquanto este pressupõe uma atuação dissimulada por parte da investigação através da ocultação da medida, aquele se trata de um meio aberto de obtenção de prova com regras especificas.[206]As regras para realização das buscas domiciliares no Brasil encontram-se positivadas no art. 245[207] do Código de Processo Penal, como também no art. 5, inc. XII[208], da Constituição Federal de 1988. Assim, as exigências de consentimento do morador -para ingresso no período da noite - e a garantia de ordem judicial, tornam o regime das buscas domiciliares totalmente incompatível com a metodologia *malware*.

Nesse sentido, Mendes revela ser uma "atecnia processual" equiparar as buscas e apreensões em locais físicos com o *malware*, uma vez que são institutos processuais diferentes com naturezas jurídicas distintas. O autor retromencionado pontua ainda que as buscas domiciliares possuem natureza jurídica dúplice de meio de obtenção de fontes de provas e de medida cautelar probatória, enquanto o *malware* só pode ser encarado como meio de obtenção de fontes de prova, pois jamais "será possível se estabelecer o contraditório judicial sobre às informações constantes nas *fontes* de prova decorrentes das *buscas online* pela incapacidade da comprovação da "mesmidade" do material probatório."[209]

De acordo com ele, como após a instalação do *malware* não há a garantia que serão conservados os arquivos de interesse da investigação, não há como enquadrá-lo como medida cautelar probatória.[210] Tem-se, então, que os elementos colhidos através de *malware* possuem natureza indiciária, de modo que não podem ingressar de imediato no processo penal como prova, sendo necessário o prévio exercício do contraditório e a certificação de que os mesmos não foram alteradas, para que haja a posterior validação em juízo.

Neste prosseguimento, no que se refere ao ordenamento português, Ramalho afirma que a "busca *online*" não se compatibiliza com a busca domiciliária. Primeiro porque aquela

---

[206] CASTRO, Luiz Augusto Sartori de. Busca e apreensão mediante uso de malware. In: **Boletim IBCCRIM**, São Paulo, v. 21, n. 251, p. 6-8, out..2013, p. 7.

[207] BRASIL. **Código de Processo Penal.** Art. 245: as buscas domiciliares serão executadas de dia, salvo se o morador consentir que se realizem à noite, e, antes de penetrarem na casa, os executores mostrarão e lerão o mandado ao morador, ou a quem o represente, intimando-o, em seguida, a abrir a porta.

[208] BRASIL. **Constituição Federal**. Art. 5°, inc. X**:** a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial.

[209] MENDES, Carlos Hélder. **Malware do estado e processo penal: a proteção de dados informáticos face à infiltração por software na investigação criminal**. 2018. Dissertação de Mestrado. Pontifícia Universidade Católica do Rio Grande do Sul, p. 154-155.

[210] Idem, p. 196-197.

não se trata efetivamente de uma busca, possuindo maior amplitude. Segundo porque o interesse protegido na busca domiciliária é a inviolabilidade de domicílio, interesse este que é resguardado incidentalmente e não de forma prioritária na "busca *online*", que também pode ser efetuada em dispositivos móveis *(smartphones* e *tablets*), ocasião em que não haverá a violação do domicílio do investigado.[211]

Por sua vez, Andrade também rechaça qualquer comparação, aduzindo que ao contrário do que ocorre com a busca domiciliária em que o investigado recebe o mandado de busca e pode acompanhar sua execução, a "busca *online*" ocorre de maneira oculta e silenciosa, de modo que é classificada como um método oculto de investigação, enquanto aquela é tida como método aberto.[212] Valendo salientar que, assim como no ocorre no Brasil, as buscas domiciliares em Portugal também deve ser executadas à luz de alguns requisitos e garantias, que estão estampados entre os arts. 174 a 177[213] do Código de Processo Penal Português.

Nessa esteira, Campos também afasta a ideia de equiparação. Segundo a autora "ainda que se reduza a compreensão de *malware* a uma simples 'busca', o 'parâmetro' para aferir da sua previsão terá de ser a LC, que incide sobre dados informáticos (os quais não são algo tangível ou corpóreo) e não o artigo 174 do CPP".[214]

Deste modo, observa-se que as doutrinas brasileira e portuguesa afastam por completo a possibilidade de legitimação do *malware* no regime das buscas domiciliares. Havendo mais ênfase na doutrina portuguesa, que apesar de frequentemente denominar o *malware* de "busca *online*", rechaça qualquer possibilidade de enquadramento da referida metodologia no regime das buscas. Sendo as principais razões as seguintes: (1) a busca por *malware* possibilita a obtenção de provas não alcançadas nas buscas comuns em espaço físico; (2) a busca por *malware* pode ser realizada para além do domicílio, no caso da infiltração em dispositivos móveis; (3) a busca por *malware* é oculta enquanto a busca domiciliar é um método aberto; (4) existe dispositivo próprio na Lei do Cibercrime para "buscas" em ambiente digital.

---

[211] RAMALHO, David Silva. **Métodos ocultos de investigação criminal em ambiente digital.** Editora Almedina, 2017, p. 315 -316.

[212] ANDRADE, Manuel da Costa. "**Bruscamente no verão passado", a reforma do Código de Processo Penal.** Coimbra Editora, 2009. p, 115.

[213] PORTUGAL. **Código de Processo Penal**. Art. 177, n° 1 - A busca em casa habitada ou numa sua dependência fechada só pode ser ordenada ou autorizada pelo juiz e efectuada entre as 7 e as 21 horas, sob pena de nulidade. 2 - Entre as 21 e as 7 horas, a busca domiciliária só pode ser realizada nos casos de: a) Terrorismo ou criminalidade especialmente violenta ou altamente organizada; b) Consentimento do visado, documentado por qualquer forma; c) Flagrante delito pela prática de crime punível com pena de prisão superior, no seu máximo, a 3 anos.

[214] CAMPOS, Juliana Filipa Sousa. **O malware como meio de obtenção de prova em processo penal: a investigação oculta em ambiente digital – (monografias).** Coimbra: Editora Almedina, 2021, p. 68.

Assim sendo, não havendo a possibilidade de enquadramento do *malware* nas buscas comuns, chama-se atenção para a pesquisa de dados informáticos (art. 15, da Lei n° 109/2009), metodologia oculta de investigação prevista na lei portuguesa sobre o cibercrime, que termina por adaptar as buscas domiciliárias para o ambiente digital. A referida lei através do seu art. 15, n° 1[215] e n° 5[216] estabelece duas modalidades de pesquisa de dados informáticos para obtenção de elementos de prova digital. A primeira é a pesquisa simples, realizada localmente no próprio sistema informativo alvo com a finalidade de recolher prova específica e determinada. Já a segunda modalidade, denominada de pesquisa remota ou por extensão, é aquela realizada de forma *online* para acessar através do sistema inicial dados informáticos que se encontram em outro sistema, ou noutra parte do sistema inicialmente pesquisado.

Segundo Ramalho, a pesquisa por extensão consagra a possibilidade de acesso remoto a dados alojados em sistemas de computação em nuvem. Entretanto, o autor ressalta que a pesquisa por extensão não pode se dar de forma oculta, uma vez que esta decorre de uma pesquisa inicial feita presencial e diretamente no sistema informático em questão. Em outras palavras, a *ratio* da pesquisa à remota é que esta parta de uma diligência aberta em ambiente físico, sendo realizada após o decurso de uma pesquisa inicial no sistema informático, e não de forma isolada, com o acesso inicial remoto ao sistema informático.[217]

Deste modo, tem-se que na pesquisa de dados, o acesso inicial a um dispositivo informático é estabelecido mediante um mandado direcionado para cumprimento de forma presencial no local em que o dispositivo se encontra. Para em seguida, se necessário, a pesquisa ser ampliada para outras partes do dispositivo investigado ou para outro dispositivo informático. Ocasião em que o acesso ocorrerá de forma remota. Não havendo que se falar, assim, em acesso inicial remoto ao sistema informático do suspeito na metodologia de pesquisa de dados informáticos.

Nessa esteira, Campos rechaça a possibilidade de legitimação do *malware* pelo regime das pesquisas informáticas. Primeiro porque com o uso do *malware* não se consegue

---

[215] PORTUGAL. **Lei n° 109/2009 (Lei do Cibercrime).** Art. 15, n° 1: Se no decurso do processo se tornar necessário à produção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos e determinados, armazenados num determinado sistema informático, a autoridade judiciária competente ordena a quem tenha disponibilidade ou controlo desses dados que os comunique ao processo ou que permita o acesso aos mesmos, sob pena de punição por desobediência.

[216] PORTUGAL. **Lei n° 109/2009 (Lei do Cibercrime).** Art. 15, n° 5: Quando, no decurso de pesquisa, surgirem razões para crer que os dados procurados se encontram noutro sistema informático, ou numa parte diferente do sistema pesquisado, mas que tais dados são legitimamente acessíveis a partir do sistema inicial, a pesquisa pode ser estendida mediante autorização ou ordem da autoridade competente, nos termos dos n.os 1 e 2.

[217] RAMALHO, David Silva. **Métodos ocultos de investigação criminal em ambiente digital.** Coimbra: Editora Almedina, 2017, p. 272-273.

assegurar que apenas serão obtidos dados "específicos e determinados", conforme determina o art. 15, n° 1, da Lei n° 109/2009. Segundo porque o *malware* não acessa apenas os dados armazenados no sistema informático, mas também todos aqueles produzidos em tempo real e que não estão armazenados. Terceiro porque o *malware* infiltra-se remota e diretamente no sistema informático alvo, sem a necessidade de prévio acesso a um sistema inicial, como se exige na pesquisa por extensão, prevista no art. 15°, n° 5, da Lei n° 109/2009, da Lei n° 109/2009. Quarto porque o *malware* não se resume a uma mera busca, possuindo mais funcionalidades. Quinto porque o acesso ao sistema inicial às claras comprometeria o caráter oculto do *malware* enquanto método de obtenção de prova.[218]

Em sentido oposto, apesar de entender que a Lei do Cibercrime deveria ter restringido o conteúdo dos dados que podem ser alcançados através do método da pesquisa de dados informáticos, e apesar de considerar inconstitucional as disposições do art. 15, n° 3[219], da Lei n° 109/2009, que autoriza os órgãos de polícia criminal a proceder com a pesquisa de dados sem a necessidade de prévia autorização judicial, Albuquerque, ainda assim, admite a consagração das "buscas *online*" (*malware*) através do regime legal da pesquisa de dados informáticos.[220] Com exceção do supracitado autor, tem-se que a maioria da doutrina portuguesa rechaça o enquadramento do malware na pesquisa de dados informáticos. Não havendo manifestação doutrinária brasileira por lá não existir Lei do Cibercrime, nem dispositivo legal semelhante, a não ser a já mencionada medida de busca e apreensão comum ou busca domiciliária.

Outra hipótese seria a legitimação do *malware* através das normas que versam sobre a interceptação das comunicações. Nas palavras de Prado, entende-se por interceptação a "atividade efetuada por um terceiro, captando, mediante instrumentos técnicos de percepção, o conteúdo de uma conversação ou de uma comunicação em curso, entre duas ou mais pessoas."[221]

---

[218] CAMPOS, Juliana Filipa Sousa. **O malware como meio de obtenção de prova em processo penal: a investigação oculta em ambiente digital – (monografias)**. Coimbra: Almedina, 2021, p. 91.

[219] PORTUGAL. **Lei n° 109/2009 (Lei do Cibercrime).** Art. 15, n° 3: O órgão de polícia criminal pode proceder à pesquisa, sem prévia autorização da autoridade judiciária, quando: a) A mesma for voluntariamente consentida por quem tiver a disponibilidade ou controlo desses dados, desde que o consentimento prestado fique, por qualquer forma, documentado; b) Nos casos de terrorismo, criminalidade violenta ou altamente organizada, quando haja fundados indícios da prática iminente de crime que ponha em grave risco a vida ou a integridade de qualquer pessoa.

[220] ALBUQUERQUE, Paulo Pinto de. **Comentário do Código de Processo Penal à luz da Constituição da República Portuguesa e da Convenção Europeia dos Direitos do Homem**. 4.ª edição, Lisboa: Universidade Católica Editora, 2011, p. 502.

[221] GIACOMOLLI, Nereu José. **A fase preliminar do processo penal: crises, misérias e novas metodologias investigatórias.** Rio de Janeiro: Editora Lumen Juris, 2011, p. 141.

No Brasil, o procedimento das medidas investigativas que incidem no fluxo comunicacional entre duas ou mais pessoas possui previsão na Lei n° 9296/96[222], que trata tanto das interceptações telefônicas quanto das telemáticas. Já em Portugal, tem-se o art. 18°[223] da Lei do Cibercrime - o qual permite a interceptação nos crimes previstos no mencionado diploma legal - bem como também há o regime das escutas telefônicas que possui campo de aplicabilidade distinto e é referido pelo próprio art. 18°, n° 4, da referida lei.

Importante frisar que tanto na interceptação telefônica como na telemática, a ingerência no fluxo comunicacional é realizada por terceira pessoa, que capta as declarações prestadas no curso de uma comunicação, bem como determinados tipos de dados. Sendo a instantaneidade a marca das interceptações, uma vez que ela não alcança, por exemplo, os dados de um *e-mail* ou de uma comunicação já realizada. Neste sentido, Sidi destaca que a interceptação capta apenas a comunicação que está acontecendo durante a execução da medida investigativa de obtenção de prova, e não a passada, que já ocorreu.[224]

Ao contrário das interceptações tradicionais, observa-se uma abordagem oposta na instalação de *malware*. Um primeiro ponto de diferenciação é ressaltado por Mendes ao aduzir que diferentemente do que ocorre nas interceptações telemáticas comuns em que a ação é realizada externamente em relação ao sistema informático, nas interceptações por *malware* a intrusão é direta, sendo efetuada internamente no dispositivo alvo.[225] Um segundo ponto de

[222] BRASIL. **Lei n° 9296/96**. Art. 1º: A interceptação de comunicações telefônicas, de qualquer natureza, para prova em investigação criminal e em instrução processual penal, observará o disposto nesta Lei e dependerá de ordem do juiz competente da ação principal, sob segredo de justiça. Parágrafo único. O disposto nesta Lei aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática.

[223] PORTUGAL. **Lei n° 109/2009 (Lei do Cibercrime).** Art. 18, n° 1: É admissível o recurso à intercepção de comunicações em processos relativos a crimes: a) Previstos na presente lei; ou; b) Cometidos por meio de um sistema informático ou em relação aos quais seja necessário proceder à recolha de prova em suporte electrónico, quando tais crimes se encontrem previstos no artigo 187.º do Código de Processo Penal. 2 - A intercepção e o registo de transmissões de dados informáticos só podem ser autorizados durante o inquérito, se houver razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter, por despacho fundamentado do juiz de instrução e mediante requerimento do Ministério Público. 3 - A intercepção pode destinar-se ao registo de dados relativos ao conteúdo das comunicações ou visar apenas a recolha e registo de dados de tráfego, devendo o despacho referido no número anterior especificar o respectivo âmbito, de acordo com as necessidades concretas da investigação. 4 - Em tudo o que não for contrariado pelo presente artigo, à intercepção e registo de transmissões de dados informáticos é aplicável o regime da intercepção e gravação de conversações ou comunicações telefónicas constante dos artigos 187.º, 188.º e 190.º do Código de Processo Penal.

[224] SIDI, Ricardo. **A interceptação das comunicações telemáticas no processo penal.** Belo Horizonte: Editora D'Plácido, 2016, p. 73.

