



**FACULDADE DE DIREITO  
DOUTORAMENTO EM DIREITO  
CIÊNCIAS JURÍDICO-CRIMINAIS**

**O *MALWARE* COMO AGENTE INFILTRADO NA CRIMINALIDADE  
ORGANIZADA**

**MÔNICA BARROSO COSTA**

**Orientador: Professor Doutor Augusto Manuel Gomes da Silva Dias**

**Orientador Substituto: Professor Doutor Paulo Manuel Mello de Sousa Mendes**

Tese especialmente elaborada para obtenção do grau de Doutor no ramo de Direito,  
na especialidade Ciências Jurídico-Criminais

2023

UNIVERSIDADE DE LISBOA  
FACULDADE DE DIREITO

O *MALWARE* COMO AGENTE INFILTRADO NA CRIMINALIDADE  
ORGANIZADA

MÔNICA BARROSO COSTA

Orientador: **Professor Doutor Augusto Manuel Gomes da Silva Dias**

Orientador Substituto: **Professor Doutor Paulo Manuel Mello de Sousa Mendes**

Tese especialmente elaborada para obtenção do grau de Doutor no ramo de Direito, na especialidade Ciências Jurídico-Criminais

**Júri:**

**Presidente: Doutor Miguel Fernando Pessanha Teixeira de Sousa**, Professor Catedrático e membro do Conselho Científico da Faculdade de Direito da Universidade de Lisboa

**Vogais:**

**Doutor Mário João Ferreira Monte**, Professor Catedrático da Escola de Direito da Universidade do Minho;

**Doutor André Filipe Lamas Leite**, Professor Auxiliar da Faculdade de Direito da Universidade do Porto, arguente;

**Doutora Maria Fernanda Dos Santos Martins Da Palma Pereira**, Professora Catedrática da Faculdade de Direito da Universidade de Lisboa;

**Doutor Eduardo Augusto Alves Vera-Cruz Pinto**, Professor Catedrático da Faculdade de Direito da Universidade de Lisboa, arguente;

**Doutor Paulo Manoel Mello De Sousa Mendes**, Professor Catedrático da Faculdade de Direito da Universidade de Lisboa, orientador;

**Doutora Helena Marisa Pinheiro Costa Morão**, Professora Auxiliar da Faculdade de Direito da Universidade de Lisboa.

**Sistema de Bibliotecas da Universidade de Lisboa**

Costa, Mónica Barroso.

O *malware* como agente infiltrado na criminalidade organizada/ Mónica Barroso Costa. - 2023.  
212 f.

Não inclui anexos.

Orientador: Prof. Doutor Augusto Manuel Gomes da Silva Dias.

Orientador Substituto: Prof. Prof. Doutor Paulo Manuel Mello de Sousa Mendes

Tese (doutorado) - Universidade de Lisboa, Ciências jurídico-criminais, Lisboa, 2021.

1. O Crime Organizado. 2. O Crime Organizado no Brasil. 3. O uso da tecnologia na investigação da criminalidade organizada. 4. A utilização do *malware* como agente infiltrado. 5. Esteio Constitucional. 6. Direito à segurança pública no Estado Democrático de Direito.

CDD - 401.3

*Dedico este trabalho a meus filhos, razão maior da minha vida, Nathália, Victória, Heitor, Antônio e Danielle. Tenho inúmeras razões para lhes ser grata, por terem aceitado mudar de país, de casa, de escola, deixar os amigos para me acompanharem na realização de um sonho; por terem alegrado meus dias quando a tristeza apertou e a vontade de desistir apareceu; por suportarem minhas lágrimas, minha irritação, minhas ausências; por terem sido companheiros de jornada; por terem me incentivado a continuar, mesmo quando eu achava que não conseguiria; por acreditarem mais em mim que eu mesma; por todo amor, carinho, compreensão, colo e afagos que vinham em formas inesperadas, como um lanche na mesa de trabalho, interrupção do trabalho para eu descansar, massagem nos pés, nos ombros, nas costas, doloridos após horas de digitação. A vocês, meus filhos, meus eternos amores, minha gratidão.*

## AGRADECIMENTOS

A construção de uma tese, da apresentação do resultado de uma pesquisa, é trabalho árduo, solitário, que impõe sacrifícios e custos materiais e emocionais, mas não só a pesquisadora. Para que o trabalho possa chegar ao seu bom termo, é necessária uma rede de suporte e apoio onde nos momentos de dúvida, de tristeza, de descrença, a pesquisadora possa se apoiar, repousar, descansar e recobrar o ânimo e a força para a etapa seguinte, até atingir sua meta. É a essa rede invisível, porém presente, sentida a todo instante, que quero dirigir meu agradecimento.

A permissão para eu chegar a Lisboa e iniciar meus estudos, veio da Força Divina que permeia minha existência, a qual honro e agradeço. Ela esteve presente em cada momento, em cada simples respiração, observando, protegendo, livrando e orientando, e ainda que minha fé seja muito menor que seu Amor, Ela nunca me abandonou.

Agradeço aos meus pais que me permitiram aportar neste momento da minha existência, que, mesmo sem terem cursado nível superior, pautaram minha formação educacional com o lema “o saber morre com seu dono”, portanto que o conhecimento é o bem mais precioso que se pode deixar como legado a um filho, e assim infundiram em mim o gosto pelo estudo, o respeito pelo trabalho, a crença de que o conhecimento é libertador.

Registo meu agradecimento as Instituições que possibilitaram a conclusão desse grau acadêmico, ao CDEMP (Colégio de Diretores de Escolas e Centros de Estudos e Aperfeiçoamento Funcional dos Ministérios Públicos do Brasil), a Faculdade de Direito da Universidade de Lisboa e ao Ministério Público do Estado da Bahia.

Agradeço ao meu orientador, Professor Doutor Augusto Manuel Gomes da Silva Dias, que partiu deste plano físico dias antes do depósito da tese, não chegando a ver o trabalho pronto. Nutro pelo Professor profundo respeito e consideração. Suas observações, sugestões, correções, me permitiram descobrir o caminho a ser trilhado, com ele pude dividir angústias e dificuldades, especialmente na fase da conclusão do trabalho, quando dificuldades profissionais se apresentaram, mas seu incentivo me encorajou a não esmorecer.

Ante o infortúnio da precoce partida do meu orientador, o Professor Doutor Paulo Manuel Mello de Sousa Mendes, não hesitou em assumir a sua orientação, adotando com presteza todas as providências necessárias, fazendo as necessárias observações ao trabalho em andamento, possibilitando que o mesmo seguisse seu caminho visando submissão ao júri. Minha profunda gratidão por ter confiado no meu trabalho e permitido que eu chegasse até aqui.

Quero manifestar meu agradecimento a meus colegas de academia, com quem pude dividir as agruras do caminho, que estiveram presentes em cada fase, ainda que na maior parte das vezes em espaço virtual, desde o rascunho, passando pelo sumário, até a conclusão. Obrigada pela companhia, pelo incentivo, pelo auxílio, pela solidariedade e pela amizade.

Agradeço a minha amiga Monia Lopes, que antes mesmo de me conhecer, me hospedou e orientou para que eu pudesse fazer minha mudança para Lisboa com tranquilidade. Éramos ao mesmo tempo colegas de curso e de profissão, por isso dividimos alegrias, tristezas, decepções e agora essa grande vitória.

Meu agradecimento as minhas amigas e a todos aqueles que, ainda que silenciosamente, torceram, vibraram e estiveram em positiva sintonia com meu sucesso neste trabalho.

Grata a Lisboa e a Portugal por terem acolhido a mim e a minha família e ter nos proporcionado momentos de alegria e união, lembranças felizes que marcaram com tinta indelével nossos corações.

## RESUMO

O crime organizado é um fenômeno crescente, de dimensões mundiais, e que desafia a conhecida ordem jurídica penal e processual penal a buscar defini-lo, embora afastada a unanimidade sobre o entendimento desse problema social. Sua atuação inspira sensação de insegurança na sociedade, que muitas vezes, inadvertidamente, pede por intervenção estatal com soluções mais duras, em prejuízo até mesmo de direitos fundamentais. Ele apresenta contornos difusos, atua em diversas áreas, podendo variar de acordo com o local ou objeto do crime. No Brasil, o crime se organizou pela primeira vez dentro dos presídios, partindo da prática de delitos comuns, para se especializarem no tráfico de drogas, tendo este como objeto da empresa criminosa, mas passando por outras dezenas de delitos para garantir o sucesso da empreitada. Para a prática de delitos, bem como para garantir sua impunidade, é comum ao crime organizado o uso do ambiente virtual, utilizando ferramentas consideradas maliciosas, muitas delas de uso proibido, portanto não autorizadas para uso durante a investigação pela polícia judiciária. O objetivo deste trabalho foi analisar a utilização de meios considerados maliciosos, e por isso chamados *malware*, como método de obtenção de prova na investigação do crime organizado, seja em relação a delitos já cometidos, seja em relação a delitos que estão em andamento ou em vias de acontecer. Tal análise foi feita tanto quanto ao aspecto técnico operacional, quanto ao aspecto jurídico de respeito aos princípios constitucionais do direito ao silêncio, à proporcionalidade e à ponderação. Na análise do uso de *malware*, a atenção está fincada no seu uso como agente infiltrado virtual, não se prendendo a um tipo de *malware* especificamente, podendo adotar qualquer uma de suas variações, tais como *Trojan horse*, *spyware*, *adware*, *keylogger*, entre outras, constituindo método de obtenção de prova que realiza sua atividade, mesmo quando ausente fisicamente o investigador judiciário. A possibilidade de ausência do investigador durante a coleta remota das provas, bem como a escolha dos dados a serem utilizados, cálculos feitos imediatamente pelo *malware* programado para tanto, garantem maior cobertura e agilidade na coleta de provas, facilitando o trabalho de sua recolha bem como de indícios que possam vir, inclusive, a evitar a prática delitiva. Por não respeitar limite ou balizamento legal para sua atuação, o crime organizado apresenta grande agilidade quando atua em ambiente virtual, sendo fundamental o estreitamento das janelas de passagem para sua atuação em tal terreno. Cabe ao Estado encontrar alternativas e possibilidades para aí investigar, como já iniciou com a Lei do Cibercrime, mas que ainda precisa avançar, garantindo à sociedade que é possível realizar uma investigação do crime organizado de maneira mais eficiente, utilizando as ferramentas tecnológicas disponíveis, sem que isso implique mitigar direitos fundamentais.

**Palavras chave: Processo Penal; Crime Organizado; *malware*; agente infiltrado virtual; método de obtenção de prova; direito ao silêncio; segurança.**

## ABSTRACT

Organized crime is a growing phenomenon, of global dimensions, and challenges the well-known criminal and penal procedural law to seek to define it, although the unanimity of the understanding of this social problem. His performance inspires a sense of insecurity in society, which often inadvertently calls for state intervention with tougher solutions, even undermining fundamental rights. It has diffuse contours, acts in several areas, and may vary according to the location or object of the crime. In Brazil, crime is organized for the first time inside the prisons, starting from the practice of common crimes, to specialize in drug trafficking, having this as the object of the criminal enterprise, but passing through dozens of other crimes to guarantee the success of the crime. contract. For the practice of crimes, as well as to guarantee their impunity, it is common to organized crime to use the virtual environment, using for it tools considered malicious, many of them of prohibited use, therefore not authorized for use during the investigation by the judicial police. The objective of this work was to analyze the use of means considered malicious and therefore called *malware*, as a method of obtaining evidence in the investigation of organized crime, whether in relation to crimes already committed, or in relation to crimes that are in progress or in ways to happen. This analysis was done as much as the technical operational aspect, as for the legal aspect of respect for the constitutional principles of the right to silence, proportionality and weighting. In the analysis of the use of *malware*, the attention is focused on its use as a virtual infiltrator, not attaching itself to a specific type of *malware*, being able to adopt any of its variations, such as Trojan horse, spyware, adware, keylogger, among others , constituting a method of obtaining evidence that carries out its activity, even when physically absent from the judicial investigator. The possibility of the absence of the investigator during the remote collection of the tests, as well as the choice of the data to be used, calculations done immediately by the *malware* programmed for both, guarantee greater coverage and agility in the collection of evidence, facilitating the work of its collection as well as of indications that may even prevent delinquent practice. Because it does not respect a legal boundary or markings for its performance, organized crime presents great agility when acting in a virtual environment, being fundamental the narrowing of the windows of passage for its action in such terrain. It is up to the State to find alternatives and possibilities to investigate, as it has already begun with the Cybercrime Law, but still needs to move forward, guaranteeing society that it is possible to carry out an investigation of organized crime more efficiently, using the available technological tools, without implies mitigating fundamental rights.

**Keywords: Criminal proceedings; Organized crime; *malware*; virtual infiltration agent; method of obtaining evidence; right to silence; safety.**

## LISTA DE ABREVIATURAS E SIGLAS

Ac.	Acórdão
ALN	Ação Libertadora Nacional
ART	Artigo
CADH	Convenção Americana dos Direitos Humanos
CERT	Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil
CF	Constituição Federal
CEDH	Corte Europeia de Direitos Humanos
CNMP	Conselho Nacional do Ministério Público
CPI	Comissão Parlamentar de Inquérito
CPP	Código de Processo Penal
CRP	Constituição da República Portuguesa
CV	Comando Vermelho
CVRL	Comando Vermelho Rogério Lemgruber
DEIC	Departamento de Investigações Criminais de São Paulo
DNA	DeoxyriboNucleic Acid
ETSI	European Telecommunications Standards Institute
FBI	Federal Bureau of Investigation
FDN	Família do Norte
FPMR	Frente Patriótica Manuel Rodrigues
GAECO	Grupo de Atuação Especial de Repressão ao Crime Organizado
GSM	Global System for Mobile Communications
HIV/AIDS	Human Immunodeficiency Virus/Acquired Immune Deficiency Syndrome
IBCCRIM	Instituto Brasileiro de Ciências Criminais
IDHAC	Informe sobre Desarrollo Humano para America Central
IOCE	International Organization on Computer Evidence
LAN	Local Area Network
LC	Lei do Cibercrime
LONMP	Lei Orgânica Nacional do Ministério Público
MMS	Multimedia Message Service
MR-8	Movimento Revolucionário 8 de outubro
M.º P.º	Ministério Público

OEA	Organização dos Estados Americanos
ONU	Organização das Nações Unidas
PCC	Primeiro Comando da Capital
PC	Personal Computer
PNUD	Pesquisa das Nações Unidas para o Desenvolvimento
SDC	Sindicato do Crime
SIM	Subscriber Identity Module
SP	São Paulo
STF	Supremo Tribunal Federal
STJ	Supremo Tribunal de Justiça
SWGDE	Scientific Working Group on Digital Evidence
TC	Tribunal Constitucional
TRE	Tribunal da Relação de Évora
UNDP	United Nation Development Programme
UNESCO	Organização das Nações Unidas para Educação, Ciência e Cultura.
VAR	
Palmares	Vanguarda Armada Revolucionária Palmares
VPR	Vanguarda Popular Revolucionária

## SUMÁRIO

<b>INTRODUÇÃO</b>	13
<b>1. O CRIME ORGANIZADO</b>	17
1.1 O CENÁRIO	17
1.2 A EMPRESA CRIMINOSA	21
1.3 O ESTADO COMO PARCEIRO	26
1.4 O CONCEITO	30
1.4.1 O fenômeno da criminalidade organizada	30
1.4.2 Delimitando o objeto	33
<b>2 O CRIME ORGANIZADO NO BRASIL</b>	39
2.1 APRESENTAÇÃO	39
2.2 PRINCIPAIS ORGANIZAÇÕES CRIMINOSAS QUE ATUAM NO SISTEMA PRISIONAL BRASILEIRO	43
2.2.1 Primeiro Comando da Capital (PCC)	43
2.2.2 Comando Vermelho	50
2.2.3 Primeiro Comando da Capital (PCC) versus Comando Vermelho (CV)	53
2.2.4 A ineficiência do Estado	57
2.2.5 Novas Organizações Criminosas	59
<b>3 O USO DA TECNOLOGIA NA INVESTIGAÇÃO DA CRIMINALIDADE ORGANIZADA</b>	68
3.1 O MÉTODO PARA INVESTIGAR A CRIMINALIDADE ORGANIZADA	69
3.2 O FÁCIL ACESSO ÀS TECNOLOGIAS DA INFORMAÇÃO	75
3.3 O <i>MALWARE</i>	81
3.4 O USO DE <i>MALWARE</i> COMO INSTRUMENTO OCULTO DE MEIO DE OBTENÇÃO DE PROVA NA INVESTIGAÇÃO DA CRIMINALIDADE ORGANIZADA	91
3.5 EXPERIÊNCIA ESTRANGEIRA DO USO DE <i>MALWARE</i> EM INVESTIGAÇÃO CRIMINAL	99

<b>3.5.1 Estados Unidos</b>	100
<b>3.5.2 Alemanha</b>	104
<b>3.5.3 Itália</b>	108
<b>3.5.4 Espanha</b>	113
<b>4 UTILIZAÇÃO DO <i>MALWARE</i> COMO AGENTE INFILTRADO</b>	120
<b>4.1 BUSCAS <i>ON-LINE</i></b>	120
<b>4.2 PESQUISAS DE DADOS INFORMÁTICOS</b>	122
<b>4.3 AGENTE INFILTRADO VIRTUAL</b>	125
<b>4.3.1 Ação encoberta</b>	127
<b>4.3.2 Agente infiltrado ou encoberto</b>	129
<b>4.3.3 Elementos de admissibilidade de uma ação encoberta</b>	134
<b>4.3.4 A utilização do <i>malware</i> como agente infiltrado virtual</b>	137
<b>5 ESTEIO CONSTITUCIONAL</b>	148
<b>5.1 PRINCÍPIOS E POSTULADOS CONSTITUCIONAIS</b>	149
<b>5.2 DOS PRINCÍPIOS</b>	153
<b>5.2.1 Direito ao silêncio</b>	154
<b>5.2.1.1 Garantia da não autoincriminação (<i>nemo tenetur se detegere</i>)</b>	156
<b>5.2.2 Direito a Intimidade</b>	163
<b>5.3 DOS POSTULADOS</b>	167
<b>5.3.1 Proporcionalidade</b>	167
<b>5.3.2 Ponderação</b>	172
<b>6 O DIREITO À SEGURANÇA PÚBLICA NO ESTADO DEMOCRÁTICO DE DIREITO</b>	176
<b>6.1 SOCIEDADE DE RISCO</b>	178
<b>6.2 SEGURANÇA CIDADÃ</b>	181
<b>6.3 SOCIEDADE DE RISCO, SEGURANÇA PÚBLICA E DIREITO PENAL</b>	189
<b>7 CONSIDERAÇÕES FINAIS</b>	195
<b>REFERÊNCIAS BIBLIOGRÁFICAS</b>	199

## INTRODUÇÃO

O trabalho de pesquisa que aqui se apresenta teve por objetivo analisar a possibilidade de utilização de novas ferramentas no combate ao crime organizado, visando intensificar seu enfrentamento e tornar mais célere e eficiente a atuação do Estado. Dessa maneira, recursos tecnológicos já utilizados em larga escala pela criminalidade organizada poderiam vir a ser incluídos no ordenamento processual penal e considerados, portanto, como método de obtenção de prova.

A elaboração do trabalho ocorreu por meio de pesquisa bibliográfica em idioma português e estrangeiro, com singular olhar para a doutrina de origem ibérica, fonte comum e próxima das questões penais que aqui foram pensadas, sem se descuidar da aplicação dos conceitos doutrinários na prática forense portuguesa e brasileira, analisando casos que foram apreciados pelas Cortes Constitucionais dos dois países, e ainda o julgamento do caso *Teixeira de Castro v. Portugal* pelo Tribunal Europeu dos Direitos Humanos (TEDH), que guarda relação com a questão do agente encoberto que aqui será abordado.

A observação empírica que pode ser realizada no contexto da prática de investigação do crime organizado, permitiu a identificação da necessidade de utilização de métodos investigatórios mais eficientes para apuração deste tipo de criminalidade. Em regra, a sofisticação da prática delitiva passa pela utilização fraudulenta de meios tecnológicos acessíveis e de fácil manuseio. Esse tipo de crime pode ser cometido por quem detém conhecimento mediano sobre navegação em ambiente virtual. Essa conduta ilícita pode gerar resultados de relevante impacto para a sociedade, que vão desde a invasão de sítios que hospedam agentes financeiros, desviando recursos de contas bancárias sem deixar rastros, até a manipulação de informações, com o deliberado falseamento da verdade, visando subvencionar agentes políticos (alterando resultado de eleições, por exemplo), que beneficiam a criminalidade organizada por meio da corrupção.

Tais condutas criminosas devem ser reprimidas, como já o faz a Lei de Cibercrime (Lei nº 109/2009) ao considerar criminosas as condutas que atentam contra o sistema de informação. A tipificação legal de determinadas práticas não conduz à conclusão de que as mesmas não serão praticadas, ao contrário, é justamente a possibilidade de sua prática que impõe ao Estado a necessidade de apená-las.

Se é previsível e até esperada a manipulação do sistema de informação, visando obter vantagem ilícita, é fundamental que o Estado esteja apto a identificar e combater tais condutas antes mesmo que elas aconteçam, não bastando o alcance do caráter repressivo, imposto pela pena, mas é necessário o caráter preventivo, que só é possível obter se a atuação estatal ocorrer antes ou durante a prática criminosa.

Da observação da prática de crimes em sistema informático, foram identificadas várias condutas que, para sua prevenção e investigação, se faz necessário que o Estado ingresse no ambiente virtual pelas mesmas portas que o criminoso cruza, utilizando idênticas ferramentas que o crime se utiliza, sob pena de enveredar em uma investigação de olhos fechados, pouco efetiva, procurando em lugar diverso daquele da prática do crime, condenando-a ao insucesso.

A criminalidade organizada é aquela que apresenta maior grau de complexidade em sua prática, sobretudo quando se analisa sua estrutura empresarial, e quando se observa o modo como ocorre a prática dos delitos que a sustentam. A investigação da criminalidade organizada exige atenção especial, pois os tradicionais métodos de prova, previstos no ordenamento penal, não são mais suficientes para explicar a sua complexidade.

Analisando o caso de pedofilia em ambiente virtual, por exemplo, que nem sempre constitui caso de crime organizado, portanto, em tese, de menor complexidade, a investigação conseguirá pouco resultado se os investigadores não se aventurarem pela *deep web*, ambiente que tem regras diversas daquelas praticadas na rede internacional de computadores, conhecida como *Internet*. Terão pouca chance de lograr êxito, se não adotarem uma identidade falsa, visando identificar e localizar criminosos que consomem e espalham pornografia infantil. Essas condutas, apesar de poderem ser tipificadas como criminosas, são imprescindíveis à investigação criminal, pois sem o acesso a *deep web*, aos sites de pornografia infantil, por exemplo, e sem o contacto com criminosos que lá transitam, por meio do uso do artifício da identidade falsa, não é possível a investigação obter sucesso.

A ideia defendida neste trabalho é a possibilidade de utilização de *malware* para efeito de investigação e localização de criminosos e para o rastreamento do produto do crime organizado. Ressalta-se que esse recurso é operado em larga escala pela criminalidade organizada. O objetivo do trabalho é mostrar a possibilidade de inocular programa informático (*malware*) no sistema informático investigado, a fim de que aquele atue como

agente infiltrado virtual, comunicando-se com o usuário investigado, transmitindo informações ao investigador em tempo real. Tem a função de revelar a identificação do usuário e extrair senhas em sítios virtuais, mapeando pesquisas, sugerindo caminhos a seguir e sítios virtuais a visitar, sendo que estes possibilitam a comprovação da prática delitiva e de sua autoria.

Tal modalidade de agente virtual, por ser um programa desenhado para fins específicos, apresenta vantagens em relação ao agente infiltrado comum. Entre elas, o fato de não ter contacto com os agentes criminosos, portanto sem necessidade de exposição a risco de agente estatal. Sendo um programa informático, ele estará em atuação constante, não havendo risco de deixar de registrar alguma movimentação do investigado em momento de pausa do investigador.

No primeiro capítulo, que trata do Crime Organizado, parte-se da análise das condições que permitem a atual configuração do que se considera criminalidade organizada, trazendo à discussão o debate acerca do sentimento de insegurança como resultado da sociedade de risco, e como esse sentimento incrementa o real risco que o crime organizado representa para a coletividade.

Em seguida, apresenta-se um panorama do Crime Organizado no Brasil, remontando à origem das principais organizações criminosas que atuam em solo nacional. Descreve-se como aconteceu a organização inicial das mesmas, como migraram da criminalidade patrimonial para o tráfico de drogas, assim como realizar-se-á uma análise sobre a atual situação de guerra engendrada pelo tráfico. Nessa oportunidade, é trazida à discussão a atuação do Estado, sua ineficiência para combater e controlar o atual estado de beligerância que acomete a sociedade brasileira, destacando a necessidade de se utilizar de métodos mais rápidos e eficazes para fazer frente à prática e à ocultação de delitos pelas organizações criminosas.

A utilização de ferramentas tecnológicas durante a investigação penal não pode ocorrer por analogia ou equiparação à legislação em vigor, reclamando estudo rigoroso, para que sua admissão no ordenamento ocorra respeitando as liberdades individuais, não implicando em violação aos direitos fundamentais agasalhados em sede constitucional.

O capítulo III cuida do uso da tecnologia na investigação da criminalidade organizada, especialmente o uso de *malware*, atentando para as peculiaridades deste tipo de

investigação, bem como traz o vocabulário específico ligado a programas informáticos.

São apresentados, a título de exemplo, como esses recursos tecnológicos vêm sendo disciplinados em outras legislações, com destaque para a alemã, norte americana, italiana e espanhola. Demonstra, ainda, de que maneira esses instrumentos podem ser manejados como meio de obtenção de prova durante a investigação criminal.

No capítulo seguinte, busca-se analisar a nomenclatura atual na literatura jurídica, sendo apresentada uma proposta de nomeação para os métodos de obtenção de prova com utilização de recursos informáticos, em especial o uso encoberto de tais recursos. Para análise da possibilidade de ação encoberta utilizando programa informático, é discutida a ação encoberta, sua admissibilidade, a atividade legal do agente infiltrado, para ao final ser apresentada a proposta de admissão no ordenamento processual penal do *malware* como agente infiltrado virtual.

Em capítulo subsequente, estão apresentados os esteios constitucionais da proposta de introdução de novo método de obtenção de prova, onde são discutidos os princípios e postulados constitucionais que autorizam o legislador a agregar no ordenamento esse método, sem que isso implique em mitigação de direitos fundamentais.

Ainda tratando dos fundamentos constitucionais do Estado Democrático de Direito, discutiu-se em capítulo próprio sobre o Direito à Segurança Pública, partindo da premissa de as sociedades deste tempo perceberem-se em iminente risco de serem vitimadas por alguma tragédia. Diante da sensação de insegurança gerada como resultado da sociedade de risco socialmente construída, é importante refletir sobre os limites do dever do Estado em garantir a segurança dos indivíduos, pensar sobre as bases do direito à segurança e de que forma essa prerrogativa dialoga com a sociedade de risco e com o ordenamento jurídico penal.

## 1. O CRIME ORGANIZADO

*Há um alfabeto, uma semântica, uma gramática que nos ajude a interpretar a criminalidade em um mundo globalizado?*<sup>1</sup>

O fenómeno da globalização, marcado pela relativização das fronteiras entre os Estados e pelo encurtamento das distâncias, produz efeitos em cada organização social individualmente considerada e na configuração do conjunto dos Estados soberanos. Além desses impactos, importa observar que a globalização trouxe uma nova dinâmica para o crime organizado, pois este adapta-se a tal realidade global de forma vertiginosa, com larga capacidade de causar consequências devastadoras em várias partes do planeta. Por essas razões, torna-se fundamental entender esse processo.

### 1.1 O CENÁRIO

O fim do Grande Cisma<sup>2</sup>, período marcado por disputas pela hegemonia global entre blocos ideológicos e económicos antagónicos, desorganizou as relações de forças do mundo, provocando nas pessoas um sentimento mais acentuado de imprevisibilidade e insegurança em face das complexidades de um contexto em profunda metamorfose. A intelectualidade esclarecida interpreta esse momento da humanidade a partir de uma categoria conceitual que convenciou-se denominar de “globalização”, admitindo-se que se trata de um fenómeno que perpassa de forma transversal todos os países, e que produz transformações substantivas em todas as áreas do conhecimento, e na própria percepção das pessoas sobre a realidade.

Após o período da Guerra Fria, durante a segunda metade do século XX, o mundo esteve marcado por uma bipolaridade de forças, por uma sensação de interdependência e aproximação entre os povos e pela relativização das fronteiras e divisões. Ao mesmo tempo,

---

<sup>1</sup>COSTA, José de Faria. **Direito Penal e Globalização**. Coimbra: Wolters Kluwer Portugal sob a marca Coimbra Editora, 2010. p. 55.

<sup>2</sup>“Tudo no mundo tinha um significado e esse significado emanava de um centro dividido mas único — dos dois enormes blocos de poder presos e colados um ao outro em combate total. Com o Grande Cisma fora do caminho, o mundo não parece mais uma totalidade e, sim, um campo de forças dispersas e díspares, que se reúnem em pontos difíceis de prever e ganham impulso sem que ninguém saiba realmente como pará-las.” BAUMAN, Zygmunt. **Globalização: as consequências humanas**. Trad. Marcus Penchel. Rio de Janeiro: Jorge Zahar Ed., 1999. p. 65.

há uma sensação paradoxal de vulnerabilidade e insegurança ante as mudanças globais, em que se evidencia uma realidade de questionamento de valores, princípios e instituições da modernidade, fazendo surgir organizações societárias com regras ainda por serem definidas e, pelo que se vislumbra até agora, mais desiguais.<sup>3</sup>

O questionamento sobre as atribuições do Estado também está inserido nesse contexto de indefinições. Antes havia dois blocos económico-militares distintos, que forneciam uma superestrutura para cada um dos grupos de Estados que os integravam, possuindo, cada bloco, identidade própria, exteriorizada pelo sistema económico que adotava. Tal ligação identitária proporcionava aos Estados membros uma sensação de pertencimento e, principalmente de proteção, frente a possíveis investidas de integrantes do bloco rival. Finda a divisão do mundo em dois blocos, os Estados perceberam-se incapazes militar e economicamente de impor suas regras<sup>4</sup>, especialmente os neonatos que são a grande maioria.

Restou apenas à organização política a função de manter sob controle as pressões sociais, exercendo o comando sobre diversos âmbitos da administração pública, sem imiscuir em questões referentes à economia, pois as demandas dessa área passaram a ser pautadas pelo mercado financeiro internacional que se autorregula e exige equilíbrio fiscal das contas públicas dos Estados, visando evitar a anarquia dos mercados.<sup>5</sup> Acentuou-se ainda mais a fragilidade da relação entre a vontade do Estado, emanada do voto popular nos países de inclinação democrática, e o caminho económico por ele trilhado, visto que as decisões são

<sup>3</sup> “A globalização é um fenómeno que está associado à crescente sensação de interdependência e de aproximação entre povos, assim como ao esbater das divisões e fronteiras, mas que, paradoxalmente, se articula com uma forte sensação de vulnerabilidade e de insegurança face à disseminação e escala das mudanças globais. Assim sendo, a globalização é uma realidade que une ao mesmo tempo que divide, e está a criar um mundo sem regras e mais desigual.” MIGUEL, Nuno Gonçalo Caseiro. **Globalização, crime organizado e terrorismo: que relação?**. In: Revista Negócios Estrangeiros, abril, n. 14, publicação semestral do Instituto Diplomático do Ministério dos Negócios Estrangeiros, 2009. p. 114.

<sup>4</sup> “A soberania externa do Estado sempre teve como sua principal justificação a necessidade de defesa contra inimigos externos. Hoje, com a diminuição dessa necessidade devido ao fim dos blocos contrapostos, a intensificação das interdependências e também as promessas não mantidas do direito internacional (todas elas inscritas naquele pacto constituinte que é a Carta da ONU: a paz, a igualdade, o desenvolvimento, os direitos universais dos homens e dos povos) estão produzindo uma crise de legitimação desse sistema de soberanias desiguais e de relações cada vez mais assimétricas entre países ricos e países pobres, em que a comunidade internacional se transformou.” FERRAJOLI, Luigi. **A soberania no mundo moderno**. Trad. Carlo Cocciolli e Márcio Lauria, 2ª ed.. São Paulo: Martins Fontes, 2007. p. 47 e 48.

<sup>5</sup> “O que quer que restou da política, espera-se, deve ser tratado pelo Estado, como nos bons velhos tempos — mas o Estado não deve tocar em coisa alguma relacionada à vida económica: qualquer tentativa nesse sentido enfrentaria imediata e furiosa punição dos mercados mundiais. A impotência económica do Estado seria então mais uma vez flagrantemente exposta para horror da equipe governante. (...) A única tarefa económica permitida ao Estado e que se espera que ele assuma é a de garantir um “orçamento equilibrado”, policiando e controlando as pressões locais por intervenções estatais mais vigorosas na direção dos negócios e em defesa da população face às conseqüências mais sinistras da anarquia de mercado.” BAUMAN, Zygmunt. **Globalização: as conseqüências humanas**. Tradução Marcus Penchel. Rio de Janeiro: Jorge Zahar Ed., 1999. p. 73.

tomadas em outro centro, privilegiando interesses alheios ao conjunto majoritário da população, e não mais discutidas exclusivamente pelo próprio Estado<sup>6</sup>.

O contrato social está em desequilíbrio, e as categorias económico-sociológicas de capital e trabalho não mais são regidas pela vontade de uma comunidade específica, mas sim pelo interesse da comunidade global, mesmo em prejuízo àquela comunidade celular. O Estado de Bem-Estar Social (*Welfare State*), gestado como resposta à crise financeira eclodida no período do pós-guerra, cede espaço à lógica do liberalismo económico. Esse modelo económico, que ganhou proeminência na década de 1970, privilegia a privatização de qualquer empresa capaz de gerar lucro, mesmo que isso implique em desproteção de setores estratégicos da vida social e para a preservação da soberania do país.

Ao desviar-se da obrigação de assistir aos seus integrantes e constituintes, o Estado foi levado ao enfraquecimento de sua legitimidade real, simbólica e discursiva como principal responsável pela organização da vida em sociedade. Ao perder de vista a importância do emprego, da geração interna de renda e da justa distribuição de riquezas, o Estado optou por privilegiar o aumento exponencial dos lucros. Esse *modus operandi* da perspectiva neoliberal produziu uma crise de renda na classe média, nivelando todos os trabalhadores ao mesmo patamar de deterioração dos meios de manutenção da vida, submetendo-a ao processo de precarização da sua força de trabalho, portanto condição de mão-de-obra desvalorizada e desprotegida<sup>7</sup>.

Esse Estado que está em busca de uma nova expressão ante à diluição do conceito de Estado-Nação, e de bem localizar-se no contexto da organização internacional das disputas económicas, alterou os padrões de emprego, de segurança, de cultura e, especialmente, de capacidade de resposta frente a crimes mais complexos. Esse movimento global que alterou toda a dinâmica internacional de organização da vida social, criou condições favoráveis ao

---

<sup>6</sup>“Os centros estratégicos de decisão económica mundializaram-se e *desterritorializaram-se*, sobrepondo-se aos centros de decisão estaduais que, num quadro de sistemático enfraquecimento e redução à expressão mais simples do exercício de um núcleo restrito de funções (defesa e segurança), já não exercem na maioria dos casos, com plenitude democrática, o poder soberano que emana do voto popular.” BRAZ, José. **Investigação Criminal**. A organização, o método e a prova. Os desafios da nova criminalidade. 3 ed. Coimbra: Almedina, 2013. p. 287-288.

<sup>7</sup>“Com efeito, o profundo desequilíbrio do contrato social entre capital e trabalho conduz à destruição da classe média e à denominada *reproletarização* de vastos sectores da população, dando origem a uma mão-de-obra desvalorizada e desprotegida e a um aumento exponencial de lucros acumulados no sector financeiro que especula e cresce desmedidamente e duma forma virtual, sem qualquer sustentação na riqueza e na economia real.” BRAZ, José. **Investigação Criminal**. A organização, o método e a prova. Os desafios da nova criminalidade. 3 ed. Coimbra: Almedina, 2013. p. 288.

surgimento de um novo modo de produção de riqueza, um mercado que surge à margem do Estado de Direito.