[225] MENDES, Carlos Hélder. **Malware do estado e processo penal: a proteção de dados informáticos face à infiltração por software na investigação criminal**. 2018. Dissertação de Mestrado. Pontifícia Universidade Católica do Rio Grande do Sul, p. 140.

distinção, conforme Torre, é que o *malware* possui uma maior capacidade de recolher informações quando comparado com a interceptação tradicional.[226]

Essa maior capacidade de recolha de informações também é destacada por Ramalho. Segundo ele, diferentemente das interceptações, as "buscas online" são mais abrangentes e possibilitam a recolha de um maior número de dados informáticos, incluindo todas as atividades, lícitas ou não lícitas, desempenhadas no dispositivo informático investigado. Isso significa que o Estado terá amplo acesso a intimida e vida privada do seu alvo, tendo a sua disposição o "diário pessoal" do mesmo.[227]

Campos também chama atenção para o caráter mais intrusivo do *malware*, que pode aceder oculta e remotamente, o que não ocorre com as interceptações, a todas as atividades desempenhadas de maneira interna ou externa ao sistema informático. Para além disso, destaca que enquanto a interceptação é feita no próprio fornecedor de serviços, tendo-se acesso apenas aos dados oriundos do processo de comunicação, na metodologia de infiltração por *malware* realiza-se verdadeira "vigilância na fonte", sendo possível acessar os dados desencriptados, de forma pretérita ao envio da mensagem, no remetente, e *a posteriori*, no momento da chegada, no destinatário.[228]

Tem-se, então, que a interceptação tradicional (de dados telemáticos) não consegue aceder ao conteúdo das mensagens trocadas, por exemplo, no *WhatsApp*, que é um prestador de serviço de comunicação que utiliza da tecnologia de criptografia de ponta a ponta. De modo que através da interceptação tradicional, o investigador apenas consegue identificar os números dos telefones que interagiram entre si no referida aplicativo. Diferindo, assim, do *malware* que é capaz de acessar o conteúdo das mensagens, como já ressaltado.

A possibilidade de o *malware* acessar o conteúdo de mensagens protegidas pela encriptação também é salientada por Torre. De acordo com o retromencionado autor, o *malware* trata-se de uma interceptação ativa, que capta as informações no dispositivo alvo somente após o tramite de decodificação, não sendo afetado pelos serviços de encriptação, presentes na maioria dos serviços de comunicações da atualidade, diferentemente do que ocorre com as interceptações tradicionais que não conseguem acessar os dados das conversas encriptadas.[229]

---

[226] TORRE, Marcos. **Indagini informatiche e processo penale.** Dottorato di ricerca in scienza giuridiche, ciclo XXVIII. Università degli studi Firenze. Anni 2012/2015. p, 151.
[227] RAMALHO, David Silva. O uso de *malware* como meio de obtenção de prova em processo penal. In: **Revista de concorrência e regulação**, Lisboa, Ano 4, nº 16, 2013, p. 226.
[228] CAMPOS, Juliana Filipa Sousa. **O malware como meio de obtenção de prova em processo penal: a investigação oculta em ambiente digital – (monografias).** Coimbra: Almedina, 2021, p. 92-93.
[229] TORRE, Marcos. **Indagini informatiche e processo penale.** Dottorato di ricerca in scienza giuridiche, ciclo XXVIII. Università degli studi Firenze. Anni 2012/2015. p, 151.

Assim, me parece que é unânime na mais fortes doutrina brasileira e portuguesa a não habilitação do *malware* à luz dos preceitos das tradicionais interceptações.

Neste prosseguimento, uma terceira possibilidade de admissão do *malware*, seria através de sua legitimação no regime das ações encobertas. No ordenamento brasileiro, a sistemática das ações encobertas está estampada do art. 10[230] ao art. 14 da Lei n° 12.850/2013. Sendo que no art.-10-A[231] se estabelece a possibilidade de realização da ação encoberta em ambiente digital, por meio da *internet*. Ademais, a figura do agente encoberto em ambiente digital também pode ser verificada no art. 190-A[232] da Lei n° 8.069/90, que prevê a infiltração de agentes policiais na *internet* para investigar crimes contra a dignidade sexual de crianças e adolescentes.

No ordenamento português, a figura do agente encoberto encontra repouso na Lei n° 101/2001, a qual estabelece procedimentos, requisitos, bem como o âmbito de aplicação da infiltração dos agentes de polícia nas investigações criminais para fins de prevenção e repressão de crimes, podendo o conceito da ação encoberta ser encontrado no art. 1, n° 2[233] do referido regime geral. No que se refere ao âmbito digital, o art. 19, n° 1[234], da Lei n° 109/2009 (Lei do Cibercrime) faz remissão para o regime geral, de modo que a ação encoberta em ambiente digital parte das premissas inerentes ao procedimento comum dos agentes encobertos no mundo físico.

---

[230] BRASIL. **Lei n° 12.850/2013**. Art. 10. A infiltração de agentes de polícia em tarefas de investigação, representada pelo delegado de polícia ou requerida pelo Ministério Público, após manifestação técnica do delegado de polícia quando solicitada no curso de inquérito policial, será precedida de circunstanciada, motivada e sigilosa autorização judicial, que estabelecerá seus limites.

[231] BRASIL. **Lei n° 12.850/2013**. Art. 10-A. Será admitida a ação de agentes de polícia infiltrados virtuais, obedecidos os requisitos do caput do art. 10, na internet, com o fim de investigar os crimes previstos nesta Lei e a eles conexos, praticados por organizações criminosas, desde que demonstrada sua necessidade e indicados o alcance das tarefas dos policiais, os nomes ou apelidos das pessoas investigadas e, quando possível, os dados de conexão ou cadastrais que permitam a identificação dessas pessoas.

[232] BRASIL. **Lei n° 8.069/90 (Estatuto da Criança e do Adolescente)**. Art. 190-A: A infiltração de agentes de polícia na internet com o fim de investigar os crimes previstos nos arts. 240 , 241 , 241-A , 241-B , 241-C e 241-D desta Lei e nos arts. 154-A , 217-A , 218 , 218-A e 218-B do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal).

[233] PORTUGAL. **Lei n° 101/2001**. Art. 1, n° 2: consideram-se acções encobertas aquelas que sejam desenvolvidas por funcionários de investigação criminal ou por terceiro actuando sob o controlo da Polícia Judiciária para prevenção ou repressão dos crimes indicados nesta lei, com ocultação da sua qualidade e identidade.

[234] PORTUGAL. **Lei n° 109/2009 (Lei do Cibercrime)**. Art 19, n° 1- É admissível o recurso às ações encobertas previstas na Lei n.º 101/2001, de 25 de agosto, nos termos aí previstos, no decurso de inquérito relativo aos seguintes crimes; a) Os previstos na presente lei; b) Os cometidos por meio de um sistema informático, quando lhes corresponda, em abstrato, pena de prisão de máximo superior a 5 anos ou, ainda que a pena seja inferior, e sendo dolosos, os crimes contra a liberdade e autodeterminação sexual nos casos em que os ofendidos sejam menores ou incapazes, a burla qualificada, a burla informática e nas comunicações, o abuso de cartão de garantia ou de cartão, dispositivo ou dados de pagamento, a discriminação racial, religiosa ou sexual, as infrações económico-financeiras, bem como os crimes consagrados no título iv do Código do Direito de Autor e dos Direitos Conexos.

Importante destacar que a infiltração por agente encoberto – metodologia investigativa permitida tanto no Brasil como em Portugal -, em que o agente obtém informações após adquirir a confiança do suspeito, não se confunde com a figura do agente provocador, devendo a prova através desta metodologia ser considera proibida (ilícita), e, portanto, inutilizável.

Neste sentido, aponta-se as lições de Sousa, que ao diferenciar as duas figuras, agente encoberto e provocador, aduz que a prova será proibida apenas quando for possível atestar o nexo causal entre a conduta enganosa e o crime praticado pelo suspeito, pois não havendo a prova da suficiência do engano ou se ficar comprovada a prévia intenção do agente em praticar o crime, independente da atuação enganosa, não haverá que se falar em ilicitude dos elementos colhidos.[235]

Assim, no que se refere ao ambiente digital, Campos ressalta que o agente infiltrado tem que se restringir a recolher informações, não podendo eles mesmos fomentar a prática de crimes, através, por exemplo, do envio de material infectado por *malware* para o suspeito. Segundo a autora a criação de "hiperlinks que supostamente dariam acesso a conteúdo pedo-pornográfico" revelam ser ações provocadoras, o que vai de encontro aos princípios investigativos.[236]

Ainda segundo a autora retromencionada, apesar de existirem pontos de convergência entre as medidas do *malware* e das ações encobertas, quais sejam, ambas possibilitam a recolha de dados armazenados e fabricados em tempo real, bem como possuem caráter oculto e invadem a vida privada da pessoa investigada. Há inultrapassáveis diferenças entre as duas metodologias. A primeira é o caráter passivo do *malware*, que não se confunde com a atuação ativa do agente infiltrado, que obtém as informações relevantes para a investigação interagindo com o suspeito. A segunda relaciona-se com a natureza das metodologias que são bem distintas, pois na medida em que o *malware* trata-se de um *software* autoprogramado, as ações encobertas são realizadas por pessoas, agentes policiais, que executam *per si*, a ação infiltrada.[237]

Desta feita, apesar das notáveis diferenças entre as supracitadas metodologias, alguma doutrina portuguesa entende que o *malware* pode ter seu uso admitido nas investigações

[235] SOUSA, Susana Aires de. **Agent provocateur e meios enganosos de prova: algumas reflexões**, Separata de Liber Discipulorum para Jorge de Figueiredo Dias. Coimbra: Coimbra Editora, 2002, p. 1233
[236] CAMPOS, Juliana Filipa Sousa. **O malware como meio de obtenção de prova em processo penal: a investigação oculta em ambiente digital – (monografias).** Coimbra: Editora Almedina, 2021, p. 94-95.
[237] Idem, p. 95-96.

criminais através das ações encobertas, especificadamente em razão do art. 19, n° 2[238], da Lei n° 109/2009 (Lei do Cibercrime). A referida tese é adotada por Ramalho e Correia, dentre outros.

Segundo Ramalho ao fazer referência a "meios e dispositivos informáticos" no artigo que trata do agente encoberto e, simultaneamente, fazer remissão para o regime das intercepções, o legislador português teria criado um método oculto de investigação de natureza excepcional, mais gravoso em relação ao agente encoberto, que no caso seria o *malware*. O autor retromencionado sustenta sua posição de que o *malware* teria sido consagrado pelo dispositivo legal em questão, entre outras razões, pelo fato de a terminologia "meios técnicos" já ser utilizada em outras ordens jurídicas, a exemplo da Lei de Proteção da Constituição da Renânia do Norte-Vestefália, que se refere ao *malware* em seu § 5.2 (11) através do nome "dispositivos técnicos".[239]

Ainda segundo Ramalho, o curso de uma ação encoberta constitui pressuposto indispensável para o recurso ao *malware*, que, por sua vez, deve ser utilizado de forma subsidiária – quando a prova do crime for impossível ou difícil de ser recolhida de outro modo -, adequada e proporcional a gravidade do crime em concreto. Não podendo ser manuseado para fins de prevenção criminal.[240] Contudo, apesar de admitir o uso do *malware* através da disposição legal supramencionada, o autor supracitado considera inadequada a norma existente para regular a matéria, tendo em vista a avassaladora intrusão desta metodologia nos direitos fundamentais do investigado.[241] Por outro lado, partindo de uma perspectiva apenas literal e utilizando o termo "busca *online*", Correia entende que o recurso ao *malware* estaria consagrado tanto no art. 19, n° 2, bem como no art. 15, n° 5, todos da Lei do Cibercrime.[242]

Em sentido oposto, Campos defende a não legitimação do *malware* de forma complementar a uma ação encoberta. Segundo a autora, o termo "meios e dispositivos informáticos" utilizado pelo art. 19, n° 2, da Lei do Cibercrime é insuficiente para legitimar o *malware*, tanto pelo aspecto de danosidade da referida metodologia, como também à luz do

[238] PORTUGAL. **Lei n° 1019/2009 (Lei do Cibercrime)**. Art. 19, n°2: sendo necessário o recurso a meios e dispositivos informáticos observam-se, naquilo que for aplicável, as regras previstas para a interceção de comunicações.
[239] RAMALHO, David Silva. **Métodos ocultos de investigação criminal em ambiente digital. Coimbra:** Editora Almedina, 2017, p. 343-346.
[240] Idem, p. 347.
[241] Idem, p. 351.
[242] CORREIA, João Conde. Prova digital: as leis que temos e a lei que devíamos ter. In: **Revista do Ministério Público**, ano 35, n° 139 (julho/setembro), 2014, p. 42-43.

princípio da precisão e da determinabilidade dos atos normativos, razões estas que tornam imprescindível a regulação autônima do *malware* para fins de persecução criminal.[243]

Uma quarta hipótese seria enquadrar o *malware* nas escutas ambientais. No Brasil, o art. 3, inc. II[244], da Lei n° 12. 850/2013 há bastante tempo já prevê a captação ou escuta ambiental enquanto método oculto de obtenção de prova. Acontece que só recentemente, no ano de 2019, é que o procedimento para utilização da referida metodologia foi regulamentado, tendo sido disposto no art. 8-A[245] da Lei n° 9296/96. Por outro lado, em Portugal, a escuta ambiental é consagrada no art. 189, *in fine*[246], do CPP e tem seus pressupostos de admissibilidade e formalidades procedimentais estabelecidos nos arts. 187 e 188, ambos também do CPP.

Todavia, apesar de algumas similitudes o *malware* não se confunde com a escuta ambiental, pois apresenta um maior nível de danosidade, podendo recolher dados não apenas em tempo real, como também os já produzidos e armazenados[247]. Além disso, especificadamente em relação ao dispositivo português das escutas há ainda a cláusula de barreira estipulada pelo art. 18, n° 4[248] da Lei do Cibercrime, que exclui deliberadamente as escutas do seu âmbito de aplicação.

Por fim, de modo genérico, Barbiero defende o uso do *malware* no processo penal brasileiro para os casos de criminalidade complexa e organizada. Segundo o retromencionado autor, para esses tipos de casos é possível usar o *malware* por meio da utilização de

---

[243] CAMPOS, Juliana Filipa Sousa. **O malware como meio de obtenção de prova em processo penal: a investigação oculta em ambiente digital – (monografias).** Coimbra: Almedina, 2021, p. 97.

[244] BRASIL. **Lei n° 12.852/2013**. Art. 3, inc. II: Em qualquer fase da persecução penal, serão permitidos, sem prejuízo de outros já previstos em lei, os seguintes meios de obtenção da prova: II- captação ambiental de sinais eletromagnéticos, ópticos ou acústicos.

[245] BRASIL. **Lei n° 9296/96**. Art. 8º-A: Para investigação ou instrução criminal, poderá ser autorizada pelo juiz, a requerimento da autoridade policial ou do Ministério Público, a captação ambiental de sinais eletromagnéticos, ópticos ou acústicos, quando: I - a prova não puder ser feita por outros meios disponíveis e igualmente eficazes; e II - houver elementos probatórios razoáveis de autoria e participação em infrações criminais cujas penas máximas sejam superiores a 4 (quatro) anos ou em infrações penais conexas. § 1º O requerimento deverá descrever circunstanciadamente o local e a forma de instalação do dispositivo de captação ambiental.

[246] PORTUGAL. **Código de Processo Penal**. Art.189, in fine, n 1 - O disposto nos artigos 187.º e 188.º é correspondentemente aplicável às conversações ou comunicações transmitidas por qualquer meio técnico diferente do telefone, designadamente correio electrónico ou outras formas de transmissão de dados por via telemática, mesmo que se encontrem guardadas em suporte digital, e à intercepção das comunicações entre presentes.

[247] CAMPOS, Juliana Filipa Sousa. **O malware como meio de obtenção de prova em processo penal: a investigação oculta em ambiente digital – (monografias).** Coimbra: Editora Almedina, 2021, p. 99.

[248] PORTUGAL. **Lei n° 1019/2009 (Lei do Cibercrime)**. Art. 18, n°4: Em tudo o que não for contrariado pelo presente artigo, à intercepção e registo de transmissões de dados informáticos é aplicável o regime da intercepção e gravação de conversações ou comunicações telefónicas constante dos artigos 187.º, 188.º e 190.º do Código de Processo Penal.

interpretação extensiva dos dispositivos relacionados à interceptação telefônica, busca e apreensão e captação de sinais sonoros.[249]

Em sentido semelhante e de forma mais ampla, ainda se referindo ao Brasil, Smanio defende o emprego de novas tecnologias nas investigações criminais pelo uso da analogia. Para o autor, o processo penal não consegue acompanhar o dinamismo das novas tecnologias, razão pela qual as novas técnicas investigativas pautadas na tecnologia podem ser empregadas sem prévia regulamentação legal, desde que seja de modo temporário, sendo imprescindível a posterior regulação da matéria em lei específica. [250]

Assim sendo, nota-se que há um mar revolto de posições doutrinárias acerca da temática, algumas legitimando e admitindo o uso do *malware*, outras rechaçando. No que se refere ao ordenamento brasileiro, o que observa é que a doutrina que defende a utilização da referida metodologia ainda é tímida e não procura fazer o enquadramento em dispositivo legal específico, buscando apenas admitir o uso da tecnologia através de uso de interpretação extensiva ou analógica com outras disposições legais, sem, contudo, fazer uma análise pormenorizada das funcionalidades e direitos fundamentais atingidos com o uso do malware. Por outro lado, a doutrina portuguesa que admite a utilização de tal tecnologia no processo penal português, busca fazer enquadramento legal de modo literal, através de dispositivos legais amplos, previsto na Lei do Cibercrime.

2. O *MALWARE* COMO MEIO DE OBTENÇÃO DE PROVA ATÍPICO?

Em um sistema processual de estrutura acusatória, com o exercício do direito de punir do Estado limitado por direitos e garantias individuais dos cidadãos, o tema das provas ilícitas ou proibidas ganha maior relevo, pois a demonstração da autoria e materialidade de um fato supostamente ocorrido no mundo real, deve se dar nos limites do que a lei permite, sob pena de sua inutilização daquele elemento colhido de maneira dissonante.

Portanto, a demonstração de um fato ilícito imputado ao acusado deve respeitar certos princípios, não podendo a investigação criminal se sobrepor as formalidades legais e, assim, utilizar métodos proibidos de prova na busca de uma suposta verdade irrefutável. Assim, conforme ensina Hassemer, o que se busca no processo penal é a verdade formalmente

[249] BARBIERO, Diego Roberto. **Implantação de Malwares em Investigações Complexas**. Curitiba: Juruá, 2021, p. 150.
[250] SMANIO, Gianluca Martins. **A vigilância policial em meio digital: entre o garantismo e a eficiência**. 2021. Dissertação (Mestrado em Direito). Faculdade de Direito da Universidade de São Paulo, São Paulo, p. 158.

alcançada, ou seja, é a verdade objetiva.[251] Neste sentido, com o escopo de resguardar a dignidade humana do investigado perante a persecução penal, o Código de Processo Penal Português, à luz do que dispõe a Constituição Portuguesa em seu art. 32, n° 8[252], estabelece a "legalidade da prova" e os "métodos proibidos de prova", respectivamente, nos artigos 125 e 126 do referido diploma legal.

Em uma análise descompromissada dos dispositivos em comento, poderia se entender que todos aqueles métodos de obtenção de prova que não forem legalmente proibidos poderiam ser utilizados, ou seja, seriam permitidos.

Contudo, tal interpretação, conforme ensina Ramalho, está equivocada, pois o postulado da legalidade da prova impõe que a prova penal seja obtida não à margem da lei, mas nos termos dela, admitindo-se o recurso aos métodos atípicos de obtenção de prova apenas excepcionalmente, desde que as leis existentes se mostrem insuficientes para regular a nova metodologia de recolha de prova e o método em questão não confronte direitos fundamentais.[253]

Em sentido semelhante, Albuquerque afirma ser necessária lei expressa para regular o procedimento do meio de obtenção de prova que afronte potencialmente direitos fundamentais. Para além do aspecto formal, o autor retromencionado chama atenção para os aspectos materiais que limitam a utilização de métodos atípicos de prova. Segundo ele, não pode ser admitido meio de obtenção de prova que constitua numa "vigilância total" do suspeito, nem os discriminatórios e desproporcionais.[254]

A necessidade de lei prévia para utilização de método investigativo de obtenção de prova também é destacada por Mendes. Nas lições do autor:

> a proibição de utilização (= valoração) de provas proibidas afigura-se como sendo a melhor maneira de o legislador prevenir a tentação de obtenção de provas a qualquer preço, por parte das instâncias formais de controlo social. É como se o legislador anunciasse aos virtuais prevaricadores: Não sucumbam ao canto de sereia se obtenção de provas a qualquer preço, porquanto isso vos custaria a inutilização absoluta dos meios de prova ilicitamente obtidos, nem sequer podendo repetir essas provas por outros meios! Por exemplo, se invadistes o domicílio de um sujeito sem autorização

---

[251] HASSEMER, Winfried. **Fundamentos del derecho penal**, trad. de Arroyo Zapatero y Muñoz Conde, Barcelona: Bosch, 1984, p. 190.

[252] PORTUGAL **Constituição Federal**. Art. 32, n° 8: "nulas 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". E em sentido semelhante, a Constituição Brasileira, em seu art. 5°, inc. LVI, assim aduz "são inadmissíveis, no processo, as provas obtidas por meios ilícitos."

[253] RAMALHO, David Silva. **Métodos Ocultos de Investigação Criminal em Ambiente Digital**. Coimbra: Editora Almedina, 2017, p. 214

[254] ALBUQUERQUE, Paulo Pinto de. **Comentário do Código de Processo Penal à luz da Constituição da República Portuguesa e da Convenção Europeia dos Direitos do Homem**. 4.ª edição, Lisboa: Universidade Católica Editora, 2011, p. 332-333.

> judicial e nesse local encontrastes a arma do crime, então é como se tivestes destruído essa prova material.[255]

No Brasil, assim como ocorre em Portugal, tanto a Constituição Federal (art. 5°, inc. LXI[256]), como também o Código de Processo Penal (art. 157), disciplinam a matéria das provas proibidas, que aqui recebe o nome de prova ilícita, sendo a consequência processual a mesma, qual seja, seu desentranhamento ou sua inutilização no processo.

Destaca-se, pois, a diferenciação feita por Lopes Jr sobre meios de prova e meios de obtenção de fontes de prova. Para o autor admitir as chamadas provas atípicas, está se referindo na verdade aos meios de prova e não aos meios de obtenção de fontes de prova, uma vez que estes se destinam a investigação e devem sempre possuir previsão normativa por incidir diretamente em direitos fundamentais. Ainda segundo o autor, os meios de prova não devem ser confundidos com os meios de obtenção de fontes de prova, pois enquanto estes são instrumentos utilizados para descobrir fontes e chegar à origem das provas, aqueles destinam-se ao julgador para formação de sua convicção acerca do caso concreto. [257]

Neste mesmo sentido, Ríboli esclarece que os direitos fundamentais só podem ser restringidos por novas técnicas investigativas intrusivas através de decisão judicial, desde que a medida esteja devidamente regulamentada em lei e esteja em conformidade com a Constituição.[258] Tem-se, assim, que a atividade de recolha de prova deve ser orientada por métodos legais, respeitosos aos direitos fundamentais, sendo provas proibidas ou ilícitas, impróprias de serem valoradas, aquelas obtidas por métodos ocultos investigativos que violam direitos fundamentais. Pois para além de lei expressa prevendo a medida, entende-se que o procedimento de aplicação também deve estar regulamentado, devendo haver ainda autorização judicial para sua aplicabilidade.

Nesta senda, nas próximas linhas serão abordados os princípios da reserva de lei, proporcionalidade, subsidiariedade e reserva de jurisdição. Bem como, os principais direitos fundamentais atingidos pelo uso do *malware*, dando se ênfase na perspectiva do monitoramento *online*. Para ao final, tratarmos do questionamento acerca da possibilidade de utilização do *malware* como método atípico de obtenção de prova no processo penal brasileiro e português.

---

[255] MENDES, Paulo de Sousa. As proibições de prova no processo penal. Coord. Maria Fernanda Palma. In: **Jornadas de direito processual penal e direitos fundamentais**. Coimbra: Editora Almedina, 2004, p. 142.
[256] BRASIL. **Constituição Federal**. Art. 5°, inc. LVI - são inadmissíveis, no processo, as provas obtidas por meios ilícitos.
[257] LOPES JR. Aury. **Direito processual penal.** 13ª ed. São Paulo. Saraiva, 2016. p, 366.
[258] RIBOLI, Eduardo Bolsoni. "Eu sei o que vocês fizeram no verão passado": o uso de software de espionagem como meio de obtenção de prova penal. **Revista Brasileira de Ciências Criminais**, São Paulo, v. 27, n. 156, p. 91-139, jun. 2019, p. 107.

2.1. A reserva de lei

De acordo com o código de processo penal português, no seu artigo 125, são permitidos na investigação criminal, todos os meios de provas que não sejam expressamente proibidos por lei. Desta forma, pode-se interpretar que estão abrangidos os meios típicos (regulamentados) e os meios atípicos. No entanto, não se mostra tão simples esta análise acerca da legalidade dos meios de provas, uma vez que deve ser feita, primeiramente, a sua ponderação com os meios já positivados, através da verificação da similitude entre eles, para se certificar de que não existe no ordenamento, uma norma que tipifique o caso em questão, ainda que de forma subsidiária. Portanto, o primeiro elemento para que se busque um meio atípico de prova, é a falta de um meio probatório típico.[259]

Posteriormente, deve ser feita uma análise em relação aos limites da sua admissibilidade, tendo em vista a relatividade da valoração dos meios de prova (a exemplo daquelas obtidas através do consentimento), com exceção daqueles absolutamente inconcebíveis por expressa proibição legal. Em síntese, deve-se verificar a existência ou não de obstáculos à utilização do meio de prova proposto.[260]

Etapa final deste processo é o estudo acerca do impacto do meio oculto de investigação na restrição aos direitos fundamentais do visado. Esta análise deve ser feita considerando os parâmetros constitucionais e do processo penal de proteção aos direitos dos indivíduos, presente no ordenamento jurídico, de forma a ser utilizado de maneira racional, justificada e com observância, entre outros, do contraditório. Ademais, estas restrições devem ser mínimas, de forma que não lesionem os direitos fundamentais.[261]

Apesar de todo procedimentalismo acima exposto, ainda assim, se afigura flagrante o risco de indevida intromissão relevante dos meios atípicos de investigação nos direitos fundamentais dos indivíduos. É imperiosa a atuação do legislador na demarcação dos limites legais através de critérios objetivos, bem como do aplicador do direito, para que sejam respeitadas as garantias constitucionais dos indivíduos contra arbitrariedades estatais.[262]

Nesse contexto, é crucial que, além de identificar claramente os direitos afetados e estabelecer rigorosamente o grau de interferência permitido, a legislação também preveja e defina de maneira precisa e normativa os fundamentos, propósitos e limites da intromissão. Em

[259] RAMALHO, David Silva. **Métodos Ocultos de Investigação Criminal em Ambiente Digital**. Coimbra: Editora Almedina, 2017, p. 213-214.
[260] Idem, p. 215.
[261] Idem, p. 217.
[262] Idem, p. 226.

outras palavras, a intromissão autorizada por lei está intrinsecamente vinculada a uma finalidade específica, o que impõe ao legislador a obrigação de determinar de maneira precisa o propósito da coleta de determinadas informações.[263]

Conforme art. 8, n° 2, da Convenção Europeia dos Direitos do Homem:

> Não poderá haver ingerência da autoridade pública no exercício do direito [à vida privada e às comunicações] salvo se esta ingerência estiver prevista em lei e constitua medida que, em uma sociedade democrática, seja necessária para a segurança nacional, a segurança pública, o bem-estar econômico do país, a defesa da ordem e a prevenção de infrações penais, a proteção da saúde ou da moral, dos direitos e das liberdades dos demais.[264]

Acrescente-se à reserva de lei, outro pressuposto complementar crucial: o catálogo de infrações. Ele deve legitimar cada um dos meios ocultos de obtenção de provas. Considerando o potencial impacto social significativo dos métodos ocultos, é essencial que esse catálogo seja restrito e definido de acordo com critérios de proporcionalidade. Esses critérios devem levar em consideração tanto a gravidade das infrações quanto as necessidades específicas da investigação.[265]

2.2. A proporcionalidade

O princípio da proporcionalidade tem como objetivo evitar abusos, arbitrariedades e excessos nos objetivos de uma investigação criminal, uma vez que frequentemente ocorrem restrições aos direitos fundamentais do suspeito ou acusado na busca da verdade e da justiça. Esse princípio estabelece que as medidas tomadas durante a investigação criminal devem ser proporcionais à gravidade do caso e aos interesses legítimos envolvidos. Portanto, as restrições impostas aos direitos fundamentais devem ser estritamente necessárias, adequadas e proporcionais aos objetivos da investigação, evitando-se, assim, qualquer excesso ou desproporcionalidade na busca pela verdade processual.[266]

A legitimidade do sacrifício de direitos fundamentais em prol da busca de outro interesse constitucional, deve ser estabelecida por meio do uso de critérios de

---

[263] ANDRADE, Manuel da Costa. "**Bruscamente no verão passado", a reforma do Código de Processo Penal.** Coimbra: Coimbra Editora, 2009. p, 113.

[264] Convenção Europeia dos Direitos do Homem (art. 8, n°2). Disponível em: https://echr.coe.int/documents/convention_por.pdf. Acesso em 12/06/2022.

[265] Idem, p.114.

[266] RAMALHO, David Silva. **Métodos Ocultos de Investigação Criminal em Ambiente Digital**. Coimbra: Editora Almedina, 2017, p. 226-227.

proporcionalidade. Esses critérios são definidos primeiramente pelo legislador ao configurar os pressupostos para tal sacrifício e, posteriormente, pelo aplicador do direito em sua atividade prática. Isso significa que é necessário um equilíbrio cuidadoso entre a restrição dos direitos fundamentais e a importância do interesse ou fim que se pretende alcançar. A análise da proporcionalidade leva em consideração se a restrição é adequada, necessária e proporcionalmente justificada, diante do contexto e dos valores constitucionais em jogo.[267]

O princípio da proporcionalidade divide-se em três vertentes: I. adequação ou idoneidade; II. necessidade ou exigibilidade; III. proporcionalidade em sentido estrito.

I. A adequação/idoneidade estabelece que as medidas restritivas previstas em lei, devem ser adequadas para alcançar os objetivos pretendidos pela legislação. Isso significa que as restrições impostas devem ser eficazes e capazes de atingir os propósitos estabelecidos legalmente. As medidas adotadas devem ser meios apropriados para alcançar os resultados desejados, levando em consideração a natureza do problema e os interesses envolvidos. Dessa maneira, é necessário verificar se o uso de *malware* é objetivamente adequado para a prossecução do fim desejado. Isso significa que as restrições impostas devem ser eficazes e capazes de atingir os propósitos estabelecidos pela lei.[268]

II. Na necessidade/exigibilidade, analisa-se se as medidas empregadas poderiam ser obtidas por outros meios idôneos menos intrusivos e agressivos aos direitos e garantias fundamentais. A necessidade do meio deve ser avaliada em relação a um determinado grau de suspeita da prática do crime e a um catálogo específico de infrações penais que justifiquem a medida. Esse catálogo de crimes deve abranger delitos suficientemente graves, pois, a obtenção da verdade material não pode ocorrer a qualquer custo. Isso significa que a medida restritiva de direitos fundamentais só deve ser utilizada quando for realmente necessário para a investigação de crimes que apresentem uma gravidade significativa. A avaliação da necessidade do meio leva em consideração a natureza e a seriedade do crime em investigação, assim como a suficiência dos indícios de envolvimento do suspeito na infração. Dessa forma, busca-se encontrar um equilíbrio entre a busca pela verdade material e a proteção dos direitos fundamentais, evitando a aplicação indiscriminada de medidas restritivas sem uma justificativa sólida.[269]

---

[267] Idem, p. 226-227.
[268] ANDRADE, Manuel da Costa. "**Bruscamente no verão passado", a reforma do Código de Processo Penal.** Coimbra: Coimbra Editora, 2009. p, 116.
[269] DA SILVEIRA, Maria Ana Barroso de Moura. **Da problemática da investigação criminal em ambiente digital - em especial, sobre a possibilidade de utilização de malware como meio oculto de obtenção de prova**, (dissertação de mestrado). Universidade Católica Portuguesa: Lisboa, 2016, p. 40.