Enquanto os Estados não definem seu lugar na pós-modernidade, um *locus* de diálogo e convivência para resolverem questões socioeconômicas de aguda complexidade, a criminalidade se instaura nesse hiato, cujo funcionamento depende exatamente da omissão e da negligência do poder público, trazendo como consequência a ampliação da percepção de insegurança e injustiça, sobretudo nos Estados mais frágeis economicamente.<sup>8</sup>

A globalização difundiu conhecimentos, criou condições para complexos avanços tecnológicos, sobretudo no campo da informática e das telecomunicações, tornando-os acessíveis em qualquer parte do globo; encurtou distâncias, propiciou a liberalização da circulação de mercadorias, assim como facilitou o trânsito de pessoas entre Estados, trazendo relevantes avanços para o bem-estar da sociedade, em uma velocidade maior que aquela conferida às mudanças das estruturas política e jurídica dos Estados.

Vale frisar que a relação entre a criminalidade e a resposta do Estado, mesmo dentro das estruturas jurídico-políticas tradicionais do Estado-nação, sempre ocorreu de maneira lenta. Esse tempo entre a atividade criminosa e a resposta final do Estado era compreendida com normalidade, e visto como fundamental para o exercício das liberdades, direitos e garantias individuais<sup>9</sup>.

Ocorre que a criminalidade que hoje atua por meios informáticos, atinge velocidade muito superior àquela que se compreende dentro dos tipos penais previstos na legislação de base, sendo necessário, portanto, imprimir nova velocidade as respostas apresentadas pelo Estado, sob pena de, quando a mesma chegar, se respeitar a comum velocidade dada a comum criminalidade, já não surta mais efeito, nem tenha mais sentido sua aplicação<sup>10</sup>.

<sup>8</sup> “Estas novas dimensões do crime organizado constituiriam um “poder secreto”, “sub- Estados”, “cripto-governos”, com enorme poder de influencia tanto na política como na administração. Formariam um substrato que ameaçaria profundamente o exercício da democracia e a possibilidade de um Estado de Direito, com seu exercício de poder necessariamente ligado à visibilidade e transparência.” SCHILLING, Flávia. **Corrupção, crime organizado e democracia**. Revista Brasileira de Ciências Criminais, São Paulo, v. 36, 2001.

<sup>9</sup> “E se, de certa maneira, o “jogo” entre a criminalidade, entre os comportamentos criminais e o direito penal, mesmo dentro das estruturas jurídico-políticas tradicionais do Estado-nação, se fazia e ainda faz com uma resposta necessariamente lenta – e todos percebem que esta lentidão não tem nada de patológico mas antes de fisiológico, porquanto é a manifestação dos direitos, das liberdades e das garantias...” COSTA, José de Faria. **Direito Penal e Globalização**. Coimbra: Wolters Kluwer Portugal sob a marca Coimbra Editora, 2010. p. 47.

<sup>10</sup> “Se o crime organizado e o terrorismo empregam processos altamente dinâmicos, o Estado encontra-se no outro extremo. Não se defende que o Estado utilize essas mesmas armas. No entanto, é urgente que o Estado adeque as suas instituições à nova realidade, de forma a agilizar processos, desburocratizando tomadas de decisão, e garantindo outros níveis de eficácia no combate a estas ameaças.” MIGUEL, Nuno Gonçalo Caseiro. **Globalização, crime organizado e terrorismo: que relação?.** In: Revista Negócios Estrangeiros, abril, n. 14,

## 1.2 A EMPRESA CRIMINOSA

A rapidez e a fluidez da comunicação e do transporte trazidas pelas inovações tecnológicas modificaram a dinâmica das operações financeiras, especialmente as internacionais. Isso aconteceu porque o imperativo da velocidade para circulação do capital, junto à fluidez com que as transações comerciais estavam se processando, possibilitou o surgimento de zonas de livre comércio. Assim, eram necessárias áreas de comércio entre os países onde houvesse uma significativa redução no controle aduaneiro para possibilitar que as trocas se realizassem com maior liberdade e rapidez.

Esses fatores que serviriam para simplificação e redução do aparato burocrático de regulação do comércio internacional, desmontando de forma substantiva a fiscalização nas fronteiras, são os mesmos aproveitados para o incremento das redes de crime organizado<sup>11</sup> que, como toda empresa moldada sob a égide de uma sociedade consumista, assentada sob bases capitalistas, objetiva o alcance do lucro, perseguindo incansavelmente oportunidades de acumular riqueza, especialmente onde encontre atividade econômica desregulamentada<sup>12</sup> ou de fiscalização precária.<sup>13</sup>

A velocidade, o volume e a facilidade na troca de informações permitiu que a ação da criminalidade ocorresse quase em tempo real. Esse dinamismo dos câmbios de toda ordem aliado à falta de eficiência e lentidão da burocracia estatal, dificulta a fiscalização de vultosas transações financeiras, e abre espaço para atividades ilegais. Assim, ao tornar a propriedade do capital anônima, permite-se, sem constrangimentos institucionais, a livre circulação monetária por paraísos fiscais, garantindo a infraestrutura operacional para o financiamento

---

publicação semestral do Instituto Diplomático do Ministério dos Negócios Estrangeiros, 2009. p. 120

<sup>11</sup>“E neste viés, voltamos a insistir que a maior interconexão das economias no marco da globalização acabou por proporcionar a criação e desenvolvimento de numerosas zonas de livre comércio a nível mundial, cujos benefícios em termos de redução de controles aduaneiros possibilitaram um melhor e menos complicado acesso entre as fronteiras dos Estados.” PEREIRA, Flávio Cardoso. **Crime Organizado e suas Infiltrações nas Instituições Governamentais**. São Paulo: Ed. Atlas, 2015. p. 32.

<sup>12</sup> Na Itália, por exemplo, se identificou a influência da máfia em transações comerciais ligadas ao meio ambiente. “Com o termo “ecomáfia”, criado em 1994, a associação ambientalista Legambiente indicou o envolvimento da criminalidade organizada, em todas as suas articulações (Camorra, Ndrangheta, Cosa Nostra e Nuova Sacra Corona Unita), no ciclo econômico-cultural, a partir do chamado “ciclo do cimento” até o denominado “ciclo do lixo”, com gravíssimas consequências, quer para o ambiente, quer para a economia italiana. PELLEGRINI, Angiolo e COSTA, Jr., Paulo José da. **Criminalidade Organizada**. São Paulo: Ed. Atlas, 2008. p. 64

<sup>13</sup>“A busca do lucro por parte da criminalidade organizada faz com que o proveito econômico seja farejado onde há maior riqueza e atividade econômica desregulamentada ou não fiscalizada.” CABETTE, Eduardo Luis Santos e NAHUR, Marcius Tadeu Maciel. **Criminalidade organizada & globalização desorganizada**. Rio de Janeiro: Ed. Freitas Bastos, 2014. p. 76.

de operações como tráfico de drogas, de pessoas e de órgãos humanos; contrabando de armas, fraudes fiscais e financeiras; pirataria de mercadorias e de serviços; falsificação de medicamentos; difusão de jogos de azar, entre tantas outras modalidades<sup>14</sup>. Para esse tipo de criminalidade, as respostas não chegam ou, quando chegam, operam em uma outra dinâmica temporal, ensejando ineficiência dos aparelhos coercitivos para se contraporem à estrutura criminoso.<sup>15</sup>

Seja qual for o tipo ou modelo de empresa criminoso adotado, todas elas têm em comum a busca do lucro<sup>16</sup>, e o único critério racional conhecido para consecução dos seus objetivos é a razão entre custo e benefício. É possível admitir a afirmação de que o capitalismo encontra sua plena manifestação no crime organizado, que plasma o desenvolvimento do modo de produção e a própria narrativa ideológica que subsidia o capitalismo<sup>17</sup>. Isso porque todas as ações são meticulosamente planejadas visando o lucro, não importando que, para alcançar o fim colimado, seja necessário o uso da violência, sem hesitações, sem qualquer ponderação moral ou ética.<sup>18</sup>

Ao utilizar o termo empresa para se referir ao crime organizado, é necessário tecer algumas considerações, pois empresa comercial é criação legal, portanto lícita e integrante do

---

<sup>14</sup>“Essas mudanças promoveram em curto espaço de tempo profunda desregulamentação dos mercados, sobretudo financeiros, desencadeando uma seqüência ordenada de processos: alteração das tradicionais fronteiras nacionais; incentivo ao fluxo cada vez mais maleável de capitais; abertura de espaço para atividades ilegais...” ADORNO, Sérgio; SALLA, Fernando. Criminalidade organizada nas prisões e os ataques do PCC. **Estudos avançados**, v. 21, n. 61. p. 7-29, 2007. Disponível em <http://www.scielo.br/pdf/ea/v21n61/a02v2161>. Acessado em 08/08/17.

<sup>15</sup>“...se a criminalidade resultante ou que actua já dentro da globalização age à velocidade quase do tempo real, as respostas da sociedade, quer de um ponto de vista nacional ou mesmo internacional, ou não existem ou quando existem operam-se dentro dos quadros tradicionais.” COSTA, José de Faria, **Direito Penal e Globalização**. Coimbra: Wolters Kluwer Portugal sob a marca Coimbra Editora, 2010. p. 47.

<sup>16</sup>“...estas multinacionais do crime atuam com uma aparência externa de licitude e se aproveitam dos avanços tecnológicos e da internacionalização das relações, com a finalidade última de maximizar os benefícios e ao mesmo tempo reduzir ao máximo os custos. Assim, seu principal objetivo seria a obtenção do lucro.” PEREIRA, Flávio Cardoso. **Crime Organizado e suas Infiltrações nas Instituições Governamentais**. São Paulo: Ed. Atlas, 2015. pág. 28.

<sup>17</sup>“O crime organizado funciona à margem de toda transparência e numa clandestinidade quase perfeita. Ele realiza a máxima “maximização” do lucro. Acumula mais-valia a uma velocidade vertiginosa.(...) Qual capitalista, em seu foro, íntimo, não sonha com semelhante liberdade, uma tal rapidez de acumulação, semelhante ausência de transparência e lucros dessa ordem?” ZIEGLER, Jean. **Senhores do Crime**. Rio de Janeiro. Ed. Record, 2003. pág. 51-52.

<sup>18</sup>“Por outras palavras: à determinação do lucro – com os riscos inerentes a este tipo de actividade – não se pode opor qualquer outra lógica.” (...) as próprias organizações criminosas se deixaram elas próprias, adaptando-se aos tempos, de se moverem dentro desses “códigos de conduta” e se assumem como autênticas empresas de alto risco cuja actividade fundamental é a prática organizada de actuações criminosas possibilitadora de lucros fabulosos. Nesse sentido, aqui, a relação capital/lucro é quase infinitamente favorável no sentido do lucro.” COSTA, José de Faria, **Direito Penal e Globalização**. Coimbra: Wolters Kluwer Portugal sob a marca Coimbra Editora, 2010. pág. 93.

sistema jurídico. Aqui, utiliza-se o termo empresa de maneira mais abrangente, incluindo não apenas a empresa formal, pessoa jurídica, legalmente constituída, com objetivos lícitos declarados, portanto integrante do sistema jurídico, como também toda organização que se comporte como se empresa fosse, ainda que constituída para objetivos ilícitos, como o narcotráfico. Uma mesma organização criminosa pode abranger apenas um modelo ou outro, ou os dois ao mesmo tempo.

Uma atividade lícita, regularmente constituída sob a forma de empresa, pode praticar atividades ilícitas em sua atividade meio, mas o seu objetivo final ser lícito. Uma empresa regularmente constituída pode ter um fim aparentemente lícito, mas o mesmo ser apenas para ocultar sua real finalidade, que é a lavagem de dinheiro de outra empresa, esta informal, pois constituída apenas para a prática de atos ilícitos<sup>19</sup>. Há ainda a possibilidade de um terceiro modelo em que atuam três empresas distintas: a primeira é a empresa fundante, que é aquela que tem o objetivo ilícito, a geradora do lucro, objetivo final da atividade criminosa. A segunda é a empresa legalmente constituída, que opera regularmente na sociedade segundo seus objetivos declarados por ocasião da sua constituição legal, mas que tem por finalidade a lavagem do dinheiro proveniente da primeira empresa; e a terceira empresa, legalmente constituída, cujo fim de suas atividades é sempre lícito, mas que tem por objetivo se relacionar com a política, a justiça e a economia, criando espaços possíveis de atuação da atividade ilícita.<sup>20</sup>

Assim como não é possível encontrar uma definição para crime organizado, não se pode também pretender classificar os modelos de empresa voltada para o crime ou estabelecer

---

<sup>19</sup>“Nesse paradigma, podem ser vislumbradas, basicamente, três espécies empresariais: a empresa criminosa propriamente dita, isto é, constituída, mas que viabiliza a prática sistemática, em seu meio, de ilícitos econômicos, financeiros, tributários, fiscais, previdenciários, ambientais, entre outros, e a empresa constituída como “fachada” para encobrir a lucratividade ou atividades ilícitas em si, valendo-se dos chamado “testas de ferro” e dos “laranjas”, ou seja, aquelas pessoas físicas que serão usadas para acobertamento das mais diversas falcaturas dessas pessoas jurídicas espúrias, compostas por verdadeiros “empresários do crime”. CABETTE, Eduardo Luis Santos; NAHUR, Marcius Tadeu Maciel. **Criminalidade organizada & globalização desorganizada**. Rio de Janeiro: Ed. Freitas Bastos, 2014. p. 77.

<sup>20</sup>“Fundamentalmente, os diferentes três grupos assumem-se funcionalmente da seguinte maneira: o grupo central ou nuclear tem como finalidade principal levar a cabo o aprovisionamento, o transporte e a distribuição dos bens ilegais. Ligam-se, aqui claramente, coacção e corrupção para expansão de poder e de lucro. Um outro grupo tem como propósito primacial servir de protecção institucional a toda a rede ou teia. É a tentativa de chamar à organização, de forma subtil ou directa, a política, a justiça e a economia, as quais, através do estatuto dos seus representantes, permitem criar bolsas ou espaços onde a actuação criminosa se torna possível. Finalmente, surge um terceiro grupo que tem como fim primeiro estabelecer a lavagem de todo dinheiro ilegalmente conseguido. Operam-se, por conseguinte, ligações com instituições bancárias, com casinos e ainda com outras sociedades legalmente constituídas.” COSTA, José de Faria, **Direito Penal e Globalização**. Coimbra: Wolters Kluwer Portugal sob a marca Coimbra Editora, 2010. p. 92.

uma tipologia única e definitiva, que possa classifica-las, ficando a critério de cada autor que se debruce sobre o tema adotar um critério próprio, visando categorizar as organizações que se dedicam ao crime.

Dessa forma, encontram-se classificações, a depender do parâmetro utilizado, que podem ser: por território ocupado (grandes ou transnacionais, médias ou intermunicipais e pequenas ou municipais)<sup>21</sup>; pelo tipo de estrutura organizacional da empresa (tradicional, rede empresarial e endógena)<sup>22 23</sup>; pela origem dos integrantes da empresa criminosa (integrarem uma mesma origem étnica ou uma mesma religião)<sup>24</sup>; ou ainda construindo o conceito de Crime Organizado por diferenciação<sup>25</sup> de outros tipos de fenómenos que lhe são assemelhados, como a criminalidade de massa <sup>26 27</sup>, criminalidade profissional e o crime

<sup>21</sup> MENDRONI, Marcelo Batlouni. **Crime Organizado**: São Paulo. Ed. Atlas, 2012. p. 53 e 54.

<sup>22</sup>“Atualmente são conhecidas quatro formas básicas de Organizações criminosas: 1.Tradicional (ou Clássicas) - das quais o exemplo mais clássico são as máfias. (...) 2.Redes (Network - Rete Criminale – Netzstruktur) – cuja principal característica é a globalização. Forma-se através de um grupo de *experts* sem base, vínculos, ritos, e também sem critérios mais rígidos de formação hierárquica. É provisória, por natureza, e se aproveita das oportunidades que surgem em cada setor e local. (...) 3.Empresarial – formada no âmbito de empresas lícitas.(...) Mantém as suas atividades primárias lícitas, fabricando, produzindo e comercializando bens de consumo para, secundariamente, praticar crimes fiscais, crimes ambientais, cartéis, fraudes(...) 4. Endógena – Trata-se de espécie de organização criminosa que age dentro do próprio Estado, em todas as suas esferas – Federal, Estaduais e Municipais, envolvendo, conforme a atividade, cada um dos Poderes, Executivo, Legislativo ou Judiciário. É formada essencialmente por políticos e agentes públicos de todos os escalões, envolvendo, portanto, necessariamente, crimes praticados por funcionários públicos contra a administração pública (...) MENDRONI, Marcelo Batlouni. **Crime Organizado**. São Paulo. Ed. Atlas, 2012. p. 21 a 23.

<sup>23</sup> Também tratam tais formas de organização como modelos, paradigmas. “O paradigma mafioso traz a a ideia de uma organização criminosa com efetivo domínio territorial, fortemente hierarquizada, dotada até mesmo de uma comissão dirigente (...) O paradigma da rede é também chamado modelo do entrelaçamento de agentes criminosos. (...) O paradigma empresarial adquire sua conformação na figura imponente da empresa, como motor da vida econômica de todo o mundo, dentro do modelo do capitalismo global, com seus reflexos inevitáveis na criminalidade.” CABETTE, Eduardo Luis Santos e NAHUR, Marcius Tadeu Maciel. **Criminalidade organizada & globalização desorganizada**. Rio de Janeiro: Ed. Freitas Bastos, 2014. p. 75 e 76.

<sup>24</sup>“Para compreender o funcionamento, a eficácia mortal da maioria dos cartéis, parece portanto indispensável levar em conta a questão étnica. (...) Nada mais poderoso, motivador e engeguecedor que uma crença. Em seu reino, com efeito, os fatos não penetram. As fantasias, os sonhos, as angústias, as afirmações apodícticas ocupam o campo da consciência. Por isso é que as formações sociais cujo cimento fundamental é a etnia são tão poderosas, mobilizadoras e praticamente indestrutíveis.” ZIEGLER, Jean. **Senhores do Crime**: Rio de Janeiro, Ed. Record, 2003. p. 71.

<sup>25</sup>“Alguns autores procuram a definição de criminalidade organizada por contraposição à definição de criminalidade comum ou de massa. Enquanto esta integra condutas ilícitas, praticadas geralmente de forma isolada e individual, susceptíveis de assumir formas de violência gratuitas, destituídas de qualquer sentido estratégico, aquela compreende o conjunto de condutas ilícitas praticadas de forma colectiva, sistemática, integrada e continuada, visando alcançar objectivos estrategicamente predefinidos.” BRAZ, José. **Investigação Criminal**. A organização, o método e a prova. Os desafios da nova criminalidade. Coimbra, Almedina, 2013. p. 299.

<sup>26</sup>“Na verdade, a população encontra-se realmente sobressaltada e agredida por uma forma de criminalidade que nada tem a ver com a criminalidade organizada: é a criminalidade de massa.” HASSEMER, Winfried. **A Segurança Pública no Estado de Direito**. Lisboa. Associação Académica da Faculdade de Direito de Lisboa, 1995. p. 91.

perpetrado de modo organizado<sup>28</sup>.

O crime organizado funciona, assim, direcionado exclusivamente para obtenção da maior acumulação de capital, no menor espaço de tempo possível, ou seja, no lucro rápido, preferencialmente sem qualquer controle, regra ou limite imposto pelo Estado. Desse modo, ao não estar submetido a regras estatais sobre o “que” comercializar ou “como” comercializar, liberado, inclusive, de pagar um preço público pela exploração de determinadas atividades e ainda não se sujeitando a limites, sejam físicos ou legais, o crime organizado materializa a forma mais aguda, intensa e selvagem do capitalismo. Isso possibilita a criação de monopólios pela uso força, sem restrições ou regras que não aquelas que a lei do mais forte impõe.<sup>29</sup>

A ineficiência do Estado em controlar e fiscalizar as atividades financeiras que estão à sua volta propicia a infiltração do crime organizado na máquina estatal, dificultando o controle da sua disseminação na sociedade, produzindo elevação nos índices de violência. Os grupos criminosos, especialmente os que operam no mercado transnacional, são rapidamente adaptáveis e apresentam alto nível de organização que dificultam o trabalho das autoridades responsáveis pela investigação, bem como de todos os órgãos encarregados de prevenir e combater a atividade criminosa.

Os criminosos tendem a maximizar a oportunidade de oferta dos seus serviços tanto no mercado interno quanto no mercado externo, e a minimizar os riscos de serem identificados, presos, condenados e, especialmente, de perderem os lucros auferidos com a atividade criminosa. Visando garantir a viabilidade das suas operações e a obtenção de lucros sempre crescentes, o crime organizado ingressa nas engrenagens do Estado, corrompendo funcionários localizados na base da pirâmide de comando, bem como aqueles que elaboram as leis, e ainda definem e executam políticas públicas.

---

<sup>27</sup> “No entanto, há uma zona cinza entre a criminalidade organizada e a criminalidade de massas, na qual elas se confundem. É quando a segunda é decorrente da primeira, que aparece como geratriz, de sorte que, a despeito de constituírem diferentes tipos de criminalidade, da organização criminosa deriva parte da criminalidade de massas.” FERRO, Ana Luiza Almeida. **Crime Organizado e Organizações Criminosas Mundiais**. Curitiba: Juruá, 2012. p. 328.

<sup>28</sup> “...também é preciso vislumbrar fenômenos assemelhados à criminalidade organizada, os quais podem ser divididos, basicamente, em quatro espécies: criminalidade de grupo, criminalidade profissional, criminalidade de massa e crime cometido de modo organizado.” CABETTE, Eduardo Luis Santos; NAHUR, Marcius Tadeu Maciel. **Criminalidade organizada & globalização desorganizada**. Rio de Janeiro: Ed. Freitas Bastos, 2014. p. 78.

<sup>29</sup> “O capitalismo encontra sua essência no crime organizado. Mais precisamente, o crime organizado constitui a fase paroxística do modo de produção e da ideologia capitalistas.” ZIEGLER, Jean. **Senhores do Crime**. Rio de Janeiro. Ed. Record, 2003. p. 51

O crime organizado encontra, portanto, ambiente propício para o crescimento de sua influência, valendo-se de todas as oportunidades oferecidas pela globalização dos mercados, das novas tecnologias de comunicação e gestão da informação. A própria natureza da atividade internacional de branqueamento de capitais (lavagem de dinheiro), por exemplo, confirma que o seu desenvolvimento está associado a maior segurança trazida pelo desenvolvimento da tecnologia nas áreas de informática e comunicação.

### 1.3 O ESTADO COMO PARCEIRO

O traço comum a maioria dos modelos de organização criminosa, é valer-se da corrupção<sup>30 31</sup>. É possível afirmar que sem a corrupção não se pode falar em crime organizado<sup>32</sup>. O crescimento da empresa criminosa em direção à maximização dos lucros depende do estreitamento das relações com o Estado, e a porta de acesso desse relacionamento é a corrupção.<sup>33</sup>

O Estado é uma criação jurídica, uma vez que sua implementação ocorre a partir de um ato jurídico – a Carta Constitucional – gerador do sistema jurídico<sup>34</sup>, que operacionaliza

<sup>30</sup> “Na atualidade, entendemos como corrupção os atos de atribuição de uma vantagem patrimonial, que não seja devida, a um funcionário, no âmbito ou por causa das suas funções, ou a aceitação de tal vantagem por parte deste”. CALDAS, André Moz. **A Magistratura dos Censores e o Combate à Corrupção em Roma**. Lisboa: AAFDL, 2017. p. 137

<sup>31</sup> “ Se puede definir a los actos de corrupción, entonces, como aquellos que constituyen la violación, activa o pasiva, de un deber posicional o del incumplimiento de alguna función específica realizados em un marco de discreción com el objeto de obtener um beneficio extraposicional, cualquiera sea a su naturaliza.” SEÑA, Jorge F. Malem. **Globalización, comercio internacional y corrupción**. Barcelona: Editorial Gedisa, 2000. p. 28

<sup>32</sup> “O relacionamento da organização criminosa e o aparelho estatal se tornou uma de suas características, sendo este contato pelo menos com o aparelho repressivo, seja na forma de deliberada impunidade dos delinquentes, seja por meio do clientelismo, através do qual se obtém licenças para os destinatários dos serviços da organização, ou outros favores de órgãos públicos.” BORGES, Paulo César Corrêa. **Crime Organizado**. São Paulo: Associação Paulista do Ministério Público, 2000. p.24

<sup>33</sup>“...há os que reservam a designação de “Crime Organizado” principalmente para o tipo de organização criminosa que é capaz de cooptar agentes do Estado e, desse modo, tornar-se quase invulnerável à ação repressiva da lei. No entanto, é difícil distinguir onde há cooptação e onde há apenas mais um mercado ilegal, um mercado que transaciona mercadorias políticas (Misse, 2006) e que, como tal, não se distinguiria de nenhum outro mercado ilegal, a não ser pelo fato de que “oferece” uma mercadoria muito especial, constituída por relações de força e poder ou extraída simplesmente da autoridade pública, como uma fração privatizada e mercantilizada da soberania do Estado.” MISSE, Michel. **Mercados ilegais, redes de proteção e organização local do crime no Rio de Janeiro**. São Paulo: Instituto de Estudos Avançados da Universidade de São Paulo, v. 21, 2007. p. 141-142

<sup>34</sup>“O sistema jurídico atinge sua clausura ou autonomia auto-referencial com a “invenção” do acto jurídico, que se reproduz continuamente a si próprio gerando novos actos jurídicos.” TEUBNER, Gunther. **O Direito como Sistema Autopoiético**. Trad. de José Engrácia Antunes. Lisboa: Fundação Calouste Gulbekian, 1989. p. 57.

suas decisões por códigos binários “lícito/ilícito”<sup>35</sup>, marcando assim todos os atos subsequentes à criação do Estado de licitude. Assim, o Estado interage e relaciona-se com os demais sistemas, por meio de atos jurídicos, não sendo possível o relacionamento estatal por intermédio de outro ato que não jurídico, ou seja, ato lícito.

Em algum momento da cadeia produtiva, a organização criminosa estabelecerá relações com o Estado, e isso só ocorre de maneira ilícita, já que a empresa tem objetivo ilícito, operando em código oposto àquele que opera o Estado. Seguindo esse raciocínio, conclui-se que a relação da organização criminosa não pode ser diretamente com o Estado, pois seria impossível a prática de um ato jurídico lícito para quem opera com código da não juridicidade, para quem atua no espaço do ilícito.

O que ocorre é a prática de ação ilícita perpetrada pelo representante do Estado, com roupagem de ação lícita, visando favorecer vantagens à empresa criminosa, mediante recompensa, gerando prejuízos ao Estado. Assim, um fiscal aduaneiro pratica duas ações quando recebe propina para emitir recibo de quitação de tributo devido, sem efetivo recolhimento dos valores pelo fisco, com as formalidades legais atendidas: a primeira ilegal (recebimento de propina) e a segunda legal (emissão de recibo de quitação, obedecidas as formalidades legais). Esse segundo ato passa a gerar atos jurídicos, portanto legais.

Neste momento é possível verificar a corrupção do código lícito/ilícito que orienta o sistema jurídico, pois, no exemplo posto, foi praticado um ato jurídico, porém ilícito, que gera outros atos jurídicos, sendo que não foi observada a licitude necessária para sua prática. Emitir um recibo de quitação quando quitação não houve é corromper o código, pois tratou como lícito um ato que não preencheu os requisitos da licitude. Desse modo, o código lícito/ilícito foi violado, pois ingressou no sistema jurídico um ato que não obedeceu ao código da licitude.

A empresa criminosa não opera sob a égide do código binário lícito/ilícito, portanto seus atos estão necessariamente fora do sistema jurídico e, por consequência, fora do corpo do Estado, só podendo existir comunicação se houver a corrupção do código lícito/ilícito. Só com a corrupção deste código, um ato não jurídico pode gerar efeitos no mundo jurídico, que é exatamente o que acontece no caso do crime organizado, sendo que tal corrupção traz como

---

<sup>35</sup>“Como os restantes sistemas, também o jurídico pode ser observado (do interior e do exterior) e pode sofrer pressão e impacto do ambiente, mas o significado dessa influência é exclusivamente pelo seu sentido interno, mormente pelo seu código binário “lícito” (“Recht”) - “ilícito” (“Unrecht”) DIAS, Augusto Silva. **“Delicta in Se” e “Delicta Mere Prohibita”**. Coimbra: Coimbra Editora, 2008. p. 447/448.

efeito para a sociedade a sensação de descrença, de impunidade, de desvalor dos atos praticados pelo Estado por intermédio dos seus representantes.

A capacidade de danosidade social do crime organizado noticiada pela mídia, especialmente quando evidencia práticas violentas de organizações criminosas, bem como a capilaridade e o entranhamento em todos os setores da sociedade, ativa um sentimento de urgência para o desenvolvimento de medidas de combate à criminalidade, em que a sociedade reclama a adoção por parte do Estado de atitudes radicais, como o endurecimento das leis e a mitigação de direitos e garantias individuais, na frágil esperança de que providências de características populistas, alardeadas em um contexto de clamor social, possam ser suficientes para debelar o crime organizado.

O debate público em torno desse grave problema social é necessário, pois é imperioso o resgate da moralidade pública e do senso ético, visando criar uma conscientização por parte da sociedade de que o crime organizado é uma doença grave e pernicioso para o desenvolvimento de qualquer comunidade. Se hoje ele pode oferecer emprego a pessoas que vivem em condição de profunda vulnerabilidade, a contrapartida poderá ser cobrada a um custo incomensurável<sup>36 37</sup>. É necessário, portanto, opor resistência ao crime organizado.

Essas discussões não podem ser pautadas por pressões mediáticas ou por situações ocasionais de emergência, tampouco limitar-se a pauta da alteração da legislação penal, como se o fenómeno do crime organizado pudesse ser resolvido apenas pela aplicação de leis mais severas. O direito penal e processual penal não podem ser utilizados como instrumentos de reforma social, pois não se prestam a este fim, podendo ao máximo contribuir para restabelecer a ordem das liberdades coexistentes<sup>38</sup>

---

<sup>36</sup> “É necessário uma consciencialização da sociedade de que o crime organizado é uma doença prolongada e devastadora para o desenvolvimento harmonioso da comunidade: hoje, pode-lhes dar trabalho, dinheiro para alcançar fins pessoais e profissionais, oportunidades económicas, sociais e políticas, mas amanhã têm de pagar (e muito) a ajuda antes dada como esmola.” VALENTE, Manuel Monteiro Guedes. **Criminalidade Organizada e Criminalidade de Massa**. Coimbra: Edições Almedina S.A., 2009. pág. 161.

<sup>37</sup> “...urge o resgate da moralidade pública e do senso ético, através do incentivo à resistência por parte da sociedade, de modo a neutralizarem-se as práticas ligadas à exploração dos atos de corrupção, os quais funcionam como instrumental para o êxito das atividades criminosas perpetradas pela delinquência organizada.” PEREIRA, Flávio Cardoso. **Crime Organizado e suas Infiltrações nas Instituições Governamentais**. São Paulo: Ed. Atlas, 2015. pág. 34.

<sup>38</sup> “O direito penal e o direito processual que serão produzidos e aplicados não podem cair na armadilha de se tornarem meros direitos promocionais.” CABETTE, Eduardo Luis Santos e NAHUR, Marcius Tadeu Maciel. **Criminalidade organizada & globalização desorganizada**. Rio de Janeiro: Editora Freitas Bastos, 2014. pág. 101.

A participação da sociedade é fundamental para se debelar o crime organizado na forma aguda que hoje se apresenta. A corrupção infiltrada nas engrenagens do Estado é uma realidade que reflete um grave problema social, não sendo prevenida e debelada exclusivamente pelo direito, mas sim por mudanças profundas nos padrões coletivos de comportamento.

O Estado deve empreender esforços para a conscientização da sociedade sobre as formas como agem as organizações criminosas, assunto que deve estar em evidência no debate público<sup>39</sup>. A estreita ligação da corrupção com as organizações criminosas deve estar presente nas rodas de conversa, nos âmbitos da educação básica e superior, para que não reste dúvidas de que combater a corrupção significa combater o crime organizado. Todos os integrantes da sociedade devem, portanto, aprender a não pactuar com a corrupção, fomentando a cultura da denúncia, a fim de que o crime organizado seja desmontado.

A corrupção debilita o Estado, enfraquece os sistemas legais e judiciais<sup>40</sup>, dificulta o investimento, impedindo o crescimento económico, a promoção do bem-estar social dos indivíduos, o que leva à descrença por parte da sociedade do papel do Estado como agente de desenvolvimento e promoção de justiça e igualdade social<sup>41</sup>. Essa descrença fragiliza o conteúdo da cidadania, gera uma desconfortável sensação de impotência ante o enfrentamento da corrupção, pois a mesma parece distante, desconectada das preocupações quotidianas dos indivíduos, que não associa com facilidade o impacto causado na sua vida pelo ato ilícito praticado pelo corruptor ou pelo corrupto<sup>42</sup>.

---

<sup>39</sup>“Talvez possa argumentar-se que o Estado, através de seus órgãos competentes, esteja empregando estratégias de enfrentamento equivocadas, desprovidas de um conteúdo voltado para a prevenção, através, principalmente, do resgate da responsabilidade cívica do cidadão, em especial dos servidores públicos, e do aperfeiçoamento de controles de transparência em nossas instituições públicas. Destarte, fato incontestável é que a persecução e prevenção a este fenômeno encontram-se aquém das nossas expectativas.” PEREIRA, Flávio Cardoso. **Crime Organizado e suas Infiltrações nas Instituições Governamentais**. São Paulo: Ed. Atlas, 2015. pág. 43.

<sup>40</sup>“Uma polícia corruptível ou, até mesmo uma justiça e uma legislação corruptíveis envenenam internamente um ordenamento democrático-libertário.” HASSEMER, Winfried. **Direito Penal Libertário**. Trad. de Regina Greve. Belo Horizonte: Del Rey, 2007. pág. 97.

<sup>41</sup>“Corrupção significa nesses termos e, portanto, de forma direta, a debilidade do Estado de Direito em razão de condutas ilegais ou imorais que corroem interesses públicos em detrimento de interesses privados. (...) a corrupção dificulta e distorce quaisquer investimentos, impedindo o crescimento económico e o desenvolvimento sustentável, destruindo, por fim, os sistemas legais e judiciais. (...) Como consequência dessa situação, surge o enfraquecimento do ideal de cidadania, o que contribuirá sobremaneira para uma omissão deliberada da participação popular no enfrentamento a esta problemática. Nesse cenário reinam a omissão e o comodismo por parte de uma população contaminada por um estado notório de “anestesia moral e ética”. PEREIRA, Flávio Cardoso. **Crime Organizado e suas Infiltrações nas Instituições Governamentais**. São Paulo: Ed. Atlas, 2015. págs. 45 e 46.

<sup>42</sup> “ Desde un punto de vista estrictamente económico, la delincuencia organizada puede reportar, en un primer momento, beneficios para el consumidor. Éste encuentra productos más baratos, pero el coste general es enorme. Ésta es una de las razones por las cuales muchas veces la sociedad no es muy consciente de la importancia que

## 1.4. CONCEITO

No caso específico da criminalidade organizada, como se apresentou até então, não há univocidade quanto à nomenclatura a ser utilizada, podendo ser encontrada na literatura nacional e estrangeira mais de uma dezena de termos para se referir a ela. Pode-se citar alguns a título de exemplo: associação criminosa, associação mafiosa, associação organizada, associação ilícita, associação delinquencial complexa, organização criminal, grupo organizado, sodalício criminal, bando criminosa, empresa criminosa, sindicato criminoso, sindicato do crime, etc<sup>43</sup>

### 1.4.1 O fenômeno da criminalidade organizada

A exemplo do código penal, que varia de sociedade para sociedade a depender dos valores que cada uma elege para serem tutelados pela legislação punitiva, assim também ocorre com o crime, especificamente com o chamado crime organizado. Ele se manifesta como espelho da deficiência ou anomalia que sofre aquela organização social<sup>44</sup>.

Assim, a depender de como se estrutura o sistema social, o conceito de crime organizado pode apresentar variantes e peculiaridades que se refiram a ele, produzindo questionamentos como: há um conceito para crime organizado que delimite seu contorno e lhe atribua identidade própria? É possível estabelecer que o crime organizado é uma nova categoria de apresentação do crime dentro do Direito Penal ou o crime organizado é apenas uma nova qualidade para apresentação da comum criminalidade?<sup>45</sup> Não partir do pressuposto

---

tiene la delincuencia organizada o el blanqueo.” ROBLES, Diego Torrente. **La Inseguridad creada por la Delincuencia Económica Transnacional** in PUIG, Santiago Mir e Queralt Joan J.. **La Seguridad Pública ante el Derecho Penal**. Buenos Aires: Euros Editores S.R.L, 2010. pág.263

<sup>43</sup>“De fato, não há uma nomenclatura unívoca e universal sobre o tema.” CABETTE, Eduardo Luis Santos e NAHUR, Marcio Tadeu Maciel. **Criminalidade organizada & globalização desorganizada**. Rio de Janeiro: Ed. Freitas Bastos, 2014. pág. 102.

<sup>44</sup>“O crime não é encontrado somente na maioria das sociedades desta ou daquela espécie, mas em todas as sociedades de todos os tipos. Não existe nenhuma em que não haja alguma forma de criminalidade. Esta muda de feição, os atos qualificados de crimes não são os mesmos em toda a parte...” DURKHEIM, Émile. **As Regras do Método Sociológico**. São Paulo: Companhia Editora Nacional, 1976. p. 57.

<sup>45</sup>“Os criminologistas, enquanto eles percebem e reconhecem o fenômeno da “criminalidade organizada”, são uníssomos que isso é uma nova forma qualitativa de apresentação da criminalidade.” HASSEMER, Winfried. **Direito Penal Libertário**. Belo Horizonte. Editora Del Rey, 2007. p. 140.

de que é possível encerrar o crime organizado em um único conceito<sup>46 47</sup>, é, portanto, o primeiro cuidado que se deve ter, pois tal assertiva pode ou não se confirmar, dependendo do ângulo sob o qual se analisa o fato e da abordagem a ser feita.

Para a criminologia e a sociologia, o fenômeno social aqui estudado pode não ter um conceito fixo, apresentando-se, inclusive, por modelos de estruturas cambiantes<sup>48</sup>. Para o direito, há a necessidade de uma delimitação clara e precisa, como se exige de toda questão de matéria penal<sup>49</sup>. Para a criminologia trata-se de um fenômeno social a ser estudado como tal, suas ações e consequências, e não como uma nova figura a reclamar tipificação penal<sup>50</sup>. Já a ciência jurídica insiste na necessidade de definição<sup>51</sup> para que possa ser adequadamente compreendido e incluído no rol dos crimes previstos na legislação penal, com vistas à sua

<sup>46</sup>“À primeira vista, ao tentar se formular – ou ao menos delimitar – o conceito de crime organizado, é preciso ter cuidado para que não se parta do pressuposto de que é possível encontrar-se uma definição única para o fenômeno.” BECK, Francis Rafael. **Perspectivas de controle ao crime organizado e crítica à flexibilização das garantias**. São Paulo: IBCCrim, 2004. p. 65, 66.

<sup>47</sup> “Como hemos dicho otras veces, definir és una tarea difícil y frágil, ya que toda definición “congela” un estágio, siempre temporal de las sociedades e el pensamiento, y deja afuera los hitos de los câmbios. Y así como no hay preguntas finales en la sociedade, tampoco hay respuestas definitivas” CASTRO, Lola Anyar de. **Formas de Delincuencia Organizada em America Latina**, la Simbologia del Narcotráfico e das Técnicas de Control. São Paulo: Revista Brasileira de Ciências Criminais nº 112, 2015, p. 126

<sup>48</sup>“Pode-se inferir a existência de pelo menos dois tipos distintos, embora aparentados, de organização criminosa. O mais conhecido é o Tradicional ou Territorial. Um segundo tipo é o Empresarial. (...) *Crime Organizado Tradicional*: Grupo de pessoas voltadas para atividades ilícitas e clandestinas que possui uma hierarquia própria e capaz de planejamento empresarial, que compreende a divisão de trabalho e o planejamento de lucros. Suas atividades se baseiam no uso da violência e da intimidação, tendo como fonte de lucros a venda de mercadorias ou serviços ilícitos, no que é protegido por setores do Estado. Tem como características distintas de qualquer outro grupo criminoso um sistema de clientela, a imposição da lei do silêncio aos membros ou pessoas próximas e o controle pela força de determinada porção de território. (...) O segundo modelo de organização criminosa é menos definido, mais difícil de diferenciar das simples quadrilhas ou de uma empresa legal. Sua característica mais marcante é transpor para o crime métodos empresariais, ao mesmo tempo que deixam de lado qualquer resquício de conceitos como Honra, Lealdade, Obrigação, etc.” MINGARDI, Guaracy. **O Estado e o Crime Organizado**. São Paulo: IBCCrim, 1998. p. 81 a 83 e 87/88.

<sup>49</sup>“O conceito de *organização criminosa* é complexo e controverso, tal como a própria atividade do crime nesse cenário. Não se pretende obter uma definição tão abrangente quanto pacífica, mas um horizonte a perseguir, com bases seguras para identificar a atuação da delinquência estruturada, que visa ao combate de bens jurídicos fundamentais para o Estado Democrático de Direito.” NUCCI, Guilherme de Souza. **Organização Criminosa**. Rio de Janeiro: Editora Forense, 2017. p. 13

<sup>50</sup>“A criminalidade organizada constitui antes de tudo (é este, como se disse já, o seu ponto de partida) um fenômeno social, econômico, político, cultural, fruto da sociedade contemporânea; de tal modo significativo na vida dos povos e das pessoas que não pôde deixar de apelar para a sua consideração pelo direito. (...) Isto porém é uma coisa, outra completamente diferente é a tentativa de elevar a criminalidade organizada à categoria de crime, de a *criminalizar qua tale*, de a *tipificar*, de a constituir em um *tipo-de-ilícito* ou em um *tipo-de-crime* autônomos, de procurar a determinação de um *bem jurídico* específico que por via dela se vise tutelar e proteger.” DIAS, Jorge de Figueiredo. **Criminalidade Organizada**. In: Revista Brasileira de Ciências Criminais, n. 71: São Paulo: Ed. Revista dos Tribunais, 2008, p. 14.

<sup>51</sup>“L'appréhension du phénomène passe nécessairement par as définition. Malgré la réticence persistante de nombreux criminologues, certains se sont essayés à l'exercice.” PARIZOT, Raphaële. **La Responsabilité Pénale à L'épreuve de La Criminalité Organisée**: Paris. Lextenso éditions, 2010. p. 7.

**Em livre tradução:** A apreensão do fenômeno passa necessariamente por sua definição. Apesar da persistente relutância de muitos criminologistas, alguns fizeram esse exercício.

prevenção e combate<sup>52</sup><sup>53</sup>. Assim reconhecido como fenômeno que cabe na moldura do direito repressivo, cabe ao legislador definir como ele será incluído na legislação, quais suas características e nomenclatura<sup>54</sup>

A dualidade do discurso, entretanto, encontra um ponto de convergência, que ocorre a partir da percepção da criminalidade organizada como fenômeno social. Como defendido pela criminologia, esse fenômeno é identificado pelo sistema jurídico penal como um código válido, portanto, como integrante do seu escopo de estudo. Isso ocorre em virtude da alteração que vem acontecendo nos últimos anos no direito penal e processual penal, que têm abandonado as garantias individuais como parâmetros de validade e adotado a segurança do cidadão como novo paradigma. Mais adiante neste trabalho, será tratada a questão da segurança e como a mesma, em uma sociedade de risco como a nossa, passa a servir de parâmetro para a elaboração de normas penais.

Esse novo modelo de direito penal permite a inclusão de questões em sua análise até então restritas ao campo da política criminal, estendendo sua intervenção a fenômenos sociais, tais como a criminalidade organizada.<sup>55</sup> Em virtude dessa modificação de parâmetros que vem

---

<sup>52</sup>Cabe trazer aqui a justa crítica “Criminalidade não é para ser combatida, porque não encerra nenhuma guerra, mas prevenida e reprimida. Esse cânone da cultura jurídica penal não muda em nada só porque, agora, se fala de criminalidade organizada.” CABETTE, Eduardo Luis Santos e NAHUR, Marcius Tadeu Maciel. **Criminalidade organizada & globalização desorganizada**. Rio de Janeiro: Ed. Freitas Bastos, 2014. p. 105.

<sup>53</sup>“A questão situava-se, no entanto, na grande dificuldade, inclusive doutrinária, de estabelecer exatamente o conceito de crime organizado, até para que se pudessem utilizar adequadamente os meios repressivos postos à disposição da Polícia e da Justiça criminal no combate a esse tipo de atividade e, ao mesmo tempo, impedir que fossem aplicados tais atos investigatórios (evidentemente mais drásticos e gravosos) em casos que não eram especificamente de “organização criminosa”. MOREIRA, Rômulo de Andrade. **A Nova Lei do Crime Organizado**. Porto Alegre: Editora Magister, 2014. p.18

<sup>54</sup>“Pour les législateurs, une question se pose, qui est celle de savoir quelle définition ils peuvent donner de ce phénomène. L’intérêt de la question tient aux peines et surtout à la procédure applicable, les unes et l’autre étant évidemment plus rigoureuses en cas de criminalité organisée. Deux méthodes se présentent: celle de l’énumération sèche des comportements qui semblent suffisamment graves pour mériter la qualification d’infractions de criminalité organisée et celle d’une définition plus criminologique ou plutôt juridico-criminologique.» PRADEL, Jean e DALLEST, Jacques. **La Criminalité Organisée**. Paris: LexisNevis, 2012. p. 2.

**Em livre tradução:** Para os legisladores, surge a questão de saber que definição eles podem dar a este fenômeno. O interesse da questão reside nas penas e, sobretudo, no procedimento aplicável, ambos obviamente mais rigorosos nos casos de crime organizado. Dois métodos se apresentam: o da enumeração simples de comportamentos que parecem suficientemente graves para merecer a qualificação de infrações de crime organizado e o de uma definição mais criminológica, ou melhor, jurídico-criminológica.

<sup>55</sup>“Eso puede ser visto claramente en los discursos de los políticos y en los debates sobre seguridad pública. También se revela a la hora de la aprobación de nuevas leyes penales imbuidas de carácter represivo con supresión de garantías o ampliación de las conductas típicas. Dicho de otro modo, la revelación de esa nueva legislación muchas veces no demuestra de inmediato este sesgo, sin embargo, nunca se vio una apertura tan grande en los tipos penales, donde el principio de la taxatividad que orientaba el Derecho Penal fue olvidado.” CALLEGARI, André Luis. **Control Social y Criminalidad Organizada**. n Crimen Organizado: Lima. ARA Editores E.I.R.L., 2009. p. 14, 15.

ocorrendo com o direito penal, reflexo da sociedade de riscos<sup>56</sup> em que se vive, é que passa a ser cabível a inclusão do crime organizado como tipo autónomo na legislação. Assim vencida essa questão, atualmente ruma o direito penal para a tipificação do crime organizado como figura penal própria, mesmo com as diversas opiniões contrárias à juridicização de um conceito criminológico<sup>57</sup>.

### 1.4.2 Delimitando o objeto

Em sede de trabalho jurídico, cujo escopo é discutir métodos legais de persecução criminal do crime organizado, é necessário que o fenómeno da criminalidade organizada ingresse na compreensão do mundo jurídico e seja tipificado como conduta delitativa, para que só depois se discuta sua persecução penal. Sendo assim, não farão parte do estudo, a partir de então, conceitos criminológicos sobre criminalidade organizada. Serão adotados como referência apenas conceitos jurídicos, respeitando a nomenclatura adotada por cada legislação ao se referir ao fenómeno jurídico, objeto do presente estudo.

A literatura jurídica referente ao crime organizado é vasta e toda ela se depara com a difícil tarefa de conceituar e diferenciar o crime organizado, produto da organização criminosa, e o crime praticado por membros de uma associação ilícita, já devidamente tipificada na maior parte dos ordenamentos, mas que não seja uma organização criminosa (quadrilha, bando, gangue)<sup>58</sup>. Mesmo com a diversidade de conceitos, alguns pontos

<sup>56</sup>Como preconizada por Beck: “En el centro figuran riesgos y consecuencias de la modernización que se plasman en amenazas irreversibles a la vida de las plantas, de los animales y de los seres humanos. Al contrario que los riesgos empresariales y profesionales del siglo XIX y de la primera mitad del siglo XX, estos riesgos ya no se limitan a lugares y grupos, sino que **contienen una tendencia a la globalización que abarca la producción y la reproducción y no respeta las fronteras de los Estados nacionales, con lo cual surgen unas amenazas globales que en este sentido son supranacionales y no específicas de una clase y poseen una dinámica social y política nueva**”. Sem destaque no texto original. BECK, Ulrich. *La sociedad del riesgo*: Barcelona. Paidós, 1998.

<sup>57</sup>“Lentamente van perdiendo fuerza las voces que exigen llanamente la eliminación de los delitos de organización como contrarias a un sistema jurídico-penal legítimo, y múltiples propuestas y decisiones de ampliación del arsenal jurídico-penal dominan sin apenas discusión el terreno.” MELIÁ, Manuel Cancio. *El Injusto de Los Delitos de Organización: Peligro y Significado* In: Crimen Organizado. Lima: ARA Editores E.I.R.L, 2009. p. 35/36.

<sup>58</sup>“Enquanto “quadrilha ou bando” é terminologia adotada pelo Código Penal brasileiro, outros diplomas acolhem expressões, com pequenas variações de significação, como “associação ilícita” (art. 515 do Código Penal espanhol, art. 210 do Código Penal argentino, art. 292 do Código Penal chileno), “associação criminosa” (§ 129 do Código Penal alemão, conhecido como StGB, art. 299º do código Penal português), “associação de malfeitores” (art. 450-1 do Código penal francês) e “associação para delinquir” (art. 416 do Código Penal italiano, art. 207 do Código Penal cubano). Para o *Codex* lusitano, por exemplo, a associação criminosa é aquela

essenciais são comuns entre os autores e os diplomas legais que tratam do tema, a saber: pluralidade de agentes, ânimo delitivo, estabilidade, divisão do trabalho, finalidade de lucro e estrutura ou planeamento empresarial.<sup>59</sup>

A primeira alusão à criminalidade organizada encontrada na legislação portuguesa está na Lei n.º 36 de 26 de setembro de 1994, que se refere, na alínea d) do seu artigo 1.º<sup>60</sup>, a infrações do âmbito económico-financeiro cometidas de forma organizada, com recurso à tecnologia informática. A menção à prática de delito de maneira organizada não foi acompanhada de sua conceituação, restando delito de conteúdo aberto, cujo perímetro coube ser delimitado pela doutrina e jurisprudência.

Em 1998, o Conselho da União Europeia conceituou organização criminosa no art. 1.º da sua Ação Comum<sup>61</sup>, seguido pela Convenção das Nações Unidas contra o Crime Organizado Transnacional, que adota na data de 15 de dezembro de 2000, em Nova York, essa definição para grupo criminoso organizado<sup>62</sup>. Ambos os cadernos legislativos conceituam ora

---

“cuja finalidade ou actividade seja dirigida à prática de um ou mais crimes.” (art. 299º) FERRO, Ana Luiza Almeida. **Crime Organizado e Organizações Criminosas Mundiais**. Curitiba: Juruá, 2012. p. 354.

<sup>59</sup>“En consecuencia, se evidencia que la mayoría de los ordenamientos e instrumentos internacionales coinciden al momento de precisar el concepto de criminalidad organizada, como la manifestación criminal conformada por varias personas y caracterizada por la permanencia, ánimo delictivo, organización funcional, comisión de delitos graves y utilización de medios violentos o que afecten gravemente bienes jurídicos relevantes, para de este modo lograr sus finalidades.” BARBOSA, Paula Andrea. **Nuevas Tendencias Político-Criminales en La Lucha Contra La Criminalidad Organizada**. In Crimen Organizado: Lima: ARA Editores E.I.R.L., 2009. p. 98/99.

<sup>60</sup>“Lei n.º 36/94, de 29 de Setembro

Medidas de combate à corrupção e criminalidade económica e financeira

#### **Artigo 1.º**

##### **Acções de prevenção**

1 - Compete ao Ministério Público e à Polícia Judiciária, através da Unidade Nacional de Combate à Corrupção, realizar, sem prejuízo da competência de outras autoridades, ações de prevenção relativas aos seguintes crimes:

- a) Recebimento ou oferta indevidos de vantagem, corrupção, peculato e participação económica em negócio;
- b) Administração danosa em unidade económica do sector público;
- c) Fraude na obtenção ou desvio de subsídio, subvenção ou crédito;
- d) Infrações económico-financeiras cometidas de forma organizada, com recurso à tecnologia informática;
- e) Infrações económico-financeiras de dimensão internacional ou transnacional.” Disponível em

[https://www.pgdlisboa.pt/leis/lei\\_mostra\\_articulado.php?nid=145&tabela=leis&so\\_miolo=](https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=145&tabela=leis&so_miolo=). Acesso em 21/08/17

<sup>61</sup>“Artigo 1.º Para efeitos da presente acção comum, entende-se por «organização criminosa» a associação estruturada de duas ou mais pessoas, que se mantém ao longo do tempo e actua de forma concertada, tendo em vista cometer infrações puníveis com pena privativa da liberdade ou medida de segurança privativa da liberdade cuja duração máxima seja de, pelo menos, quatro anos, ou com pena mais grave, quer essas infrações constituam um fim em si mesmas, quer um meio de obter benefícios materiais e, se for caso disso, de influenciar indevidamente a actuação de autoridades públicas.” Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:31998F0733>. Acesso em: 21/08/17.

<sup>62</sup> “Article 2. Use of terms For the purposes of this Convention:

(a) “Organized criminal group” shall mean a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offenses established in accordance with this Convention, in order to obtain, directly or indirectly, a financial or other material benefit;” Disponível em: <http://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf>. Acesso em: 21/08/17.

organização criminosa ora grupo criminoso organizado, embora sem considerar nenhuma das duas figuras como ilícito penal.

Posterior a tais diplomas, surge a Lei 5/2002, em Portugal, datada de 11 de janeiro, concebida para o combate da criminalidade organizada e económico-financeira, introduzindo alterações na Lei nº 36/94, mas ainda sem estabelecer o conceito sobre a criminalidade organizada, optando o legislador por definir um catálogo dos crimes que assim considerou enquadrar-se nessa classificação<sup>63</sup>.

Idêntico o proceder do Código de Processo Penal Português, ao introduzir a alínea *m*) ao seu art. 1.º, a Lei 26/2010, de 30 de agosto, em que traz um novo elenco de delitos considerados como de criminalidade altamente organizada<sup>64</sup>, inaugurando aqui outro catálogo, com denominação diversa daquele estabelecido na lei anterior, sem que integre nenhum dos dois diplomas antes citados a figura típica de criminalidade organizada.<sup>65</sup>

---

**Em tradução livre:** Art. 2.º, *a*), "Grupo criminoso organizado" - um grupo estruturado de três ou mais pessoas, existindo durante um período de tempo e actuando concertadamente com a finalidade de cometer um ou mais crimes graves ou infracções estabelecidas na presente Convenção, com a intenção de obter, directa ou indirectamente, um benefício económico ou outro benefício material.

<sup>63</sup> “Lei n.º 5/2002, de 11 de janeiro:

Estabelece medidas de combate à criminalidade organizada e económico-financeira e procede à segunda alteração à Lei n.º 36/94, de 29 de Setembro, alterada pela Lei n.º 90/99, de 10 de Julho, e quarta alteração ao Decreto-Lei n.º 325/95, de 2 de Dezembro, alterado pela Lei n.º 65/98, de 2 de Setembro, pelo Decreto-Lei n.º 275-A/2000, de 9 de Novembro, e pela Lei n.º 104/2001, de 25 de Agosto. A Assembleia da República decreta, nos termos da alínea c) do artigo 161.º da Constituição, para valer como lei geral da República, o seguinte:

Artigo 1.º

Âmbito de aplicação

1 - A presente lei estabelece um regime especial de recolha de prova, quebra do segredo profissional e perda de bens a favor do Estado, relativa aos crimes de:

a) Tráfico de estupefacientes, nos termos dos artigos 21.º a 23.º e 28.º do Decreto-Lei n.º 15/93, de 22 de Janeiro; b) Terrorismo, organizações terroristas, terrorismo internacional e financiamento do terrorismo; c) Tráfico de armas; d) Tráfico de influência; e) Corrupção activa e passiva; f) Peculato; g) Participação económica em negócio; h) Branqueamento de capitais; i) Associação criminosa; j) Contrabando; l) Tráfico e viciação de veículos furtados; m) Lenocínio e lenocínio de menores; n) Tráfico de pessoas; o) Contrafacção de moeda e de títulos equiparados a moeda.”

<sup>64</sup> “Lei 26/2010, de 30 de agosto:

Artigo 1.º - Definições legais

Para efeitos do disposto no presente Código considera-se: (...) *m*) 'Criminalidade altamente organizada' as condutas que integrarem crimes de associação criminosa, tráfico de pessoas, tráfico de armas, tráfico de estupefacientes ou de substâncias psicotrópicas, corrupção, tráfico de influência, participação económica em negócio ou branqueamento.”

<sup>65</sup> “A lei consagra o modelo unitário alemão, por contraposição ao modelo diferenciador austríaco, de acordo com o qual se distingue a “associação criminosa” (*kriminelle Vereinigung*) punida pelo § 278º do StGB austríaco, e a “organização criminosa” (*kriminelle Organisation*), punida pelo § 278ºa do mesmo código. O StGB suíço também seguiu o modelo alemão no artigo 260ter, introduzido pela Lei federal de 18.03.1994.” ALBUQUERQUE, Paulo Pinto. **O Crime de Organização Criminosa no Código Penal Português**. In: AMBOS, Kai e ROMERO, Eneas **Crime Organizado**, Análise da lei 12.850/2013: São Paulo. Ed. Marcial Pons, 2017. p. 279

Além de tais diplomas não terem trazido essa conceituação penal, ainda não permitiram que fossem conhecidos os critérios que foram utilizados para categorização dos delitos em um dos dois catálogos, nem quais foram utilizados para estabelecer a diferença entre a criminalidade organizada e a altamente organizada, conforme a denominação adotada por tais diplomas legais.

Como visto, o ordenamento português optou por abrigar em seu corpo a terminologia criminalidade organizada, sendo esta sob a ótica de fenómeno jurídico-social, não como fato típico<sup>66</sup>, pois tanto a criminalidade organizada quanto a altamente organizada não são conceituadas, mas exemplificadas, não havendo um tipo penal com todos os elementos que são ínsitos a dar-lhe contorno. Esse contorno é o catálogo e o conceito poderia surgir da análise dos pontos em comum entre os crimes insertos nos referidos catálogos.

Ocorre que ambos os catálogos, tanto o previsto no art. 1º, al. *m*) do CPP, quanto o previsto no art. 1º da Lei 5/2002, não adotam um critério objetivo que justifique a escolha de tais ou quais delitos para compô-los, o que gera instabilidade e desconfiança na relação jurídica entre o sujeito e o Estado, pois, ante a ausência de balizamento conhecido, não se pode inferir o que o ordenamento jurídico penal entende como crime organizado ou como criminalidade organizada.

A delimitação desse conceito, ainda que por via transversa, é fundamental que seja feita, tanto para o entendimento do que é considerado crime organizado quanto para a estabilização das relações entre o indivíduo e o sistema penal, especialmente porque em ambos os diplomas legais antes citados há previsão de aplicação de regras mais rígidas, tanto processuais quanto sancionatórias que limitam severamente direitos e liberdades.<sup>67 68</sup>

---

<sup>66</sup>“Deste modo, aparecerá clara a desnecessidade e a inconveniência da construção de um crime singular de *criminalidade organizada*: como puro conceito-meio ou conceito instrumental, ele deve ligar-se antes de tudo ao crime de associação criminosa, embora com ele se não confunda ou a ele se limite...”DIAS, Jorge de Figueiredo. **Criminalidade Organizada**. In: Revista Brasileira de Ciências Criminais, n. 71: São Paulo. Ed. Revista dos Tribunais, 2008. p. 15.

<sup>67</sup>“O quadro descrito não pode deixar de causar insegurança jurídica se tivermos presente que a definição do que é criminalidade organizada funciona como pressuposto da aplicação de um regime processual e sancionatório mais severo, consistente em medidas fortemente restritivas de direitos e liberdades.” DIAS, Augusto Silva. **Criminalidade Organizada e combate ao lucro ilícito**. In: 2º Congresso de Investigação Científica: Coimbra, Almedina, 2010. p. 24/25.

<sup>68</sup> Ao discorrer a respeito do conceito de criminalidade organizada, assim Hassemer pontuou: “Nós precisamos de uma melhor definição sobre o fenómeno criminal proposto; isso não apenas aumentaria concretamente a efetividade da persecução, como também desoneraria em geral e por um longo tempo a atividade preventiva jurídica.” HASSEMER, Winfried. **Direito Penal Libertário**. Belo Horizonte: Ed. Del Rey, 2007. p. 141.

Além dos vários problemas de ordem técnica que essa imprecisão terminológica-concetual apresenta, é de se observar que arrimada em um discurso sedutor de combate ao aumento da criminalidade,<sup>69</sup> há uma real restrição a direitos e garantias individuais cujos fundamentos se alicerçam apenas em prática retórica, desassociada de fundamentação legal que a legitime.

No Brasil, o primeiro diploma legal a tratar de crime organizado foi a Lei nº 9.034 de 03 de maio de 1995<sup>70</sup>, que introduziu meios de prova e procedimentos investigatórios específicos para a repressão aos delitos praticados por organizações criminosas, sem ainda defini-los ou tipificá-los. Foi ratificada por este país, a Convenção das Nações Unidas contra o Crime Organizado Transnacional de 15 de dezembro de 2000, também conhecida como Convenção de Palermo, conforme Decreto nº 5.015/2004, que conceitua “grupo criminoso organizado”, como visto anteriormente.

Entrou em vigor a Lei nº 12.694/12 que trata do julgamento dos crimes praticados por organizações criminosas, denominação que passa doravante a ser adotada pelo ordenamento em questão, trazendo conceito próprio para organização criminosa<sup>71</sup>, mas ainda sem incluir tal figura no rol das condutas típicas. É com a atual legislação a respeito de organização criminosa que, além de conceito, cria-se também a figura penal distinta e específica para essa modalidade de conduta<sup>72</sup>. Desse modo, a Lei nº 12.850 de 02.08.13<sup>73</sup> traz

<sup>69</sup>“No entanto, a linguagem da redução dos direitos, das liberdades e das garantias, quando sustentada em reais problemas de aumento qualitativo da criminalidade (e este é um ponto que jamais podemos esquecer)” COSTA, José de Faria. **Direito Penal e Globalização**. Wolters Kluwer Portugal sob a marca Coimbra Editora, Coimbra, 2010. p. 58.

<sup>70</sup>“Lei nº 9.034, de 3 de maio de 1995, dispõe sobre a utilização de meios operacionais para a prevenção e repressão de ações praticadas por organizações criminosas.

Capítulo I

Da definição de ação praticada por organizações criminosas e dos meios operacionais de investigação e prova.

Art. 1º. Esta Lei define e regula meios de prova e procedimentos investigatórios que versarem sobre crime resultante de ações de quadrilha ou bando.

Art. 2º. Em qualquer fase de persecução criminal que verse sobre ação praticada por organizações criminosas são permitidos, além dos já previstos na lei, os seguintes procedimentos de investigação e formação de provas: (...). Disponível em: <http://www2.camara.leg.br/legin/fed/lei/1995/lei-9034-3-maio-1995-348988-publicacaooriginal-1-pl.html>. Acesso em 21/08/17.

<sup>71</sup>“Art. 2º Para os efeitos desta Lei, considera-se organização criminosa a associação, de 3 (três) ou mais pessoas, estruturalmente ordenada e caracterizada pela divisão de tarefas, ainda que informalmente, com objetivo de obter, direta ou indiretamente, vantagem de qualquer natureza, mediante a prática de crimes cuja pena máxima seja igual ou superior a 4 (quatro) anos ou que sejam de caráter transnacional.” Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2012/lei/112694.htm](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/112694.htm). Acesso em 21/08/17.

<sup>72</sup> “Com a nova Lei, a figura da organização criminosa deixou de ser “apenas” uma forma de se praticar crimes para se tornar delito autônomo, punido com reclusão de 3 a 8 anos.” CUNHA, Rogério Sanches e PINTO, Ronaldo Batista. **Crime Organizado**: Salvador, Editora JusPodium, 2015. p.17

<sup>73</sup>“Art. 1º Esta Lei define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal a ser aplicado.

no parágrafo 1º do seu art. 1º a conceituação de organização criminosa, para no artigo seguinte tipificá-lo como crime<sup>74</sup>

A tipificação do delito de organização criminosa, por sua vez, é mais restritiva que os conceitos utilizados pelos diplomas anteriores. Enquanto a Convenção de Palermo e a Lei nº 12.694/2012 exigiam a participação de 3 (três) ou mais pessoas na empresa criminosa, para que seja considerado crime organizado são necessárias ao menos 4 (quatro) pessoas.

Se para Convenção de Palermo bastava a prática de um delito para se caracterizar o grupo criminoso, no Brasil, desde a Lei nº 12.694/12, exige-se uma pluralidade de delitos – ou seja, ao menos dois – para que se possa falar em organização criminosa.

A Convenção de Palermo não estabelece um limite mínimo de pena do crime praticado pelo grupo para que este seja incluído no conceito gravoso. A Lei nº 12.694/12 reclama que as penas dos crimes praticados pela organização sejam iguais ou superiores a 4 (quatro) anos ou que tenham caráter transnacional. A Lei nº 12.850/13 que tipifica o delito exige que as penas dos crimes praticados pela organização criminosa sejam superiores a 4 (quatro) anos ou que tenham caráter transnacional.

A inclusão do tipo penal de organização criminosa não revoga o crime previsto no art. 288 do Código Penal, que após a promulgação da Lei nº 12.850/13, deixa de ter por *nomen iuris* quadrilha ou bando, para se chamar associação criminosa<sup>75</sup>, mantendo, entretanto a mesma estrutura. Assim, a associação de quatro ou mais pessoas com o fim de praticar delitos, cuja pena máxima de cada um deles seja igual ou inferior a quatro anos, não configura o delito de organização criminosa, mas poderá vir a se enquadrar no delito tipificado como associação criminosa, como previsto no Código Penal.

---

§ 1º Considera-se organização criminosa a associação de 4 (quatro) ou mais pessoas estruturalmente ordenada e caracterizada pela divisão de tarefas, ainda que informalmente, com objetivo de obter, direta ou indiretamente, vantagem de qualquer natureza, mediante a prática de infrações penais cujas penas máximas sejam superiores a 4 (quatro) anos, ou que sejam de caráter transnacional.” Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2013/lei/112850.htm](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/112850.htm). Acesso em 21/08/17.

<sup>74</sup>Art. 2º Promover, constituir, financiar ou integrar, pessoalmente ou por interposta pessoa, organização criminosa:

Pena - reclusão, de 3 (três) a 8 (oito) anos, e multa, sem prejuízo das penas correspondentes às demais infrações penais praticadas.” Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2013/lei/112850.htm](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/112850.htm), Acesso em: 21/08/17.

<sup>75</sup> “Associação Criminosa

Art. 288. Associarem-se 3 (três) ou mais pessoas, para o fim específico de cometer crimes:

Pena - reclusão, de 1 (um) a 3 (três) anos.” Disponível em: [http://www.planalto.gov.br/ccivil\\_03/decreto-lei/del2848compilado.htm](http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm)

## 2. O CRIME ORGANIZADO NO BRASIL

No Brasil, o fenômeno do crime organizado tem uma característica que o distingue daquele que acontece em outras partes do mundo: sua origem está em presídios ou em estabelecimentos para cumprimento de pena. No Brasil, - diferentemente do que ocorre com organizações criminosas que surgiram em outras sociedades, em que os elementos raciais ou étnicos são as bases para a criação dos laços de aproximação e identidade entre os membros- fazer parte de uma organização criminosa guarda estreita relação com o fato de o indivíduo ter cometido um delito e estar encarcerado em determinado estabelecimento prisional<sup>76</sup>.

### 2.1. APRESENTAÇÃO

Para compreender as particularidades do surgimento e estruturação da criminalidade organizada no Brasil, é imprescindível fazer uma observação crítica dos modelos de análise que se utilizam do conceito de máfia, a exemplo do que foi proposto para refletir sobre a criminalidade que acometeu a sociedade italiana e a subsequente expansão para os Estados Unidos. Alguns conceitos desenvolvidos a partir das experiências internacionais não servem para analisar o fenômeno da organização coletiva da criminalidade na atual sociedade brasileira. A rigor, o conhecimento a respeito das organizações criminosas no Brasil ainda está em construção, as informações quanto a sua gênese ainda são esparsas e, por vezes, contraditórias. Menos ainda se sabe como elas se organizam dentro da prisão.<sup>77</sup>

---

<sup>76</sup> “A origem no interior das prisões é sem dúvida uma característica fundamental do fenômeno no Brasil e que a distingue das formas mais comuns de emergência desses grupos no mundo. (...) No Brasil, a criminalidade organizada que se estabeleceu no interior dos presídios teve como elemento agregador a prática das ações criminosas, a condição dos indivíduos como encarcerados e ainda uma certa identificação social em razão da maioria dos presos pertencerem às camadas pobres da população. SALLA, Fernando. **Considerações Sociológicas sobre o crime organizado no Brasil**. In Revista Brasileira de Ciências Criminais, ano 16 n. 71: São Paulo: Editora Revista dos Tribunais, 2008. p. 373

<sup>77</sup> “A peculiaridade da criminalidade organizada no Brasil – e, de todo modo, seu enraizamento nas prisões – põe em evidência aspectos que o distinguem de outras modalidades existentes no mundo. em diversos países, os componentes étnicos ou raciais, ou procedências nacionais (por exemplo, italianos e irlandeses, nos estados unidos, no século passado) são, muitas vezes, decisivos para estabelecer laços identitários entre membros de uma associação delinqüente. Já no Brasil, a urdidura das relações de identidade de grupos criminosos está antes no próprio conteúdo da ação criminosa, na condição de criminoso encarcerado, e muito provavelmente na filiação social a que pertence a esmagadora maioria dos seus participantes, ou seja, aos estratos socioeconômicos onde são preferencialmente recrutados, nos territórios metropolitanos, aqueles que vivem nas fronteiras entre legalidade e ilegalismos.” ADORNO, Sérgio; SALLA, Fernando. Criminalidade organizada nas prisões e os ataques do PCC. **Estudos avançados**, v. 21, n. 61. p. 14, 2007. Disponível em:

É possível concluir, no entanto, que a pernicioso proximidade entre os presos que se amontoam nos cárceres, aliada à reduzida oferta de ocupação para os mesmos, e, ainda, a identificação quanto à filiação social a que pertence a maioria dos seus integrantes, ou seja, aos estratos socioeconômicos mais pobres onde são preferencialmente recrutados, criou o ambiente fértil para que ideias e projetos criminosos fossem cambiados e organizados, propiciando o surgimento no Brasil da primeira organização criminosa<sup>78</sup>. Ela foi logo seguida por outras, que adotaram estruturas semelhantes, incorporando métodos quase sempre violentos com objetivo de conquistar territórios, objetivando o lucro com atividades ilícitas, especialmente o tráfico de drogas.

O fator de destaque para o surgimento dos primeiros grupos de crime organizado foi a modernização da criminalidade. Observou-se maior eficiência na obtenção do resultado criminoso, seja pela associação a grupos constituídos, seja pela troca de experiências entre os detentos nas penitenciárias, e até mesmo pela necessidade de neutralizar os modernos e cada vez mais sofisticados mecanismos de prevenção e contenção dos crimes (como alarmes, cercas elétricas, dispositivos eletrônicos, etc.)<sup>79</sup>

A criminalidade se organizou a partir da década de 1970 no Rio de Janeiro, expandindo-se rapidamente na década seguinte. Em São Paulo, esse processo se iniciou a partir da década de 1990, pois antes disso existiam nas prisões líderes isolados, quadrilhas que se impunham à massa carcerária, limitados a um determinado estabelecimento ou a uma facção, mas que não possuíam uma identidade específica.

Os primeiros grupos de criminosos organizados, conhecidos nos anos 80 (Falange Vermelha, Serpentes Negras), tanto no Rio de Janeiro quanto em São Paulo, eram menos em

---

<http://www.scielo.br/pdf/ea/v21n61/a02v2161>. Acesso em: 08/08/17.

<sup>78</sup>“Em 1968, surge no Presídio da Ilha Grande, com junção de presos políticos e presos comuns, o embrião do Comando Vermelho cuja fundação é atribuída a Willian da Silva Lima, com a alcunha de “Professor”, visando a libertação de presos ali recolhidos com a prática de sequestros, assaltos a bancos e tráfico de entorpecentes. Em São Paulo, nos idos dos anos 80, surge o embrião do primeiro Comando da Capital, com o aparecimento da organização “Serpentes Negras”, com os mesmos objetivos do Comando Vermelho do Rio de Janeiro. Essas organizações consolidaram-se ao longo do tempo, sendo lançada em São Paulo, em 1993, o Estatuto do Primeiro Comando da Capital – PCC, que inicialmente parte de um princípio de proteção à população carcerária de eventuais abusos dentro do Sistema Prisional, para transformar-se depois numa organização criminosa predatória com a finalidade de lucro e utilizando a intimidação terrorista como metodologia em algumas de suas ações.” GOMES, José Carlos. **O Estado Democrático de Direito e o Terrorismo**. In: Repressão Penal e Crime Organizado. São Paulo: Quartier Latin, 2009. p. 332/333.