Em alguns casos específicos, o uso de *malware* pode ser considerado como o único meio capaz de contornar determinadas situações e obter a prova desejada, especialmente quando a legislação de cibercrimes não prevê meios de obtenção de prova adequados para tais casos. Nesses cenários, não restam alternativas viáveis além da necessidade de utilizar malware.

III. O princípio da proporcionalidade em sentido estrito estabelece que os meios restritivos legais e os objetivos alcançados devem estar em uma "justa medida", a fim de evitar a adoção de medidas desproporcionais em relação aos resultados obtidos. Isso significa que as restrições impostas devem ser proporcionais e equilibradas em relação aos benefícios alcançados. Deve-se avaliar se os meios utilizados são adequados para alcançar os objetivos pretendidos, se são necessários em relação à gravidade do problema enfrentado e se os benefícios alcançados superam os ônus e restrições impostos aos direitos fundamentais dos indivíduos envolvidos. Dessa forma, o princípio da proporcionalidade em sentido restrito busca garantir que as medidas restritivas adotadas sejam proporcionais ao fim almejado, evitando excessos ou desequilíbrios que possam comprometer a proteção dos direitos fundamentais. A aplicação desse princípio é essencial para garantir a justa medida entre os meios empregados e os resultados obtidos no contexto de restrições legais em uma sociedade democrática e baseada no Estado de Direito. [270] Com relação ao uso do malware, é importante destacar que, devido a sua potencial danosidade, seu uso é recomendável em casos de crimes graves, em casos excepcionais, como última medida apta para acautelar superiores valores constitucionais, especialmente a vida e integridade física dos indivíduos, a realização do Estado de Direito e da Justiça.[271]

2.3. A subsidiariedade

A utilização dos métodos ocultos de investigação, em especial o uso do malware, deve respeitar o princípio da subsidiariedade, que se aplica tanto em relação aos meios de investigação "abertos" quanto aos próprios métodos ocultos. Esse princípio estabelece que os malwares devem ser empregados apenas quando os meios tradicionais de investigação não forem eficazes ou adequados para atingir os objetivos desejados. No plano extrínseco, significa que o malware deve ser utilizado como último recurso, quando as técnicas de investigação

[270] NOVAIS, Jorge Reis. **Os princípios constitucionais estruturantes da República Portuguesa**. Coimbra: Coimbra Editora, 2004, p. 179.
[271] DA SILVEIRA, Maria Ana Barroso de Moura. **Da problemática da investigação criminal em ambiente digital - em especial, sobre a possibilidade de utilização de malware como meio oculto de obtenção de prova**, (dissertação de mestrado). Universidade Católica Portuguesa: Lisboa, 2016, p. 44.

convencionais se mostrarem insuficientes para obter as informações necessárias. Antes de recorrer a tal método oculto, é necessário esgotar as possibilidades de investigação através de meios legais e transparentes. No plano intrínseco, o princípio da subsidiariedade implica que, entre os próprios métodos ocultos, deve-se utilizar o método mais proporcional e menos invasivo possível, levando em consideração a natureza do crime, a gravidade da situação e os direitos fundamentais das pessoas envolvidas.[272]

Nas lições de Andrade "nuns casos bastará que, sem a medida, a investigação fique mais difícil; noutros exigir-se-á que ela seja consideravelmente mais difícil; noutros, mesmo impossível."[273]

Adicionalmente, o princípio da subsidiariedade impõe a proibição e contraposição da utilização simultânea ou cumulativa de dois ou mais métodos ocultos de investigação. Isso significa que, quando um método oculto já é empregado para obter determinada prova, não é justificável ou adequado utilizar outros métodos ocultos em conjunto para alcançar o mesmo objetivo. Essa restrição visa evitar o acúmulo desnecessário de técnicas invasivas e limitar o impacto sobre os direitos fundamentais dos indivíduos envolvidos na investigação. A utilização simultânea de vários métodos ocultos poderia resultar em uma interferência desproporcional em tais direitos, extrapolando os limites necessários para a busca da verdade e a persecução penal. A cumulação de meios ocultos de investigação – derivadas formas de malwares – somente deve ocorrer no combate a manifestações extremas da criminalidade, em consonância com a proporcionalidade.[274]

2.4. A reserva de juiz

É a definição da autoridade competente para tomar decisões sobre a adoção ou autorização das medidas. Essa competência deve ser atribuída exclusivamente ao juiz competente, exceto em casos de "perigo da demora", quando a demora na autorização possa comprometer a eficácia da investigação. A reserva de juiz tem como objetivo primordial garantir a proteção preventiva dos direitos de uma pessoa, geralmente o acusado, que está

[272] ANDRADE, Manuel da Costa. "**Bruscamente no verão passado", a reforma do Código de Processo Penal.** Coimbra: Coimbra Editora, 2009. p, 114.
[273] ANDRADE, Manuel da Costa. Métodos Ocultos de Investigação (plädoyer para uma teoria geral). In*:* **Que futuro para o direito processual penal? Simpósio em homenagem a Jorge de Figueiredo Dias, por ocasião dos 20 anos do Código de Processo Penal Português**, (coord. Mário Ferreira Monte entre outros). Coimbra: Coimbra Editora, 2009, p. 546.
[274] ANDRADE, Manuel da Costa. "**Bruscamente no verão passado", a reforma do Código de Processo Penal.** Coimbra: Coimbra Editora, 2009. p, 115.

sujeita a invasões e investigações intrusivas, sem ter a possibilidade de garantir sua própria defesa. É uma medida que visa assegurar que as decisões relativas a essas ações, sejam tomadas por um magistrado imparcial, que possa avaliar de forma adequada os fundamentos e a necessidade da intervenção, respeitando os direitos e garantias fundamentais do indivíduo envolvido.[275]

Além disso, os métodos ocultos, são medidas que possuem um alto potencial de causar danos, enquanto suas vantagens são incertas. Portanto, isso justifica a necessidade de intervenção de uma autoridade independente e imparcial. É fundamental que essa autoridade seja capaz de analisar, de forma objetiva e imparcial, a proporcionalidade e a necessidade das medidas, garantindo assim a proteção dos direitos e das liberdades individuais.[276]

Dessa forma, ao juiz, como entidade imparcial, desinteressada no processo, cabe a responsabilidade de analisar objetivamente os bens jurídicos em conflito, de acordo com a lei e a Constituição. Diante da proposta do Ministério Público para a utilização de métodos ocultos de obtenção de prova, o juiz deve decidir sobre a justificação específica da restrição dos direitos fundamentais. Essa análise é realizada caso a caso, levando em consideração as circunstâncias particulares e aplicando os princípios legais e constitucionais pertinentes.

A imposição de fundamentação pelo juiz também serve para garantir que a autorização da medida possa ser posteriormente examinada em um julgamento ou recurso, caso haja questionamentos sobre sua legalidade e a admissibilidade das provas obtidas por meio dela. A fundamentação adequada possibilita uma análise crítica das decisões do juiz, permitindo uma avaliação minuciosa da legalidade e validade das provas. Isso assegura a proteção dos direitos processuais das partes envolvidas e promove a transparência e confiabilidade do sistema jurídico.[277]

Cabe ao juiz desempenhar um papel de representação compensatória em relação ao acusado, analisando de forma crítica os argumentos apresentados para a concessão da autorização judicial e equilibrando-os com os interesses e direitos da pessoa em questão. Em outras palavras, o juiz deve levar em consideração os argumentos que a pessoa afetada poderia invocar se tivesse a oportunidade de fazê-lo. Isso implica ponderar cuidadosamente os interesses em jogo e garantir que a decisão tomada seja equilibrada e justa, levando em consideração as possíveis objeções que o indivíduo afetado poderia levantar.[278]

[275] Idem, p. 117.
[276] Idem, p. 117.
[277] Idem, p. 118.
[278] Idem, p. 118.

2.5. Direitos fundamentais atingidos pela utilização de *malware*

Quando se trata da utilização de malware em investigações de índole criminal é importante considerar os direitos fundamentais consagrados na Constituição Federal diretamente afetados por essa prática. A ausência de uma norma específica que fundamente e autorize a intervenção estatal por meio de malware levanta questões sobre a legalidade do seu uso e suas consequências. A proteção dos direitos fundamentais dos indivíduos é uma preocupação central em um Estado de Direito, e qualquer intervenção estatal que restrinja esses direitos deve ser devidamente fundamentada e autorizada pela lei. A falta de uma base legal sólida para a infiltração de malware coloca em dúvida a legitimidade e a legalidade dessa prática, bem como as evidências derivadas dela.

A Constituição Federal Brasileira de 1988 dispõe expressamente sobre proteções a liberdades e direitos fundamentais – ocasiona substancial releitura de todo ordenamento jurídico - de modo que novas tecnologias informáticas de investigação são passíveis de sofrer restrições diante da colisão com outros direitos fundamentais, os quais iremos abordar adiante.

No que concerne ao *malware* como meio de obtenção de prova em tempo real (monitoramento online), sua utilização, dentre outras possibilidades, pode se dar através da busca por provas internas (dados armazenados ou produzidos em tempo real) e externas (som e imagem) ao sistema informático.[279]

Em relação aos meios de obtenção de prova interna ao sistema informático, cita-se o armazenamento de dados e os produzidos, ambos em tempo real. O armazenamento de dados são os reservados ou que não estão disponíveis para acesso livre do público. Estes dados são armazenados de forma presencial ou online que se mostra ainda mais invasivo e agressivo aos direitos fundamentais.[280] Através do uso do malware na investigação criminal, não é possível garantir que se obtenha dados determinados, sendo uma devassa da vida do cidadão sem qualquer garantia de que se conseguirá abstrair uma prova concreta ou evidência relevante. Ademais, através do malware, se obtém o acesso desejado aos dados armazenados em dispositivos informáticos, mas também a outros tipos de dados, os quais não se encontram armazenados ou que estão sendo produzidos em tempo real, configurando uma devassa extrema devido a multifuncionalidade que tal método oculto pode ter.[281]

---

[279] RAMALHO, David Silva. **Métodos Ocultos de Investigação Criminal em Ambiente Digital**. Coimbra: Editora Almedina, 2017, p. 350.
[280] CAMPOS, Juliana Filipa Sousa. **O malware como meio de obtenção de prova em processo penal: a investigação oculta em ambiente digital – (monografias).** Coimbra: Editora Almedina, 2021, p. 88-89.
[281] Idem, p. 91.

Em relação aos dados produzidos em tempo real, o malware permite uma espécie de averiguação na fonte da comunicação, o que não se confunde com a interceptação das comunicações, visto que este método é capaz de captar dados de forma remota e oculta, além da possibilidade de apreender dados ainda em processo de produção. Dita intromissão só pode ser devidamente admitida se prevista expressamente em legislação específica.[282]

No caso de dados armazenados e produzidos em tempo real, o malware se configura como uma forma passiva de captação de informações e dados, diferente da infiltração de agentes que necessita de funcionários qualificados e que gozem da confiança do estado para se obter tais dados.[283] Portanto, considerando o alcance do método oculto de investigação em comento e seu expressivo potencial para ferir direitos fundamentais, apenas através de lei em sentido formal o *malware* poderia ser utilizado.[284]

Quando se fala dos meios de obtenção da prova externa ao sistema informático, refere-se a possibilidade do malware ativar mecanismos externos ao sistema, ativando, por exemplo, câmeras e microfones.[285] Essa ferramenta ultrapassa os limites inerentes aos direitos constitucionais consagrados no ordenamento jurídico, a partir do momento em que tal ativação pode alcançar outros dados, imagens e comunicações que não apenas as almejadas pela investigação no caso concreto. Ademais, a ativação de câmera e microfone em sede domiciliar contraria toda proteção constitucional dada a privacidade e intimidade do indivíduo em seu espaço particular.[286] Diante disso, o malware, para ser utilizado como método de investigação através da apreensão de prova externa ao dispositivo informático, deve se valer de casos excepcionalíssimos, baseado num regime legal garantístico para os investigados.[287]

De acordo com o a extensão de informações que o malware pode obter, bem como dos direitos fundamentais que ele pode restringir, este método sigiloso de investigação criminal pode interferir de forma agressiva na individualidade do investigado, e até mesmo, de terceiros envolvidos. Por ser um método oculto de averiguação, se torna também mais propícia a ocorrência de arbitrariedades estatais, contrariando a legalidade normativa do ordenamento jurídico, de forma que tal intromissão, somente poderia ocorrer de acordo com uma legislação que a regulamente, sob pena de incorrer em inconstitucionalidade material e nulidade das provas adquiridas.[288]

---

[282] Idem, p. 93.
[283] Idem, p. 96.
[284] Idem, p. 97.
[285] Idem, p. 98.
[286] Idem, p. 98.
[287] Idem, p. 99.
[288] Idem, p. 100.

A Carta Magna do Brasil garante aos cidadãos direitos essenciais que podem ser exercidos perante todas as esferas de poder estatal - o Poder Executivo, o Legislativo e o Judiciário (conforme disposto no artigo 5º da Constituição Federal). Existem áreas nas quais, em princípio, o Estado não pode intervir, regiões chamadas de direitos fundamentais. Diante da obrigação jurídica de proteger os indivíduos e a sociedade e de buscar os objetivos que lhe são atribuídos, o Estado pode ser compelido a invadir essas esferas individuais protegidas, se houver forte justificativa para tal. Esse movimento denomina-se intervenção estatal e ocorre quando o comportamento do Estado dificulta a prática de algo que está dentro do escopo de proteção dos direitos individuais. Uma intervenção deve ser devidamente justificada, caso contrário, se configura indevida violação aos direitos fundamentais.[289]

Existem, pelo menos, três cláusulas importantes que devem ser respeitadas em relação a todos os direitos fundamentais: o primeiro é de natureza formal e exige a existência de um embasamento legal; os outros dois são de natureza material e consistem em ser proporcional, além de garantir que a intervenção não comprometa o núcleo essencial ou a aprendizagem desses direitos.[290]

O limite formal, relacionado a reserva de lei, ao qual os direitos fundamentais estão sujeitos, está estabelecido constitucionalmente no artigo 5º, inciso II, da Constituição Federal: "ninguém será obrigado a fazer ou deixar de fazer algo senão em virtude de lei." Ademais, tanto o Poder Executivo quanto o Judiciário precisam de um embasamento legal que os habilite a tomar medidas contra os cidadãos. Isso ocorre porque, em uma democracia, na qual "todo o poder emana do povo, que o exerce por meio de representantes eleitos ou diretamente" - conforme artigo 1º, parágrafo único, da Constituição Federal - somente o povo tem a autoridade para conceder o poder de intervenção, através de seu consentimento expresso nas leis elaboradas por seus representantes.[291]

A lei não apenas regula as intervenções, mas também as fundamenta, autoriza e torna juridicamente viáveis. Portanto, não é possível justificar intervenções com o argumento de que não existem direitos absolutos ou com base na proporcionalidade, mas sim através de lei expressa que o permita intervir.[292] A lei deve ser precisa e estabelecer de forma clara e específica o que determina. Isso significa que é inadmissível estender o alcance da lei a

[289] GRECO, Luís; GLEIZER, Orlandino. A infiltração online no processo penal – Notícia sobre a experiência alemã. In: **Revista Brasileira de Direito Processual Penal**, Porto Alegre, vol. 5, n. 3, p. 1483-1518, set./dez. 2019. Disponível em: https://doi.org/10.22197/rbdpp.v5i3.278. Acesso em: 03 mai. 2023. p. 1485.
[290] Idem, p. 1486.
[291] Idem, p. 1486.
[292] Idem. p. 1486.

situações que não estão expressamente previstas nela, pois isso violaria o princípio da proibição da analogia. Em outras palavras, a lei deve ser interpretada estritamente de acordo com seu texto e não pode ser aplicada por analogia a casos não contemplados de forma explícita.[293]

No que concerne aos limites materiais, temos que uma intervenção declarada não pode comprometer o núcleo dos direitos fundamentais, também conhecido como conteúdo essencial ou de dignidade. Isso significa que mesmo que o Estado intervenha em certas circunstâncias, deve-se preservar a essência e o valor intrínseco dos direitos fundamentais, de forma que tal núcleo é intocável. O terceiro requisito geral para justificar uma intervenção em um direito fundamental é o princípio da proporcionalidade. Esse princípio atua como uma barreira que os direitos fundamentais de defesa estabelecem também em relação ao próprio legislador, impondo limites à imposição de restrições ao exercício dos direitos fundamentais. Dessa forma, os direitos fundamentais estabelecem "limites aos limites" que podem ser impostos pelo legislador, garantindo que qualquer intervenção seja proporcional e equilibrada em relação ao objetivo legítimo buscado. Uma intervenção nos direitos fundamentais deve ser idônea, necessária e adequada para alcançar o objetivo pretendido. Esse é o nível mais complexo na operacionalização da justificação das intervenções nos direitos fundamentais, uma vez que requer a consideração de questões de naturezas diversas. Nesse contexto, é necessário avaliar se a medida proposta é adequada para atingir o fim desejado, se é necessária no sentido de que não existem alternativas menos intrusivas disponíveis e se é idônea, ou seja, se possui uma relação de causa e efeito direta com o objetivo a ser alcançado. É nesse nível que considerações de diferentes naturezas se tornam relevantes para a justificação das intervenções nos direitos fundamentais.[294]

Feitos estes breves esclarecimentos sobre o funcionamento do *malware* na obtenção de dados, sejam estes internos ou externos ao sistema informático, além de esclarecimentos sobre os limites de restrições que podem ser impostas aos direitos fundamentais, cabe agora trazer alguns destes direitos constitucionalmente consagrados, que podem ser gravemente feridos pelo uso do *malware* como método investigativo autônomo não regulamentado.

O direito à privacidade abrange diversas dimensões e é considerado um dos direitos com maior relevância prática. Em outras palavras, não se resume apenas ao direito de se opor

[293] Idem, p. 1487.
[294] GRECO, Luís; GLEIZER, Orlandino. A infiltração online no processo penal – Notícia sobre a experiência alemã. In: **Revista Brasileira de Direito Processual Penal**, Porto Alegre, vol. 5, n. 3, p. 1483-1518, set./dez. 2019. Disponível em: https://doi.org/10.22197/rbdpp.v5i3.278. Acesso em: 03 mai. 2023. p. 1487-1488.

à divulgação da vida privada, mas também inclui o direito ao respeito dessa esfera íntima.[295] Este direito é definido pela habilidade de impedir que terceiros tenham acesso a informações sobre a vida privada e familiar, bem como pelo direito de não ter essas informações divulgadas. A abrangência normativa desse direito deve considerar três aspectos fundamentais: o respeito aos comportamentos individuais, a preservação do anonimato e o respeito às relações interpessoais.[296]

Na busca pela obtenção de provas no âmbito da justiça penal, existem limites constitucionais claros relacionados à esfera da vida privada. Por exemplo, não são permitidas buscas domiciliares nem interferências na correspondência, telecomunicações e outros meios de comunicação, uma vez que isso seria uma intromissão abusiva na vida privada.[297] Em resumo, a proteção da vida privada é fundamental para preservar os direitos fundamentais e os bens jurídicos pessoais. Ela impede a intromissão arbitrária e indiscreta em aspectos íntimos da vida, como vivências, espaços, segredos e emoções que o indivíduo, legítima e conscientemente, deseja manter reservados para si e para aqueles que escolhe compartilhar.[298]

A definição do cerne inalienável que constitui o direito à intimidade deriva da "teoria das esferas", que utiliza a figura de três círculos concêntricos de tamanhos progressivamente menores para demonstrar os níveis de restrições possíveis na esfera privada do indivíduo. No círculo mais externo se inclui situações de natureza pública, é a esfera social. O círculo intermediário representa a esfera da confiança ou sigilo, onde estão incluídas conversas e eventos íntimos, os quais não são do conhecimento público em geral. [299] No terceiro círculo está o âmago da esfera privada, o seu núcleo intocável, não há razão para qualquer intervenção. Para Greco, este círculo reflete a dignidade humana. Para Costa Jr. compreende uma parte da vida privada preservada em segredo. São situações e sentimentos que o sujeito, no seu interior, acredita não estar ao alcance de terceiros. [300]

O *malware* quando utilizado como meio de obtenção de prova, há uma clara restrição ao direito à reserva da intimidade. Primeiro porque o software malicioso possibilita,

---

[295] MIRANDA, Jorge; MEDEIROS, Rui**. Constituição Portuguesa Anotada**, tomo I, 2.a edição, Coimbra: Coimbra Editora, 2010, p. 290.
[296] CANOTILHO, J. J. Gomes; MOREIRA, Vital. **Constituição da República Portuguesa Anotada**, 4.a edição revista, volume I. Coimbra: Coimbra Editora, 2007, p. 468
[297] MIRANDA, Jorge; MEDEIROS, Rui**. Constituição Portuguesa Anotada**, tomo I, 2.a edição, Coimbra: Coimbra Editora, 2010, p. 291.
[298] ANDRADE, Manuel da Costa. "**Bruscamente no verão passado", a reforma do Código de Processo Penal.** Coimbra: Coimbra Editora, 2009. p, 155 e MIRANDA, Jorge; MEDEIROS, Rui**. Constituição Portuguesa Anotada**, tomo I, 2.a edição, Coimbra: Coimbra Editora, 2010, p. 291.p. 619-622.
[299] COSTA JR., Paulo José da. **O direito de estar só: tutela penal da intimidade.** Editora Revista dos Tribunais Ltda. 1970, p, 31.
[300] Idem, p. 34.

por exemplo, a ativação da webcam e do microfone do dispositivo informático do suspeito, de forma que é possível capturar, em tempo real, todos os momentos da sua vida íntima, expondo-o na sua intimidade mais brutal e transparente. Além disso, o sistema informático armazena uma enorme variedade de dados, como os relativos a negócios, atividades financeiras, trabalhos, escritos pessoais, fotos, vídeos, correspondências, entre outros. Dessa forma, o sistema funciona como uma espécie de diário, refletindo a essência e a vida do indivíduo.[301]

Diante disso, é possível restringir o direito à intimidade de forma legítima, desde que haja justificativas condicionadas aos princípios da investigação criminal orientada pela Constituição. Isso significa que a intervenção do Estado na esfera privada da intimidade do indivíduo deve ser autorizada por uma base legal estabelecida. A legitimidade da atuação estatal baseia-se na legalidade e no respeito à dignidade humana, que exige o respeito ao núcleo intocável da intimidade.

O direito à autodeterminação informativa, por sua vez, é o direito dos cidadãos de terem conhecimento de quem, quando e em que circunstâncias são conhecidas informações sobre eles. Ele representa uma proteção dos indivíduos diante do uso, armazenamento e transmissão ilimitados de seus dados pessoais. Esse direito busca garantir que as pessoas tenham controle sobre suas informações e possam decidir como elas são utilizadas, evitando abusos e violações de sua privacidade. O Tribunal Constitucional alemão tem entendimento sobre a questão que destaca a importância de se estar atento ao rápido avanço das tecnologias de informação e ao seu uso como medida de investigação. O tribunal ressaltou que tais práticas podem comprometer o direito constitucional à autodeterminação informativa, uma vez que permitem uma vigilância abrangente sobre um indivíduo e a construção de um perfil completo de sua personalidade. Essa abordagem seria considerada inadmissível do ponto de vista constitucional. O tribunal alertou para a necessidade de se encontrar um equilíbrio adequado entre a investigação criminal e a proteção dos direitos fundamentais dos cidadãos, levando em consideração os princípios de proporcionalidade e dignidade humana.[302]

A proteção de dados como um direito fundamental não absoluto, pode ser objeto de restrições. No entanto, trata-se de uma regra constitucional, o que significa que a intervenção do Estado em sua esfera deve ser a exceção e não a regra. Essa intervenção só é admissível quando há previsão constitucional que a justifique. Dito de outra forma, é necessário que

[301] ANDRADE, Manuel da Costa. "**Bruscamente no verão passado", a reforma do Código de Processo Penal.** Coimbra: Coimbra Editora, 2009. p, 167.
[302] ORTIZ PRADILLO, Juan Carlos. "**El impacto de la tecnología en la investigación penal y en los derechos fundamentales**", em VV.AA. Problemas actuales de la justicia penal, Madrid: Ed. Colex, 2013, p. 327.

existam fundamentos legais claros e específicos que autorizem a restrição do direito à proteção de dados, garantindo assim um equilíbrio adequado entre a preservação desse direito e as necessidades legítimas da sociedade, como a investigação criminal. O princípio da legalidade é essencial nesse contexto, assegurando que as restrições aos direitos fundamentais sejam estabelecidas de forma clara, precisa e em conformidade com a Constituição.[303]

De acordo com a interpretação constitucional, o conceito de domicílio abrange o lugar em que alguém habita, independentemente de ser moradia fixa, temporária, principal ou secundária, além do local onde essa pessoa exerce sua atividade profissional. Todos os indivíduos que habitam na residência estão protegidos por este direito, sendo irrelevantes as relações jurídicas existentes.[304] O Supremo tribunal de justiça português considera domicílio como:

> Aquela área que tem por objeto a habitação humana, aquele espaço fechado e vedado a estranhos, onde recatada e livremente se desenvolve toda uma série de condutas e procedimentos característicos da vida privada e familiar, ou seja, um núcleo restrito sob o signo da intimidade, de proteção da vida privada, da liberdade e da segurança individual, onde se desenrola a vivência essencial, no aspecto existencial, da pessoa.[305]

A violação jurídica do domicílio sempre foi caracterizada pela presença física e contínua de pessoas indesejadas, atravessando as barreiras concretas do local. Assim, a área protegida desse direito fundamental somente era invadida quando o agente ingressava de forma presencial e arbitrariamente no espaço físico delimitado.[306] Entretanto, os avanços tecnológicos permitiram a introdução de novas formas de interferência e invasão na esfera da privacidade e intimidade que estão no âmbito de proteção da inviolabilidade do domicílio. Essas novas modalidades de invasão têm em comum o fato de não necessitarem da entrada corpórea do agente no espaço físico da residência, mas que ainda assim podem resultar em um abalo irreversível deste direito.[307]

---

[303] RUARO, Regina Linden. **Privacidade e autodeterminação informativa: obstáculos ao Estado de vigilância?** Arquivo Jurídico – ISSN 2317-918X – Teresina-PI – v. 2 – n. 1 – p. 41-60. Jan./Jun. de 2015, p. 45.
[304] PALMA, Maria Fernanda. Tutela da vida privada e processo penal – realidades e perspectivas constitucionais. In: **Jurisprudência Constitucional**, número 10, abril/junho, Coimbra: Coimbra Editora, 2006.
[305] Acórdão do Supremo Tribunal de Justiça de Portugal, 2009, proc. n.º 06P2321.
[306] ANDRADE, Manuel da Costa. "**Bruscamente no verão passado", a reforma do Código de Processo Penal.** Coimbra: Coimbra Editora, 2009. p, 151.
[307] CANOTILHO, J. J. Gomes; MOREIRA, Vital. **Constituição da República Portuguesa Anotada**, 4.a edição revista, volume I. Coimbra: Coimbra Editora, 2007, p. 540.

A violação do ambiente domiciliar não se restringe apenas à entrada não autorizada na residência de alguém. Os avanços tecnológicos modernos permitem a invasão do domicílio por meios eletrônicos, que possibilitam a intrusão nas conversas e na vida privada do investigado, bem como dos demais moradores.[308] Diante dessa realidade, a solução para combater dita agressão a esse direito fundamental foi ampliar sua área de tutela. Dessa maneira, novas condutas, além da entrada física, passaram a ser reconhecidas como violadoras do domicílio, como a introdução de dispositivos de escuta, transmissão de imagens e sons, ou mesmo por meio de captação remota, em que o dispositivo não precisa necessariamente estar dentro do domicílio.[309]

De acordo com Roxin, a medida em comento tem sido objeto de críticas justificadas, devido ao fato de que ela não apenas afeta de forma pontual a esfera privada, mas sim a suprime por completo. Isso implica que todas as manifestações acústicas da vida, inclusive aquelas que ocorrem dentro do ambiente domiciliar, são controladas pelo Estado, representando assim um verdadeiro ataque à dignidade humana.[310]

Com o uso de *malware*, é potencial a violação desse direito, visto que atualmente, os sistemas informáticos, como smartphones, tablets e laptops, nos permitem utilizar suas funcionalidades em qualquer lugar, a qualquer momento. No entanto, o uso indevido de malware pode comprometer a privacidade e a segurança desses sistemas, representando uma ameaça à proteção dos dados pessoais e à intimidade dos usuários. É essencial adotar medidas de segurança adequadas para evitar e combater possíveis violações causadas por *malware*. Costa Andrade defende que, em termos de proteção da privacidade, não importa se alguém protege seus segredos nas folhas de um diário guardado em casa ou em um texto arquivado no computador localizado no mesmo local. Não há justificativa para tratamentos distintos em relação ao acesso indevido ao diário por meio de entrada não autorizada na casa ou pelo uso de técnicas de hacker.[311]

Com base no que foi exposto, é inegável que o domicílio está sujeito a novas formas de invasão e violação que não se limitam à entrada física, mas nem por isso menos prejudiciais. Devido à natureza oculta dessas novas formas de invasão e espionagem, advindas do progresso

[308] ANDRADE, Manuel da Costa. "**Bruscamente no verão passado", a reforma do Código de Processo Penal.** Coimbra: Coimbra Editora, 2009. p, 151-152.
[309] Idem, p. 152.
[310] ROXIN, Claus. "**La protección de la persona en el derecho processal alemán**", em La evolución de la política criminal, el derecho penal y el proceso penal, Valencia: Tirantlo Blanch, 2000, p. 155.
[311] ANDRADE, Manuel da Costa. "**Bruscamente no verão passado", a reforma do Código de Processo Penal.** Coimbra: Coimbra Editora, 2009. p, 154.

tecnológico, a inviolabilidade do domicílio agora enfrenta riscos diferentes e mais significativos, sobretudo com a ativação de mecanismos de malware.