<sup>79</sup> “À medida que se sofisticavam os mecanismos de prevenção e contenção dos crimes (como alarmes, dispositivos eletrônicos, etc.), também se sofisticaram as ações criminosas, a começar pela maior capacidade de organização dos grupos.” SALLA, Fernando. **Considerações Sociológicas sobre o crime organizado no Brasil**. In Revista Brasileira de Ciências Criminais, ano 16 n. 71: São Paulo: Editora Revista dos Tribunais, 2008. p. 374.

virtude da convivência de presos comuns com presos políticos e mais em consequência da modernização da criminalidade. O assalto a banco e o tráfico de drogas, que antes eram atividades criminosas realizadas sem grande sofisticação ou planejamento, passaram a demandar ações organizadas entre seus autores para alcançar o êxito desejado.

Tal organização, além de lograr êxito no intento criminoso, começou a gerar dividendos econômicos e garantir prestígio aos protagonistas do submundo do crime, tendo cada vez mais ascendência entre os encarcerados. Assim foram lançadas as bases para a constituição de grupos que funcionam como organização no âmbito da criminalidade. Suas lideranças se fortaleceram exercendo a monopolização dos recursos disponíveis no sistema prisional, acumulando riqueza e explorando, mesmo de dentro da prisão, atividades ilegais como o tráfico de drogas, a extorsão de outros presos e de seus familiares, o controle de pontos de comércio, além de atividades diversas.

A população carcerária, embora pouco agressiva, acaba sendo cooptada pelas lideranças da criminalidade organizada, principalmente por causa do medo das permanentes ameaças de violência física contra o próprio preso, mesmo quando em condição de liberdade, e também contra seus familiares. A violência integra o código normativo dessas organizações criminosas.<sup>80</sup>

Para um amontoado de homens presos em cubículos, sem qualquer atividade laborativa, todo evento no contexto prisional é passível de distúrbios e disputas: a posse de objetos pessoais; a obtenção de favores sexuais que envolvem não apenas os presos mais jovens, como também suas esposas e filhas; a suspeita de delação; confronto entre quadrilhas; o fato de possuir influência com os detentores de poder dentro da massa carcerária ou com os agentes do Estado. Todos esses eventos são invariavelmente cercados de atos de extremada brutalidade, transmitidos oralmente como demonstração de coragem e virilidade, e que se traduzem em parcela de poder atribuída aos algozes.

Além do medo de ser vítima de violência, há também a necessidade de autoproteção, pois uma das características da organização criminosa é prover com recursos materiais seus integrantes, dentro ou fora do sistema prisional. Essa proteção em relação a grupos rivais e contra arbitrariedades policiais pode ser a diferença entre a vida e a morte daquele que se

---

<sup>80</sup> O medo está associado com a permanente ameaça de violência física. venha de onde e de quem vier, a violência constitui código normativo de comportamento”. ADORNO, Sérgio; SALLA, Fernando. Criminalidade organizada nas prisões e os ataques do PCC. *Estudos avançados*, v. 21, n. 61. p. 16, 2007. Disponível em: <http://www.scielo.br/pdf/ea/v21n61/a02v2161>. Acesso em: 08/08/17

encontra na condição de interno em uma penitenciária. O Estatuto do Primeiro Comando da Capital (PCC), por mais de uma vez, traz textualmente a obrigatoriedade do cuidado mútuo e a severidade da aplicação da pena de morte para aquele que descumpra essa regra.

O medo e a autoproteção são razões consistentes para a adesão a uma organização criminosa contra a qual o preso tem improváveis condições de resistir. Além desses fatores, ainda se pode falar da resignação, melhor seria da aceitação por um esdrúxulo tipo de temor reverencial, dessa forma primitiva e rude de dominação pessoal, aliada à construção de um sentimento de pertencimento a uma comunidade que lhe empresta força e identidade, que lhe são subtraídas no meio prisional.<sup>81</sup>

A reunião desses elementos resulta na organização do crime com características de empresa, já que tem nome próprio, estrutura formalmente estabelecida, por vezes até documentada, e cadeia hierárquica definida com divulgação dos ocupantes dos postos. Pertencer aos postos de comando implica em conquista de respeito, proporcional à parcela de poder derivado do exercício das funções na cadeia hierárquica da organização. Implica também em obediência às regras da organização, em que toda transgressão é exemplarmente punida mediante sanções prévia e internamente definidas por aquele que ocupa o posto hierárquico de poder e que tem a prerrogativa de definir qual a sanção a ser imposta.

Todas as atividades desenvolvidas por essa organização estão à margem da lei. O lucro advém de condutas consideradas criminosas, não fazendo parte do seu funcionamento, a princípio, relacionar-se com o Estado. Essa relação acontece quando o Estado, detentor do poder de punir os que transgridem a lei, alcança algum dos integrantes da organização criminosa e o submete ao processo devido.

Quando a organização criminosa se relaciona com o Estado, utiliza-se das mesmas práticas de outro tipo de organização criminosa que atua especificamente no âmbito dos aparelhos burocráticos, estabelecendo uma relação promíscua de troca de favores e benesses. Quanto a esse tipo de organização criminosa, as informações são ainda mais escassas e a compreensão desse objeto de estudo está por ser construída.

---

<sup>81</sup>“É certo que violência física e autoproteção constituem dimensões importantes como recurso de opressão das lideranças sobre a massa de presos destituídos de poder próprio ou capacidade de se contrapor à organização, todavia, esses elementos não operam per si. Combinam-se com um terceiro, a forte resignação dos presos em aceitar essa forma tosca e primitiva de dominação pessoal.” ADORNO, Sérgio; SALLA, Fernando. Criminalidade organizada nas prisões e os ataques do PCC. *Estudos avançados*, v. 21, n. 61, p. 17, 2007. Disponível em: <http://www.scielo.br/pdf/ea/v21n61/a02v2161>. Acesso em: 08/08/17.

## 2.2 PRINCIPAIS ORGANIZAÇÕES CRIMINOSAS QUE ATUAM NO SISTEMA PRISIONAL BRASILEIRO

Sem a pretensão de exaurir a relação das atuais organizações criminosas em atividade no sistema prisional brasileiro, será dado destaque as duas principais organizações criminosas, matrizes de todas as facções hoje em atividade no país, o Primeiro Comando da Capital, liderado por Marcola, e o Comando Vermelho, de Fernandinho Beira Mar, ambos presos em penitenciárias de segurança máxima.

### 2.2.1 Primeiro Comando da Capital (PCC)

A organização que atualmente tem maior número de seguidores em presídios de outros Estados do país nasceu em agosto de 1993, originalmente como um time de futebol que disputava campeonato interno no Anexo da Casa de Custódia e Tratamento Dr. Arnaldo Amado Ferreira de Taubaté (São Paulo), presídio também conhecido como “Piranhão”, inaugurado no início dos anos de 1980 e considerado o mais severo do sistema. Nele havia imposição de um regime mais rígido com limitações a visitas e o ao banho de sol, e tantas outras restrições impostas pela administração prisional, além de episódios cada vez mais comuns de espancamentos e ocorrência de maus tratos infringidos aos custodiados, funcionando como uma espécie de castigo para presos indisciplinados<sup>82 83</sup>.

Ao chegar ao final do campeonato, os integrantes do time resolveram acertar contas com dois integrantes do time adversário, resultando na morte de vários presos. Esse ato que

---

<sup>82</sup> “O PCC surgiu em 1993, no Anexo da Casa de Custódia de Taubaté, região do Vale do Paraíba, no estado de São Paulo. O presídio, também conhecido como “Piranhão”, foi inaugurado no início dos anos 1980 e era uma espécie de castigo para presos indisciplinados, na medida em que lá eles passavam o tempo imersos em um regime de restrições, com limitação a visitas e a banhos de sol.” DIAS, Camila Caldeira Nunes. **Ocupando as brechas do direito formal: O PCC como instância alternativa de resolução de conflitos.** In: Dilemas. Revista de Estudos de Conflito e Controle Social, vol. 2, n. 4. Rio de Janeiro, 2009. p. 86. Disponível em: <https://revistas.ufrj.br/index.php/dilemas/article/view/7165/5744>. Acesso em: 08/08/2017.

<sup>83</sup> “Além dessas restrições oficiais, o local era conhecido pela crueldade e pela arbitrariedade no trato com os presos, sistematicamente espancados e expostos a toda sorte de maus-tratos.” DIAS, Camila Caldeira Nunes. **Da pulverização ao monopólio da violência: expansão e consolidação do Primeiro Comando da Capital (PCC) no sistema carcerário paulista.** 2011. Tese de Doutorado. Universidade de São Paulo. Disponível em: <http://www.teses.usp.br/teses/disponiveis/8/8132/tde-13062012-164151/en.php>. Acesso em: 07/08/2017. p. 165

surgiu de uma rivalidade entre detentos tomou contornos de reivindicação em virtude das péssimas condições do sistema prisional, tendo como consequência o surgimento da facção criminosa Primeiro Comando da Capital.<sup>84</sup>

A meta inicial do PCC era dominar o sistema carcerário e realizar o tráfico de entorpecentes no interior dos presídios e cadeias públicas. Para tanto, praticavam extorsões contra os presos e seus familiares e ordenava execuções de outros internos que se opusessem às suas ordens. A partir do sucesso da empreitada, o PCC sai dos presídios e ordena a execuções de inúmeras outras ações criminosas fora do sistema prisional. A organização criminosa não encontrou resistência ao seu crescimento por parte do Estado, sendo que este se limitava a negar sua existência, criando ambiência favorável para proliferar-se, no primeiro momento, pelo sistema prisional do Estado de São Paulo, depois pelo sistema prisional de todo país.

A estrutura da facção criminosa era basicamente piramidal. No topo estavam os chamados “fundadores”, assim como aqueles que ao longo do tempo conquistaram prestígio dentro da entidade, quer por serem executores de assassinatos contra outros presos, quer por liderarem ações especialmente proveitosas para a organização. Esses integrantes, por vezes denominados “batizados”, são reconhecidos pelos líderes como membros ativos, e recebem cópia do “estatuto”<sup>85</sup>, ou seja, das regras com as quais concordam em obedecer.

<sup>84</sup>“Originariamente, o Primeiro Comando da Capital era o nome de um time de futebol que disputava o campeonato interno do presídio de Taubaté, na época estabelecimento apelidado pelos detentos como “piranhão” ou “masmorra”, por ser considerado o mais severo do sistema. Os detentos da Casa de Custódia tomavam banho de sol apenas uma hora por dia, ao lado de um pequeno grupo de encarcerados, no máximo dez. Todos permaneciam em celas individuais, sem direito a visita íntima.” PORTO, Roberto. **Crime Organizado e Sistema Prisional**. São Paulo: Editora Atlas, 2008. p. 73.

<sup>85</sup> No ano de 1997, o “estatuto” foi publicado no Diário Oficial do Estado de São Paulo, sendo reproduzido no dia 25 de maio do mesmo ano pelo jornal Folha de S. Paulo e que pode ser acessado no sítio abrigado sob o seguinte endereço: [https://pt.wikisource.org/wiki/Estatuto\\_do\\_PCC](https://pt.wikisource.org/wiki/Estatuto_do_PCC). Em sua íntegra:

“Estatuto do PCC:

1. Lealdade, respeito, e solidariedade acima de tudo ao Partido.
2. A Luta pela liberdade, justiça e paz.
3. A união da Luta contra as injustiças e a opressão dentro das prisões.
4. A contribuição daqueles que estão em Liberdade com os irmãos dentro da prisão através de advogados, dinheiro, ajuda aos familiares e ação de resgate.
5. O respeito e a solidariedade a todos os membros do Partido, para que não haja conflitos internos, porque aquele que causar conflito interno dentro do Partido, tentando dividir a irmandade será excluído e repudiado do Partido.
6. Jamais usar o Partido para resolver conflitos pessoais, contra pessoas de fora. Porque o ideal do Partido está acima de conflitos pessoais. Mas o Partido estará sempre Leal e solidário à todos os seus integrantes para que não venham a sofrerem nenhuma desigualdade ou injustiça em conflitos externos.
7. Aquele que estiver em Liberdade "bem estruturado" mas esquecer de contribuir com os irmãos que estão na cadeia, serão condenados à morte sem perdão
8. Os integrantes do Partido tem que dar bom exemplo à serem seguidos e por isso o Partido não admite que haja assalto, estupro e extorsão dentro do Sistema.

Ao longo dos anos, a ordem hierárquica desenvolveu uma ordenação escalonada mais complexa e a estrutura piramidal foi se alterando para uma organização por células que facilitava a administração à distância, bem como a rápida tomada de decisões por dirigentes locais - mais próximos das ocorrências - assim como a pronta mudança no comando, em caso de aniquilamento ou isolamento de algum dos líderes. Essa estratégia foi fundamental porque a organização se expandiu para outros presídios, dentro e fora do Estado de São Paulo, e serviu para evitar ceder espaço para facções rivais.

Foram criados os postos de “pilotos” e “torres”, presidiários que detêm o poder de mando dentro de determinado presídio ou pavilhão, estando os pilotos subordinados às torres que representam os “fundadores”. O pavilhão ou presídio sob o comando de determinado “piloto” passa a ser conhecido como “raio”, dentro do qual nova escala hierárquica de natureza piramidal se estabelece. A organização criminosa começa a aspirar contornos políticos, planeando utilizar a sigla PCC para significar Partido da Comunidade Carcerária.

---

9. O partido não admite mentiras, traição, inveja, cobiça, calúnia, egoísmo, interesse pessoal, mas sim: a verdade, a fidelidade, a hombridade, solidariedade e o interesse como ao Bem de todos, porque somos um por todos e todos por um.

10. Todo integrante tem que respeitar a ordem e a disciplina do Partido. Cada um vai receber de acordo com aquilo que fez por merecer. A opinião de Todos será ouvida e respeitada, mas a decisão final será dos fundadores do Partido.

11. O Primeiro Comando da Capital PCC fundado no ano de 1993, numa luta descomunal e incansável contra a opressão e as injustiças do Campo de concentração "anexo" à Casa de Custódia e Tratamento de Taubaté, tem como tema absoluto a "Liberdade, a Justiça e Paz".

12. O partido não admite rivalidades internas, disputa do poder na Liderança do Comando, pois cada integrante do Comando sabe a função que lhe compete de acordo com sua capacidade para exercê-la.

13. Temos que permanecer unidos e organizados para evitarmos que ocorra novamente um massacre semelhante ou pior ao ocorrido na Casa de Detenção em 02 de outubro de 1992, onde 111 presos foram covardemente assassinados, massacre este que jamais será esquecido na consciência da sociedade brasileira. Porque nós do Comando vamos mudar a prática carcerária, desumana, cheia de injustiças, opressão, torturas, massacres nas prisões.

14. A prioridade do Comando no montante é pressionar o Governador do Estado à desativar aquele Campo de Concentração "anexo" à Casa de Custódia e Tratamento de Taubaté, de onde surgiu a semente e as raízes do comando, no meio de tantas lutas inglórias e a tantos sofrimentos atrozes.

15. Partindo do Comando Central da Capital do KG do Estado, as diretrizes de ações organizadas simultâneas em todos os estabelecimentos penais do Estado, numa guerra sem trégua, sem fronteira, até a vitória final.

16. O importante de tudo é que ninguém nos deterá nesta luta porque a semente do Comando se espalhou por todos os Sistemas Penitenciários do estado e conseguimos nos estruturar também do lado de fora, com muitos sacrifícios e muitas perdas irreparáveis, mas nos consolidamos à nível estadual e à médio e longo prazo nos consolidaremos à nível nacional. Em coligação com o Comando Vermelho-CV e PCC iremos revolucionar o país dentro das prisões e nosso braço armado será o Terror "dos Poderosos" opressores e tiranos que usam o Anexo de Taubaté e o Bangú I do Rio de Janeiro como instrumento de vingança da sociedade na fabricação de monstros.

Conhecemos nossa força e a força de nossos inimigos Poderosos, mas estamos preparados, unidos e um povo unido jamais será vencido.

**LIBERDADE! JUSTIÇA! E PAZ!**

O Quartel General do PCC, Primeiro Comando da Capital, em coligação com Comando Vermelho CV UNIDOS VENCEREMOS.”

A proliferação do PCC se deveu, principalmente, à facilidade de comunicação dos custodiados com o mundo externo, a princípio por intermédio de “centrais telefônicas”<sup>86</sup> e telefones celulares irregularmente introduzidos nos presídios. Depois, com a evolução da telefonia e o advento dos *smartphones* que também funcionam como aparelhos de acesso à rede internacional de computadores (Internet), a comunicação passa a acontecer - extra e intramuros – por intermédio apenas de telefones celulares, por comunicação telefônica ou telemática.

Após rebeliões simultâneas em presídios, no início dos anos 2000, alguns líderes do PCC foram transferidos de São Paulo para o Rio de Janeiro, entre eles Marco Camacho, o Marcola, fato posteriormente considerado como equívoco pelas autoridades policiais<sup>87</sup>. No Rio, Marcola, que até então era delinquente de crimes menores, construiu relações com o Comando Vermelho, uma organização mais estruturada e com redes de atuação dentro e fora de presídios, aprimorando assim a organização do PCC.

De presos organizados por interesses difusos, começaram a existir como crime organizado, liderando ações como tráfico de drogas e de armas, contrabando, roubo a bancos e sequestros orquestrados de dentro dos presídios. O resultado dessa organização foi a denominada “Megarrebelião” que aconteceu em 18 de fevereiro de 2001, envolvendo 29 presídios e mais de 20 mil rebelados, fazendo com que a organização criminosa viesse a alcançar notoriedade nacional e internacional. O êxito dessa organização só foi possível devido à comunicação entre os presos por intermédio de telefones celulares, indiscriminadamente espalhados no interior dos presídios.

Em 2005, o sistema prisional aproxima Marcola do chileno Maurício Norambuena, experiente militante da Frente Patriótica Manuel Rodrigues (FPMR) e um dos responsáveis pelo sequestro de grande repercussão nacional do publicitário Washington Olivetto. Ambos estavam presos na Penitenciária em Presidente Bernardes (SP).

---

<sup>86</sup>“... a proliferação do primeiro comando da capital foi possível só graças a existência das chamadas “centrais telefônicas”, expressão hoje já popularizada, e que consiste sempre em linhas telefônicas instaladas em locais quaisquer, programadas com o escopo de efetuarem a transferência de chamadas ou o que se denomina “teleconferência” (três pessoas falando ao mesmo tempo)”. PORTO, Roberto. **Crime Organizado e Sistema Prisional**. São Paulo: Ed. Atlas, 2008. p. 75.

<sup>87</sup>“No início de 2000, após rebeliões simultâneas em presídios, alguns líderes do PCC, entre eles Marco Camacho, o Marcola, foram transferidos para o Rio de Janeiro. “Esse foi o nosso maior erro”, lamenta o delegado Godofredo Bittencourt, diretor do Departamento de Investigações Criminais de São Paulo (Deic), especializado no combate ao crime organizado.” RODRIGUES, Alan. **Como nasceram as facções**. Revista Istoé. 24052016. Disponível em: [http://istoe.com.br/22098\\_COMO+NASCERAM+AS+FACCÕES/](http://istoe.com.br/22098_COMO+NASCERAM+AS+FACCÕES/). Acesso em: 09/08/17.

Após esse convívio entre os dois internos, o PCC partiu para uma estratégia mais ousada e com um objetivo específico: atacar, desgastar e desmoralizar a estrutura de segurança do Estado. Comandante Ramiro, nome de guerra de Norambuena, deu a Marcola noções de como uma facção do porte do PCC poderia se transformar em uma organização de dominação política para afrontar o Estado. Marcola, leitor voraz, cujos autores prediletos são Voltaire e Nietzsche, conforme seu depoimento na CPI do Tráfico de Armas<sup>88</sup>, soube aproveitar o conhecimento obtido nas conversas no cárcere para operacionalizar a segunda investida do PCC contra o Estado.

Em maio de 2006, o PCC viria a repetir a façanha de organizar outra Megarrebelião, sendo esta maior que a ocorrida em 2001, agora envolvendo 74 presídios do Estado de São Paulo, com resultados mais devastadores. No período entre os dias 12 e 21 de maio daquele ano, foram mortas 564 pessoas e mais 110 feridas, resultado tanto da ação do PCC quanto da desastrosa resposta policial aos ataques promovidos pela facção criminosa<sup>89</sup>. A onda de ataques só findou após um encontro secreto entre a cúpula do governo paulista e Marcola<sup>90 91</sup>, dentro

<sup>88</sup> “**O SR. DEPUTADO RAUL JUNGSMANN** - Ai fora se fala muito que você é um leitor voraz de livros. Ai eu queria pedir que você me dissesse quais são os seus 5 principais autores, ou 3. Como você queira. Quem mais você gostou?

**O SR. MARCOS WILLIANS HERBAS CAMACHO** (Marcola) - Nietzsche...

**O SR. DEPUTADO RAUL JUNGSMANN** - Nietzsche?

**O SR. MARCOS WILLIANS HERBAS CAMACHO** (Marcola) - Nietzsche, Voltaire...

**O SR. DEPUTADO RAUL JUNGSMANN** - Hã, hã. Quem mais?

**O SR. MARCOS WILLIANS HERBAS CAMACHO** (Marcola) – Victor Hugo, *Les Miserables*. Sei lá. Eu adoro ler. Santo Agostinho, em determinados momentos — *Confissões*. É uma gama muito grande. Depende do momento e da situação, a gente tem um determinado prazer a mais de ler determinado autor.” Depoimento de **Marcos Willians Herbas Camacho** para a CPI – TRÁFICO DE ARMAS, Número: 0871R/06, Câmara dos Deputados, Brasília, em 08/06/2006. Disponível em: [http://www1.folha.uol.com.br/folha/cotidiano/20060708-marcos\\_camacho.pdf](http://www1.folha.uol.com.br/folha/cotidiano/20060708-marcos_camacho.pdf). Acesso em: 10/08/2017.

<sup>89</sup> Dos 564 mortos por arma de fogo no Estado de São Paulo entre 12 e 21 de maio de 2006, quando o Primeiro Comando da Capital atacou as forças de segurança, 59 eram agentes públicos. Os outros 505 eram civis. Os números fazem parte do relatório final da pesquisa Análise dos Impactos dos Ataques do PCC. O trabalho foi realizado pelo Laboratório de Análise da Violência da Universidade Estadual do Rio de Janeiro e coordenado pelo sociólogo Ignácio Cano. Disponível em: <http://ponte.cartacapital.com.br/crimes-de-maio-completam-9-anos-564-pessoas-morreram/> Acesso em: 20/01/2017.

<sup>90</sup> “No dia 16 de maio, o jornal *Folha de S. Paulo* noticiou que as autoridades teriam feito um “acordo” com o PCC, fato que foi veemente negado pelo governo paulista. A manchete da *Folha* gerou polêmica. Um “acordo” entre o PCC e o Estado foi negado pelo Comandante Geral da Polícia Militar e pelo Delegado Geral do DEIC, dentre outras autoridades. (...) Resta que ao menos o encontro foi confirmado pelo Estado como tendo acontecido entre Marcola e a advogada e ex delegada Iracema Vasciaveo, que dizia poder influenciar a facção. Tal encontro no pico da crise necessariamente levantou suspeita de que fora oferecido algo à facção para conseguir o fim tão imediato dos ataques.” **São Paulo sob achaque: Corrupção, Crime Organizado e Violência Institucional** em maio de 2006. Pesquisa realizada pela Justiça Global e Clínica Internacional de Direitos Humanos da Universidade de Direito de Harvard. Disponível em: <http://hrp.law.harvard.edu/wp-content/uploads/2011/05/full-with-cover.pdf>. Acesso em: 20/01/2017. p. 56

<sup>91</sup> “Hoje em dia, o próprio governador da época, Cláudio Lembo, admite que fez, que sugeriu acordo entre a liderança do Primeiro Comando da Capital e as forças de segurança. É fato notório que policiais, delegados, policiais militares, oficiais, foram até onde estava o Marcola, em Presidente Prudente, no CRD, e lá conversaram

do presídio onde ele está cumprindo uma pena de 234 anos de prisão. O Estado, portanto, havia se rendido.

O PCC cresceu e se estruturou física e financeiramente, com capacidade para arrecadação mensal de grandes somas em dinheiro, que serve para financiar outros crimes, seja na sua execução, seja na manutenção da corrupção dos agentes estatais que possibilitam que o crime se consume, inclusive dentro do sistema prisional.<sup>92</sup>

Mesmo após evidentes demonstrações de força e organização do PCC, o Estado de São Paulo não apresentou resposta igualmente forte e organizada. Ao contrário, segue com a falida receita de repressão e encarceramento e, ante a falta de punição adequada aos agentes estatais envolvidos com a organização criminosa, assiste ao incremento da violência e da corrupção policial. Apenas entre os meses de janeiro e novembro de 2014 registou-se a morte de mais de 800 pessoas, nem todas envolvidas com o tráfico de drogas.<sup>93</sup>

A transferência de líderes do PCC para diversos presídios brasileiros visando sua desarticulação, sem a adoção das necessárias medidas de isolamento dos seus membros, mostrou-se medida desastrosa. O efeito produzido foi exatamente o oposto. A facção criminosa cresceu e se alastrou por todos os estados da federação com o fito de alcançar a liderança no tráfico de drogas, impondo a sua estrutura organizacional e usando da intimidação e violência, já que nenhum dos demais estados, à exceção do Rio de Janeiro com o Comando Vermelho e outras facções, tinha um grupo organizado que pudesse minimamente

---

com ele. E logo após essa conversa, no dia seguinte, os ataques começaram a cessar e em 48 horas não havia mais nada”(...) CRUZ, Elaine Patrícia. **Crimes de maio causaram 564 mortes em 2006; entenda o caso.** Disponível em: <http://agenciabrasil.ebc.com.br/direitos-humanos/noticia/2016-05/crimes-de-maio-causaram-564-mortes-em-2006-entenda-o-caso>. Acesso em: 20/01/2017.

<sup>92</sup> “Criaram uma estrutura financeira capaz de arrecadar mensalmente cerca de R\$ 1 milhão, dinheiro usado para bancar outros crimes, corromper agentes penitenciários, manter as famílias dos presos e até custear a formação de advogados de confiança. O mais recente investimento se dá na qualificação de sua mão-de-obra. O PCC coloca alguns de seus membros em cursos promovidos por empresas de segurança privada para que aprendam a manusear armas mais modernas e até a fazer direção defensiva. Para consolidar sua liderança sob os 100 mil comandados no sistema penitenciário e dez mil “soldados” que agem fora das muralhas, Marcola usa o tacão do terror. Os números do governo são alarmantes. São quase 500 mortos por ano nos presídios paulistas. Só em 2004 cresceu em 200% o número de suicídios dentro dos presídios. “Muitos dos presos que têm dívidas com a facção ou não querem mais cumprir as ordens são ‘obrigados’ a se suicidar”, diz o padre Valdir José Silveira, coordenador estadual da Pastoral Carcerária, entidade não governamental que trabalha em defesa dos presidiários. Após eliminar líderes rivais (alguns decapitados), Marcola adotou posturas que aumentaram sua popularidade dentro dos presídios. Aboliu o uso do *crack* nas prisões, droga que segundo ele mesmo afirma acaba matando seu exército. Também decretou o fim dos estupros que vitimavam os presos mais fracos, e assim ganhou respeito” RODRIGUES, Alan. **Como nasceram as facções.** Revista Istoé, 24/05/2016. Disponível em: [http://istoe.com.br/22098\\_COMO+NASCERAM+AS+FACCOES/](http://istoe.com.br/22098_COMO+NASCERAM+AS+FACCOES/). Acesso em: 09/08/17.

<sup>93</sup> Disponível em: <http://ponte.cartacapital.com.br/crimes-de-maio-completam-9-anos-564-pessoas-morreram/>, Acesso em: 20/01/2017.

se comparar com o PCC. Além disso, propiciou o surgimento de outras facções, como a Família do Norte (FDN)<sup>94</sup>, protagonista, juntamente com o PCC, de conflitos bárbaros e sangrentos na região norte do país, locais onde as rotas de tráfico de drogas estavam em disputa.

No segundo dia de 2017, o Complexo Penitenciário Anísio Jobim, em Manaus, foi palco de um sangrento duelo entre o PCC e a FDN resultando em mais de oitenta mortes de custodiados ligados ambas as facções.<sup>95</sup> Eclodiu um novo confronto no dia 14 de janeiro do mesmo ano, agora na Penitenciária de Alcaçuz, região metropolitana de Natal, Rio Grande do Norte, local onde o PCC disputa o poder com o Sindicato do Crime (SDC), resultando em mais de 20 mortes<sup>96 97</sup>. No dia 18 de janeiro, também no Rio Grande do Norte, na cidade de Caicó, Penitenciária Estadual do Seridó, ocorreu outra rebelião resultando mortes e envolvendo o PCC<sup>98</sup>.

Em todos os confrontos, a marca mais evidente desta guerra são as mortes violentas, por decapitações, esquartejamentos e canibalismo, com o nítido propósito de intimidar a facção rival e conquistar o território sob disputa.<sup>99</sup> O ano de 2017, portanto, já contabiliza

<sup>94</sup>“Dois fatores permitiram o crescimento para fora do Estado de São Paulo: o primeiro o fato de lideranças terem sido removidas para outros estados (detalhe, quem os recebia não sabia quem eram) e segundo que nenhum dos demais estados, à exceção do Rio de Janeiro com o Comando Vermelho e outras facções, tinha um grupo organizado que pudesse minimamente se comparar com o PCC. É possível comprovar a existência e atuação da facção em diversos estados onde seus membros estão envolvidos em tráfico de drogas, homicídios, fugas, etc. Este transbordo influenciou a disseminação de facções como a agora afamada Família do Norte (FDN), e outras mais que se espelharam no sucesso da facção paulista.” CHRISTINO, Márcio Sérgio. **Rebeliões não estão relacionadas às más condições das cadeias ou superlotação**. Consultor Jurídico, ISSN 1809-2829. Disponível em: <<http://www.conjur.com.br/2017-jan-16/marcio-christino-rebelioes-nao-relacionadas-superlotacao>. Acesso em: 08/08/2017>.

<sup>95</sup>“Fontes atribuiu o problema a uma guerra entre facções rivais pelo controle de tráfico de entorpecentes em Manaus. A facção conhecida como FDN (Família do Norte) teria atacado membros do PCC (Primeiro Comando da Capital.” Disponível em: <<https://noticias.uol.com.br/cotidiano/ultimas-noticias/2017/01/02/rebeliao-no-amazonas-termina-com-aomenos-50-mortos-diz-governo.htm>>

<sup>96</sup>“Pelo menos 26 presos morreram durante a rebelião que aconteceu neste sábado (14) na Penitenciária de Alcaçuz, na região metropolitana de Natal (RN). A informação é da Secretaria da Segurança Pública do Rio Grande do Norte.” Disponível em: <<http://www1.folha.uol.com.br/cotidiano/2017/01/1850078-rebeliao-em-presidio-deixa-ao-menos-27-mortos-diz-governo-do-rn.shtml>>.

<sup>97</sup>“O levante em Alcaçuz começou na tarde de sábado (14), logo depois do horário de visita. Segundo agentes penitenciários, presos do PCC derrubaram o muro que os separava da ala ocupada pelo SDC e partiram para a matança.”<<http://epoca.globo.com/brasil/noticia/2017/01/trapalhada-do-governo-culminou-em-sete-dias-de-rebeliao-no-rn.html>>. Acesso em: 08/08/2017.

<sup>98</sup>“Ao menos um preso foi morto e outros ficaram feridos na rebelião iniciada na noite desta quarta-feira (18) na Penitenciária Estadual do Seridó, localizada em Caicó (região oeste do Rio Grande do Norte).” Disponível em: <<https://noticias.uol.com.br/cotidiano/ultimas-noticias/2017/01/18/nova-rebeliao-no-rn-deixa-ao-menos-um-morto-e-varios-feridos.html>>. Acesso em: 08/08/2017.

<sup>99</sup>“A barbárie que vemos está bem próxima das ações dos cartéis mexicanos em sua crueldade, lá penduram cadáveres em viadutos ou os dissolvem em ácido após uma tortura selvagem. Está é a características dos cartéis, a morte cruel pelo domínio...”. CHRISTINO, Márcio Sérgio. **Rebeliões não estão relacionadas às más condições das cadeias ou superlotação**. Consultor Jurídico, ISSN 1809-2829. Disponível em:

mais de 130 presos mortos, resultado da luta entre facções criminosas que disputam a primazia do controle do tráfico de drogas. Em todas as disputas, o PCC se faz presente.

A influência do PCC se estende além da regulação do tráfico de drogas. Nos seus territórios de influência, ele controla toda a criminalidade, pois não tem interesse em atrair a polícia para essas áreas, mantendo sob controle o tipo de crime que ali é praticado, evitando ao máximo a prática de homicídios que poderiam atrair com maior intensidade a ação policial.<sup>100</sup> Em áreas de maior controle do espaço territorial, especialmente em presídios, a facção exerce também poderes legislativo, executivo e judiciário, não se limitando aos seus integrantes, mas a todos que habitem aquele território, que devem se reportar aos líderes para pedir favores, fazer justiça e resolver conflitos.<sup>101</sup>

### 2.2.2 Comando Vermelho

A origem do Comando Vermelho (CV) está associada à facção Falange Vermelha que se originou na década de 1970 no Rio de Janeiro. Objetivava o tráfico de drogas e a prestação de assistência aos integrantes enquanto estivessem presos. O cumprimento da pena ocorria no Instituto Penal Cândido Mendes, localizado em Ilha Grande, litoral sul do Rio de Janeiro, que a princípio fora destinado a presos políticos, mas que desde a década de 60 passou a abrigar presos comuns.

---

<http://www.conjur.com.br/2017-jan-16/marcio-christino-rebelioes-nao-relacionadas-superlotacao>. Acesso em: 08/08/2017.

<sup>100</sup> “Mas um dos reflexos do domínio de uma organização criminosa sobre um determinado lugar é o seu predomínio sobre tudo o que acontece ali. O crime organizado não aceita concorrência, não aceita que os seus negócios sejam perturbados. Então eles dominam o espaço e, lá, não permitem que nada ocorra para não ferir os seus próprios interesses comerciais. É evidente que eles não vão permitir que sejam praticados roubos ali, que sejam cometidos homicídios. Outro ponto é que as facções criminosas têm um aspecto semelhante a organizações militares. Não é que eles estejam atuando em brigadas, é como se fosse uma ocupação militar, como se tivessem invadido um espaço, e, a partir daquele momento, eles controlam o ambiente em todos os sentidos — não permitem que se faça a, b ou c lá. Essa ocupação do PCC, de certa forma, afeta os índices de criminalidade.” Entrevista concedida pelo Procurador de Justiça do Estado de São Paulo, Márcio Sérgio Christino. Disponível em: <http://www.conjur.com.br/2017-fev-26/entrevista-marcio-christino-procurador-justica-mp-sp>. Acesso em: 08/08/2017.

<sup>101</sup> “Em algumas áreas, especialmente no interior dos presídios, a facção exerce poderes legislativo, judiciário e executivo, à qual todos – sejam ou não membros da facção – devem se reportar para pedir justiça e favores, resolver conflitos etc.”. DIAS, Camila Caldeira Nunes. **Ocupando as brechas do direito formal: O PCC como instância alternativa de resolução de conflitos**, in Dilemas Revista de Estudos de Conflito e Controle Social, vol. 2, n. 4: Rio de Janeiro, 2009, pág. 86. Disponível em: <http://revistas.ufjf.br/index.php/dilemas/article/view/7165/5744>. Acesso em: 08/08/2017.

A tentativa do governo em desqualificar a organização da esquerda, em plena vigência do golpe militar, tratando seus integrantes como criminosos comuns, visava tanto sua desarticulação quanto à diminuição da pressão internacional em face das denúncias de prática de torturas, e em favor da anistia aos presos políticos. O resultado foi o efeito reverso. O preso político levou para o presídio de Ilha Grande a ideologia que findou por contaminar todo sistema.<sup>102</sup>

Algumas organizações de esquerda alinhavam os políticos presos em Ilha Grande, entre elas estavam o Movimento Revolucionário 8 de Outubro (MR-8), a Ação Libertadora Nacional (ALN), de Carlos Marighella, a Vanguarda Popular Revolucionária (VPR), do ex-capitão do Exército Brasileiro Carlos Lamarca e a Vanguarda Armada Revolucionária Palmares (VAR-Palmares).