O direito de não se autoincriminar garante que ninguém é obrigado a fornecer evidências contra si mesmo ou produzir provas que o incriminem. Nenhum indivíduo pode ser compelido, seja por uma autoridade ou por pessoa privada, a fornecer involuntariamente qualquer tipo de informação ou prova que possa levá-lo à incriminação. Esse direito visa proteger a dignidade e a liberdade individual, assegurando que cada pessoa não seja forçada a agir contra seus próprios interesses no âmbito de um processo legal. Dessa forma, qualquer tipo de prova contra o réu que dependa diretamente de sua ação só será considerada válida se for realizada de forma consciente e voluntária. É absolutamente inadmissível o uso de fraude, como através do uso do *malware,* ou de qualquer outra forma de violação dos direitos individuais para obtenção de provas.[312]

Nesse contexto, é importante mencionar as observações feitas por Cleunice Bastos Pitombo, que destaca que o responsável pela busca e apreensão deve seguir certos procedimentos antes de iniciá-la. Estes procedimentos são I. declarar sua identidade e o objetivo da diligência (conforme o artigo 245, parágrafo 1º, do CPP); II. exibir e ler o mandado de busca, exceto no caso da autoridade judiciária; III. notificar o investigado para mostrar o que está sendo procurado (parágrafo 5º). Essa forma de proceder é de extrema importância para a validade do ato processual.[313]

Partindo desse pressuposto, é justificável argumentar que a realização de uma busca e apreensão pelo meio do uso de um malware é ilegal, pois não cumpre os requisitos acima elencados, muito menos o da cientificação do investigado. A utilização de *malware* como meio para conduzir uma busca e apreensão é considerada ilegal de acordo com o artigo 8º, parágrafo 2º, "g" da Convenção Americana de Direitos Humanos - Pacto de San José da Costa Rica - da qual o Brasil é signatário. De acordo com o artigo 5º, parágrafos 2º e 3º, da Constituição Federal, tratados internacionais de direitos humanos têm status equivalente às emendas constitucionais, prevalecendo sobre qualquer interesse processual secundário estabelecido na legislação processual penal. Portanto, a Convenção mencionada possui uma hierarquia superior em relação às leis processuais penais brasileiras. Isso significa que o direito de não se autoincriminar, consagrado nesse tratado internacional, deve ser respeitado e aplicado,

[312] ROXIN, Claux. **La prohibición de autoincrinación y de las escuchas domiciliares**, apresentação de Francisco Muñoz Conde e Marcela De Langhe, Buenos Aires: Hammurabi, 2008, p. 28.
[313] PITOMBO, Cleunice Bastos. **Da busca e da apreensão no processo penal**. 2. Ed. São Paulo: Editora Revista dos Tribunais, 2005. 133-134.

independentemente de disposições processuais penais que possam estabelecer requisitos diferentes.[314]

Conforme destacado por João Cláudio Couceiro, o direito ao silêncio é parte de um direito mais amplo de todo indivíduo de não contribuir para a produção de qualquer prova que possa prejudicá-lo.[315]

2.6. Por que o malware não pode ser considerado método atípico de investigação?

O uso do *malware* como método de investigação oculto surgiu da evolução tecnológica, a qual está presente em vários aspectos da vida humana, não sendo indiferente ao direito processual penal. Tal instrumento de investigação, por ser algo relativamente atual, não veio, em muitos ordenamentos jurídicos, como o brasileiro e o português, acompanhado de legislação pertinente que direcione sua aplicação. O que se tenta, muitas vezes, é o seu uso no caso concreto, tendo por referência outras legislações, como a que trata do agente oculto, interceptação telefônica e escuta ambiental. Dessa maneira, o *malware* acaba sendo utilizado como método atípico de investigação, tendo em vista a falta de aparato legal específico que regulamente a sua prática, de forma que tal uso se dá sem a observância das garantias constitucionais e processuais penais, basilares do ordenamento jurídico.

Como explanado ao longo deste capítulo, existem princípios constitucionais que norteiam toda a atuação estatal, especialmente quando se trata de investigação criminal, seara na qual os direitos e garantias fundamentais ficam ainda mais expostos a potencial violação. Cita-se como exemplo destes princípios, os quais foram retratados neste trabalho, a reserva de lei, reserva de jurisdição, proporcionalidade e subsidiariedade. Sem perquirir a observância de tais fundamentos, se torna impossível o uso do *malware* como método sem expressa regulamentação legal no processo penal.

Ademais, além de contrariar todo ordenamento jurídico de um Estado de Direito, o qual é pautado no respeito às garantias e princípios constitucionais, a utilização do *malware* de forma indiscriminada, baseada apenas em legislações supostamente semelhantes, acaba por ferir de forma profunda e, por vezes, irreversível os direitos fundamentais dos cidadãos, a depender da forma e variação desse uso. Alguns destes direitos foram abordados ao longo deste

[314] Convenção Americana sobre Direitos Humanos (Pacto de São José da Costa Rica), de 22 de novembro de 1969.
[315] COUCEIRO, João Cláudio. **A garantia constitucional ao direito ao silêncio**. São Paulo: Editora Revista dos Tribunais, 2004, p. 152-155.

capítulo, são eles o direito à Vida Privada, Autodeterminação Informativa, Inviolabilidade do Domicílio e o direito à Não Autoincriminação. A preservação desses valores é de fundamental importância para a persecução de um processo penal justo e garantista.

A impossibilidade de tratamento do *malware* como método atípico, é evidenciada nas lições de Caprioli, que chama a atenção acerca do elevado nível de intromissão na vida privada do sujeito investigado decorrente do uso da referida metodologia. Segundo o autor, devem existir cautelas para o uso de tal ferramenta e para que esta que não macule direitos individuais. [316]

Diante do funcionamento do método *malware* como recurso investigativo, deve ser observado e até mesmo questionado se essa fonte de prova, caso usada pelo Estado, respeita os direitos e garantias fundamentais. Pois antes de uma medida coercitiva ser usada, conforme Bruzzone deve-se observar preliminarmente a sua tipicidade processual e os seus limites. Uma vez que qualquer interferência em direitos fundamentais deve ser proporcional e resguardar o que está previsto constitucionalmente.[317]

Acentua Tortosa que em face da divisão de poderes, o julgador penal só tem como incumbência a sua aplicação e não a criação no tangente a leis penais. Sendo a reserva legal um respeito aos direitos fundamentais. Devendo assim existir uma enorme cautela quanto ao cerceamento ou não de direitos e garantias fundamentais face a uma investigação criminal. Dentro dessa investigação, deve-se entender que não pode existir uma sobreposição a todo custo de um resultado no que concerne os fins que justifiquem seu uso, pois como requisitos tem-se a proporcionalidade, legalidade, jurisdicionalidade e motivação. [318]

Outros pontos são observados quando se aborda a reserva legal na esfera jurídica. A legislação penal guia-se pela taxatividade, não devendo existir uso arbitrário dos meios investigativos, muito menos de medidas cautelares. Devendo sempre serem observados os requisitos para utilização de medidas excepcionais, pois no meio digital não deve haver a inobservância de garantias face a privacidade, assim como é necessário existir um mandado de busca e apreensão tratando-se do meio físico, real - não virtual-, faz-se necessária também a existência de tais elementos no meio digital.

---

[316] CAPRIOLI, Francesco. **Il "captatore informatico" come strumento di ricerca della prova in Italia**. Revista Brasileira de Direito Processual Penal, Porto Alegre, vol. 3, n. 2, p. 483-510, mai./ago. 2017. https://doi.org/10.22197/rbdpp.v3i2.71. p, 485.

[317] BRUZZONE, Gustavo. **La nulla coactio sine lege como pauta de trabajo en matéria de medidas de coerción en el proceso penal.** Estudios sobre Justicia Penal: Homenaje al Profesor Julio B. J. Maier. Editores del Puerto Buenos Aires, 2005. p, 248.

[318] PUJADAS TORTOSA, Virgínia. **Para una teoria general de las medidas cautelares penales.** Tesis doctoral, Universitat de Girona, Departament de Dret Públic. Girona, enero de 2007, p. 357- 358.

Assim como no meio físico existem requisitos autorizadores para a invasão da privacidade, no meio digital deve existir também. Torre inclusive disserta acerca de alguns requisitos para o uso do malware como meio investigativo de prova, tendo em vista seu alto grau de detalhes e de inviolabilidade quanto a vida privada do investigado e das pessoas com quem ele mantém contato. Além disso, deve existir também uma delimitação quanto aos crimes suscetíveis ao uso de tal *software*.[319]

O autor retromencionado também evidencia a necessidade de existir uma individualização no concernente aos requisitos probatórios do uso do método investigativo. Tais requisitos, certamente restringem e impõe limites ao uso desenfreado de métodos ocultos de investigação, pois é de certa forma uma ponderação e proporcionalidade face ao direito do sujeito investigado, bem como a necessidade de colher informações criminais.[320]

As medidas excepcionais não podem se tornar regras dentro do rito processual penal, pois o que ocorrerá é a banalização do seu uso, bem como um desdém aos direitos individuais e fundamentais.

Dessa forma, por todo o discorrido nestas linhas, observamos que o uso do *malware* como método atípico de investigação criminal, sem uma legislação expressa que regulamente de forma específica sua utilização, acaba por se transformar num instrumento de poder do Estado frente ao indivíduo, intervindo na esfera da vida inviolável e sendo gerador de potencial arbitrariedades e agressão a valores sagrados, inerentes aos cidadãos e assegurados pela Carta Magna, no contexto de um Estado de Direito.

Como solução desta questão, a regulamentação, através de lei em sentido estrito, estabelecedora dos limites formais e materiais de sua atuação, se mostra a única maneira de se fazer uso deste método oculto de investigação criminal, uma vez que não cabe intervenção sem lei que a autorize, com o que se mostra inadmissível estender seu alcance a hipóteses não previstas expressamente. Para tanto, passaremos a expor a seguir, uma proposta de sistematização de lei formal com base na normatividade alemã, que já possui legislação específica para o uso do *malware*.

3. PROPOSTA DE SISTEMATIZAÇÃO PARA BRASIL E PORTUGAL.

[319] TORRE, Marco et al. il captatore informatico dopo la legge cd "spazza-corrotti. In: **Diritto penale e processo**. 2019. p. 648-652.
[320] Idem, p. 648-652.

Realizada a análise acerca dos principais métodos ocultos de investigação que poderiam legitimar o uso do *malware* nos ordenamentos brasileiro e português, e tendo sido apontado os principais posicionamentos doutrinários sobre o tema, os quais tentam admitir o acesso a referida metodologia investigativa, com base em dispositivos já consagrados. Tendo sido feita também uma análise principiológica e de direitos fundamentais atingidos com o uso do *malware*, e tendo se chegado à conclusão de que o mesmo não pode ser admitido de forma atípica, nem no Brasil, nem em Portugal, uma vez que viola profundamente direitos fundamentais do investigado e daqueles que com ele interagem, especialmente quando usado como forma de monitoramento *online*.

Sob outro prisma, tendo-se em vista também que a referida metodologia já se encontra positivada em outros ordenamentos jurídicos, a exemplo do alemão, espanhol e italiano, e que a informatização e o avanço tecnológico advindos da sociedade da informação não permitem o desprezo das novas ferramentas tecnológicas de investigação, fica ainda mais clara a necessidade de regulamentar taxativamente o *malware* nas duas ordens jurídicas em comento. De modo que se consiga alcançar um equilíbrio entre os interesses conflitantes em jogo (direitos fundamentais x eficácia das investigações).

Assim, a regulamentação do *malware* deve prezar pela sua natureza excepcional, sendo utilizada de forma subsidiária, ou melhor, como *última ratio* para fins de elucidar supostas práticas delitivas. Deve também a lei regular o estrito procedimento referente ao seu uso, atentando-se para necessidade de reserva de juiz, restrição dos sujeitos passivos que podem ser alvos da medida, definição da fase processual em que se admite sua utilização, delimitação do período da diligência, dentre outros procedimentos pertinentes. Desta feita, partindo-se das inspiradoras disposições sobre *malware* previstas na norma alemã, alguns requisitos, a partir de agora, serão trabalhados visando uma proposta de sistematização para Brasil e Portugal.

Um primeiro e óbvio ponto trata-se da necessidade de expressa previsão em lei. Assim, para que seja ponderada a utilização do *malware* como meio de obtenção de prova penal, é preciso que o Poder Legislativo, através de lei autônoma, introduza a referida metodologia nas ordens jurídicas dos países em análise.

Sobre este aspecto formal, Greco e Gleizer aduzem que a intervenção estatal em direitos fundamentais deve ser sempre justificada por meio de lei, sendo essa que "fundamenta, autoriza, torna juridicamente possível a intervenção". Sendo inaceitável, segundo os autores,

utilizar da proporcionalidade ou do argumento de que inexiste direito absoluto para autorizar a intrusão em direitos fundamentais sem lei expressa para tanto.[321]

Neste mesmo sentido, Campos também considera indispensável a reserva de lei para positivação do *malware*. De acordo com a autora retromencionada, a referida metodologia investigativa tem de estar prevista em legislação distinta das que regulam os demais métodos ocultos. E com fim de tornar claro o conceito de *malware*, a autora pondera que o legislador deve afastar terminologias abstratas, a exemplo de "meios e dispositivos informáticos", bem como os termos "buscas" ou "pesquisas" (*online*).[322]

Assim, o *malware* deve ser previsto em legislação autônoma, que estabeleça o seu conceito e indique as várias funcionalidades inerentes ao seu uso, diferindo, assim, do que ocorre na Alemanha, em que o *StPO* utiliza alguns termos abertos e estabelece as várias possibilidades de intrusão, por *malware*, em dispositivos legais distintos. Como exemplo, cita-se que a *quellen-tkü* ou "vigilância na fonte" (§100a, n° 1, p. não numerado) encontra-se em posição geográfica distante da *online-durchsuchung* ou "busca *online*" (§100b) e é referida por "meios técnicos", no *StPO*.

Em relação aos crimes suscetíveis de investigação pela referida metodologia, aponta-se a necessidade de criação de um catálogo específico de crimes, de modo que o referido método alcance, apenas, os delitos considerados mais graves pelo legislador, de acordo com a realidade social de cada país.

Nas lições de Campos, o catálogo de crimes para o *malware* não pode fazer remissão para os crimes constantes no rol de outros meios de obtenção de prova e deve se ater "as formas mais graves de criminalidade, tendo em conta o seu grau de lesividade para os direitos, de modo a respeitar-se o princípio da proporcionalidade ou da proibição de excesso."[323]

E no que tange ao espectro do monitoramento *online*, por óbvio, o catálogo de crimes deve ser ainda mais delimitado, uma vez que a possibilidade de recolha, em tempo real, de prova interna e externa ao dispositivo informático, macula com, ainda mais, ênfase os direitos fundamentais do investigado do que um simples e único acesso ao dispositivo infectado.

Diante disso, ainda que o catálogo de crimes seja elaborado de acordo com a função do *malware*, que será ativada pelo investigador, pensa-se que o rol de crimes não pode ser tão

---

321 GRECO, Luís; GLEIZER, Orlandino. A infiltração online no processo penal – Notícia sobre a experiência alemã. In: **Revista Brasileira de Direito Processual Penal**, Porto Alegre, vol. 5, n. 3, p. 1483-1518, set./dez. 2019. Disponível em: https://doi.org/10.22197/rbdpp.v5i3.278. Acesso em: 03 mai. 2023. p. 1486.

322 CAMPOS, Juliana Filipa Sousa. **O malware como meio de obtenção de prova em processo penal: a investigação oculta em ambiente digital – (monografias).** Coimbra: Editora Almedina, 2021, p. 181 -182.

323 Idem, p. 183.

abrangente como ocorre com a *quellen-tkü* "vigilância na fonte" (§ 100a n° 1, p. não numerado), como ressalta Campos.[324]

Além disso, a gravidade dos crimes suscetíveis de utilização de *malware* não pode ser aferida apenas de forma abstrata, pela simples previsão do tipo penal no catálogo de crimes, mas também concretamente, por meio das especificidades ou particularidades do caso concreto.

Conforme Greco e Gleizer, no que diz respeito ao nível de suspeita acerca da prática do crime, pondera-se que o legislador alemão não delimitou o grau de suspeita necessário para introdução de *malware* no dispositivo alvo, sendo o tema trabalhado pela jurisprudência alemã que ao analisar outros métodos ocultos, divide os níveis de suspeita em inicial, suficiente e forte.[325] Assim, pensa-se que o nível de suspeita deve ser "assente em factos e racionalmente sustentada".[326] É dizer: uma denúncia anônima ou mera suspeita com poucos elementos fáticos, por si só, é insuficiente para autorizar a utilização do *malware*.

Campos, por sua vez, entende que a suspeita tem de ser "qualificada" e que atenda a um "determinado nível de concretização". Ainda segundo ela, o uso do *malware* também pode ser justificado ainda que seja direcionado a uma pessoa que não seja efetivamente suspeita da prática de um crime, mas que possa fornecer elementos de provas indispensáveis para resolução do caso. Contudo, a autora ressalta que nesta hipótese deve se ter cuidado para que o *malware* não seja usado sem causa provável ou escopo tangível, como verdadeiro mecanismo de "*fishing expeditions*".[327] Em outras palavras, o investigador deve identificar minimamente o suspeito alvo da técnica malware, sob pena da investigação torna-se ilícita.

Em sentido semelhante, Grego e Gleizer ponderam que invariavelmente terceiros não investigados poderão ser afetados pela infiltração por *malware*, o que é uma consequência inevitável da medida, visto que os sistemas informáticos atuais armazenam informações não apenas do usuário, mas também de amigos e familiares deste.[328]

Para além da necessidade de lei expressa, é preciso que essa lei determine a função do malware que vai ser ativada no caso concreto, tratando especificamente se serão recolhidos os dados armazenados, dados produzidos em tempo real, ambos ou se será ativado o hardware

---

[324] Idem, p. 183.
[325] GRECO, Luís; GLEIZER, Orlandino. A infiltração online no processo penal – Notícia sobre a experiência alemã. In: **Revista Brasileira de Direito Processual Penal**, Porto Alegre, vol. 5, n. 3, p. 1483-1518, set./dez. 2019. Disponível em: https://doi.org/10.22197/rbdpp.v5i3.278. Acesso em: 03 mai. 2023. p.1498-1499.
[326] CAMPOS, Juliana Filipa Sousa. **O malware como meio de obtenção de prova em processo penal: a investigação oculta em ambiente digital – (monografias).** Coimbra: Editora Almedina, 2021, p.183.
[327] Idem, p. 183-185.
[328] GRECO, Luís; GLEIZER, Orlandino. A infiltração online no processo penal – Notícia sobre a experiência alemã. In: **Revista Brasileira de Direito Processual Penal**, Porto Alegre, vol. 5, n. 3, p. 1483-1518, set./dez. 2019. Disponível em: https://doi.org/10.22197/rbdpp.v5i3.278. Acesso em: 03 mai. 2023. p.1503.

para recolha de elementos externos. Nesse mesmo sentido, Campos ressalta que a delimitação da funcionalidade também é importante no que concerne à proteção dos direitos fundamentais que serão atingidos. Ela destaca que os requisitos deverão ser diferentes de acordo com o nível de intrusão, de forma que se for instalado no âmbito domiciliar, não será possível a recolha de prova externa ao dispositivo informático.[329]

Assim, ainda que seja possível a recolha de prova externa ao dispositivo informático na Alemanha no âmbito do domicílio (§100c, *StPO*), entendemos que tal hipótese não se afigura admissível, uma vez que a inviolabilidade domiciliar é prevista como garantia constitucional intocável. Além disso, ativar o *hardware* para recolha de prova externa, faz com que o investigado, de sujeito de direito passa para condição de objeto processual.

No que diz respeito a duração da medida, acreditamos que a legislação a ser elaborada deve fixar um período limítrofe de tempo para que a medida seja executada, baseando-se na proporcionalidade, de forma que não dure tempo maior do que o previsto para outros meios menos intrusivos já existentes. [330]

Ademais, todos os requisitos abordados, servem também como base para proporcionar o direito ao contraditório, de forma que o investigado poderá ter acesso de aferir a credibilidade das provas produzidas e ser capaz de defender-se dignamente. Do contrário ocorreria, nas palavras de Campos "uma radical desigualdade material de partida entre o arguido e o Estado". Para tanto, é necessário estabelecer mecanismos para preservar os dados acessados, bem como a integridade do malware utilizado, através do registro do seu código-fonte.[331]

A proibição do excesso, como vertente do princípio da proporcionalidade, deve orientar os requisitos materiais, no que concerne ao seu conteúdo e procedimentos, bem como deve ser considerado pelo aplicador do direito, no caso concreto, na autorização ou não do uso dessas medidas.[332]

Desse modo, o *malware* deve ser encarado como a última opção para obtenção da prova penal. É dizer: primeiro se opta por um método aberto de investigação, caso insuficiente, parte-se para o uso dos métodos ocultos, e por último, em caso de novo insucesso, é que se

[329] CAMPOS, Juliana Filipa Sousa. **O malware como meio de obtenção de prova em processo penal: a investigação oculta em ambiente digital – (monografias).** Coimbra: Editora Almedina, 2021, p.183.
[329] Idem, p. 185.
[330] Idem, p. 185-186.
[331] Idem, p. 186.
[332] Idem, p. 187-188.

lança mão do *malware*, respeitando-se o seu caráter subsidiário.[333] De modo que a opção menos intrusiva em direitos fundamentais deve ser escolhida, seja quando se está diante de um método aberto e outro oculto, ou entre dois métodos ocultos.[334]

Diante de todo o exposto, tem-se, que cumpre ao poder legislativo do brasil e de Portugal, elaborar projeto de lei prevendo expressamente um dispositivo legal, específico sobre malware, de modo que este contenha todo o procedimento para a utilização da referida metodologia, respeitando o seu caráter subsidiário, proporcional, bem como a reserva de jurisdição. Ao autorizar a medida, de forma excepcional, o juiz terá que informar, ainda que em momento posterior, o tipo de malware e a sua funcionalidade ativada, devendo ficar comprovado que não houve alteração no dispositivo informático acessado, de modo que tenha sido preservada a integridade da prova e do sistema de informática.

Portanto, fica evidente que se faz necessária a sistematização normativa de forma autônoma, nas duas ordens jurídicas aqui tratadas. No entanto, é importante destacar que, diferentemente do que ocorre na Alemanha, acreditamos que a recolha de prova externa dentro do âmbito domiciliar é contrária a todo ordenamento jurídico inserido no contexto de um estado democrático de direito, uma vez que este método de obtenção de prova invade o núcleo fundamental do direito a inviolabilidade domiciliar consagrado na Carta Maior, a qual serve de base e orientação para todo ordenamento jurídico. O desrespeito a esse postulado, pode acarretar a inutilização do material recolhido, no Brasil, sob a égide da prova ilícita, e em Portugal sob o parâmetro do método proibido de prova. Pensar de modo contrário, é ir de encontro a todo o aparato de garantias e proteção a dignidade humana e aos seus direitos fundamentais, sob pena de se transformar o processo penal num instrumento de arbitrariedade e injustiça social.

---

[333] GRECO, Luís; GLEIZER, Orlandino. A infiltração online no processo penal – Notícia sobre a experiência alemã. In: **Revista Brasileira de Direito Processual Penal**, Porto Alegre, vol. 5, n. 3, p. 1483-1518, set./dez. 2019. Disponível em: https://doi.org/10.22197/rbdpp.v5i3.278. Acesso em: 03 mai. 2023. p.1501.

[334] ANDRADE, Manuel da Costa. Métodos Ocultos de Investigação (plädoyer para uma teoria geral). In*:* **Que futuro para o direito processual penal? Simpósio em homenagem a Jorge de Figueiredo Dias, por ocasião dos 20 anos do Código de Processo Penal Português**, (coord. Mário Ferreira Monte entre outros). Coimbra: Coimbra Editora, 2009, p. 546.

CONCLUSÃO

É inegável o rápido avanço e impacto das inovações tecnológicas e científicas nas últimas décadas que têm transformado todos os aspectos do cotidiano. Essas mudanças abrangem todas as esferas da existência humana, incluindo o ramo jurídico e especificamente, o sistema de justiça penal. Este, como reflexo do Estado e dos conflitos sociais, deve acompanhar as transformações nas condições socioeconômicas, políticas e culturais da sociedade, tanto em relação aos crimes cometidos, quanto à dinâmica do processo penal.

No âmbito do direito penal, a evolução tecnológica foi consagrada através do surgimento de novos tipos de crimes, como também, pelo *modus operandi* das tradicionais condutas delitivas que passaram a ocorrer não apenas no mundo físico, mas também e, principalmente, no ambiente digital. Nesse diapasão, o tema da prova digital ganhou destaque, uma vez que esta desempenha papel importante no sistema judiciário, devido ao crescente uso da tecnologia na sociedade. Todavia, ao tempo que trouxe mais facilidade para os procedimentos burocráticos, a aquisição da prova digital apresenta questionáveis problemas para a cadeia de custodia da prova, uma vez que não há garantia acerca da confiabilidade dos dados coletados.

Outra característica desse novo cenário, é dar maior relevo a fase de investigação criminal em detrimento do processo penal, o qual é orientado pelo contraditório e a ampla defesa. Observa-se, assim, uma propensão para que o julgamento se transforme em um mero procedimento formal, enquanto o enfoque principal recai sobre os resultados das apurações clandestinas.

Se de um lado, a tecnologia trouxe consigo o surgimento de novos tipos de crimes, bem como a possibilidade de os tradicionais serem perpetrados no ambiente digital. Por outro lado, os métodos tradicionais de obtenção de provas revelaram-se insuficientes, em razão do avanço tecnológico e o recurso a técnicas anonimizadoras por parte dos criminosos, para ocultação e identificação de crimes. Diante disso, o Estado passou a necessitar de técnicas investigativas inovadoras, o que resultou na introdução de novos elementos e abordagens, e com eles o *malware*. Este pode ser enquadrado como método oculto de investigação por possuir as mesmas características desta categoria doutrinal. É dizer, com o *malware*, assim como ocorre nas escutas telefônicas e no agente encoberto, as provas são adquiridas clandestinamente, sem o conhecimento do investigado, que de forma involuntária fornece elementos auto incriminatórios para a investigação.

O *malware* possui relevância prática para a investigação criminal por possibilitar a recolha à distância, dos dados armazenados, não armazenados ou produzidos em tempo real, constantes no sistema informático alvo. Assim, por possuir diversas funcionalidades, tal metodologia representa um significativo risco para a garantia dos direitos fundamentais dos investigados, razão pela qual deve-se buscar um equilíbrio para sua utilização.

O ponto de tensão do presente trabalho gira em tono do eterno debate entre a eficácia das investigações e os direitos fundamentais. Desta forma, buscou-se uma solução que garantisse a utilização desses modernos métodos investigativos, sem abrir mão dos direitos fundamentais do investigado.

No contexto deste trabalho, foram estudados os ordenamentos jurídicos do Brasil e Portugal, os quais não preveem expressamente recurso à metodologia *malware* para obtenção de prova penal. Para isto, foi necessário buscar inspiração em legislações estrangeiras, em especial, a alemã, a qual possui experiências com a utilização do *malware*, tanto de forma preventiva – no combate ao terrorismo – como também em suas investigações criminais.

Num primeiro momento, buscou-se legitimar o *malware* no regime de outros métodos ocultos já positivados, não obtendo-se êxito, pois apesar de algumas similitudes, se identificou barreiras intransponíveis, razões pelas quais rechaçou-se o enquadramento do *malware* no regime das buscas domiciliares, das interceptações telefônicas, do agente encoberto e nos demais. No que se refere ao ordenamento jurídico português, ainda que a doutrina tente enquadrar o referido método na Lei do Cibercrimes, mais especificamente, nos dispositivos das pesquisas de dados informáticos e do agente encoberto em ambiente digital, verificou-se a impossibilidade de enquadramento legal, uma vez que toda intervenção em direitos fundamentais necessita ser justificada e autorizada pela lei formal.

Assim, da análise do ordenamento alemão, notou-se que o *malware* encontra-se positivado por meio de quatro dispositivos legais, os quais regulam diferentes funcionalidades deste método oculto. Estabelecem critérios e procedimentos para recolha da prova por meio do *malware*, entre eles citam-se a suspeita do fato, gravidade em concreto do fato, subsidiariedade e proporcionalidade em sentido estrito.

Posto isto, tem-se que diante da falta de uma regulamentação legal completa e especificamente direcionada, é necessário considerar que o uso de *malware*, como método de obtenção de provas, deve ser proibido, não podendo enquadrá-lo como método atípico de investigação. Essa proibição implica na impossibilidade de valorar as informações obtidas por meio desse invasivo instrumento.

Desta maneira, compete ao poder legislativo, tanto no Brasil quanto em Portugal, a elaboração de um projeto de lei que inclua um dispositivo legal explícito e específico sobre o uso de *malware*. Esse dispositivo deve abranger todo o procedimento para a utilização dessa metodologia, respeitando sua natureza subsidiária, proporcional e a necessidade de autorização judicial. A finalidade é estabelecer um marco legal que regulamente de maneira adequada o uso de *malware*, garantindo que sua aplicação seja realizada de forma justa e em conformidade com os princípios legais.

No que tange a hipótese de monitoramento *online* por *malware*, em que se pode obter prova interna e externa ao dispositivo informático em tempo real, pensa-se que deve haver uma maior cautela por parte do legislador. Assim, defendemos que não se admite a realização de monitoramento *online*, seja para recolha de prova interna ou externa, pois viola o núcleo essencial dos direitos fundamentais consagrados constitucionalmente.

Podemos concluir que as auto incriminações obtidas por esta metodologia, no frigir dos ovos, ressuscita sistemas políticos de natureza autoritária e estruturas inquisitórias, as quais fundam-se na procura da verdade a qualquer preço, ainda que em detrimento aos direitos e garantias fundamentais. Deste modo, busca-se a utilização desta ferramenta de forma prudente na persecução criminal.

BIBLIOGRAFIA

ABEL, W; SCHAFER, B. **The German Constitutional Court on the Right in Confidentiality and Integrity of Information Technology Systems**. in V Madhuri (ed.), Hacking: A Legal Quandary. Icfai University Press. Disponível em: https://www.pure.ed.ac.uk/ws/portalfiles/portal/15050731/The_German_Constitutional_Court_on_the_Right_in_Confidentiality_and_Integrity_of_Information_Technology_Systems.pdf.

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

ANDRADE, Manuel da Costa. **"Bruscamente no verão passado", a reforma do Código de Processo Penal**. Coimbra: Coimbra Editora, 2009.

ANDRADE, Manuel da Costa. Métodos Ocultos de Investigação (plädoyer para uma teoria geral). In: **Que futuro para o direito processual penal? Simpósio em homenagem a Jorge de Figueiredo Dias, por ocasião dos 20 anos do Código de Processo Penal Português**. Coimbra: Coimbra Editora, 2009.

BADARÓ, Gustavo Henrique. Os standards metodológicos de produção na prova digital e a importância da cadeia de custódia. In: **Boletim IBCCRIM**, ano, v. 29, 2021.

BARBIERO, Diego Roberto. **Implantação de Malwares em Investigações Complexas**. Curitiba: Juruá, 2021.

BATISTA, Lydie Jorge Batista. **O malware como meio de obtenção de prova em processo penal**. 2018. Dissertação (Mestrado em Direito) Faculdade de Direito da Universidade de Lisboa, Lisboa, 2018.

BRUZZONE, Gustavo. **La nulla coactio sine lege como pauta de trabajo en matéria de medidas de coerción en el proceso penal.** Estudios sobre Justicia Penal: Homenaje al Profesor Julio B. J. Maier. Editores del Puerto Buenos Aires, 2005

CAIRES, João Gouveia de. "Métodos ocultos de criminalidade econômico-financeira: entre a (a)tipicidade e a cumulação. In: **Revista Julgar**, n° 38, (maio/agosto), 2019.

CAMPOS, Juliana Filipa Sousa. **O malware como meio de obtenção de prova em processo penal: a investigação oculta em ambiente digital – (monografias).** Coimbra: Almedina, 2021.

CANOTILHO, J. J. Gomes; MOREIRA, Vital. **Constituição da República Portuguesa Anotada**, 4.a edição revista, volume I. Coimbra: Coimbra Editora, 2007.

CAPRIOLI, Francesco. **Il "captatore informatico" come strumento di ricerca della prova in Italia**. Revista Brasileira de Direito Processual Penal, Porto Alegre, vol. 3, n. 2, p. 483-510, mai./ago. 2017.