Uma reunião de presos com o objetivo de resistir às enormes dificuldades encontradas no presídio onde ocorriam frequentes roubos, assassinatos e estupros cometidos pelas falanges que detinham o controle da penitenciária, deu origem ao Comando Vermelho. Seus membros originários buscavam a sobrevivência naquele que era considerado à época o pior presídio do país. Eram eles: William da Silva Lima, vulgo Professor, condenado por formação de quadrilha e assaltos a banco; Carlos Alberto Mesquita, conhecido também como Professor e condenado de igual modo por assaltos a bancos; Paulo Nunes Filho, chamado de Flávio ou Careca e condenado por assalto a banco; Paulo César Chaves, vulgo PC Branco, condenado por assalto a mão armada e homicídio; José Jorge Saldanha, o Zé do Bigode, condenado por assalto a banco; Eucanan de Azevedo, vulgo Canã, condenado por roubo; Lassy de Castro, o Lacy, condenado por roubo seguido de morte (latrocínio) e Apolinário de Souza, vulgo Nanai, condenado por assalto a banco. Todos incursos nas penas do artigo 27, da Lei de Segurança Nacional (com exceção de Eucanan de Azevedo).

---

<sup>102</sup> “Os presos políticos levaram para lá a sua organização, logo fortalecida com a chegada de outros condenados pela Lei de Segurança Nacional. Entre eles estavam agora deputados, funcionários públicos, universitários. O mesmo processo de união para enfrentar o ambiente se repete. Com mais força. O preso ideológico não se contém com a prisão. Ao contrário, ele cresce. Na Ilha Grande, ocorreu um fenômeno ideológico por contaminação. Acabou gerando o Comando Vermelho, que perdeu a formação política original, nobre como movimento de libertação nacional, mas que absorveu a estrutura para se organizar como crime comum. Os bandidos adotaram o princípio da organização para verticalizar o poder dentro do grupo.” AMORIM, Carlos. **Comando Vermelho: a estória secreta do crime organizado**. 4ª ed. Rio de Janeiro: Record, 1994. p. 44. Disponível em: [https://s3.amazonaws.com/academia.edu.documents/38992612/Carlos\\_Amorim\\_-\\_Comando\\_Vermelho.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1502208123&Signature=VcYiaeTEVf2UQt33WJQIeLmUGac%3D&response-content-disposition=inline%3B%20filename%3DCarlos\\_Amorim\\_-\\_Comando\\_Vermelho.pdf](https://s3.amazonaws.com/academia.edu.documents/38992612/Carlos_Amorim_-_Comando_Vermelho.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1502208123&Signature=VcYiaeTEVf2UQt33WJQIeLmUGac%3D&response-content-disposition=inline%3B%20filename%3DCarlos_Amorim_-_Comando_Vermelho.pdf). Acesso em: 08/08/2017.

O planejamento das ações do neonato Comando Vermelho, traz lições da guerrilha urbana aprendidas com os grupos revolucionários, tais como o uso de clínicas médicas particulares em regiões periféricas para o socorro de emergência dos feridos em confronto, ao invés de levá-los aos hospitais públicos para evitar possível captura por autoridade policial; o uso de carros roubados recentemente na fuga de assaltos, e que por isso ainda não constavam nos registros policiais e também a utilização não do automóvel mais potente, mas sim do mais discreto que conseguia passar despercebido nas ruas das cidades.

Os ideais dessa organização que outrora eram a sobrevivência dos membros, a extinção dos abusos e o aumento da união entre eles, foram se modificando a partir da fuga de algumas pessoas da Ilha Grande para assaltar bancos, joelharias e, assim, angariar fundos visando financiar a fuga do maior número possível de associados.

A princípio se estabelece a comunicação com o meio exterior através de recados levados e trazidos por advogados e familiares dos presos, que recebeu o nome de “correio”, sendo atualmente substituído pelo telefone celular, aos poucos introduzidos no interior dos presídios, tornando a comunicação mais fácil, rápida e eficiente. O início da simbiose entre o Comando Vermelho e o tráfico de entorpecentes aconteceu com a solicitação de auxílio financeiro para o fundo criado pela organização em troca de bom tratamento ofertado aos traficantes que porventura ingressassem no sistema penitenciário.

A partir de então, os assaltos passaram a ter como finalidade financiar a compra de entorpecentes, agora objetivo final da organização criminosa, bem como o contrabando de armas. Todos os outros delitos praticados pelos integrantes da organização eram apenas desdobramentos dessas ações. Desse modo, os assaltos, sequestros e homicídios só eram praticados se voltados para os fins comerciais da organização.

Com o crescimento e fortalecimento do Comando Vermelho, as autoridades de segurança pública do Estado do Rio de Janeiro resolveram transferir os vários membros dessa organização para diversos presídios com o objetivo de enfraquecê-la, medida que produziu efeito contrário ao esperado. Tal aparente desmembramento, serviu para fortalecer e ampliar a influência do Comando Vermelho nas penitenciárias, com a formação espontânea de vários tentáculos.<sup>103</sup>

---

<sup>103</sup>DAMASCENO, Leandro et al. **A Lei nº 9.034/95 e as Organizações Criminosas Brasileiras**. **THEMIS: Revista da Esmec**. v. 11. 2016. p. 267-280. Disponível em: <http://revistathemis.tjce.jus.br/index.php/THEMIS/article/view/70/69>. Acesso em: 08/08/17.

Em meados de 1984, a organização firmou acordo com os cartéis colombianos produtores de cocaína que forneciam a droga, enquanto o Comando Vermelho operava a distribuição e venda no Rio de Janeiro<sup>104</sup>. Naquela época, o tráfico no Estado era feito por pequenas quadrilhas independentes, que foram persuadidas a associarem-se ao esquema. Aquelas que se opuseram foram simplesmente destruídas.

O auge do poderio dos cartéis colombianos, tanto em termos de organização quanto de movimentação financeira, inspirou a organização nacional a adotar seus métodos e estratégias para crescimento, especialmente aplicando parte do lucro da venda das drogas em melhorias para a comunidade, como a construção de redes de esgoto, segurança, pavimentação de vias, conquistando assim o apoio popular<sup>105</sup>. Na década de 1980, segundo estimativa feita pela Polícia Civil de São Paulo, a maior parte da droga comercializada pelo Comando Vermelho era proveniente dos cartéis.

O atual líder do Comando Vermelho, Fernando Luiz da Costa, ou simplesmente Fernandinho Beira-Mar, chegou ao ápice da hierarquia da organização em 11 de setembro de 2002, quando comandou uma rebelião no Presídio de Bangu Um. Por ordem sua, foram mortos o antigo líder do Comando Vermelho, Ernaldo Pinto de Medeiros, o “Uê”, e mais três pessoas. É um traficante de drogas altamente perigoso e, atualmente, o Poder Judiciário dos Estados Unidos demonstra grande interesse em julgá-lo sob a égide das leis americanas, atualmente preso e condenado a 430 anos de prisão.

### **2.2.3 Primeiro Comando da Capital (PCC) *versus* Comando Vermelho (CV)**

A confluência de propósitos e o inimigo comum a ser combatido propiciaram um acordo comercial entre as duas maiores organizações criminosas do país, facilitando a compra

---

<sup>104</sup>“O primeiro acerto para importação de cocaína é firmado em Medellín, na Colômbia. Pablo Escobar, o maior traficante do mundo, é quem vai fornecer para o crime organizado no Rio de Janeiro. Outros estarão participando das grandes remessas, ligadas também ao Cartel de Cali.” AMORIM. Carlos. **CV-PCC: A irmandade do crime**. Rio de Janeiro: Record, 2004. p. 235

<sup>105</sup> “Uma população que tem medo, deve muitos favores e protege as atividades do crime organizado com um silêncio impenetrável. O Comando Vermelho foi também o incentivador de importantes iniciativas comunitárias nos “territórios conquistados”. Financiou e construiu creches.(...) O “trabalho social” do Comando Vermelho nas favelas tem - além de um interesse imediato, de segurança do tráfico - uma característica diferenciá-lo dos antigos donos dos morros.” AMORIM. Carlos. **CV-PCC: A irmandade do crime**. Rio de Janeiro: Record, 2004. p. 217

e o ingresso da droga no Brasil<sup>106</sup>. O comércio de entorpecentes agregou o tráfico de armas, e possibilitou que ambas as organizações sejam atualmente detentoras de poderio bélico que inclui armamentos capazes de abater helicópteros e pequenos aviões<sup>107</sup>

O acordo comercial entre as duas organizações, que já durava quase duas décadas, traduzido em redução do número de homicídios em vários Estados da Federação, sofreu sério abalo no início de 2017, com a rebelião no Presídio Anísio Jobim, em Manaus, e pôs todo o sistema de segurança pública nacional em estado de alerta. O rompimento do acordo comercial entre PCC e CV havia sido identificado pelos grupos de inteligência do sistema de segurança estatal desde meados do ano de 2016. Quando foram identificadas as primeiras ordens de integrantes de uma facção contra os integrantes da outra, nas intercetações telefônicas, imaginava-se que havia uma guerra a ser anunciada, como sinalizava a imprensa especializada no tema<sup>108 109 110 111</sup>.

Para especialistas em sistema prisional como os integrantes do Ministério Público que atuam no combate ao crime organizado, assim como os policiais que atuam na área, dois

<sup>106</sup>“As condições em que se realizam essas transações, nas fronteiras ou nos países produtores, é algo de que se dispõe de pouquíssima informação. Sabe-se apenas que as transações ocorrem com a formação de consórcios, entre os principais grupos que distribuem essas drogas no Brasil, sobretudo PCC e Comando Vermelho (CV)” DIAS, Camila Caldeira Nunes. **Da pulverização ao monopólio da violência: expansão e consolidação do Primeiro Comando da Capital (PCC) no sistema carcerário paulista**. 2011. Tese de Doutorado. Universidade de São Paulo, disponível em: <<http://www.teses.usp.br/teses/disponiveis/8/8132/tde-13062012-164151/en.php>> p. 239.

<sup>107</sup> “O PCC é comandado por Marcos Willians Herbas Camacho, o Marcola, condenado a 234 anos de prisão; o CV é liderado por Luiz Fernando da Costa, o Fernandinho Beira-Mar, com condenação de 430 anos. Ambos se abastecem do narcotráfico pesado, ambos são donos de poderio bélico que inclui armamentos capazes de abater helicópteros e pequenos aviões.” PRADO, Antônio Carlos. **Marcola versus Fernandinho Beira Mar**. Revista IstoÉ, 21/10/16. Disponível em: <http://istoe.com.br/marcola-versus-fernandinho-beira-mar>. Acesso em 09/08/17.

<sup>108</sup>“O possível fim da aliança de quase duas décadas entre as duas maiores facções criminosas do país, o Comando Vermelho (CV) e o Primeiro Comando da Capital (PCC), mergulha os presídios brasileiros em tensão e há o temor de que tudo termine em sangue. As organizações, originárias respectivamente do Rio de Janeiro e de São Paulo, sempre conviveram de forma relativamente harmoniosa no sistema prisional e nas ruas de quase todos os Estados. Chegaram a ser parceiras em várias empreitadas, atuando em uma espécie de *consórcio criminoso* na compra de armas e drogas no Paraguai, Colômbia e Bolívia.” ALESSI, Gil. **Rebeliões sinalizam fim de pacto entre PCC e CV e espalham tensão em presídios**, Jornal El País, 20/10/2016. Disponível em: [https://brasil.elpais.com/brasil/2016/10/17/politica/1476734977\\_178370.html](https://brasil.elpais.com/brasil/2016/10/17/politica/1476734977_178370.html). Acesso em: 11/08/2017.

<sup>109</sup> “Temo confrontos dentro e fora dos presídios, e com dimensões nacionais”, diz o ministro da Justiça, Alexandre de Moraes. “A harmonia entre PCC e CV acabou”, sentencia um dos mais eficientes penitenciários do Brasil, Lourival Gomes, quatro décadas de experiência nessa área e secretário da Administração Penitenciária de São Paulo.” PRADO, Antônio Carlos. **Marcola versus Fernandinho Beira Mar**. Revista IstoÉ, 21/10/16. Disponível em: <http://istoe.com.br/marcola-versus-fernandinho-beira-mar>. Acesso em: 09/08/17.

<sup>110</sup> ROCHA, Lyvia. **PCC acusa Comando Vermelho por fim de pacto de paz**, Tribuna do Ceará, 19/10/2016. Disponível em: <http://tribunadoceara.uol.com.br/noticias/segurancapublica/pcc-acusa-comando-vermelho-por-fim-de-pacto-de-paz/>. Acesso em: 11/08/2017.

<sup>111</sup> **Ruptura entre PCC e Comando Vermelho pode gerar 'carnificina', diz pesquisadora**. Entrevista concedida por Camila Nunes Dias a BBC, 18/10/2016. Disponível em: <http://ultimosegundo.ig.com.br/brasil/2016-10-18/pcc-comando-vermelho-ruptura.html>. Acesso em: 10/08/2017

fatores precipitaram o fim do acordo entre as duas facções criminosas. O primeiro deles foi a morte do traficante Jorge Rafaat Toumani, durante uma emboscada, em uma ação onerosa e meticulosamente planejada<sup>112</sup> provavelmente pelo PCC, em junho de 2016, na cidade de Pedro Juan Caballero, fronteira com o Mato Grosso do Sul. Ele era considerado pelos Estados Unidos como um dos barões do tráfico internacional de drogas e armas na fronteira, e fornecedor tanto do PCC quanto do CV. Sua retirada da rota do tráfico iniciou o desentendimento entre as duas facções, cuja razão específica ainda é desconhecida. O segundo fator teria sido um rompimento bilateral das facções após apoio do CV a grupos rivais do PCC em vários estados<sup>113</sup>.

Confirmando essas suspeitas, em meados do mês de julho daquele ano, ocorreu em Manaus o episódio que viria a ser conhecido como “o fim de semana sangrento”, onde 38 pessoas, supostamente ligadas ao PCC, foram mortas sob ordens da Família do Norte (FDN), aliada comercial do CV.<sup>114</sup>

<sup>112</sup>“O vídeo de uma câmera de segurança marcava 18h44 quando um Toyota Hilux prata parou num cruzamento de Pedro Juan Caballero, em 15 de junho do ano passado. O veículo esperou ser alcançado, propositadamente, por um Hummer preto escoltado por três carros. Rafaat estava dentro do Hummer. De repente, a porta traseira do Hilux se abriu e disparou uma rajada de balas. A rua se iluminou com os tiros. A metralhadora .50 foi usada para perfurar a grossa blindagem do Hummer, em um procedimento digno de ataques perpetrados em zonas de conflito armado como Iraque e Afeganistão. Os capangas de Rafaat, armados com pistolas automáticas e fuzis, não tiveram nenhuma chance diante dos mais de 100 tiros disparados contra ele. A batalha durou dez minutos. Aos 56 anos, Rafaat morreu com 16 tiros, quase todos na cabeça. Entre arsenal, logística e pistoleiros, a operação custou, segundo estimativas do serviço de inteligência da Senad, US\$ 1 milhão. É um investimento inédito para o PCC no combate a inimigos – e uma demonstração clara de quanto Rafaat atravancava seus negócios e quão promissores eles eram.” (...)

“A operação milionária, vantajosa e barulhenta para matar Rafaat abriu um grande mercado, mas gerou uma nova guerra para o PCC. A relação com o Comando Vermelho ficou estremecida. As facções costumavam ser parceiras nos negócios. Não só compravam do mesmo fornecedor, como também despachavam a droga da fronteira para seus respectivos estados num mesmo carregamento. O caminhão parava em São Paulo, descarregava parte da mercadoria e depois seguia para o Rio de Janeiro. Depois da morte, algum acerto não cumprido, ainda desconhecido, contribuiu para que as organizações rompessem. “Hoje cada uma tem sua lavoura e ambas estão em terras demarcadas: Capitán Bado é PCC, Paranhos é CV, Pedro Juan é PCC, Aral Moreira é CV”, afirma um agente da Polícia Rodoviária Federal. A cisão não ficou restrita ao Paraguai – o sangue e a barbárie explodiram no Brasil. Desde o final do ano passado, “salves” que correram presídios provocaram 11 rebeliões, resultando em pelo menos 150 mortes, com episódios repulsivos como homens sendo degolados como animais por pertencerem à organização criminosa rival.” RIBEIRO, Aline; CORREA, Hudson. **O violento plano de expansão no Paraguai da maior facção brasileira**. Revista Época, 26/06/2017. Atualizado em 24/07/2017. Disponível em: <http://epoca.globo.com/brasil/noticia/2017/06/o-violento-plano-de-expansao-no-paraguai-da-maior-facciao-brasileira.html>. Acesso: 11/08/2017.

<sup>113</sup>“O apoio do Comando Vermelho a facções rivais do PCC nos estados, como a FDN no Norte do país, o Primeiro Grupo Catarinense (PGC), em Santa Catarina, e o Bonde dos 40, no Maranhão, acirrou a disputa. O CV proibiu o batismo de novos integrantes do PCC em presídios e, em seguida, nos estados em que tinha mais poder, o PCC declarou guerra à facção carioca e demais rivais.” STOCHERO, Tahiane. **Entenda: o que a disputa nacional entre facções tem a ver com a barbárie no presídio do Amazonas**, 03/01/2017. Disponível em: <http://g1.globo.com/am/amazonas/noticia/entenda-o-que-a-disputa-nacional-entre-faccoes-tem-a-ver-com-a-barbarie-no-presidio-do-amazonas.ghtml>. Acesso em: 10/08/17.

<sup>114</sup>“Três lideranças da facção criminosa paulista Primeiro Comando da Capital (PCC) foram brutalmente degoladas entre junho e julho de 2015 dentro de presídios de Manaus. Era apenas o começo do episódio que

Após tal ocorrência, o clima de tensão se agravou no Presídio Antônio Jobim, em Manaus, pois se temia um revide do PCC às mortes ordenadas pela FDN. Entretanto, a FDN preferiu surpreender o PCC e iniciou, no primeiro dia de 2017, uma carnificina brutal, assombrosamente sangrenta e cruel contra integrantes do PCC, que se estenderia até o estado do Rio Grande do Norte, onde 15 dias depois ocorreu outra intensa batalha, resultando em ainda mais mortes.

A barbárie imposta e os ataques sanguinolentos têm um objetivo que vai além de retaliação<sup>115</sup>. No ambiente de selvageria em que atuam, não basta matar para demonstrar força. É fundamental ser violento, viril, destemido. Essas qualidades agregam valor a quem pratica e infunde o necessário temor ao grupo, que sucumbe às exigências dos seus tiranos<sup>116</sup>. Vigie a lei do mais forte.

Naquele momento, o motivo da disputa está centrado no controle comercial da entrada de drogas no país e, sobretudo, a definição de quem controlará a rota do tráfico após a morte de Jorge Rafaat, sendo o PCC a organização que está disposta a exercer o protagonismo das ações. Suas técnicas são agressivas, e a chacina ocorrida em Manaus e Rio Grande do Norte não restarão impunes. Ainda acontecerão outros episódios graves até uma nova pacificação, um novo acordo econômico entre as facções.<sup>117</sup>

---

ficou conhecido na capital amazonense como o *Fim de Semana Sangrento*. Entre a tarde de sexta-feira, dia 17 de julho, e a manhã de segunda-feira dia 20, foram 38 homicídios nas ruas da capital amazonense, boa parte de pessoas supostamente ligadas ao PCC e a outros grupos criminosos.” ALESSI, Gil. **Família do Norte, a facção que fez a guerra entre o PCC e o Comando Vermelho**. Jornal El País, 01/11/2016. Disponível em: [https://brasil.elpais.com/brasil/2016/10/25/politica/1477406310\\_192891.html](https://brasil.elpais.com/brasil/2016/10/25/politica/1477406310_192891.html). Acesso em: 11/08/2017.

<sup>115</sup>“A professora Isabel Figueiredo, que integrou a Secretaria de Direitos Humanos do Ministério da Justiça, ressalta também a “rearrumação de território” que está ocorrendo com a briga entre as facções após a morte do barão da droga no Paraguai. “A morte dele abriu espaço para a disputa. Em última instância, é uma briga por dinheiro e mercado. O PCC entrou no RJ e se projeta para o resto do país. Isso reflete no sistema penitenciário como um todo. É uma bola já cantada, já havia vários relatórios de que a bomba estava prestes a estourar”, diz ela (...)

“Ao longo da faixa de fronteira está havendo uma reacomodação das facções que controlam, do Mato Grosso para cima. E o pano de fundo é a situação prisional caótica. A violência irracional tem uma intenção bem pensada”, acredita o professor do departamento de Sociologia da Universidade de Brasília Arthur Trindade.” In: STOCHEIRO, Tahiane. **Entenda**: o que a disputa nacional entre facções tem a ver com a barbárie no presídio do Amazonas, 0301/2017. Disponível em: <http://g1.globo.com/am/amazonas/noticia/entenda-o-que-a-disputa-nacional-entre-faccoes-tem-a-ver-com-a-barbarie-no-presidio-do-amazonas.ghtml>. Acesso em: 10/08/17

<sup>116</sup>“Sobre as decapitações e corações arrancados na rebelião em Manaus, Fernandes diz se tratar de uma demonstração de poder. “Eles vivem numa selva e fugiu da razoabilidade de qualquer situação. A forma como as mortes ocorreram retratam códigos de respeito”, diz ele, ressaltando que o PCC restringe a violência em presídios por tratar o tema dentro de uma questão “mercantilista”. “Não interessa demonstrações de força e estes espetáculos”. STOCHEIRO, Tahiane. **Entenda**: o que a disputa nacional entre facções tem a ver com a barbárie no presídio do Amazonas, 0301/2017. Disponível em: <http://g1.globo.com/am/amazonas/noticia/entenda-o-que-a-disputa-nacional-entre-faccoes-tem-a-ver-com-a-barbarie-no-presidio-do-amazonas.ghtml>. Acesso em: 10/08/17

<sup>117</sup>“O que ocorreu em Manaus tem um contexto mais amplo, envolve um contexto mais amplo da disputa entre o

## 2.2.4 A ineficiência do Estado

A estruturação, organização e fortalecimento do PCC, assim como das demais facções criminosas existentes no sistema prisional brasileiro, ocorreram, em grande parte, por uma sucessão de decisões equivocadas que foram adotadas pela política prisional estatal. O Estado foi conivente com condutas que deveriam ter sido prontamente combatidas no interior do ambiente prisional.

Ao permitir o fortalecimento de lideranças entre os presos, a conivência com a comunicação via telefone celular, a negligência em relação à construção de privilégios dentro da cadeia, a não apuração rigorosa dos crimes cometidos dentro do ambiente prisional, a transferência de presos sem o amparo de uma programação estratégica, o Estado produziu as condições deletérias para o ambiente prisional funcionar em estado de anomia. Nesse local é comum observar o dilaceramento psicossocial de indivíduos com baixo potencial de periculosidade, convertendo-os em soldados do crime organizado, por força da dominação exercida pela ampla estrutura de controle dos corpos, submetidos a todas as regras de cumprimento de funções, dinâmicas de atuação e punições, cujo itinerário do detento é a absoluta subserviência ao *modus operandi* do grupo.

Além das equivocadas decisões voltadas diretamente para o sistema prisional, uma série de fatores e de decisões em matéria criminal e policial podem ser apontados para que o Estado, por meio dos seus agentes, viesse a se portar de uma forma tão contraproducente diante de problemas sociais do âmbito criminal. É possível apontar alguns desses pontos, tais como: incapacidade técnica de quem operava o sistema; escassez de recursos destinados à política penitenciária; falta de interesse em tomar decisões que exigiriam vultosos esforço para sua implementação; tibieza nas decisões e, em muitos casos, envolvimento dos agentes com a organização criminosa pela prática da corrupção.

---

CV e o PCC no país, que começou em 2016, quando eles declararam guerra em grande parte dos estados. O PCC tem a intenção de se tornar hegemônico no país e não tem limite de esforços para isso”, diz o promotor. “Havia um prenúncio de que algo iria acontecer e de que o PCC atacaria o FDN e o CV. Eles foram surpreendidos no presídio. Este ataque vai ter consequências”, afirma Lincoln Gakiya, Promotor de Justiça, integrante do grupo de combate ao Crime Organizado (GAECO/SP)”. STOCHEIRO, Tahiane. **Entenda:** o que a disputa nacional entre facções tem a ver com a barbárie no presídio do Amazonas, 0301/2017. Disponível em: <http://g1.globo.com/am/amazonas/noticia/entenda-o-que-a-disputa-nacional-entre-faccoes-tem-a-ver-com-a-barbarie-no-presidio-do-amazonas.ghtml>. Acesso em: 10/08/17

Além disso, há carência de investimento em tecnologias e aparatos investigativos que aumentem a eficácia da estrutura burocrática para o esclarecimento de crimes, que permitiriam à polícia uma atuação efetiva, sem a perniciosa abertura das portas da prisão para presos que praticaram delitos de menor potencial ofensivo, mas já enredados em alguma organização criminosa. Essa prática, aliada ao crescimento do mercado consumidor de drogas ilícitas, facilitou o avanço das organizações criminosas, pois estruturou vinculações com a rede carcerária em todo país, propiciando entendimentos e confluência de propósitos, mas também competições e conflitos, sempre acompanhados pela ocorrência de um número elevado de homicídios, resultado de ações de extrema violência.

A atuação de integrantes das organizações que surgiram no Rio de Janeiro (CV) e São Paulo (PCC) em outros Estados, com o objetivo de efetuar roubos a instituições financeiras, abre caminho para a ampliação da área de influência por todo o país, favorecendo o surgimento de organizações locais que ou a elas se aliam ou com elas rivalizam.<sup>118</sup>

O Estado se mostra ineficiente, conivente, incapaz de se contrapor ao domínio do crime organizado<sup>119</sup>. Assiste, parcimoniosamente, ao fortalecimento de um poder que afronta a sociedade, submetendo-a ao jugo de uma instância paralela de autoridade. Não chega a causar estranheza o recebimento via aplicativo de *smartphone*, de um “salve”, que é uma ordem dada pelo comando de uma facção local para que o comércio, os serviços públicos, e as escolas de determinadas localidades fechem suas portas em sinal de respeito à morte de um dos líderes locais do tráfico, por exemplo, ou para facilitar a execução de um plano de fuga sob pena de retaliações que podem resultar em morte. A sentença aos que descumprem,

---

<sup>118</sup>“Neste cenário institucional, não é difícil compreender como ocorreu o processo de “faccionalização” do país. Considerando a forma de atuação desses grupos, podemos identificar ao menos quatro movimentos: 1. um projeto de expansão do PCC através da rede carcerária com a criação de “Sintonias” vinculadas organicamente à estrutura paulista; 2. migração de indivíduos foragidos e vinculados ao CV ou ao PCC e, em geral, envolvidos em roubos a instituições financeiras; 3. o surgimento de grupos locais, em quase todos os estados, em aliança (ex: GDE-CE, Bonde dos 13-AC, Estados Unidos-PB, Bonde dos Malucos-BA), ou em oposição (ex: FDN-AM, PGC-SC, Okaida-PB, Sindicato do Crime-RN) ao PCC; 4. a expansão do CV através da abertura de franquias em outros estados e da coligação com grupos locais.” DIAS, Camila Nunes MANSO, Bruno Paes. Tecendo redes criminais: as políticas de encarceramento e a nacionalização das facções prisionais. *In: Anuário Brasileiro de Segurança Pública 2014 a 2017, Edição Especial*. Fórum Brasileiro de Segurança Pública. Disponível em: <http://www.forumseguranca.org.br/atividades/anuario/>. Acesso em: 09/09/2018.

<sup>119</sup>“Nada disso teria prosperado se, do lado do poder público, as autoridades penitenciárias não tivessem hesitado, com frequência, em coibir com rigor os ilegalismos praticados pelas lideranças e o crescente prestígio e poder adquirido entre os presos e entre criminosos em liberdade. Temerosas de que ações, exigindo disciplina correcional, pudessem comprometer o frágil equilíbrio da ordem interna prisional, acabaram por favorecer a constituição dessas lideranças organizadas.” ADORNÓ, Sérgio; SALLA, Fernando. Criminalidade organizada nas prisões e os ataques do PCC. *Estudos avançados*, v. 21, n. 61, p. 7-29, 2007. Disponível em <http://www.scielo.br/pdf/ea/v21n61/a02v2161>. Acesso em: 08/08/17.

costuma ser rigorosamente obedecida.

### **2.2.5 Novas Organizações Criminosas**

A criminalidade organizada no Brasil está umbilicalmente ligada ao tráfico de drogas, sendo esta a face mais conhecida pela sociedade. Entretanto, nos últimos anos, outro tipo de criminalidade organizada vem ocupando os noticiários e chamando a atenção das autoridades responsáveis: trata-se daquele grupo criminoso cujos integrantes residem em condomínios de luxo, que realiza viagens internacionais, frequenta restaurantes de alto padrão, usa joias exclusivas, e aporta dentro do aparato estatal com notoriedade e distinção. Estabelece-se, de forma recorrente, uma relação marcadamente patrimonialista, em que a noção de separação entre o público e o privado se perde, imiscuindo-se interesses escusos, evidenciando um grau de corrupção tão acentuado que atinge inclusive os mais altos escalões de governo.

A prática da corrupção, ainda que prevista como conduta criminosa, era tolerada pela sociedade, que fazia ouvidos moucos aos casos que chegavam a vir a público. Ainda que tecnicamente se pudesse enquadrar em uma ou outra figura delituosa, havia uma conivência silenciosa, uma resignação tácita em relação a atos ilícitos praticados por agentes públicos que possuíam o dever funcional de zelar pela lisura e transparência da coisa pública, o que impedia a tomada de qualquer atitude. Aliado a isso, havia também a falta de identificação da vítima como sujeito passivo do crime cometido, o que dificultava sua apuração e responsabilização, pois muitas vezes os autores são considerados pela sociedade como pessoas de conduta ilibada, empresários bem sucedidos, responsáveis pela geração de emprego e renda para a comunidade.

Após a Constituição Federal de 1988, o novo desenho dado à instituição do

Ministério Público<sup>120</sup>, com novas atribuições<sup>121</sup> que vão além de promover privativamente a ação penal pública, mas podendo também instaurar e presidir investigações criminais<sup>122</sup>, permite que a engrenagem estatal, corroída pela corrupção, passe por um processo de depuração.

Sucessivas ações de improbidade administrativa e de responsabilização criminal contra agentes públicos e governantes surgem nas mais diversas esferas de poder, levando funcionários que ingressaram na carreira pública mediante concurso e mandatários eleitos por voto popular à prisão e à perda do direito de exercer cargos públicos.

O poder político, sentindo-se ameaçado, tendo seus métodos escusos e criminosos investigados e postos à mostra, alia-se a uma imprensa conivente e beneficiária de milionários contratos de publicidade, para juntos iniciarem campanhas contra o Ministério Público e a Magistratura, acusando-os de gozarem de privilégios, o que justificaria, portanto, que os pretensos ajustes dos gastos da máquina estatal se iniciem por essas carreiras.

Evidencia-se o caráter intimidatório dessas campanhas e o objetivo de conseguir apoio da opinião pública para desmerecer órgãos que têm o dever de fiscalizar as atividades

<sup>120</sup> “Art. 129. São funções institucionais do Ministério Público:

- I - promover, privativamente, a ação penal pública, na forma da lei;
- II - zelar pelo efetivo respeito dos Poderes Públicos e dos serviços de relevância pública aos direitos assegurados nesta Constituição, promovendo as medidas necessárias a sua garantia;
- III - promover o inquérito civil e a ação civil pública, para a proteção do patrimônio público e social, do meio ambiente e de outros interesses difusos e coletivos;
- IV - promover a ação de inconstitucionalidade ou representação para fins de intervenção da União e dos Estados, nos casos previstos nesta Constituição;
- V - defender judicialmente os direitos e interesses das populações indígenas;
- VI - expedir notificações nos procedimentos administrativos de sua competência, requisitando informações e documentos para instruí-los, na forma da lei complementar respectiva;
- VII - exercer o controle externo da atividade policial, na forma da lei complementar mencionada no artigo anterior;
- VIII - requisitar diligências investigatórias e a instauração de inquérito policial, indicados os fundamentos jurídicos de suas manifestações processuais;
- IX - exercer outras funções que lhe forem conferidas, desde que compatíveis com sua finalidade, sendo-lhe vedada a representação judicial e a consultoria jurídica de entidades públicas.” (Constituição da República Federativa do Brasil de 1988)

<sup>121</sup> “A Constituição reconheceu que a abertura democrática não dispensa um Ministério Público forte e independente, que efetivamente possa defender as liberdades públicas, os interesses difusos e coletivos, o meio ambiente, o patrimônio público, as vítimas não só da violência como da chamada criminalidade do colarinho branco – ainda que o agressor seja muito poderoso ou até mesmo seja o governante. Cometeu ao Ministério Público o zelo do próprio regime democrático. Enfim, a Constituição de 1988 assegurou à instituição novas atribuições e um relevo que jamais se conferiu ao Ministério Público, mesmo no Direito Comparado.” MAZZILLI, Hugo Nigro. **Introdução ao Ministério Público**. São Paulo: Saraiva, 2002, 4ª ed., págs. 48 e 49

<sup>122</sup> “Art. 1º O procedimento investigatório criminal é instrumento de natureza administrativa e inquisitorial, instaurado e presidido pelo membro do Ministério Público com atribuição criminal, e terá como finalidade apurar a ocorrência de infrações penais de natureza pública, servindo como preparação e embasamento para o juízo de propositura, ou não, da respectiva ação penal.” (Resolução nº 13/2006 do CNMP)

da administração pública, visando retirar-lhes as prerrogativas que hoje os permitem investigar e julgar com imparcialidade os detentores de poder estatal. Apesar da influência dessas campanhas que se prolongam no tempo, mesmo com dificuldades orçamentárias impostas a tais instituições, as investigações prosseguem, as condenações se enfileiram e a guerra contra a corrupção se intensifica.

As investigações dos casos de improbidade administrativa e de crimes contra a administração da justiça, especialmente a corrupção, revelam que os crimes são cometidos em teia, por organizações de agentes que se unem para regularmente se locupletarem de recursos públicos. A ideia de organização criminosa, antes restrita ao tráfico de drogas, passa a se aplicar adequadamente às organizações integradas por executivos de grandes empresas e ocupantes de cargos públicos do alto escalão estatal.

Essas organizações não adotam os modelos tradicionais de organização criminosa, não se encaixam em uma definição, pois têm estruturas e objetivos cambiantes, não sendo possível uma categorização. Em comum, todas elas têm como vítimas, o Estado e o bem público, e como autores contumazes dos delitos, agentes públicos e representantes do capital financeiro.

O primeiro caso de grande repercussão nacional foi o julgamento da Ação Penal 470 pelo Supremo Tribunal Federal, conhecido como caso do “Mensalão”, que levou a julgamento 38 ocupantes de cargos públicos (ministros, deputados, diretores de partidos políticos) e dirigentes de grandes empresas, sendo 25 deles condenados por envolvimento em esquema milionário de pagamento regular de propina a congressistas no período entre 2003 e 2005. À época dos julgamentos, ainda não havia legislação específica para tratar de organização criminosa<sup>123</sup>, razão pela qual foram os mesmos condenados pelo crime de formação de quadrilha, previsto no art. 288 do Código Penal<sup>124</sup>.

---

<sup>123</sup>Atualmente a Lei nº 12.850 de 02 de agosto de 2013, define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal.

<sup>124</sup>**Decisão:** Prosseguindo no julgamento quanto ao **item VI** da denúncia, o **Ministro Joaquim Barbosa (Relator) julgou procedente a ação para condenar** os réus Pedro da Silva Corrêa de Oliveira Andrade Neto (item VI.1, subitens b.1, b.2 e b.3 da denúncia), Pedro Henry Neto (item VI.1, subitens b.1, b.2 e b.3 da denúncia) e João Cláudio de Carvalho Genú (item VI.1, subitens c.1, c.2 e c.3 da denúncia) **pela prática dos crimes de formação de quadrilha (art. 288 do Código Penal)**, corrupção passiva (art. 317 do Código Penal) e lavagem de dinheiro (art. 1º, V e VI, da Lei nº 9.613/1998), este último em continuidade delitiva (cinco vezes através de João Cláudio de Carvalho Genú; quatro vezes através de funcionários da BÔNUS BANVAL; sete vezes através da NATIMAR/BÔNUS BANVAL), havendo as operações de lavagem de dinheiro sido realizadas em continuidade delitiva (item VI.1, subitens b.1, b.2, b.3, c.1, c.2 e c.3), absolvido o réu João Cláudio de Carvalho Genú de duas imputações de corrupção passiva, considerando ter havido a prática de conduta única; condenar os réus Enivaldo Quadrado e Breno Fischberg (item VI.1, subitens d.1 e d.2 da denúncia) **pela prática**

Em março de 2014, um grupo de integrantes do Ministério Público Federal, em conjunto com a Polícia Federal, iniciou uma investigação a respeito do uso de uma rede de postos de combustíveis e serviço de lava a jato de automóveis para movimentar recursos ilícitos e proceder à lavagem de dinheiro. A ideia inicial dos condutores do caso era que as investigações levariam de três a quatro meses, previsão contrariada pelo volume de investigações que foram sendo conduzidas ao longo do caso. O transcurso das fases da assim denominada “Operações da Lava Jato” durou sete anos, tendo suas ações encerradas em fevereiro de 2021.