CARRELL, Nathan E. **Spying on the mob: United Sta Tes v. Scarfo - a constitutional analysis**. JOURNAL OF LAW, TECHNOLOGY & POLICY. Vol. 2002.

CASEY, Eoghan. **Digital evidence and computer crime: forensic Science, computers and the internet.** Third Edition. Waltham: Elsevier, 2011.

CASTELLS, Manuel. **A Sociedade em rede**. Vol. 1. 8ª ed. rev. e ampl. São Paulo: Paz e terra, 2005.

CASTRO, Luiz Augusto Sartori de. Busca e apreensão mediante uso de malware. In: **Boletim IBCCRIM**, São Paulo, v. 21, n. 251, p. 6-8, out..2013.

CHIRINO SANCHEZ, Alfredo. Las tecnologias de la informacion y el processo penal: análisis de uns crisisanunciada. **Revista de ciências penales de Costa Rica.** Rep. Fed. de Alemania 6, 1982.

CORREIA, João Conde. Prova digital: as leis que temos e a lei que devíamos ter. In: **Revista do Ministério Público**, ano 35, n° 139, 2014.

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

COSTA JR., Paulo José da. **O direito de estar só: tutela penal da intimidade.** Editora Revista dos Tribunais, 1970.

COUCEIRO, João Cláudio. **A garantia constitucional ao direito ao silêncio**. São Paulo: Editora Revista dos Tribunais, 2004.

CRIADO POVEDA, Miguel Ángel. **Delitos em la red: cibercrimen, ciberdelitos, ciberseguidad, ciberespionage y ciberterrorismo**. Madrid: Fragua, 2015.

DA SILVEIRA, Maria Ana Barroso de Moura. **Da problemática da investigação criminal em ambiente digital - em especial, sobre a possibilidade de utilização de malware como meio oculto de obtenção de prova**, (dissertação de mestrado). Universidade Católica Portuguesa: Lisboa, 2016.

DE LA CUEVA, Pablo Lucas Murillo. La construcción del derecho a la autodeterminación informativa. **Revista de Estudios Políticos** (Nueva Época), n. 104, p. 35-60, abr./jun. 1999.

DELGADO MARTIN, Joaquin. **La prueba electronica en el proceso penal**. Diario La Ley, Nº 8167, Sección Doctrina, 10 Oct. 2013, Año XXXIV, Editorial La Ley, 2013.

DE MENEZES, Isabela Aparecida; BORRI, Luiz Antonio; SOARES, Rafael Junior. A quebra da cadeia de custódia da prova e seus desdobramentos no processo penal brasileiro. In: **Revista brasileira de direito processual penal**, v. 4, n. 1, 2018.

DIAS, Jorge de Figueiredo. Revisitação de algumas ideias-mestras da teoria das proibições de prova em processo penal (Também à luz da jurisprudência constitucional portuguesa). In: **Revista de Legislação e de Jurisprudência**, Coimbra, A. 146, n. 4000, 2016.

DI GIORGI, Alessandro; PRADO, Geraldo. Mesa 3: O processo penal das formações sociais do capitalismo pós-industrial e globalizado e o retorno à prevalência da confissão – da subsistiência da tortura aos novos meios invasivos de busca de prova e à pena negociada. In: KARAM, Maria Lúcia (Org.). **Globalização, sistema penal e ameaças ao Estado Democrático de Direito**. Rio de Janeiro: Lumen Juris. 2005.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

ENDERS, Christoph. **The Right to have Rights**: The concept of human dignity in German Basic Law. Revista de Estudos Constitucionais, Hermenêutica e Teoria do Direito. 2018.

FACCHINI NETO, Eugênio. Reflexões histórico- evolutivas sobre a constitucionalização do direito privado, In: SARLET, Ingo Wolfgang (org). **Constituição, Direitos Fundamentais e Direito Privado**. Porto Alegre: Liv. Do Advogado, 2003.

FERRAJOLI, Luigi. **Derecho y Razon: teoría del garantismo penal**. Madrid: Editorial Trotta, 1995.

FRANÇA, Leandro Ayres. Cibercriminologias. In: **Criminologias alternativas.** Organizado por Pat Carlen e Leandro Ayres França. Porto Alegre: Canal Ciências Criminais, 2017.

GERCKE, Marco. **Understanding Cybercrime: A Guide for Developing Countries**. Geneva: International Telecommunication Union, 2011.

GIACOMOLLI, Nereu José. **A fase preliminar do processo penal: crises, misérias e novas metodologias investigatórias.** Rio de Janeiro: Editora Lumen Juris, 2011.

GIACOMOLLI, Nereu. **O Devido Processo Penal: Abordagem conforme a Constituição Federal e o Pacto de São José da Costa Rica**. 2ª ed. rev. e ampl. São Paulo: Atlas, 2015.

GRECO, Luís; GLEIZER, Orlandino. **A infiltração online no processo penal** – Notícia sobre a experiência alemã. Revista Brasileira de Direito Processual Penal, Porto Alegre, vol. 5, n. 3, p. 1483-1518, set./dez. 2019. Disponível em: https://doi.org/10.22197/rbdpp.v5i3.278. Acesso em: 03 mai. 2023.

HARRIS, Ryan. **Arriving at an anti-forensics consensus: Examining how to define and control the antiforensic sproblem, Digital Investigation - The international Journal of Digital Forensics & Incident** Response, Vol. 03 – Suplemento, 2006.

HASSEMER, Winfried. **Fundamentos del derecho penal**, trad. de Arroyo Zapatero y Muñoz Conde, Barcelona: Bosch, 1984.

HOFFMANN-RIEM, Wolfgang. **Innovaciones en la Jurisprudencia del Tribunal Constitucional Alemán, a Propósito de la Garantía de los Derechos Fundamentales en Respuesta a los Cambios que Conducen a la Sociedad de la Información**. Direito Público, 12(64). Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/2557.

HORNUNG, G., SCHNABEL, C. **Data protection in Germany I**: The population census decision and the right to information self-determination. Computer Law & Security Report, vol. 25, número 1, 2009.

KAPPLER, Katrin. **Consequences of the German Constitutional Court's Ruling on Germany's Foreign Intelligence Service**: The Importance of Human Rights in the Cooperation of Intelligence Services. German Law Journal, 2022.

KRUGLIANSKAS, Isak; MATIAS-PEREIRA, José. Um enfoque sobre a Lei de Inovação Tecnológica do Brasil. **Revista de Administração Pública**, v. 39, n° 5, 2005.

LIMA, Manuela Ithamar; DA COSTA, Sebastião Mendes. Direito, inovação e ciência: possibilidades e desafios da sociedade do conhecimento. In: **Revista Jurídica Eletrônica da UFPI**, v. 6, n. 01, 2011.

LYOTARD, Jean François. **O Inumano, considerações sobre o tempo**. 2ª Ed: Estampa, 1997.

LOPES JR. Aury. **Direito processual penal.** 13ª ed. São Paulo. Saraiva, 2016.

LOPES JR., Aury. O problema da "verdade" no processo penal**.** In: GRINOVER, Ada Pellegrini, et all. **Verdade e prova no processo penal: Estudos em homenagem ao professor Michele Taruffo**.1 ed. Brasília, DF: Gazeta Jurídica, 2016.

MARSHALL, Angus. **Digital forensics: digital evidence in Criminal Investigation**. Wiley-Blackwell. 2008.

MACIEL, Maria Lucia. Ciência, tecnologia e inovação: ideias sobre o papel das ciências sociais no desenvolvimento. In: **Revista Parcerias Estratégicas**, v.10, n° 21, 2005.

MENDES, Carlos Hélder. **Malware do estado e processo penal: a proteção de dados informáticos face à infiltração por software na investigação criminal**. Dissertação de Mestrado. Pontifícia Universidade Católica do Rio Grande do Sul. 2018.

MENDES, Paulo de Sousa. As proibições de prova no processo penal. Coord. Maria Fernanda Palma. In: **Jornadas de direito processual penal e direitos fundamentais**. Coimbra: Editora Almedina, 2004.

MENDES, Paulo de Sousa. O processo penal entre a eficácia e as garantias. In: PALMA, Maria Fernanda; DIAS, Augusto Silva; MENDES, Paulo de Sousa; ALMEIDA, Carlota (Coords.). **Direito da Investigação Criminal e da Prova**. Coimbra: Almedina, 2014.

MENKE, Fabiano. **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 2019.

MIRANDA, Jorge; MEDEIROS, Rui**. Constituição Portuguesa Anotada**, tomo I, 2.a edição, Coimbra: Coimbra Editora, 2010.

NOVAIS, Jorge Reis. **Os princípios constitucionais estruturantes da República Portuguesa**. Coimbra: Coimbra Editora, 2004.

ORTIZ PRADILLO, Juan Carlos. "Hacking" legal al servicio de la investigación criminal: nuevos instrumentos para la investigación y prueba de la delincuencia informática**.** In: Castrillo, Eduardo de Urbano. **Delincuencia informática: tiempos de cautela y amparo.** Aranzadi, 2012.

ORTIZ PRADILLO, Juan Carlos. "**El impacto de la tecnología en la investigación penal y en los derechos fundamentales**", em VV.AA. Problemas actuales de la justicia penal, Madrid: Ed. Colex, 2013.

PALMA, Maria Fernanda. Tutela da vida privada e processo penal – realidades e perspectivas constitucionais. In: **Jurisprudência Constitucional**, número 10, abril/junho, Coimbra: Coimbra Editora, 2006.

PILATI, José Isaac; OLIVIO, Mikhail Vieira Cancelier. **Um novo olhar sobre o direito à privacidade**: caso Snowden e pós-modernidade jurídica. Seqüência (Florianópolis), n. 69, p. 281-300, dez. 2014.

PITOMBO, Cleunice Bastos. **Da busca e da apreensão no processo penal**. 2. Ed. São Paulo: Editora Revista dos Tribunais, 2005

PRADO, Geraldo. **Prova penal e sistema de controles epistêmicos**. 1 ed. São Paulo: Marcial Pons, 2014.

PUJADAS TORTOSA, Virgínia. **Para una teoria general de las medidas cautelares penales.** Tesis doctoral, Universitat de Girona, Departament de Dret Públic. Girona, enero de 2007.

RAMALHO, David Silva. **Métodos ocultos de investigação criminal em ambiente digital.** Coimbra: Almedina, 2017.

RAMALHO, David Silva. O uso de malware como meio de obtenção de prova em processo penal. In: **Revista de Concorrência e Regulação**, número 16, ano IV (outubro/dezembro), 2013.

RAMOS MÉNDEZ, Franciso. **Enjuiciamento Criminal: Duodécima lectura constitucional**. Barcelona: Atelier Libros Jurídicos, 2018.

RIBEIRO, Gustavo Alves Magalhães; CORDEIRO, Pedro Ivo Rodrigues Velloso; FUMACH, Débora Moretti. O malware como meio de obtenção de prova e a sua implementação no ordenamento jurídico brasileiro. **Revista Brasileira de Direito Processual Penal**, v. 8, p, 2022.

RIBOLI, Eduardo Bolsoni. Eu sei o que vocês fizeram no verão passado: o uso de software de espionagem como meio de obtenção de prova penal. In: **Revista Brasileira de Ciências Criminais**, São Paulo, v. 27, n. 156, 2019.

RODOTÀ, Stefano. **A vida na sociedade de vigilância: a privacidade hoje**. Rio de Janeiro: Renovar, 2008.

RODRIGUES, Benjamim Silva, **Da Prova Penal**, Tomo IV – Da Prova - Electrónico - Digital e da Criminalidade Informático-Digital (Contributo Para a Fundamentação de um Modelo Dinâmico-Reversivo de Ciência Forense Digital em sede de Investigação da Cyber-Criminalidade Informático-Digital e à Luz do Novíssimo Regime da Lei do Cibercrime Portuguesa), 1°. Edição, Rei dos Livros, 2011.

ROXIN, Claux. **La prohibición de autoincrinación y de las escuchas domiciliares**, apresentação de Francisco Muñoz Conde e Marcela De Langhe, Buenos Aires: Hammurabi, 2008.

ROXIN, Claus. **La protección de la persona en el derecho processal alemán**, em La evolución de la política criminal, el derecho penal y el proceso penal, Valencia: Tirantlo Blanch, 2000.

RUARO, Regina Linden. **Privacidade e autodeterminação informativa: obstáculos ao Estado de vigilância?** Arquivo Jurídico – ISSN 2317-918X – Teresina-PI – v. 2 – n. 1 – p. 41-60. Jan./Jun. de 2015.

SALT, Marcos. **Nuevos desafios de la evidencia digital: acceso transfornterizo y técnicas de acesso remeto a datos informáticos**. 1ª ed. Buenos Aires: Ad-hoc, 2017.

SCHWAB, Klaus. **A quarta revolução industrial**. São Paulo: Edipro, 2016.

SIDI, Ricardo. **A interceptação das comunicações telemáticas no processo penal.** Belo Horizonte: Editora D'Plácido, 2016.

SILVA, Germano Marques da. **Meios processuais expeditos no combate ao crime organizado (a democracia em perigo?).** Lisboa: Lusíada. Direito, nº 3, 2005.

SMANIO, Gianluca Martins. **A vigilância policial em meio digital: entre o garantismo e a eficiência**. Dissertação (Mestrado em Direito). Faculdade de Direito da Universidade de São Paulo, São Paulo, 2021.

SOUSA, Susana Aires de. **Agent provocateur e meios enganosos de prova: algumas reflexões**, Separata de Liber Discipulorum para Jorge de Figueiredo Dias. Coimbra: Coimbra Editora, 2002.

SYDOW, Spencer Toth. **Curso de Direito Penal Informático**. Salvador: JusPodivm, 2020.

SYDOW, Spencer Toth. **Delitos informáticos próprios: uma abordagem sob a perspectiva vitimológica**, Dissertação de Mestrado. Faculdade de Direito do Largo São Francisco: Universidade de São Paulo, 2009.

TOGIAS, Stavros. **The right in confidentiality and integrity of information technology systems according to the german federal constitutional court**: 'old wine in new bottles'? 2010.

TORRE, Marco. **Il captatore informático: nuove tecnologie investigative e rispetto delle regole processuali.** Giufrré Editore, 2017.

TORRE, Marcos. **Indagini informatiche e processo penale.** Dottorato di ricerca in scienza giuridiche, ciclo XXVIII. Università degli studi Firenze. Anni 2012/2015.

TORRE, Marco et al. IL captatore informatico dopo la legge cd "spazza-corrotti". In: **Diritto penale e processo**. 2019.

VACIAGO, Giuseppe. **Digital Evidence**. I mezzi di ricerca della prova digitale nel procedimento penale e le garanzie dell'indagato. Torino: Giappichelli, 2012.

VALENTE, Manuel Monteiro Guedes. **Os meios ocultos de investigação**. 21º Seminário Internacional de Ciências Criminais. São Paulo: IBCCRIM, 2015.

VALENTE, Manuel Monteiro Guedes. O Reforço dos Princípios Constitucionais na Obtenção de Prova no Mundo Digital. Corpus Delicti — **Revista de Direito de Polícia Judiciária**, Brasília, v. 2, n. 3, 2018.

VÁZQUEZ-ROJAS, Carmen. Sobre la cientificidad de la prueba científica en el proceso judicial. **Anuario de psicología jurídica**, v. 24, n. 1, 2014.

VELASCO NUÑEZ, Eloy. Limites a las investigaciones y a la prueba en el proceso penal. In: **Delitos tecnológicos: definición, investigación, y prueba en el proceso penal.** Madrid: Jurídica Sepín, 2016.

VELASCO NUÑEZ, Eloy. **ADSL y Troyanos: Intervención de sus datos y telecomunicaciones en la investigación penal**, La Ley Penal, nº 82, 2011.

WERTHEIN, J. A sociedade da informação e seus desafios. In: **Ciência da Informação**, v. 29, n° 2, 2000.