O início das investigações ainda guardava relação com os desvios provenientes do “Mensalão”. Trata-se de um inquérito antigo, que investigava o investimento de pouco mais de um milhão de reais em uma empresa pertencente ao Deputado José Janene, réu naquele processo e falecido no curso da sua instrução. As suspeitas eram de lavagem de dinheiro, que, entre outras atividades, também mantinha um posto de combustível onde se realizava serviço de limpeza de automóveis, servindo, inclusive, de inspiração para a o nome da Operação.

---

**dos crimes de formação de quadrilha (art. 288 do Código Penal)** e lavagem de dinheiro (art. 1º, V e VI, da Lei nº 9.613/1998), este último em continuidade delitiva (quatro vezes através de funcionários da empresa BÔNUS BANVAL; sete vezes utilizando-se da conta da NATIMAR); condenar os réus Valdemar Costa Neto (item VI.2, subitens b.1, b.2 e b.3 da denúncia) e Jacinto de Souza Lamas (item VI.2, subitens c.1, c.2 e c.3 da denúncia), em concurso material, por corrupção passiva (art. 317 do Código Penal), lavagem de dinheiro (art. 1º, incisos V e VI, da Lei nº 9.613/1998, várias vezes, em continuidade delitiva, através da Guaranhuns Empreendimentos e do esquema narrado no capítulo IV da denúncia), e **formação de quadrilha (art. 288 do Código Penal)**; condenar o réu Carlos Alberto Rodrigues Pinto (VI.2, subitens e.1 e e.2 da denúncia), em concurso material, pela prática dos crimes de corrupção passiva (art. 317 do Código Penal), e lavagem de dinheiro (art. 1º, incisos V e VI, da Lei nº 9.613/1998); condenar os réus Roberto Jefferson Monteiro Francisco (item VI.3, subitens c.1 e c.2 da denúncia), Romeu Ferreira Queiroz (item VI.3, subitens d.1 e d.2 da denúncia), e Emerson Eloy Palmieri (item VI.3, subitens e.1 e e.2 da denúncia), em concurso material, pela prática dos crimes de corrupção passiva (art. 317 do Código Penal), e lavagem de dinheiro (art. 1º, incisos V e VI, da Lei nº 9.613/1998), este último praticado em continuidade delitiva, absolvido o réu Emerson Eloy Palmieri de uma imputação de corrupção passiva e de três imputações de lavagem de dinheiro; e para condenar o réu José Rodrigues Borba (item VI.4, subitens b.1 e b.2 da denúncia), em concurso material, pela prática dos crimes de corrupção passiva (art. 317 do CP), e lavagem de dinheiro (art. 1º, incisos V e VI da Lei nº 9.613/1998), julgando improcedente a ação para absolver o réu Antônio de Pádua de Souza Lamas com base no art. 386, inciso VII, do Código de Processo Penal; quanto ao réu José Mohamed Janene, falecido em 2010, já foi declarada extinta sua punibilidade, nos termos do art. 107, I, do Código Penal. Em seguida, após o voto do Ministro Ricardo Lewandowski (Revisor), julgando procedente a ação para condenar o réu Pedro da Silva Corrêa de Oliveira Andrade Neto pelo crime de corrupção passiva (art. 317, *caput*, do Código Penal), mencionado no item VI.1, b.2 da denúncia, e julgando improcedente a ação quanto ao crime de lavagem de dinheiro (art. 1º, incisos V e VI da Lei nº 9.613/1998), item VI.1, b.3 da denúncia, para absolvê-lo com base no art. 386, VII, do Código de Processo Penal; e, quanto ao réu Pedro Henry Neto, julgando improcedente a ação quanto aos crimes de quadrilha (art. 288 do Código Penal), corrupção passiva (art. 317 do Código Penal) e lavagem de dinheiro (art. 1º, incisos V e VI da Lei nº 9.613/1998), descritos no item VI.1, subitens b.1, b.2 e b.3 da denúncia, para absolvê-lo com base no art. 386, VII, do Código de Processo Penal, o julgamento foi suspenso. Presidência do Senhor Ministro Ayres Britto. Plenário, 20/09/2012. (destaquei os delitos de formação de quadrilha). Disponível em: <http://www.stf.jus.br/portal/processo/verProcessoAndamento.asp?incidente=11541>. Acesso em: 14/08/17.

O procedimento de coleta de provas foi descortinando aos investigadores uma rede sofisticada e muito bem organizada, que atuava há pelo menos dez anos na lavagem de capitais, na qual grandes empreiteiras organizadas em cartel pagavam propina para altos executivos da Petrobrás e a outros agentes públicos, visando conseguir contratos com a estatal. O valor da propina variava de acordo com o valor total dos contratos, invariavelmente superfaturados, que atingiam somas bilionárias, sendo esse suborno distribuído por meio de operadores financeiros da organização criminosa a partidos políticos e a políticos integrantes do Poder Legislativo Federal.<sup>125</sup>

Em 2015, o Ministério Público Federal requereu ao Supremo Tribunal Federal autorização para iniciar investigação contra 49 pessoas portadoras de foro privilegiado, sendo que dessas investigações resultaram denúncias e condenações por diversos crimes, entre elas o delito de organização criminosa, agora já devidamente tipificado em legislação própria<sup>126</sup>, e perfeitamente cabível nos casos que se apresentavam.

Está assim inaugurado um novo capítulo para o sistema jurídico brasileiro. Não imune a diversas críticas que justamente lhe são feitas, a operação Lava Jato e a instrução penal que lhe seguiu foram maculadas por uma série de determinações cuja legalidade é questionável. Apesar disso, pode-se reconhecê-la como um marco, pois pela primeira vez organizações criminosas que não guardam ligação com a criminalidade comum, aquela ligada ao tráfico de drogas, foram tipificadas e condenadas.

O modelo endógeno de crime organizado, encontra aqui uma situação exemplar.<sup>127</sup>

---

<sup>125</sup> Essa a afirmação feita por Deltan Dallagnol em seu livro **A Luta Contra a Corrupção**. Rio de Janeiro: Ed. Primeira Pessoa, 2017, que à época da investigação era o Procurador da República responsável pelo caso, mas que em seguida deixou o Ministério Público para ingressar na carreira política, sendo eleito Deputado Federal.

<sup>126</sup> Art. 1º Esta Lei define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal a ser aplicado.

§ 1º Considera-se organização criminosa a associação de 4 (quatro) ou mais pessoas estruturalmente ordenada e caracterizada pela divisão de tarefas, ainda que informalmente, com objetivo de obter, direta ou indiretamente, vantagem de qualquer natureza, mediante a prática de infrações penais cujas penas máximas sejam superiores a 4 (quatro) anos, ou que sejam de caráter transnacional.” (Lei 12.850/2013)

<sup>127</sup> “O paradigma endógeno é aquele que germina e dissemina-se no interior de determinadas instituições, em especial públicas, que se valem de suas prerrogativas e posições privilegiadas para a obtenção de vantagens contínuas, na medida de suas influências tentaculares por todos os segmentos sociais possíveis de serem alcançados, aproveitando todas as oportunidades que lhe surgem no trato com os negócios públicos, afetos às suas atribuições, e suas escusas interações com os mais diversos interesses privados corporativos, que também colherão seus mais espúrios benefícios dessas relações. Já é de notório conhecimento a expressão “white collar crimes”, isto é, “crimes do colarinho branco”, definidos como aqueles que se caracterizam pelos mais diversos abusos, fraudes e acobertamentos das práticas ilícitas, independentemente do uso de violência.” CABETTE, Eduardo Luis Santos e NAHUR, Marcius Tadeu Maciel. **Criminalidade organizada & globalização desorganizada**. Rio de Janeiro: Ed. Freitas Bastos, 2014. p. 78.

Esquemas criminosos forjados em gabinetes de representação popular, trajando indumentária distinta e vocabulário rebuscado, jactando-se de não sujar as mãos de sangue, mas promovendo vultosos desvios de dinheiro dos cofres públicos, condenaram milhões à fome e à miséria, privilegiando interesses de foro privado e partidário.

Na fundamentação das sentenças<sup>128</sup>, o magistrado que instruía as ações penais resultantes da Lava Jato, justifica as sentenças condenatórias dos réus pelo delito de formação de organização criminosa, apesar dos crimes terem sido cometidos antes da entrada em vigor

<sup>128</sup>“551. Questão que se coloca diz respeito à incidência do art. 2º da Lei n.º 12.850/2013. A lei em questão foi publicada em 02/08/2013, entrando em vigor quarenta e cinco dias depois.

552. Portanto, entrou em vigor apenas após a prática da maior parte dos crimes que compõem o objeto desta ação penal.

553. Mas, como adiantado, o crime associativo não se confunde com os crimes concretamente praticados pelo grupo criminoso.

554. Importa saber se as atividades do grupo persistiam após 19/09/2013.

555. Há provas nesse sentido.

556. Paulo Roberto Costa persistiu recebendo propinas mesmo após deixar seu cargo na Petrobras, o que é ilustrado pelos contratos de consultoria por ele firmados com diversas empreiteiras e que se encontra reproduzido na fl. 45 da denúncia.

557. No caso específico da OAS, há prova cabal de que o vínculo associativo com Alberto Youssef perdurou até a efetivação da prisão deste, considerando as aludidas operações da OAS de dezembro de 2013, fevereiro e março de 2014, com Alberto Youssef, cuja origem dos recursos não foi esclarecida nos autos ou pelos acusados, mas que seguem o mesmo modus operandi anterior, entregas subreptícias de valores vultosos em espécie a terceiros, inclusive agentes políticos, mediante utilização do escritório de lavagem de dinheiro de Alberto Youssef (itens 470483).

558. Se os crimes fins da associação, que incluem operações de lavagem de dinheiro e entrega de valores a agentes políticos por transações subreptícias, encontravam-se ainda em execução depois de 09/2013, não se pode afirmar que o vínculo associativo e programa delitivo dele decorrente havia se encerrado antes da Lei n.º 12.850/2013. 559. Também o subgrupo dirigido por Alberto Youssef encontra-se em atividade, sendo ela interrompida apenas com a prisão cautelar dele em 17/03/2014.

560. Ainda que talvez não na mesma intensidade de outrora, há provas, portanto, de que o grupo criminoso encontrava-se ativo depois de 19/09/2013, assim permanecendo nessa condição pelo menos até 17/03/2014, quando cumpridos os primeiros mandados de prisão.

561. Sendo os crimes associativos de caráter permanente, incidiu, a partir de 19/09/2013, o crime do art. 2º da Lei n.º 12.850/2013, em substituição ao anterior art. 288 do CP.

562. Ao contrário do que se pode imaginar, o tipo penal em questão não abrange somente organizações do tipo mafiosas ou os grupos criminosos que, no Brasil, se organizaram em torno da vida carcerária.

563. Pela definição prevista no §1º do art. 1º da Lei n.º 12.850/2013, "considera-se organização criminosa a associação de 4 (quatro) ou mais pessoas estruturalmente ordenada e caracterizada pela divisão de tarefas, ainda que informalmente, com objetivo de obter, direta ou indiretamente, vantagem de qualquer natureza, mediante a prática de infrações penais cujas penas máximas sejam superiores a 4 (quatro) anos, ou que sejam de caráter transnacional".

564. Devido a abrangência da definição legal, deve ser empregada em casos nos quais se constate a existência de grupos criminais estruturados e dedicados habitual e profissionalmente à prática de crimes graves.

565. No caso presente, o grupo criminoso dedicava-se à prática, habitual, reiterada e profissional, de crimes contra a Petrobrás, especificamente dos crimes de cartel (art. 4º, I, da Lei n.º 8.137/1990) e de frustração, por ajuste, de licitações (art. 90 da Lei n.º 8.666/1993), de corrupção de dirigentes da Petrobrás e de lavagem de dinheiro decorrente, todos com penas máximas superiores a quatro anos.

566. O grupo praticou os crimes por longos períodos, desde 2007 pelo menos considerando os crimes narrados no presente feito.

567. Havia estruturação e divisão de tarefas dentro do grupo criminoso como já visto.

568. Integrariam o grupo diversas pessoas, entre elas os reputados responsáveis pelos crimes de lavagem.

569. No subgrupo dedicado à lavagem de dinheiro, Alberto Youssef era responsável pela estruturação das

da lei que a tipifica, como também esclarece que as organizações em julgamento não guardam semelhança com as estruturas rígidas que orientam a máfia, por exemplo, mas nem por isso deixam de ser uma organização criminosa, tendo em vista preencherem todos os requisitos exigidos por lei.

Apesar dos avanços e do papel simbólico que a Operação Lava Jato trouxe ao apurar esquemas milionários de corrupção, conduzindo a prisão importantes líderes políticos e grandes empresários, seu principal representante, o então juiz Sérgio Moro, que passou a ter reconhecimento inclusive internacional, resvalou no perigoso terreno habitado pela vaidade, demonstrando não ter habilidade para ali trafegar. Sucumbiu na tarefa de fazer prevalecer seus deveres de magistrado ante seus interesses pessoais, pondo em risco a credibilidade junto à sociedade do necessário combate a corrupção, que só pode alcançar êxito se feito dentro das regras do Estado Democrático de Direito.

Em alguns processos emblemáticos resultantes de tal operação, que tiveram por réu o ex-Presidente da República, Luis Inácio Lula da Silva, o julgador supra citado, bem como o representante do Ministério Público Federal, Deltan Dallagnol, encarregado de presidir os procedimentos investigatórios, atropelaram criminosa e perigosamente o sistema acusatório. Juiz e Ministério Público agiram em conluio, desequilibrando o necessário tripé processual, passando o juiz a agir como investigador<sup>129</sup>, inclusive autorizando a execução de métodos de operações contando com os serviços de auxílio de Waldomiro de Oliveira e outros denunciados em outros feitos, como Leonardo Meirelles e Jayme Alves de Oliveira Filho. Já Paulo Roberto Costa era o agente público na Petrobras necessário para viabilizar a obtenção dos recursos junto às empreiteiras contratantes.

570. No subgrupo das empreiteiras, na OAS, reconhecida a responsabilidade pelos crimes de corrupção e lavagem de dinheiro de três executivos e de outro empregado. Nesse subgrupo, teria havido ainda associação com os executivos das outras empreiteiras para a prática de do cartel, ajuste de licitações, corrupção e lavagem, mas que respondem à outras ações penais.

571. Assim, o grupo tem bem mais do que quatro integrantes, certamente com diferentes graus de envolvimento e de responsabilidade na atividade criminosa, atendendo à exigência legal.

**572. Evidente que não se trata de um grupo criminoso organizado como a Cosa Nostra italiana ou o Primeiro Comando da Capital, mas um grupo criminoso envolvido habitual, profissionalmente e com certa sofisticação na prática de crimes contra a Petrobrás e de lavagem de dinheiro. Isso é suficiente para o enquadramento legal. Não entendo que o crime previsto na Lei nº 12.850/2013 deva ter sua abrangência reduzida por alguma espécie de interpretação teleológica ou sociológica. As distinções em relação a grupos maiores ou menores ou mesmo do nível de envolvimento de cada integrante devem refletir somente na dosimetria da pena.**

573. Portanto, resta também provada a materialidade e autoria do crime do art. 2º da Lei nº 12.850/2013, devendo ser responsabilizados José Adelmário, Agenor Medeiros, Mateus Coutinho e José Breghirolli.” (destaquei) trecho da sentença prolatada nos autos da Ação Penal n.º 508337605.2014.404.7000, processada pela Justiça Federal, Seção Judiciária do Paraná, 13ª Vara Federal de Curitiba, disponível no endereço <http://s.conjur.com.br/dl/sentenca-oas-lava-jato.pdf>, acessado em 10.08.17. Mesma fundamentação é possível encontrar nas sentenças proferidas, pelo mesmo juízo, em outras ações penais, disponível em: 508325829.2014.4.04.7000/PR e 503042478.2016.4.04.7000/PR. Acesso em: 14/08/17.

<sup>129</sup> “Com efeito, veio a público que o referido ex-juiz empreendeu sucessivos atos ilegais e contrários às regras deontológicas da magistratura, consubstanciados, dentre outros, nos seguintes: (i) antecipação ao Parquet de

prova em desacordo com as regras procedimentais vigentes<sup>130</sup>.

Como resposta, ainda que tardiamente, após levar a prisão o importante réu, submetido que fora a processos tendenciosos, julgados por um juiz parcial, o Supremo Tribunal Federal reconheceu a parcialidade do julgador em diversos procedimentos, anulando-os desde o primeiro ato decisório do magistrado em questão, incluindo aí as demais decisões proferidas ainda que em fase investigativa<sup>131</sup>

A corrupção, objeto de combate da denominada Operação Lava Jato, atingiu os representantes estatais da Magistratura e do Ministério Público, que buscavam combatê-la. Ao desrespeitar as regras do Estado Democrático e de Direito, utilizando os cargos que ocupavam para atender a interesses políticos pessoais, ambos os representantes estatais, Juiz e Procurador da República, violaram o código que diferencia o sistema jurídico do sistema político. Tal violação de código importa em corrupção do sistema jurídico, que passa a ser instrumento da política, visando impor uma visão particular e autoritária de Estado e do modo de organização da sociedade<sup>132</sup>.

futuros provimentos jurisdicionais; (ii) sugestão de inversão de etapas das investigações; (iii) comentários acerca da decisão ilícita que autorizou o levantamento do sigilo de interceptações telefônicas; (iii) revelações sobre movimentos da defesa; e (iv) sugestões de estratégias acusatórias aos integrantes do Ministério Público. Tal atuação, levada a cabo à sorrelfa e sempre à margem dos autos, sem o conhecimento da defesa, por meio de aplicativo de celular supostamente indevassável, dentre outras ilicitudes, configura ostensiva desconsideração ao sistema acusatório que vigora entre nós e à regra processual da absoluta paridade de armas entre as partes.” Trecho do voto do Ministro Ricardo Lewandowski no Acórdão registrado sob número único 0081750-08.2018.1.00.0000, nos autos de HC 164.493, Segunda Turma do STF, Relator Ministro Gilmar Mendes, disponível no seguinte endereço: <http://portal.stf.jus.br/processos/downloadPeca.asp?id=15346606406&ext=.pdf>. Acessado em 24/08/2021

<sup>130</sup> “A questão discutida também envolvia ato processual anômalo - noticiado na exordial desta impetração -, consistente em determinação exarada ex officio pelo então juiz, às vésperas do primeiro turno da eleição presidencial e após o encerramento da instrução processual, para que fosse levantado o sigilo e transladados para os autos de ação penal trechos do depoimento prestado por delator em acordo de colaboração premiada, instantes depois vazados para a imprensa.” Trecho do voto do Ministro Ricardo Lewandowski no Acórdão registrado sob número único 0081750-08.2018.1.00.0000, nos autos de HC 164.493, Segunda Turma do STF, Relator Ministro Gilmar Mendes, disponível no seguinte endereço: <http://portal.stf.jus.br/processos/downloadPeca.asp?id=15346606406&ext=.pdf>. Acessado em 24/08/2021

<sup>131</sup> “Assim, por isonomia e segurança jurídica, é dever deste Tribunal, por meio do Relator do feito, estender a decisão aos casos pertinentes, quando há identidade fática e jurídica, nos termos do art. 580 do CPP. Diante do exposto, tendo em vista a identidade fática e jurídica, estendo a decisão que concedeu a ordem neste Habeas Corpus às demais Ações Penais conexas (5021365-32.2017.4.04.7000/PR – Caso “Sítio de Atibaia” e 5063130-17.2016.4.04.7000/PR – Caso “Imóveis do Instituto Lula”), processadas pelo julgador declarado suspeito em face do paciente Luiz Inácio Lula da Silva, de modo a anular todos os atos decisórios emanados pelo magistrado, incluindo-se os atos praticados na fase pré-processual, nos termos do art. 101 do Código de Processo Penal.” Decisão Proferida na extensão do HC 164.493, Segunda Turma do STF, Relator Ministro Gilmar Mendes. Disponível em <http://portal.stf.jus.br/processos/downloadPeca.asp?id=15346819336&ext=.pdf> Acessado em 24/08/2021

<sup>132</sup> “É verdade, no entanto, que o Direito pode ser instrumento da Política. Resta saber se o é, legitimamente, enquanto organizador da concretização pelo Estado de uma opção política e do que pode ser vinculativo ou se é, antes, instrumentalizado pela Política, de modo ilegítimo e segundo uma lógica de dominação.” PALMA, Maria Fernanda. **Direito Constitucional Penal**: Coimbra. Almedina, 2011. pág. 73

A prisão ilegalmente decretada do então candidato a Presidência da República, Luis Inácio Lula da Silva, que detinha a preferência do eleitorado, o impedindo de participar do pleito, alterou significativamente o panorama político do país, vindo a ser eleito candidato até então inexpressivo no cenário político nacional.

O magistrado antes citado, que instruiu as ações penais que condenaram e levaram a prisão o principal candidato a Presidência da República, aceitou convite para exercer o cargo de Ministro da Justiça do candidato vitorioso, opositor ao candidato preso, na disputa eleitoral de 2018.

Aproximando-se período eleitoral, com eleições presidenciais marcadas para o ano de 2022, o ex-juiz e ex-Ministro da Justiça se apresenta como candidato as eleições presidenciais, assim como o ex-Procurador da República, que presidiu as investigações da Operação Lava jato, ensaia candidatura a cargo do Poder Legislativo.

A utilização da investigação criminal, em especial aquela que pode lançar mão de métodos de obtenção de prova mais invasivos, é instrumento poderoso, que pode influenciar até mesmo o destino de um país, como aqui aconteceu. Assim, a apuração e a investigação dos delitos praticados por organizações criminosas passam a ser escrutinados rigorosamente, pois o risco de violação das regras jurídicas já se mostrou viável.

A análise dos métodos de produção de prova a serem utilizados em investigações mais complexas, como aquelas destinadas a desbaratar organizações criminosas, reclama estudo cauteloso, mas que necessita ser feito com brevidade, pois a criminalidade se especializa a cada dia e sofisticada procedimentos para a prática e a ocultação de delitos.

### 3. O USO DA TECNOLOGIA NA INVESTIGAÇÃO DA CRIMINALIDADE ORGANIZADA

As profundas modificações que ocorrem na sociedade global, em um contexto onde as bases de legitimidade da atuação do Estado estão sendo questionadas, produzem deslocamentos da noção de crime, cujas especificidades se revelam ainda desconhecidas, pouco reguladas, gerando sensação de insegurança. Transita-se em terreno novo, movediço, ainda em situação de assentamento e estruturação<sup>133</sup>.

Os aspectos de insegurança e fluidez de conceitos podem também ser identificados durante a investigação criminal, tanto no método a ser utilizado no processo investigatório, quanto em relação às ferramentas das quais se podem dispor para investigar crimes, cuja execução encontra-se cada vez mais requintada, em grande parte pela utilização de aparato tecnológico que está em constante aprimoramento<sup>134 135</sup>.

<sup>133</sup> “O desafio do operador do Direito, no plano do ser, está no reconhecimento de novos instrumentos de comunicação e informação para capacitar, no campo do dever-ser, observado o mínimo de intervenção, impondo ao legislador penal, na criação de modelos, para garantir através de novas figuras, a vida dos indivíduos na macrosociedade.” COSTA, Álvaro Mayrink da. **Temas de Direito Penal**:Rio de Janeiro. Editora Lumen Juris, 2011. p. 378

<sup>134</sup>“The investigation and prosecution of most of these crimes is complex and challenging due to the technical nature of the Internet. Investigation and prosecution in this area require both adequate substantive criminal law provisions as well as adequate procedural capabilities, such as the authority and the technical ability to identify foreign attackers, preserve stored computer data, issue production orders requiring the submission of specified computer data, engage in search and seizure of computer systems, break encryption, engage in the real-time collection of traffic data, and intercept content data.” SIEBER, Ulrich. **Instruments of International Law: Against Terrorist Use of the Internet** In WADE, Marianne e MALJEVIĆ, Almir. **War on Terror?:** New York. Spring, 2010. p. 172

**Em livre tradução:** A investigação e a persecução da maioria desses crimes são complexas e desafiadoras devido à natureza técnica da Internet. A investigação e a persecução penal nesta área exigem disposições adequadas de direito penal substantivo, bem como recursos processuais adequados, como autoridade e capacidade técnica para identificar invasores estrangeiros, preservar dados armazenados em computador, emitir ordens de produção exigindo o envio de específicos dados de computador, engajar em busca e apreensão de sistemas de computador, quebrar criptografia, envolver-se na coleta de dados de tráfego em tempo real e interceptar dados de conteúdo.

<sup>135</sup> “It is a sad fact that sometimes crimes will not be prosecuted due to a lack of resources. But for this reason, it may be advisable to explore the possibility of combining resources across local jurisdictions to adequately address cybercrime” BRENNER, Susan W. e SCHWERHA, Joseph J. IV, **Transnational Evidence Gathering and Local Prosecution of International Cybercrime**, 20 J. Marshall J. Computer & Info. L. 347 (2002), disponível em <https://repository.law.uic.edu/cgi/viewcontent.cgi?article=1139&context=jitpl>, acessado em 16.09.2021. p.394

**Em livre tradução:** É lamentável que às vezes os crimes não sejam processados por falta de recursos. Mas, por esse motivo, pode ser aconselhável explorar a possibilidade de combinar recursos entre jurisdições locais para lidar de forma adequada com o crime cibernético

Em especial na criminalidade organizada, a utilização de avançados equipamentos e recursos tecnológicos estão presentes e são instrumentos importantes, não apenas para a obtenção do resultado ilícito, como também para ocultar as rastros deixados pela empresa criminosa. Assim, cabe ao Estado se posicionar apto para investigar esse tipo de criminalidade, utilizando recursos de idêntica natureza, sob pena de se tornar inócua qualquer atuação estatal encetada para sua repressão ou prevenção.<sup>136 137</sup>

### 3.1 O MÉTODO PARA INVESTIGAR A CRIMINALIDADE ORGANIZADA

No âmbito do direito penal, sobretudo no que se refere ao fracasso do Estado no combate à criminalidade organizada, a sociedade tem tolerado, de maneira cada vez mais complacente, a admissão de métodos de prova secretos<sup>138</sup>, de medidas encobertas, prévias, antes mesmo da prática do crime, visando contribuir para evitar ou, ao menos, garantir a punição do envolvido em crimes de maior grau de perigo para a sociedade.

A investigação criminal clássica utiliza-se da técnica de volver seu olhar para o passado, com fins à reconstrução do crime, identificando aspetos como circunstância e autoria. Para tanto, analisa vestígios, indícios, local do crime, a partir das técnicas de

---

<sup>136</sup>“Diferentemente da regra geral que atua sobre a criminalidade convencional, o crime organizado é amparado por um vasto arcabouço de recursos tecnológicos de ponta. Ao mesmo passo que facilitam a conduta criminosa, a utilização de instrumentos de alta tecnologia assegura outro elemento essencial para o sucesso da empresa criminosa: a eliminação do maior número possível de vestígios do delito. Não raro se encontram ao emprego de organizações delituosas tecnologias sequer empregadas pelos próprios Estados nos quais as organizações se infiltram. A situação é ainda mais drástica nos países que poderiam ser qualificados como de médio e baixo desenvolvimentos tecnológico. Nesses casos o poder repressivo estatal se torna presa fácil do crime, a estabelecer um sucesso quase que total do empreendimento e um potencial de controle praticamente inexistente.” BECK, Francis Rafael. **Perspectivas de controle ao crime organizado e crítica à flexibilização das garantias**: São Paulo. IBCCrim, 2004. p. 82

<sup>137</sup>“The use of technology in the commission of crime presents significant challenges to government and law enforcement. Traditional criminal laws are ill-suited to deal with these challenges, and the rapid pace of technological change continually threatens to outpace efforts at regulation.” CLOUGH, Jonathan. **Cybercrime**: Sydney. Commonwealth Law Bulletin, vol. 37, nº 4, December 2011, 671-680. pág. 671. Disponível em <https://heinonline.org/HOL/LandingPage?handle=hein.journals/commwlb37&div=61&id=&page=>. Acesso em 15.12.2021

**Em livre tradução:** O uso de tecnologia na prática do crime apresenta desafios significativos para o governo e a aplicação da lei. As leis criminais tradicionais são inadequadas para lidar com esses desafios, e o ritmo acelerado das mudanças tecnológicas ameaça continuamente ultrapassar os esforços de regulamentação.

<sup>138</sup>“Dentro del ámbito de la investigación penal, el recurso a medidas de investigación secretas se ha incrementado exponencialmente y aparece aquí la tensión, presente en todo el ámbito de la justicia penal entre el respeto de los derechos individuales y el interés público de garantizar la seguridad pública.” WINTER, Lorena Bachmaier. **Investigación criminal y protección de la privacidad en la doctrina del Tribunal Europeo de Derechos Humanos**. In: 2º Congresso de Investigação Científica: Coimbra. Almedina, 2010. p. 163.

criminalística e dos demais saberes forenses disponíveis. Trata-se, portanto, de método histórico que tem por premissa o delito já ocorrido, partindo da análise do resultado para o momento da sua execução<sup>139</sup>.

Durante as análises, o investigador utiliza-se de um processo lógico-dedutivo e vale-se de elementos soltos, aparentemente desconexos, para localizar e aglutinar peças que juntas compõem o mosaico do delito consumado, identificando o amálgama que une tais peças e assim atingindo um “construído jurídico”, objetivo da investigação<sup>140</sup>. Esse processo ocorre em circuito fechado, pois não cria conhecimento novo, apenas identifica e organiza a informação obtida, utilizando os conhecimentos técnicos e o recurso tecnológico disponível que auxiliam na composição desse mosaico.

Esse método investigativo, que se baseia em uma visão retrospectiva da realidade, surte efeito e é de grande valia quando se trata de criminalidade comum, pois a conduta criminosa é realizada por meio de um ato comissivo ou omissivo que interage com o mundo exterior. Altera-se, assim, uma ordem estabelecida em que se evidencia um conjunto indiciário a ser observado pelo investigador, que é capaz de desvendar os contornos do crime cometido<sup>141</sup> por meio da análise pretérita dos casos.

O fenómeno da criminalidade organizada se delinea por traços e formas diferentes da criminalidade comum, unitária, celular, para a qual o nosso ordenamento jurídico penal foi projetado. A formação e o funcionamento de uma organização criminosa, por vezes, se constituem de uma série de atos jurídicos absolutamente inócuos na seara penal quando analisados *per si*, mas que são realçados quando encadeados, formando uma engrenagem complexa que, posta em movimento, é capaz de atingir uma infinidade de bens jurídicos tutelados penalmente.

---

<sup>139</sup>“A separação das águas passava, assim, pela fronteira do *tempo*: a justiça criminal (repressão) orientava-se para o *passado*; a polícia (prevenção) para o *futuro*.” ANDRADE, Manuel da Costa. **Bruscamente no Verão Passado**. Coimbra: Coimbra Editora, 2009. p. 129.

<sup>140</sup>“Trata-se, na verdade, não só da reunião de todos os princípios e critérios jurídicos-constitucionais que presidem à investigação criminal, mas da conjugação entre as necessidades de uma atividade de investigação e o seu objetivo que é um “construído jurídico” e não um mero dado no plano do ser.” PALMA, Maria Fernanda. **Introdução ao Direito da Investigação Criminal e da Prova**. In **Direito da Investigação Criminal e da Prova**. Coimbra: Almedina, 2014, pág. 16

<sup>141</sup>“Partindo do princípio que o acto criminoso sempre se revelará através de uma ação ou omissão, que interage inexoravelmente com o mundo exterior, alterando sempre uma ordem pré-existente, este modelo de investigação, mantém uma inquestionável e absoluta validade, sobretudo na investigação da criminalidade comum ou de massas, quando o objetivo é investigar uma ação criminosa isolada, perscrutar o passado e conseguir ver a árvore para lá da *neblina*.” BRAZ, José. **Ciência, Tecnologia e Investigação Criminal. Interdependências e Limites num Estado de Direito Democrático**. Coimbra: Almedina, 2015. p. 418.

Some-se a isso o fato de que essa engrenagem não consegue ser vislumbrada à primeira vista. Demandam-se tempo, conhecimento técnico-especializado e equipamentos tecnológicos próprios à identificação e verificação de seu funcionamento<sup>142</sup>.

A suspeita da existência de uma organização criminosa por trás de um crime comum, que nasce com a investigação por meio do método dedutivo clássico, pode ser o indício de uma rede de crimes com múltiplas ramificações que exige paciência e utilização de instrumental adequado para ser completamente desconstruída pelos aparelhos coercitivos do Estado.

Quando se inicia a investigação de uma organização criminosa, não basta apenas olhar para o passado, apurar materialidade e autoria dos crimes já praticados e submetê-los ao devido processo legal. Ao mesmo tempo, é necessário olhar para o futuro, visando mapear os lugares onde a organização poderá vir a agir, enquanto se desenrola a investigação referente aos fatos consumados<sup>143</sup>.

Esse olhar para o futuro é fundamental, pois apurar os delitos pretéritos pode não fazer cessar as atividades criminosas da organização. Ainda que os autores dos delitos praticados venham a ser identificados e punidos, é possível que a organização continue a operar sem risco de solução de continuidade das suas práticas delitivas.

Analisar o funcionamento da organização criminosa, observar sua movimentação e lançar a investigação para o futuro significa subverter a metodologia da investigação criminal. Foca-se, assim, no conjunto das suas práticas, e não mais em um ato particular, observando-se a organização como um todo e não apenas um autor isolado que pratica o crime.

O objetivo passa a ser também olhar para o presente e o futuro, objetivando conhecer em tempo real o que está acontecendo, como a organização criminosa está operando no

---

<sup>142</sup>“A investigação e punição da criminalidade organizada apresentam, pelas razões subjacentes às suas características e pela crescente complexidade das condutas a opacidade quase intransponível das máquinas organizativas, sérias dificuldades. Na verdade, tendo em conta o desenvolvimento científico tecnológico com repercussão no contexto da criminalidade organizada, o seu combate requer e exige a necessidade de uma especialização laboral técnica e científica, por parte dos órgãos de investigação criminal, muito aprofundada sob pena de algumas actividades criminosas se revelarem insindicáveis.” BRANCO, José António. **Criminalidade Organizada, Instrumentos e Mecanismos Legais de Investigação e Recuperação de Activos. “Uma Breve Incursão”**. In *Terra de Lei*, nº 2. Lisboa: Vigaprintes, 2012. p. 54

<sup>143</sup>“Utilizando a analogia proposta, o essencial na investigação do crime organizado é ver a *floresta*, para lá da *neblina*, e não apenas as *árvores*, que a constituem, sendo certo que, não é possível perceber e caracterizar a *floresta*, sem conhecer as *árvores* que lhe dão forma.” BRAZ, José. **Ciência, Tecnologia e Investigação Criminal. Interdependências e Limites num Estado de Direito Democrático**. Coimbra: Almedina, 2015. p. 419.

presente e, ao mesmo tempo, prospectar o futuro, antecipando ações criminosas possíveis e também estratégias que impeçam a consumação<sup>144</sup> dessas práticas.

A investigação criminal, além de ser instrumental do Processo Penal, operando com a finalidade de coletar provas para instruir o processo penal a ser instaurado ou já em curso; pode também ser preventiva, cujo olhar se destina a proteção das vítimas e da sociedade, visando minimizar os riscos e, se possível, evitar que o delito venha a se consumir.<sup>145</sup>

Além de diferenciar as duas possibilidades de investigação criminal – preventiva e instrumental do processo - é importante fazer a distinção entre inteligência e investigação indutiva. Ambas direcionam-se para o futuro, mas não se confundem. Na inteligência, produz-se conhecimento sem necessariamente estar ligado previamente a uma atividade criminosa, basta que, a partir de uma decisão política de segurança pública, compreenda-se a necessidade do monitoramento das atividades delitivas.

O conhecimento é produzido com base em pessoas ou organizações que não apresentam necessariamente algum interesse para o ordenamento penal, mas que no futuro, por causa desse conhecimento, podem vir a ser úteis, caso se identifique a probabilidade do cometimento de um delito ou se identifique a existência de uma organização criminosa.

Já na investigação, utilizando-se do método indutivo, todo conhecimento produzido é direcionado para uma atividade criminosa em curso, na apuração de um crime que está acontecendo ou que possa vir a acontecer<sup>146</sup>. No caso da organização criminosa, não basta ter

---

<sup>144</sup>“Numa tomada de posição naturalmente provisória e a benefício de uma mais aturada reflexão, parece-nos dever acompanhar-se, ainda aqui, a solução proposta pelo Tribunal Constitucional alemão (27.07.2005). Que, privilegiando um critério *material* ou de *fim*, aponta para uma arrumação quadripartida, dividindo as investigações de campo avançado em duas novas categorias colocadas ao lado das tradicionais. Apodando-se, respectivamente, de *providência para a perseguição (futura) de crimes (Vorsorge für die Verfolgung von Straftaten)* e *combate preventivo ao crime (vorbeugende Bekämpfung von Straftaten)*.” ANDRADE, Manuel da Costa. **Bruscamente no Verão Passado**. Coimbra: Coimbra Editora, 2009. p. 131.

<sup>145</sup>“Mas há uma distinção entre investigação preventiva e investigação instrumental do processo. Enquanto a primeira está subordinada ao interesse fundamental de proteção de vítimas e de bens jurídicos e, por isso, a lógica investigatória deve ser orientada por um ponderação generosa em favor das vítimas (...), na investigação criminal processualmente orientada, tona-se crucial a ponderação entre o valor constitucional da verdade para a realização da justiça e os direitos afetados das pessoas sujeitas à investigação...” PALMA, Maria Fernanda. **Introdução ao Direito da Investigação Criminal e da Prova**. In **Direito da Investigação Criminal e da Prova**. Coimbra: Almedina, 2014, pág. 16

<sup>146</sup>“No caso específico das organizações criminosas, a Inteligência pode ser empregada em diversos crimes como: tráfico, contrabando, jogo, prostituição, roubo de carga etc. É possível identificar pelo menos quatro aplicações para as informações produzidas pelo setor de Inteligência: 1.Prever tendências – identificar os próximos desdobramentos do crime, ou seja, para onde ele vai migrar, qual o tipo de crime que será a próxima moda etc. 2.Identificar as lideranças e os elementos-chave das organizações criminosas. 3.Monitorar a movimentação cotidiana da organização para identificar sua rotina. 4.Identificar pontos fracos e informantes em potencial.” MINGARDI, Guaracy. **O trabalho da inteligência no controle do crime organizado**. **Estudos Avançados**, v. 21, n. 61. p. 55. 2007. Disponível em: <https://www.revistas.usp.br/eav/article/view/10266/11898>. Acesso em:

conhecimento a respeito dos fatos delituosos que ela já praticou, pois isso não é suficiente para fazer cessar a atividade criminosa.

É preciso, além disso, investigar o que a organização criminosa continua fazendo, como pretende agir e, a partir dessas informações, impedir o prosseguimento das suas ações. Tal atividade é investigativa, pois está direcionada para um sujeito específico, no caso uma organização criminosa. Já a inteligência tem por finalidade coletar dados e notícias que possam impactar a segurança pública, sem que tais elementos estejam ligados a alguma atividade criminosa especificamente.

Destaca-se que não se propõe o abandono ou substituição do método clássico, dedutivo, porém a possibilidade de uso do método indutivo. Ambos devem ser operacionalizados conjuntamente, ou seja, enquanto se apura e investiga os fatos já cometidos, também se analisa como a organização está funcionando e como ela é capaz de vir a agir<sup>147</sup>.

Os atos diários de uma organização criminosa podem ser indiferentes penais que não reclamariam uma atenção do ordenamento penal, muito menos justificariam o início de uma investigação quando analisados sob a ótica do modelo dedutivo. Seguindo a dinâmica tradicional, os atos futuros poderiam vir a ser objeto de análise pela inteligência criminal, mas não por investigadores criminais.

Como esses atos se relacionam a uma empresa criminosa já em andamento, eles também não interessam à inteligência criminal, pois, como visto, os resultados que a inteligência criminal produz têm apenas valor opinativo, não se prendendo, inclusive, aos rigores e limites legais para obtenção dos dados e produção de conhecimento. Diversamente, a investigação criminal é balizada pelo Processo Penal e suas regras, não sendo de livre exercício pelo Estado.<sup>148</sup>

---

24/08/17.

<sup>147</sup>“...os dois modelos assinalados não são antagônicos, nem exigem de modo algum, caminhos estanques e alternativos: a investigação da criminalidade organizada exigirá sempre o recurso aos dois modelos, num quadro de profunda interação e complementariedade sistêmica.” BRAZ, José. **Ciência, Tecnologia e Investigação Criminal. Interdependências e Limites num Estado de Direito Democrático**. Coimbra: Almedina, 2015. p. 419.

<sup>148</sup>“...a investigação criminal é um poder limitado do Estado no seu relacionamento com cidadãos livres, é um poder instrumental do Processo Penal e da proteção de bens jurídico-penalmente relevantes e não uma atividade livre inserida nos objetivos do Estado.” PALMA, Maria Fernanda. **Introdução ao Direito da Investigação Criminal e da Prova**. In **Direito da Investigação Criminal e da Prova**. Coimbra: Almedina, 2014, pág. 15

Os conhecimentos produzidos pela inteligência criminal não servem, por isso, como prova, pois não podem ingressar no processo penal, uma vez que não se enquadraram nos limites estabelecidos pelo ordenamento processual penal para produção de provas<sup>149</sup>.

A adoção do método indutivo implica na previsão de novos métodos de produção de prova e na utilização de instrumentos legais específicos que autorizem a obtenção de prova de fatos ainda por acontecer. O ordenamento estaria assim regulando um método de obtenção de prova, referente a um possível fato criminoso cuja realização ainda não é certa. Ou seja, regula-se a investigação preventiva e autoriza-se o início da investigação, com a consequente possibilidade de produção de prova de um fato criminoso que ainda não se iniciou, cuja consumação pode estar distante, e que poderá não vir a se iniciar<sup>150</sup>.

Caso o fato criminoso possível de acontecer se realize, o investigador, em uma clara atividade de prospecção, faz prévio uso das ferramentas disponíveis para registro do ato ilícito, obtendo a prova necessária tanto para a responsabilização por aquele fato, se ele for de *per si* criminoso, como pela possibilidade de preencher algum dos requisitos da empresa criminosa, a partir daquela conduta.

O uso de métodos específicos, diferenciados, em regra mais constritivos de direitos, invadem ainda mais a privacidade do indivíduo, e tensionam com o limite constitucional estabelecido sobre garantias dos direitos fundamentais. Necessita-se de autorização legislativa para sua admissibilidade e controle judicial no momento da sua utilização.

As novidades tecnológicas, os novos e sofisticados equipamentos que surgem diariamente, a presença da Internet como um ambiente de uso diário quase que obrigatório, criam o cenário ideal para o funcionamento da criminalidade organizada, porque o crime envereda por ambientes pouco regulados, inclusive, transfronteiriços que ultrapassam delimitações formais estabelecidas de atuação, facilitando, sobretudo, o escamoteamento de

---

<sup>149</sup>“...o trabalho de Inteligência é muito mais opinativo do que o tradicionalmente feito pela polícia judiciária (...) Num inquérito, o delegado ou promotor trabalha casos individuais e necessita de provas. A informação por eles buscada tem de ter utilidade imediata, pois é visto como parte de uma investigação em curso. Os resultados da Inteligência, todavia, são de prazo mais longo e, na maioria das vezes, não servem como prova. Portanto, quanto mais separação houver entre a área operacional e a de Inteligência, melhor.” MINGARDI, Guaracy. O trabalho da inteligência no controle do crime organizado. **Estudos Avançados**, v. 21, n. 61, p. 55, 2007. Disponível em: <https://www.revistas.usp.br/eav/article/view/10266/11898>. Acesso em: 24/08/17.

<sup>150</sup>“A investigação criminal tem lugar logo que haja notícia de um crime ou de um processo criminoso em curso, mesmo que esteja longe da consumação.” PALMA, Maria Fernanda. **Introdução ao Direito da Investigação Criminal e da Prova**. In **Direito da Investigação Criminal e da Prova**. Coimbra: Almedina, 2014, pág. 16

atividades ilícitas e a autoria de práticas criminosas<sup>151</sup>.

### 3.2 O FÁCIL ACESSO ÀS TECNOLOGIAS DA INFORMAÇÃO

O uso das tecnologias da informação disponíveis se expande em velocidade vertiginosa, e aquele que não possui um aparelho telemóvel, especialmente um *smartphone*, está alijado da experiência integral da comunicação<sup>152</sup>. Grande parte dos dados pessoais relevantes e confidenciais encontram-se, muitas vezes, arquivados em ficheiros, sejam eles físicos ou virtuais<sup>153</sup>, que podem ser acessados por dispositivos informáticos convencionais (PC) e por telemóveis que apresentam tecnologia compatível.

Dentro da vastidão de possibilidades que a informática trouxe ao quotidiano, talvez sua maior inovação tenha sido a reinvenção da comunicação entre as pessoas. Os aplicativos próprios para comunicação instalados em *smartphones* modificaram hábitos, criaram novas regras de convívio social, reduziram a comunicação a textos de mensagens que pululam nas telas e fixam os olhares em pequenas caixinhas, restringindo o contacto visual, limitando a observação do mundo ao que é enviado e recebido por mensagem.

---

<sup>151</sup>“Assim, pouco tempo após a sua disponibilização, o *Tor* viu surgir diversos *websites* secretos, designados de *hidden services*, dedicados a todo o tipo de criminalidade. Começaram, então, a aparecer verdadeiros mercados de droga, documentos falsos e outros materiais ilícitos, como o célebre *The Silk Road* no qual as transações são feitas com recurso a *bitcoins*, ou o mercado de drogas, armas e explosivos chamado *Black Market Reloaded*. Adicionalmente, surgiram mercados *online* dedicados à venda de pornografia infantil ou mesmo de espécies em vias de extinção, bem como inúmeras páginas e fóruns de pornografia infantil e/ou violenta, bem como fóruns dedicados ao canibalismo, fóruns *ihadistas* e páginas que comercializavam dados relativos a cartões de crédito obtido através de quem os sistemas de *phishing*.” RAMALHO, David Silva. **A Investigação Criminal na Dark Web In Revista de Concorrência e Regulação**:Coimbra, a.4 n.14-15 (p.385 a 429), abr.-set. 2013, p.392/393

<sup>152</sup> “Não obstante todas as suas contradições, a revolução informética pode revelar-se como fator de inclusão, permitindo uma participação (mais) activa e informada dos cidadãos na discussão das opções políticas e sociais relevantes, dando expressão a uma cidadania global.” SANTOS, Cristina Máximo dos. **As Novas Tecnologias da Informação e o Sigilo das Telecomunicações In Revista do Ministério Público**: Lisboa, Ano 25º, nº 99, (p.89 a 116), julho-setembro 2004, P.116

<sup>153</sup> “Cloud users may run, typically via web browsers, application software installed on remote servers which sends results to user over the Internet. This means that relatively simple devices, such as mobile phones or tablets, may be used to obtain access to vast computational resources.” MILLARD, Christopher. **Cloud Computing Law**: Oxford. Oxford University Press p.4. Disponível em [https://www.researchgate.net/profile/Christopher-Millard-2/publication/269037199\\_Cloud\\_Computing\\_Law/links/5531016d0cf2f2a588ab843b/Cloud-Computing-Law.pdf](https://www.researchgate.net/profile/Christopher-Millard-2/publication/269037199_Cloud_Computing_Law/links/5531016d0cf2f2a588ab843b/Cloud-Computing-Law.pdf). Acesso em 21/09/2021

**Em livre tradução**: Os usuários da nuvem podem executar, normalmente por meio de navegadores da web, softwares aplicativos instalados em servidores remotos que enviam os resultados ao usuário pela Internet. Isso significa que dispositivos relativamente simples, como telefones celulares ou tablets, podem ser usados para obter acesso a vastos recursos computacionais

As mensagens e notícias veiculadas trazem uma sensação de urgência, de necessidade de leitura imediata e pronta resposta, exigindo atenção do usuário do aplicativo às informações exibidas na tela, em total desprestígio aos fatos da vida que estão acontecendo a sua volta naquele exato momento.

Nesse panorama, as conversas começam a rarear, as pessoas estão próximas fisicamente mas não se veem. Ligações telefônicas passaram a ser raras e obsoletas, sendo muitas vezes consideradas inconvenientes e enfadonhas. Essa alteração no comportamento da sociedade obviamente impacta a maneira como os crimes são praticados, tendo em vista os novos veículos que seus autores agora têm à sua disposição para prática e ocultação dos seus efeitos.

Alie-se a possibilidade da computação em nuvens (*cloud*)<sup>154</sup> onde é possível armazenar dados, aplicativos, softwares para rápido acesso, remotamente e por várias pessoas. Tal recurso já também foi recrutado para a prática de delitos, inclusive com a utilização de *malware* para o roubo de senhas de acesso a sistemas bancários<sup>155</sup>

A interceção telefônica, apesar de ainda ser um relevante método na produção de prova, cada dia perde mais espaço e importância, tendo em vista a possibilidade de

---

<sup>154</sup>“Although there is no definitive definition for cloud computing, a definition that is commonly accepted is provided by the United States National Institute of Standards and Technologies (NIST): *Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.*” PEARSON, Siani. **Privacy, Security and Trust in Cloud Computing** *In Privacy and Security for Cloud Computing*. Londres: Ed. Springer, 2013 p.3

**Em livre tradução:** Embora não haja uma definição definitiva para a computação em nuvem, uma definição comumente aceita é fornecida pelo Instituto Nacional de Padrões e Tecnologias (NIST) dos Estados Unidos: A computação em nuvem é um modelo que permite o acesso onipresente, conveniente e sob demanda à uma rede compartilhada de um conjunto configurável de recursos de computação (por exemplo, redes, servidores, armazenamento, aplicativos e serviços) que podem ser rapidamente provisionados e liberados com o mínimo de esforço de gerenciamento ou interação com o provedor de serviços.

<sup>155</sup>“Characteristic for cloud computing is fast access to numerous virtual machines within a very short time frame. This attracts not only legally acting enterprises or organizations but also individuals and organizations with more malicious intent. It has never been easier for an attacker to get legal access to a high-performance computing environment. Amazon’s cloud was already used to host malware (e.g. Trojans). Also, the Zeus botnet (a phishing Trojan that steals banking information) was known to be hosted on virtual machines within the Amazon cloud.” DOELITZSCHER, Frank; REICH, Christoph; KNAHL, Martin e CLARKE, Nathan. **Understanding Cloud Audits** *In Privacy and Security for Cloud Computing*. Londres: Ed. Springer, 2013 p.133

**Em livre tradução:** A característica da computação em nuvem é o acesso rápido a várias máquinas virtuais em um período de tempo muito curto. Isso atrai não apenas empresas ou organizações que atuam legalmente, mas também indivíduos e organizações com intenções maliciosas. Nunca foi tão fácil para um invasor obter acesso legal a um ambiente de computação de alto desempenho. A nuvem da Amazon já foi usada para hospedar *malware* (por exemplo, cavalos de Tróia). Além disso, o botnet Zeus (um cavalo de Troia de *phishing* que rouba informações bancárias) era conhecido por estar hospedado em máquinas virtuais dentro da nuvem da Amazon.

comunicação via aplicativo instalado em *smartphone*, opção atualmente mais utilizada para implementar a comunicação. Analogamente ao que acontece com as comunicações feitas via telefonia, é imprescindível a interceção da comunicação que ocorre via aplicativo, que se trata de um *software* instalado em aparelho, o *smartphone*, que conjuga tecnologia apta a transmitir ligação telefônica e dados em tempo real.

Essa grande concentração de dados pessoais em equipamentos informáticos e disponibilizados em rede podendo ser acessados remotamente e a qualquer tempo, constitui fértil manancial, que tanto pode ser utilizado para facilitar a vida do usuário, como para permitir a vigilância do indivíduo seja pelo Estado<sup>156</sup>, assim assumido apenas pelos governos de cariz autoritários, seja pelos integrantes de organização criminosa que transitam em espaço virtual<sup>157</sup>.

Em sede de direito penal, interessa, em certa medida, o estudo dos dispositivos mencionados, pois podem ser utilizados para a prática de delitos, armazenando informações importantes que podem servir para a formação de prova em processos criminais. Assim, a realização de buscas *on-line* tanto podem se dar em equipamentos informáticos fixos, como nos portáteis.

A informática, especialmente a Internet<sup>158</sup>, fez surgir uma nova relação de tempo e

---

<sup>156</sup> “Chinese citizens are also monitored and tracked online. While this is true for most and possibly all citizens of every country, the monitoring is more transparent in the sense that everyone knows it is happening very extensively. In China all non-commercial websites, including blogs, must be registered, and the sites’ developers or owners must provide their identities. Similar identity registration regulations apply to individuals who engage in microblogging, using platforms such as Weibo, a Chinese equivalent of Twitter, and QQ, a Facebook-like social media platform” BARTOW, Ann. **Privacy Laws and Privacy Levers: Online Surveillance Versus Privacy Laws and Privacy Levers: Online Surveillance Versus Economic Development in the People’s Republic of China**: 74 Ohio St. L.J. 853. Pace Law Faculty Publications, 2013. p. 868. Disponível em <http://digitalcommons.pace.edu/lawfaculty/922>. Acesso em 02/09/2021

**Em livre tradução:** Os cidadãos chineses também são monitorados e rastreados online. Embora isso seja verdade para a maioria e possivelmente todos os cidadãos de todos os países, o monitoramento é mais transparente no sentido de que todos sabem que está acontecendo de forma muito extensa. Na China, todos os sites não comerciais, incluindo blogs, devem ser registrados, e os desenvolvedores ou proprietários dos sites devem fornecer suas identidades. Regulamentos de registro de identidade semelhantes se aplicam a indivíduos que se envolvem em microblogging, usando plataformas como Weibo, um equivalente chinês de Twitter e QQ, uma plataforma de mídia social semelhante ao Facebook

<sup>157</sup> “Cyber espionage, the use of computers and networks to steal information, is not limited to nation-states that are in conflict. Business competitors, stock speculators, sports franchises, and employees may be motivated to spy on each other.” STIENNON, Richard. **Surviving Cyber War**: Lanham. The Scarecrow Press, 2010. pág. 19 **Em livre tradução:** A espionagem cibernética, o uso de computadores e redes para roubar informações, não se limita a estados-nações que estão em conflito. Concorrentes comerciais, especuladores de ações, franquias desportivas e funcionários podem ser motivados a espionar uns aos outros.

<sup>158</sup> “Internet viene perciò comunemente definita come la “rete delle reti”, o come un “accordo internazionale aperto di reti interconnesse, che rende possibile il collegamento diretto da *computer* a *computer* attraverso la volontaria adesione as uno *standard* di protocolli e procedure aperto”. Questa struttura “anarchica” pone el sistema giuridico vigente problemi analoghi a quelli che normalmente esso è chiamato a risolvere

espaço. A partir da invenção do espaço virtual, o seu estudo se tornou imprescindível, pois as novas dinâmicas dessas grandezas físicas criam um novo ambiente, que não se apresenta de forma única<sup>159</sup>, onde a prática de determinados crimes pode ocorrer de formas pouco convencionais, bem como pode ser volátil e incerto o *locus* de guarda e recolha de material probatório referente à prática de delitos que tenham ou não ocorrido em ambiente virtual<sup>160</sup>.

Para a análise de equipamentos de informática apreendidos, é importante a especialização e o treinamento adequado dos peritos e agentes encarregados da investigação, a fim de que estejam capacitados a identificar e extrair os conteúdos que interessam à persecução penal das máquinas periciadas. É preciso que sejam estabelecidos protocolos próprios, normas e rotinas para garantir a integridade dos dados, o sigilo das informações encontradas, especialmente aqueles que não guardem relação com o objeto da investigação<sup>161</sup>.

nell"individua zioni di precise responsabilità individuali all'interno di organizzazioni complesse." SIEBER, Ulrich. **Responsabilità Penali per la Circolazione di Dati nelle Reti Internazionali di Computer** In *Rivista Trimestrale di Diritto Penale dell'Economia*, anno X: Padova. Casa Editrice CEDAM, 1998. p.747

**Em tradução livre:** A Internet é, portanto, comumente definida como a "rede das redes" ou como um "acordo internacional aberto de redes interconectadas, que possibilita a conexão direta de computador a computador por meio da adesão voluntária a um padrão aberto de protocolos e procedimentos". Esta estrutura "anárquica" coloca ao ordenamento jurídico vigente problemas semelhantes aos que normalmente é chamado a resolver na identificação de responsabilidades individuais precisas em organizações complexas.

<sup>159</sup>“The word "Internet" is, perhaps surprisingly, also a collective noun. This fact is obscured because we tend to speak of "the" Internet; as a result it is very difficult not to think of it as a single entity. For the purposes of legal analysis, however, this single entity perspective is almost always misleading.” REED, Chris. **Internet Law Text and Materials**: Cambridge. Cambridge University Press, 2004. pág.7

**Em livre tradução:** A palavra "Internet" é, talvez surpreendentemente, também um substantivo coletivo. Esse fato é obscurecido porque tendemos a falar de "a" Internet; como resultado, é muito difícil não pensar que é uma entidade única. Para efeitos de análise jurídica, no entanto, esta perspectiva de entidade única é quase sempre enganosa.

<sup>160</sup>“Es decir, que, frente a la primera visión que ofrecía la criminalidad informática de ser una modalidad de delincuencia muy específica, relacionada con concretas tecnologías y con reducidos usos de la misma, hoy la única visión posible, por funcional, sobre la cibercriminalidad es la de una delincuencia amplia, variada y cambiante que ni puede asociarse a una concreta tecnología o a un específico grupo de sujetos, ni limitarse a un concreto sector de la actividad social. Por el contrario la cibercriminalidad es hoy toda la criminalidad cometida en el nuevo espacio, al igual que la delincuencia tradicional es toda la ejecutada en el viejo. **Es el lugar, en este caso el «no lugar», el que define y marca los eventos sociales** en él realizados y el que, por tanto, configura también como distinta la delincuencia en él ejecutada. Y es ese ámbito y su carácter novedoso y cambiante lo que puede explicar la anteriormente comentada sensación de «novedad perpetua» que parece asociada al cibercrimen y puede ayudar a comprender, además, el reto político criminal al que **nos enfrentamos: el de adaptar todas las estructuras políticas, jurídicas y sociales a la necesidad de protección de nuevos y viejos intereses frente a nuevas formas delictivas que son cambiantes porque lo sigue siendo el ámbito social en el que las mismas se producen.**”(destaques não presentes no original) LLINARES, Fernando Miró, **El Cibercrimen Fenomenología Y Criminología De La Delincuencia En El Ciberespacio**: Madrid. Marcial Pons, 2012. p.28

<sup>161</sup>“Asimismo, se enfrenta a problemas particulares, tales como los conocimientos exigibles a los agentes y peritos encargados de su obtención y análisis, la estandarización de normas, prácticas e protocolos que garanticen la integridad de los datos digitales obtenidos, o la continua evolución de la tecnología, y con ello, de los nuevos instrumentos, programas, formatos, capacidades, etc., todo lo cual aumenta el reto al que se enfrentan los peritos informáticos a la hora de analizar el *hardware* e el *software* para proceder a la recuperación de archivos, su descifrado, la identificación del usuario del equipo o de los intervinientes em una comunicación através de sistemas telemáticos, etc.” PRADILLO, Juan Carlos Ortiz. **“Hacking” legal al servicio de la**

O profissional do direito necessita se adequar a essa nova linguagem, conhecer e bem trabalhar os novos conceitos, assim como a legislação urge se modificar visando acompanhar os novos modos de praticar a atividade delitiva<sup>162</sup>, especialmente aquelas que se utilizam das novas tecnologias com fins à dissimulação do resultado do delito praticado<sup>163</sup>.

As técnicas de ciência forense se desenvolvem vertiginosamente, visando acompanhar as constantes modificações dos sistemas e técnicas de informática. Além disso, também integra o objeto de estudo da ciência forense, a possibilidade de utilização de

---

**investigación criminal:** nuevos instrumentos para la investigación y prueba de la delincuencia informática *in Delincuencia informática. Tiempos de cautela y amparo:* Cizur Menor (Espanha). Thomson Reuters Editorial Aranzadi, 2012. p. 185.

<sup>162</sup> “Significant concerns in this segment was created on the issue of the organization of the judicial system of the state towards creating conditions for successful combat and combat new forms of criminal activity. Specifically, whether to opt for a comprehensive systemic change, or change a number of regulations in order to create an adequate legal framework, or be oriented towards a partial amendment of certain legal provisions in order to create conditions for the timely and adequate response to new forms of criminal behaviour, that is the question each state has solved or is dealing in accordance with their capacities. The first method is without a doubt very effective, but also very demanding, since it requires a high degree of political and social consciousness of the necessity of changes that should be followed, while the second method is more economical and less demanding method, as it does not impinge on the basis of the system, but who can leave behind a series of unresolved issues such as the question of jurisdiction for certain crimes, the collision of new and existing legislation, and so on.” ZIROJEVIĆ, Mina. **Computer Related Crime – Offences Against The Confidentiality, Integrity, And Availability Of Computer Data And Systems** Disponível em [http://medial.naukaidrustvo.org/2015/07/zirojevic\\_computer\\_related\\_crime.pdf](http://medial.naukaidrustvo.org/2015/07/zirojevic_computer_related_crime.pdf). Acessado em 06/09/2021

**Em livre tradução:** Preocupações significativas neste segmento foram criadas na questão da organização do sistema judiciário do Estado no sentido de criar condições para o combate com êxito e combater as novas formas de atividade criminosa. Pode-se optar especificamente por uma mudança sistêmica abrangente ou alterar uma série de regulamentos a fim de criar um quadro jurídico adequado, ou ser orientado para uma alteração parcial de certas disposições legais a fim de criar condições para a resposta oportuna e adequada a novas formas de comportamento criminoso, assim cada Estado escolhe tratar a questão de acordo com suas capacidade. O primeiro método é sem dúvida muito eficaz, mas também muito exigente, visto que exige um elevado grau de consciência política e social da necessidade das mudanças a serem seguidas, enquanto que o segundo método é mais económico e menos exigente, visto que não interfere com a base do sistema, mas pode deixar várias questões sem solução, como a questão da jurisdição para certos crimes, a colisão de legislação nova com a existente, e assim por diante.

<sup>163</sup> “The federal computer fraud and abuse statute, 18 U.S.C. 1030, outlaws conduct that victimizes computer systems. It is a cyber security law. It protects federal computers, bank computers, and computers connected to the internet. It shields them from trespassing, threats, damage, espionage, and from being corruptly used as instrument of fraud. It is not a comprehensive provision, but instead it fills cracks and gaps in the protection afforded by other federal criminal laws. (...) the seven paragraphs of subsection 1030(a) outlaw:

(...) damaging a government computer, a bank computer, or a computer used in, or affecting, interstate or foreign commerce (e.g. a worm, computer virus, Trojan horse, time bomb, a denial of service attack, and other forms of cyber attack, cyber crime, or cyber terrorism), 18 U.S.C. 1030 (a)(5);” DOYLE, Charles. **Cybercrime: An Overview of The Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws.** Congressional Research Service, 2011. Disponível em <https://books.google.com.br/books?id=gu6epn6QeaMC&printsec=frontcover&hl=pt-BR&num=14#v=onepage&q&f=false>. Acesso em 24/09/2021

**Em livre tradução:** O estatuto federal de fraude e abuso de computador, 18 U.S.C. 1030, proíbe a conduta que vitima os sistemas de computador. É uma lei de segurança cibernética. Ele protege computadores federais, computadores bancários e computadores conectados à Internet. Ele os protege de invasão, ameaças, danos, espionagem e de serem usados de forma corrupta como instrumento de fraude. Não é uma disposição abrangente, mas em vez disso, preenche lacunas na proteção oferecida por outras leis criminais federais.(...)os sete parágrafos da subsecção 1030 (a) proíbem:

instrumentos ativos<sup>164</sup> na recolha de informações referentes à prática delitiva, tanto aquelas que se encontram armazenadas no próprio equipamento objeto da investigação, como aquelas que se encontram disponíveis na rede. As informações localizadas e recolhidas podem vir a ser úteis não só aos órgãos de investigação para apurar a prática e autoria do delito pretérito, como também podem ser úteis aos serviços de inteligência, facultada a utilização para prevenir a prática de futuras condutas criminosas<sup>165</sup>.

Os novos instrumentos colocados à disposição do Estado para fins de investigação, constituem-se em sofisticados equipamentos eletrónicos e programas informáticos, capazes de armazenar, acessar, monitorar e controlar remotamente o equipamento informático utilizado pelo investigado<sup>166</sup>. Tais recursos podem adotar diversas roupagens (*spyware*, *malware*, software malicioso, *badware*<sup>167</sup>), a depender do tipo de prova que se deseja produzir ou do crime cuja prática se pretenda evitar.

---

(...) danificar um computador do governo, um computador de banco ou um computador usado em, ou afetando, comércio interestadual ou estrangeiro (por exemplo, um *worm*, vírus de computador, cavalo de Tróia, *time bomb*, um ataque de negação de serviço e outras formas de ataque cibernético, crime cibernético ou terrorismo cibernético), 18 USC 1030 (a) (5); ”

<sup>164</sup>“The practical discipline of Forensic Computing has evolved over recent years to include pro-active involvement in the collection of intelligence relating to criminal, illegal and inappropriate computer behavior, particularly in relation to terrorist activities, organized crime syndicates and recidivist behavior.” HANNAN, Mathew. To revisit: What is forensic computing?. *In: Australian Computer, Network & Information Forensics Conference*. 2004. p. 103-111. Disponível em: <https://pdfs.semanticscholar.org/7fc8/d1c9d7fbdb7368685368954c24fc20139cc2>. Acessado em 23/08/17.

**Em livre tradução:** A disciplina prática de Computação Forense evoluiu nos últimos anos para incluir o envolvimento pró-ativo na coleta de inteligência relacionada ao comportamento criminoso, ilegal e inapropriado do computador, particularmente em relação a atividades terroristas, sindicatos do crime organizado e comportamento recorrente

<sup>165</sup>“Ahora incluye también instrumentos “activos” de búsqueda e recolección de todo tipo de información que, o bien se encuentra almacenada en determinados equipos informáticos, o bien se encuentra “circulando” (disponible) em la Red, y puede servir a los servicios de inteligencia e a las autoridades encargadas de la investigación criminal, para la prevención y descubrimiento de toda clases de delitos en los que las TICs juegan un papel importante en su preparación, ejecución u ocultación.” PRADILLO, Juan Carlos Ortiz. **“Hacking” legal al servicio de la investigación criminal: nuevos instrumentos para la investigación y prueba de la delincuencia informática in Delincuencia informática. Tiempos de cautela y amparo:** Cizur Menor (Espanha). Thomson Reuters Editorial Aranzadi, 2012. p. 185-186.

<sup>166</sup>“...capaces de conseguir la interceptación y la grabación em tiempo real de todos aquellos datos que transmitidos o recibidos a través de los distintos medios de comunicación (y tanto en lo referido al contenido propiamente dicho de las comunicaciones, como al resto de la información que llevan aparejada dichas comunicaciones, como por ejemplo, los datos de tráfico o los datos de localización), o incluso se encuentren almacenados en las unidades de memoria de dichos equipos...” PRADILLO, Juan Carlos Ortiz. **“Hacking” legal al servicio de la investigación criminal: nuevos instrumentos para la investigación y prueba de la delincuencia informática in Delincuencia informática. Tiempos de cautela y amparo:** Cizur Menor (Espanha): Thomson Reuters Editorial Aranzadi, 2012. p. 186.

<sup>167</sup>“Ya hace algunos años que distintos artificios informáticos, denominados “*spywares*”, programas espías, *malware*, software malicioso, *badware*, permiten inmiscuirse en datos almacenados en sistemas informáticos y en equipos de telefonía celular.” HAIRABEDIÁN, Maximiliano. **El Acceso a Información y Datos de Teléfonos Celulares.** *In: DUPUY, Daniela e KIEFER, Mariana. Cibercrimen.* Madrid: Editorial B de f, 2016. p. 470.

Importante destacar que a ideia de incrementar as possibilidades de investigação com mais este método de prova não significa dizer endurecimento da legislação penal nem subtração de direitos individuais. O escopo é apenas promover adequação do ordenamento penal às modernas tecnologias disponíveis para a prática de delitos cada vez mais complexos, refletindo a complexidade da própria sociedade.

Trata-se da tentativa de capacitar o Estado visando à obtenção de maior eficiência no combate ao crime organizado, pois ainda que se tolere a morosidade do poder legalmente constituído em apresentar respostas contundentes à criminalidade, essa vagareza deve ser o suficiente apenas para se verem efetivados os direitos e as garantias legais, mas não a ponto de inviabilizar a aplicação da lei penal<sup>168</sup>, nem causar a incómoda sensação de impunidade derivada da ineficiência estatal<sup>169</sup>.

### 3.3 O MALWARE

Chama-se *malware* o programa informático (*software*)<sup>170</sup> que é introduzido maliciosamente (*malicious*) em um determinado dispositivo eletrónico e que permite ao autor dessa intervenção a realização de diversas operações no sistema informático atingido,

<sup>168</sup>“É desnecessário enfatizar a enorme dificuldade com que as investigações se deparam na obtenção de elementos de prova digital, perante estes obstáculos legais. E, claro, sem possibilidade de obtenção desses elementos, é desnecessário referir o provável insucesso a que muitas destas investigações estão votadas. Acresce ainda referir a enorme volatilidade de todos os elementos de prova no ambiente digital, caracterizado pela enorme velocidade a que circulam os fluxos de informação.” VERDELHO, Pedro. **A Obtenção de Prova no Ambiente Digital** In *Revista do Ministério Público*: Lisboa, Ano 25º, nº 99, (p.117 a 136), julho-setembro 2004. p. 132

<sup>169</sup>“Ora, esta desconformidade – que haja uma desconformidade já vimos que é normal, o que é anormal é perceber que essa desconformidade ultrapassa a razoabilidade – entre o ataque e a resposta cria uma manifesta sensação de mal-estar aos homens e às mulheres desta contemporaneidade.” COSTA, José de Faria, **Direito Penal e Globalização**. Coimbra: Wolters Kluwer Portugal sob a marca Coimbra Editora, 2010. p. 47.

<sup>170</sup>“In recent years, we have been witnessing a rapid evolution of dangerous programs – the so-called “malware”. I’m referring to hardware and software capable of obtaining user data for advertising purposes or for commercial activities.” MANGIAMELI, Agata C. Amato. **Theory of Law and Computer Crimes – Teoria do Direito e Crimes Informáticos**” *Duc In Altum-Cadernos de Direito* v. 8, n.16, set-dez 2016,(2017). p. 6. Disponível em: <http://www.faculadadedamas.edu.br/revistafd/index.php/cihjur/article/view/395/379>. Acesso em: 06/07/17. Pela definição aqui trazida, um hardware pode também ser um tipo de *malware*, entretanto não foi encontrado exemplo de hardware que pudesse ser considerado um *malware*, razão porque foi considerado no texto apenas software como possibilidade de caracterização de um *malware*.

Em livre tradução: “Nos últimos anos, temos assistido a uma rápida evolução de programas perigosos – os chamados “malware”. Refiro-me a hardware e software capazes de obter dados do usuário para fins publicitários ou para atividades comerciais.”

independentemente do consentimento e mesmo do conhecimento do seu usuário<sup>171 172 173</sup>.

Além dos programas informáticos que podem ser introduzidos insidiosamente no equipamento informativo visando seu monitoramento, ainda existe a figura do *cookie* que armazena dados do usuário ou visitante de determinado sítio eletrônico, podendo tais dados serem acessados pelo proprietário do sítio<sup>174</sup>. Tais dados ajudam a personalizar a visualização do sítio para cada usuário, individualizando sua experiência naquele ambiente virtual<sup>175</sup>. Os dados coletados e armazenados também podem ser usados para alimentar programas espões (*malware*), especialmente projetados para oferecimento de produtos específicos para consumo, e que podem ser inoculados maliciosamente no equipamento informático.<sup>176</sup>

---

<sup>171</sup>Para Davi Ramalho, *malware* "... inclui todo tipo de programas instalados sub-repticiamente por terceiros num sistema informático que podem ser utilizados para, de algum modo, comprometer as suas funções, contornar os seus controlos de acesso, causar prejuízo ao seu utilizador ou ao seu sistema informático infetado, monitorizar a sua atividade ou apropriar-se, corromper, eliminar e/ou alterar dados informáticos." RAMALHO, Davi Silva. O uso de *malware* como meio de obtenção de prova em processo penal. In **Revista de Concorrência e Regulação**. Coimbra: Almedina, Ano IV, número 16, outubro-dezembro 2013. p. 202.

<sup>172</sup> "Códigos maliciosos (*malware*) são programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computador. " Cartilha de Segurança para Internet do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT). Disponível em: <https://cartilha.cert.br/malware/#footnote003>. Acesso em: 19/09/2017

<sup>173</sup>"Códigos maliciosos, também conhecidos como pragas e *malware*, são programas desenvolvidos para executar ações danosas e atividades maliciosas em equipamentos, como computadores, modems, switches, roteadores e dispositivos móveis (tablets, celulares, smartphones, etc)." Fascículo Códigos Maliciosos In **Cartilha de Segurança para Internet**. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT). Disponível em: <https://cartilha.cert.br/fasciculos/codigos-maliciosos/fasciculo-codigos-maliciosos.pdf>. Acesso em 30.08.2021

<sup>174</sup> "os cookies, em geral, são pequenos trechos de texto acondicionados no browser ou navegador Web utilizado pelo usuário, usados para armazenar informações. É uma ferramenta para personalizar páginas Web e permitir que acessos futuros do usuário ao site sejam de modo personalizado, pois podem ser reativados quando o usuário retornar à página web, identificando informações outrora coletadas e serem aplicadas naquele momento de acesso." NETO, Mário Furlaneto; DO CARMO, Júlio César Lourenço; SCARMANHÃ Bruna de Oliveira da Silva Guesso. **Cookies: Vulnerabilidade do Direito à Privacidade nos Meios Digitais no Âmbito da Legislação Brasileira**. p.1501. Disponível em : [https://www.cidp.pt/revistas/rjlb/2018/4/2018\\_04\\_1491\\_1517.pdf](https://www.cidp.pt/revistas/rjlb/2018/4/2018_04_1491_1517.pdf). Acesso em 01.09.2021

<sup>175</sup>"A software program can transmit a tracer know as a "cookie" from a website to the user's computer. Cookies can take a variety forms may retain details relating to the user's actions, either for duration of a visit to a site or for a specified and potentially unlimited period of time." LLOYD, Ian J. **Information Technology Law**, 9.<sup>a</sup> ed. Oxford: Oxford University Press, 2020. p.13

**Em livre tradução:** Um programa de software pode transmitir um rastreador conhecido como "cookie" de um site para o computador do usuário. Os cookies podem assumir várias formas e podem reter detalhes relativos às ações do usuário, seja pela duração de uma visita a um site ou por um período de tempo especificado e potencialmente ilimitado

<sup>176</sup> "Desde quando criado pela Netscape, os cookies além de permitirem uma melhor interação servidor-navegador têm sido utilizados para "espionar os hábitos dos usuários na internet", permitindo assim ser traçado um perfil social, íntimo, preferencial e econômico." NETO, Mário Furlaneto; DO CARMO, Júlio César Lourenço; SCARMANHÃ Bruna de Oliveira da Silva Guesso. **Cookies: Vulnerabilidade do Direito à Privacidade nos Meios Digitais no Âmbito da Legislação Brasileira**. p.1507. Disponível em : [https://www.cidp.pt/revistas/rjlb/2018/4/2018\\_04\\_1491\\_1517.pdf](https://www.cidp.pt/revistas/rjlb/2018/4/2018_04_1491_1517.pdf). Acesso em 01.09.2021

A depender do tipo de programa inoculado, é possível monitorizar à distância a atividade de um determinado sistema informático, assim como levar o sistema atingido a executar ações que o inoculador do programa malicioso determine que ele faça, podendo tanto danificar ou controlar o dispositivo informático onde estiver instalado, como ainda corromper os dados armazenados em outros computadores que estiverem conectados em rede ao dispositivo infetado<sup>177</sup>. A ação do *malware* pode gerar prejuízos de difícil cálculo da sua extensão, seja em valores, seja em área de abrangência<sup>178</sup>.

<sup>177</sup>“Internet hosts - especially domestic homes computers – are often hacked by viruses or malware, and then used as ‘zombie hosts’ from which all kinds of evils can be perpetrated by remote control: deluges of spam and phishing emails, distributed denial of service (DDOS) attacks, the spreading of more viruses and malware, and even in the worst potential scenario, attacks on critical infrastructure as part of so-called ‘cyber-warfare’.” EDWARDS, Lilian. **The Fall an the Rise of Intermediary Liability Online** In EDWARDS, Lilian, WAELDE, Charlotte, **Law and the Internet**. Oxford/Portland: Hart Publishing, 2009

**Em livre tradução:** Hosts de Internet - especialmente computadores domésticos - são frequentemente hackeados por vírus ou *malware* e, em seguida, usados como 'hosts zumbis' dos quais todos os tipos de males podem ser perpetrados por controle remoto: dilúvios de spam e e-mails de phishing, ataques de negação de distribuição de serviço (DDOS), a propagação de mais vírus e *malware* e, mesmo no pior cenário potencial, ataques a infraestruturas críticas como parte da chamada 'guerra cibernética'

<sup>178</sup>“Cybercriminals often utilize malware to compromise computer systems and automate attacks against computer networks (Furnell, 2002). These programs can disrupt e-mail and network operations, access private files, delete or corrupt files, and generally damage computer software and hardware (Taylor et al., 2006). The dissemination of viruses across computer networks can be costly for several reasons, including the loss of data and copyrighted information, identity theft, loss of revenue due to customer apprehension about website safety, time spent removing the programs, and losses in personal productivity and system functions (Symantec, 2003; Taylor et al., 2006). This is reflected in the dollar losses associated with malware infection. U.S. companies who participated in a recent Computer Security Institute reported losses of approximately \$15 million because of viruses in 2006 alone (CSI, 2007). An infected system in one country can spread malicious software across the globe and cause even greater damage because of the interconnected nature of computer systems. The Melissa virus, for example, caused an estimated \$80 million in damages worldwide (Taylor et al., 2006). Thus, malware infection poses a significant threat to Internet users around the globe.” BOSSLER, Adam M., HOLT, Thomas J. **On-line Activities, Guardianship, and Malware Infection: An Examination of Routine Activities Theory** International Journal of Cyber Criminology (IJCC) January - June 2009, Vol 3 (1): 400–420. pág. 401. Disponível em [https://www.researchgate.net/publication/228929213\\_On-line\\_Activities\\_Guardianship\\_and\\_Malware\\_Infection\\_An\\_Examination\\_of\\_Routine\\_Activities\\_Theory](https://www.researchgate.net/publication/228929213_On-line_Activities_Guardianship_and_Malware_Infection_An_Examination_of_Routine_Activities_Theory).

Acesso em 15.12.2021

**Em livre tradução:** Os cibercriminosos costumam utilizar *malware* para comprometer sistemas de computador e automatizar ataques contra redes de computadores (Furnell, 2002). Esses programas podem interromper as operações de e-mail e rede, acessar arquivos privados, excluir ou corromper arquivos e, em geral, danificar o software e o hardware do computador (Taylor et al., 2006). A disseminação de vírus em redes de computador pode ser cara por vários motivos, incluindo perda de dados e informações protegidas por direitos autorais, roubo de identidade, perda de receita devido à apreensão do cliente sobre a segurança do site, tempo gasto removendo os programas e perdas na produtividade pessoal e no sistema funções (Symantec, 2003; Taylor et al., 2006). Isso se reflete nas perdas de dólares associadas à infeção por *malware*. Empresas norte-americanas que participaram de um recente Computer Security Institute relataram perdas de aproximadamente US\$15 milhões devido a vírus somente em 2006 (CSI, 2007). Um sistema infetado em um país pode espalhar software malicioso por todo o mundo e causar danos ainda maiores devido à natureza interconectada dos sistemas de computador. O vírus Melissa, por exemplo, causou cerca de US\$80 milhões em danos em todo o mundo (Taylor et al.,2006). Portanto, a infeção por *malware* representa uma ameaça significativa para os usuários da Internet em todo o mundo.

Os tipos de *malware* são variados e estão passando por constantes atualizações. Apesar do *Trojan horse* (cavalo de Tróia, *trojan* ou troiano) ser o tipo mais conhecido, há uma grande variedade de *malware* disponível para utilização em investigação criminal, como o *keylogger*, *spyware*, *logic bomb*, *rootkit* e ainda as ameaças mistas (*blended threats*<sup>179</sup>), em que mais de um tipo de programa malicioso pode ser usado de maneira combinada para obtenção de dados e produção de provas.

Caso a ideia seja a captação de senha, é provável que o *malware* escolhido seja um tipo de *keylogger*. Se a finalidade é interceptar a atividade do dispositivo em tempo real, pode ser utilizado um *spyware*. Todos são inoculados na rede via *trojan* ou vírus. Os criadores (*writers*) dos programas maliciosos têm aprimorado a linguagem e sofisticado os meios de ingresso e disseminação de *malware*, sendo necessário portanto advertir que a classificação aqui trazida pode se tornar em breve obsoleta.

O tipo mais comum, por isso mais popular, é o cavalo de Tróia. Foi programado, principalmente, para dar acesso ao sistema de arquivos do dispositivo infetado. Esse programa tem a função de alterar a configuração dos arquivos, roubar conteúdos e senhas, monitorar a atividade do usuário e de outros computadores que estiverem sendo operados em rede.

O nome “cavalo de Tróia” é uma referência à estória contada por Homero na obra *Odisseia*, na qual consta que um cavalo de madeira foi oferecido como presente pelos gregos aos troianos com a finalidade de encerrar a lendária Guerra de Tróia. O presente foi aceito e levado para dentro da cidade fortificada pelos próprios troianos. Depois, revelou-se uma grande armadilha ao possibilitar a abertura dos portões da cidade, resultando na destruição da principal estratégia de defesa dos troianos, ensejando na definitiva subjugação da cidade de Tróia.

---

<sup>179</sup>“Malicious code that is referred to as a blended threat is code that can replicate itself in more than one manner, can have more than one type of trigger, and can have multiple task capabilities. A blended threat is often able to move around the Internet using e-mails virus capabilities as well as worm capabilities. A blended threat attack can also plant a Trojan on a computer. The trigger can be set off by an e-mail program action or a Web surfing action. Malicious code writers have become sophisticated in blending the characteristics and capabilities of multiple threat types.” ERBSCHELO, Michael. **Trojans, Worms and Spyware**. A Computer Security Professional's Guide to Malicious Code. Burlington (USA): Elsevier Butterworth-Heinemann, 2005. p. 24-25

**Em livre tradução:** O código malicioso conhecido como ameaça combinada é um código que pode se replicar de mais de uma maneira, pode ter mais de um tipo de gatilho e pode ter vários recursos de tarefa. Uma ameaça combinada geralmente é capaz de se mover pela Internet usando recursos de vírus de e-mail, bem como recursos de worm. Um ataque de ameaça combinada também pode implantar um cavalo de Tróia em um computador. O gatilho pode ser ativado por uma ação de programa de e-mail ou uma ação de navegação na Web. Os criadores de códigos maliciosos tornaram-se sofisticados ao combinar as características e capacidades de vários tipos de ameaças.

Da mesma maneira, os atuais cavalos de Tróia (*Trojan horse*) são programas maliciosos (*malware*) capazes de ser instalados no dispositivo informático, disfarçados de programa comum e legítimo, servindo para abrir portas que permitam a invasão do sistema informático.

São programas que visam permitir que aquele que o disparou (inoculou) possa controlar o dispositivo informático do usuário remotamente, podendo a ele aceder ocultamente (*backdoor*<sup>180</sup>) e nele desenvolver uma série de tarefas à revelia dos interesses do usuário, tais como: remover, baixar, apagar, renomear e alterar registos de arquivos; extrair senhas e dados pessoais, desabilitar (ou habilitar) o microfone, câmera, teclado e demais periféricos; desligar ou reiniciar o dispositivo; colocar em funcionamento ou desabilitar determinados aplicativos; ingressar com registros de teclado como se o usuário estivesse pressionando as teclas; desabilitar antivírus ou algum programa de segurança operacional<sup>181</sup>.

Os “troianos” são aparentemente inofensivos. Podem estar escondidos no anexo de uma mensagem enviada por *e-mail*, em uma página da Internet contaminada com programa malicioso ou na falsa atualização de um *software* legítimo, apenas aguardando uma conduta voluntária do usuário do sistema para sua instalação. Assim, permite-se ao seu inoculador a abertura de portas, ou seja, o acesso a dados, dentro do sistema infetado. Diferentemente dos

---

<sup>180</sup>“Backdoor is a program that allows unauthorized access into your system, even without knowing your username and password. This program may represent a means for gain-ing emergency access to the system. The ‘backdoor’ is often installed by the system operators in order to allow recovery of a forgotten password. However, it could also be used by a computer expert who intends to unlawfully access the system.” MANGIAMELI, Agata C. Amato. **"Theory of Law and Computer Crimes – Teoria do Direito e Crimes Informáticos"** *Duc In Altum-Cadernos de Direito* v. 8, n.16, set-dez 2016,(2017). p. 6. Disponível em: <http://www.faculadadedamas.edu.br/revistafd/index.php/cihjur/article/view/395/379>. Acesso em: 06/07/17.

**Em livre tradução:** *Backdoor* é um programa que permite acesso desautorizado a um sistema informático, mesmo que não se conheça nome de usuário e senha. O *backdoor* é frequentemente instalado pelos operadores de sistema para um acesso de emergência, para permitir a recuperação de uma senha esquecida, entretanto, também pode ser usado por um especialista em informática para acessar ilegalmente um sistema.

<sup>181</sup> “Examples of what Trojans allow remote users controlling the Trojan to do include de following: remove files from the infect computer; download files to the infected computer; make registry changes to the infected computer; delete files on the infected computer; steal passwords and other confidential information; log keystrokes of the computer e user; rename files on the infected computer; disable a keyboard, mouse, or other peripherals; shut down or reboot in the infected computer; run selected applications or terminate open applications; disable virus protection or other computer security software.” ERBSCHELO, Michael. **Trojans, Worms and Spyware. A Computer Security Professional's Guide to Malicious Code.** Burlington (USA): Elsevier Butterworth-Heinemann, 2005. p. 22.

**Em livre tradução:** Exemplos do que os cavalos de Tróia permitem que os usuários remotos que controlam o cavalo de Troia façam incluem o seguinte: remover arquivos do computador infectado; baixar arquivos para o computador infectado; fazer alterações no registro do computador infectado; excluir arquivos no computador infectado; roubar senhas e outras informações confidenciais; registrar as teclas digitadas do computador e do usuário; renomear arquivos no computador infectado; desativar um teclado, mouse ou outros periféricos; desligar ou reiniciar no computador infectado; executar aplicativos selecionados ou encerrar aplicativos abertos; desative a proteção contra vírus ou outro software de segurança do computador.

vírus, eles não têm capacidade de autorreplicação<sup>182</sup>, e por isso afeta apenas o sistema onde foi instalado.

Quando o *malware* tem por finalidade rastrear os hábitos do usuário do dispositivo informático é chamado de *spyware*. Ele é projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros. Pode ser usado tanto de forma legítima quanto maliciosa, dependendo de como é instalado, das ações realizadas, do tipo de informação monitorada e do uso que é feito por quem recebe as informações coletadas.

Seu uso pode ser considerado legítimo quando instalado em um computador pessoal, pelo próprio dono ou com consentimento deste, com o objetivo de verificar se outras pessoas o estão utilizando de modo abusivo ou não autorizado. Por outra perspectiva, será considerado malicioso quando executa ações que podem comprometer a privacidade do usuário e a segurança do computador, como monitorar e capturar informações referentes à navegação do usuário ou inseridas em outros programas, por exemplo conta de usuário e senha.

Existem alguns tipos específicos de programas *spyware*, como o *keylogger*, capazes de capturar e armazenar as teclas digitadas pelo usuário no teclado do computador, extrair em tempo real informações como o nome do usuário, o endereço, a palavra-chave, códigos e senhas. Sua ativação, em muitos casos, é condicionada a uma ação prévia do usuário, como o acesso a um sítio específico de comércio eletrônico ou a um sítio de transações bancárias.

Ocorre também com programas como o *screenlogger*, que armazena a posição do cursor e a tela apresentada no monitor nos momentos em que o rato é clicado, ou a região que circunda a posição onde o rato é clicado. É bastante utilizado por atacantes para capturar as teclas digitadas pelos usuários em teclados virtuais, disponíveis principalmente em sítios de bancos.

Muitas empresas utilizam programas tipo *spyware*, visando mapear os interesses dos seus usuários, facilitando a oferta de produtos que atendam a necessidades específicas. As

---

<sup>182</sup>“Typically, a Trojan horse is used to send spam or steal personal data. In any case, it is a program which aims at taking control of a computer. It does not have the capacity of self-replication - so it requires the direct intervention of the aggressor in order to be spread. It can be concealed in the operating system folders.” MANGIAMELI, Agata C. Amato. "Theory of Law and Computer Crimes – Teoria do Direito e Crimes Informáticos" *Duc In Altum-Cadernos de Direito* v. 8, n.16, set-dez 2016,(2017). p. 23/24. Disponível em: [://www.faculadadedamas.edu.br/revistafd/index.php/cihjur/article/view/395/379](http://www.faculadadedamas.edu.br/revistafd/index.php/cihjur/article/view/395/379). Acesso em: 06/07/17.

**Em livre tradução:** Normalmente, um cavalo de Tróia é usado para enviar spam ou roubar dados pessoais. De qualquer forma, é um programa que visa assumir o controle de um computador. Não tem capacidade de autorreplicação - por isso requer a intervenção direta do agressor para se espalhar. Pode ser escondido nas pastas do sistema operacional

ofertas são anunciadas por um outro tipo de *malware*, o *adware*<sup>183</sup>, que funciona abrindo janelas com anúncios e ofertas de acordo com os hábitos daquele usuário enquanto utilizador da rede de Internet, independentemente da sua vontade.

Assim, pode existir uma combinação de *spyware* com *adware*, ou um mesmo programa combinando as duas funções. Ressalte-se que nem todo *adware* é também um *spyware*<sup>184</sup>. Pode ocorrer, portanto, a abertura automática de janelas sobrepostas àquela do interesse do utilizador, com conteúdo diverso daquele por ele propositadamente acessado, contendo conteúdo publicitário aleatório, sem necessariamente ter sido tal conteúdo apresentado de acordo com os hábitos daquele usuário.

Esse tipo de recurso publicitário, considerado lícito e amplamente utilizado, suscita debates a respeito de violação de segurança e privacidade do usuário, como será ainda abordado neste trabalho.

O *rootkit*<sup>185</sup> é um conjunto de programas e técnicas que permite esconder a presença de um invasor ou de outro código malicioso em um computador comprometido, e que pode ser usado para instalar outros códigos maliciosos, como *backdoors*, para assegurar o acesso futuro ao computador infetado; esconder atividades e informações, como arquivos, diretórios, processos, chaves de registro, conexões de rede; mapear potenciais vulnerabilidades em outros computadores, por meio de varreduras na rede; capturar informações da rede pela intercetação

---

<sup>183</sup>“**Adware:** projetado especificamente para apresentar propagandas. Pode ser usado para fins legítimos, quando incorporado a programas e serviços, como forma de patrocínio ou retorno financeiro para quem desenvolve programas livres ou presta serviços gratuitos. Também pode ser usado para fins maliciosos, quando as propagandas apresentadas são direcionadas, de acordo com a navegação do usuário e sem que este saiba que tal monitoramento está sendo feito.” Cartilha de Segurança para Internet do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT). Disponível em: <https://cartilha.cert.br/malware/#footnote003>. Acesso em: 19/09/2017.

<sup>184</sup>“There are two kinds of software programs that perform such actions: adware displays advertisements, and spyware goes further and tracks and reports on users’ web browsing, keystrokes or anything else that the author of the software has some interest in knowing. In reality, this means that software can be adware and spyware at the same time. However, not all adware is spyware and most spyware is not easily detected by displaying ads.” JACOBSSON, Andreas; BOLDT, Martin; CARLSSON, Bengt. Privacy-Invasive Software in Filesharing Tools. In: **Information Security Management, Education and Privacy**. Springer, Boston, MA, 2004. p. 281-296. Disponível em: [https://link.springer.com/content/pdf/10.1007%2F1-4020-8145-6\\_22.pdf](https://link.springer.com/content/pdf/10.1007%2F1-4020-8145-6_22.pdf). Acesso em: 12/09/17.

**Em livre tradução:** Existem dois tipos de programas de software que executam tais ações: o adware exhibe anúncios e o spyware vai além e rastreia e relata a navegação na web dos usuários, pressionamentos de tecla ou qualquer outra coisa que o autor do software tenha algum interesse em saber. Na realidade, isso significa que o software pode ser adware e spyware ao mesmo tempo. No entanto, nem todo adware é spyware e a maioria dos spywares não é facilmente detetada pela exibição de anúncios.

<sup>185</sup>“O termo *rootkit* origina-se da junção das palavras “*root*” (que corresponde à conta de superusuário ou administrador do computador em sistemas Unix) e “*kit*” (que corresponde ao conjunto de programas usados para manter os privilégios de acesso desta conta).” Cartilha de Segurança para Internet do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT). Disponível em: <https://cartilha.cert.br/malware/#footnote003>, Acesso em: 19/09/2017.

de tráfego onde o computador comprometido está localizado.

É importante ressaltar que o nome *rootkit* não indica que os programas e as técnicas que o compõe são usadas para obter acesso privilegiado a um computador, mas sim para mantê-lo. *Rootkits* inicialmente eram usados por violadores que, após invadirem um computador, instalavam-nos para manter o acesso privilegiado sem precisar recorrer novamente aos métodos utilizados na invasão, bem como para esconder suas atividades e/ou dos usuários do computador. Apesar de ainda serem bastante usados por invasores, os *rootkits* atualmente têm sido também utilizados e incorporados por outros códigos maliciosos para ficarem ocultos e não serem detetados pelo usuário e nem por mecanismos de proteção.

Vírus<sup>186</sup> <sup>187</sup> é um programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos. Para que possa tornar-se ativo e dar continuidade ao processo de infecção, o vírus depende da execução do programa ou arquivo hospedeiro, ou seja, é preciso que o programa onde o vírus foi inoculado seja executado, para que o vírus possa infectar todo o dispositivo informático.

Há diferentes tipos de vírus, sendo que alguns procuram permanecer ocultos, infectando arquivos do disco e executando uma série de atividades sem o conhecimento do usuário<sup>188</sup>. Há outros que permanecem inativos durante certos períodos, entrando em atividade

---

<sup>186</sup>“A virus is a computer program that initiates an action on a computer without the user's consent” ERBSCHELO, Michael. **Trojans, Worms and Spyware**. A Computer Security Professional's Guide to Malicious Code. Burlington (USA): Elsevier Butterworth-Heinemann, 2005. p. 18.

**Em livre tradução:** Um vírus é um programa de computador que inicia uma ação em um computador sem o consentimento do usuário

<sup>187</sup> “Virus is a program that can reproduce and spread itself, infecting files, networks, and other computers. A virus usually damages only the software of the computer, but it can also indirectly damage the hardware. Nowadays, their favorite vehicle of infection is represented by e-mails and peer-to-peer networks.” MANGIAMELI, Agata C. Amato. "Theory of Law and Computer Crimes – Teoria do Direito e Crimes Informáticos" *Duc In Altum-Cadernos de Direito* v. 8, n.16, set-dez 2016,(2017). p. 6. Disponível em: <<http://www.faculadadedamas.edu.br/revistafd/index.php/cihjur/article/view/395/379> pág. 24>. Acesso em: 06/07/17.

**Em livre tradução:** Vírus é um programa que pode se reproduzir e se espalhar, infectando arquivos, redes e outros computadores. Um vírus geralmente danifica apenas o software do computador, mas também pode danificar indiretamente o hardware. Hoje em dia, seu veículo favorito de infecção é representado por e-mails e redes peer-to-peer

<sup>188</sup> Exemplo trazido por Brenner: “In May of 2000, the “Love Bug” virus appeared on the Internet and spread around the world in two hours. It is estimated to have affected over forty-five million users in over twenty countries, and to have caused between two and ten billion dollars in damage.” BRENNER, Susan W. e KOOPS, Bert-Jaap. **Approaches to Cybercrime Jurisdiction**, *In Journal of High Technology Law*, vol. 4, 2005. disponível em [https://www.researchgate.net/publication/228198888\\_Approaches\\_to\\_Cybercrime\\_Jurisdiction](https://www.researchgate.net/publication/228198888_Approaches_to_Cybercrime_Jurisdiction). Acessado em 16.09.2021

**Em livre tradução:** Em maio de 2000, o vírus “Love Bug” apareceu na Internet e se espalhou pelo mundo em duas horas. Estima-se que afetou mais de quarenta e cinco milhões de usuários em mais de vinte países e causou

apenas em datas ou eventos específicos, com mecanismo idêntico às chamadas *logic bombs*<sup>189</sup>, sendo que estas não são replicativas.

O vírus pode ser enviado como anexo a um *e-mail*, cujo conteúdo visa induzir o usuário a executá-lo. Quando em execução, ele infecta outros arquivos e programas e envia cópias de si mesmo para os endereços de *e-mail* que estiverem na lista de contactos do usuário. Pode também se propagar de telemóvel para telemóvel, por meio da tecnologia *bluetooth* ou de mensagens MMS (*Multimedia Message Service*). A infeção ocorre quando um usuário permite o recebimento de um arquivo infectado e o executa. Após infectar o telemóvel, o vírus pode destruir ou sobrescrever arquivos, remover ou transmitir contactos da agenda, efetuar ligações telefônicas e drenar a carga da bateria, além de disseminar-se para outros telemóveis.<sup>190</sup>

Outra categoria de *malware*, que pode ser mais danosa do que um vírus, é o *worm*<sup>191</sup>. É um programa capaz de propagar-se automaticamente pelas redes, enviando cópias de si mesmo de computador para computador, não sendo necessário para sua propagação que haja um programa hospedeiro ao qual se acoplar.

Esse software malicioso não precisa inserir-se em um programa já existente, como acontece com os vírus. Sua propagação ocorre por meio da execução direta de suas cópias ou pela exploração automática de vulnerabilidades existentes em programas instalados em

---

prejuízos entre dois e dez bilhões de dólares

<sup>189</sup>“As *logic bombs*, por seu turno, são uma forma de *malware* não replicativo que se instala num sistema informático e aguarda um incidente ou um evento que funcione como mecanismo de desencadeamento (um *gatilho*) para desempenhar uma função nociva ou ofensiva no sistema informático infectado.” RAMALHO, Davi Silva. O uso de *malware* como meio de obtenção de prova em processo penal. In: **Revista de Concorrência e Regulação**. Coimbra: Almedina, Ano IV, número 16, outubro-dezembro 2013. p. 203.

<sup>190</sup>“Vírus de telefone celular: vírus que se propaga de celular para celular por meio da tecnologia *bluetooth* ou de mensagens MMS. A infeção ocorre quando um usuário permite o recebimento de um arquivo infectado e o executa. Após infectar o celular, o vírus pode destruir ou sobrescrever arquivos, remover ou transmitir contatos da agenda, efetuar ligações telefônicas e drenar a carga da bateria.” Cartilha de Segurança para Internet do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT), Disponível em: <<https://cartilha.cert.br/fasciculos>>. Acesso em: 30/08/2021.

<sup>191</sup>“A *worm* is a malicious program that originates on a single computer and searches for other computers connected through a local area network (LAN) or a Internet connection. When a *worm* finds another computer, it replicates itself onto that computer and continues to look for other connected computers on which to replicate. A worm continues to attempt to replicate itself indefinitely or until a self-timing mechanism halts this process.” ERBSCHELO, Michael. **Trojans, Worms and Spyware**. A Computer Security Professional's Guide to Malicious Code. Burlington (USA): Elsevier Butterworth-Heinemann, 2005. p. 23.

**Em livre tradução:** Um worm é um programa malicioso que se origina em um único computador e procura outros computadores conectados por meio de uma rede local (LAN) ou uma conexão com a Internet. Quando um worm encontra outro computador, ele se replica nesse computador e continua procurando outros computadores conectados nos quais se replicar. Um worm continua tentando se replicar indefinidamente ou até que um mecanismo de temporização interrompa esse processo

computadores. Eles são notadamente responsáveis por consumir muitos recursos, devido a grande quantidade de cópias de si mesmo que costumam espalhar-se. Como consequência, podem afetar o desempenho de redes e a utilização de computadores.

Após explorar as vulnerabilidades dos programas instalados nos computadores que se encontram conectados em rede, identificando assim seus alvos, o *worm* efetua cópias de si mesmo e tenta enviá-las para esses computadores, podendo ser enviados tanto por meio de anexos a *e-mails*, quanto pode ser via programas de troca de mensagens instantâneas.<sup>192</sup>

Esses são os principais tipos de *softwares* (*malware*) que atualmente já vêm sendo utilizados para a prática de delitos em espaço virtual<sup>193</sup>, e que também podem ser utilizados como meio para obtenção de prova em ambiente digital. É de se destacar que os tipos aqui elencados não são os únicos, pois diariamente podem estar sendo criados novos softwares com múltiplas funcionalidades.

---

<sup>192</sup>“ após identificar os alvos, o worm efetua cópias de si mesmo e tenta enviá-las para estes equipamentos, por uma ou mais das seguintes formas: como parte da exploração de vulnerabilidades existentes em programas instalados no equipamento alvo; anexadas a e-mails; via canais de IRC (Internet Relay Chat); via programas de troca de mensagens instantâneas; incluídas em pastas compartilhadas em redes locais ou do tipo P2P (Peer to Peer).” **Cartilha de Segurança para Internet do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT)**. Disponível em: <https://cartilha.cert.br/fasciculos>. Acesso em: 30/08/2021.

<sup>193</sup> “Malware like trojans and bot-net programs are spread through social engineering techniques methods of deception that create a false sense of trust, to gain ‘access information’ for example a professional looking website mimicking a brand or service or via spam and phishing emails. Criminal groups are engaged in computer or network intrusions to obtain sensitive information such as identity and password information. This in turn can be used to undertake large-scale financial crime and social engineering may be the preferred method of obtaining access to such data contained in digital devices/computers. The kinds of activities vary but encompass online scams and malware such as spyware, phishing, rootkits, and bot-nets. Malware infiltrates a computer system and may include viruses, worms, backdoors, keyloggers, and trojans” BROADHURST, Roderic e CHANG, Lennon. (2013). **Cybercrime in Asia: Trends and Challenges**. In **Asian Handbook of Criminology**. Nova York: Springer, 2013. Disponível em [\(PDF\) Cybercrime in Asia: Trends and Challenges \(researchgate.net\)](#). Acesso em: 20/09/2021

**Em tradução livre:** *Malwares* como trojans e programas bot-net são espalhados através de métodos de engenharia social de engano que criam uma falsa sensação de confiança, para obter "informações de acesso", simulam um site de aparência profissional imitando uma marca ou serviço ou através de e-mails de spam e phishing. Grupos criminosos estão envolvidos em invasões de computadores ou redes para obter informações confidenciais, como informações de identidade e senha. Isso, por sua vez, pode ser usado para empreender crimes financeiros em larga escala e a engenharia social pode ser o método preferido para obter acesso a tais dados contidos em dispositivos/computadores digitais. Os tipos de atividades variam, mas englobam golpes online e *malware*, como *spyware*, *phishing*, *rootkits* e *bot-nets*. O *malware* se infiltra em um sistema de computador e pode incluir vírus, *worms*, *backdoors*, *keyloggers* e *trojans*

### 3.4 O USO DE *MALWARE* COMO INSTRUMENTO OCULTO DE MEIO DE OBTENÇÃO DE PROVA NA INVESTIGAÇÃO DA CRIMINALIDADE ORGANIZADA

A criminalidade organizada ou altamente organizada se estrutura, como visto anteriormente, em modelo empresarial, portanto os atos dos seus agentes não são vistos de maneira isolada. A atividade delitiva é o objetivo da empresa e continuará sendo praticada, mesmo com aparência de legalidade, escamoteando as ações criminosas que a sustentam.

Quando a investigação reúne fundada suspeita da reiterada prática de delito classificado como de criminalidade altamente organizada, seu direcionamento se biparte em duas frentes: uma refere-se aos delitos consumados cuja prova já está constituída, mas ainda está por ser obtida. A outra está voltada ao futuro, para atos que podem vir a acontecer, que são esperados por tratar-se de delito permanente, ou por referir-se a delito habitual ou profissional cuja constatação pretérita enseja em dificuldades de localização de vestígios materiais. Mesmo neste contexto, considera-se possível impedir a prática de novo delito ou coletar provas suficientes para comprovar a nova consumação delitiva.

Quando refere-se a crimes que já se consumaram, o objetivo da atividade policial é a repressão, pois a prática do delito é esperada, não se tratando de possibilidade, mas de certeza. A investigação parte de um resultado criminoso consumado para identificação de autoria.

No caso de atividades empresariais de uma organização criminosa, é também possível - além de investigar os delitos já cometidos - encetar métodos de obtenção de prova, voltados para o futuro, para o perigo de lesão a bens jurídicos que se encontram diante do risco real de serem afetados. O sistema penal, nesses casos, assume posição de avanço, de agir antecipadamente reunindo elementos de prova antes mesmo da prática do delito, que apesar de incerto, é possível e até mesmo passível de acontecer.<sup>194</sup>

Nesses casos, a pesquisa de dados informáticos<sup>195</sup> não é o método de prova

---

<sup>194</sup>“Trata-se antes de clarificar o campo avançado do perigo para nem sequer deixar o perigo acontecer e, concretamente, impedir a ocorrência de crimes ainda não individualizados e só possíveis num futuro indeterminado. (...) Trata-se (...), de formas de investigação de campo avançado (*Vorfeldermittlungen*)...trata-se de prevenir e afastar perigos (crimes) possíveis antes de se atingir o limiar do perigo concreto. É uma nova forma de actividade de polícia, a colocar ao lado seu modelo tradicional.” ANDRADE, Manuel da Costa. **Bruscamente no Verão Passado**. Coimbra: Coimbra Editora, 2009. pág. 130/131.

<sup>195</sup> “Artigo 15.º Pesquisa de dados informáticos

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

recomendável a ser utilizado. É necessário dispor de métodos diversos, tais como a intercetação telefônica, a telemática, as ações encobertas que podem ser executados em mais de um momento, por apresentarem desenho legislativo adequado, dividindo-se quantas vezes forem necessárias, bem como postarem-se antecipadamente ao lado dos acontecimentos, e acompanharem o momento exato da consumação delitiva.

A técnica de uso do *malware*<sup>196</sup>, em caso de delito de criminalidade organizada, consiste na vigilância mediante instalação de *software* (*malware*) em dispositivo eletrônico (computador, *smartphone*, tablet, etc) pertencente ou de uso do investigado, visando a captação de informação, transmitida ou armazenada por meio digital, que poderá servir para produção de prova<sup>197</sup>, em relação a delito cuja consumação é esperada.

O equipamento a ser monitorado pode utilizar o SIM<sup>198</sup>. Neste caso, a instalação pode

---

informático, devendo, sempre que possível, presidir à diligência.” Lei nº 109/2009 de 15 de setembro, Lei do Cibercrime (LC). Disponível em [http://www.pgdlisboa.pt/leis/lei\\_mostra\\_articulado.php?nid=1137&tabela=leis](http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1137&tabela=leis). Acessado em 01.09.2021

<sup>196</sup>“A note on terminology. In the emerging literature on this topic, different authors refer to these bits of code using different names. Jonathan Mayer speaks generically of “government hacking.” Ahmed Ghappour embraces the Justice Department’s innocuous-sounding “network investigative technique,” or NIT. Steve Bellovin, Matt Blaze, Sandy Clark, and Susan Landau speak generally of “exploits” but also point to DOJ’s mouthful, “Computer and Internal Protocol Address Verifier” or CIPAV. I, preferring not to mince words, will stick with “malware” or, occasionally, “virus.”. OHM, Paul. **The Investigative Dynamics of the Use of Malware by Law Enforcement In William & Mary Bill of Rights Journal**, v. 26 (2017-2018). Disponível em <https://scholarship.law.wm.edu/wmboj/vol26/iss2/4>. Nota de rodapé nº 37, p. 311

**Em livre tradução:** Uma nota sobre a terminologia. Na literatura emergente sobre este tópico, diferentes autores referem-se a esses trechos de código usando nomes diferentes. Jonathan Mayer fala genericamente de "pirataria governamental". Ahmed Ghappour adota a aparentemente inócua "técnica de investigação de rede" do Departamento de Justiça, ou NIT. Steve Bellovin, Matt Blaze, Sandy Clark e Susan Landau falam geralmente de "exploits", mas também apontam para grande expressão formulada pelo DOJ, "Computer and Internal Protocol Address Verifier" ou CIPAV. Eu prefiro falar o mais claro e direto possível, por isso uso “malware” ou, ocasionalmente, “vírus”.

<sup>197</sup>Digital Evidence: “Information of probative value stored or transmitted in digital form”, conforme conceituação formulada pelo Grupo de Trabalho Científico em Prova Eletrônica (Scientific Working Group on Digital Evidence – SWGDE), grupo criado em colaboração do FBI e a Organização Internacional de Prova Informática (International Organization on Computer Evidence – IOCE), encarregado de elaborar as diretrizes transversais, boas práticas e rotinas para a recuperação, preservação e estudo das provas digitais. Disponível em: <https://www.swgde.org>. Acesso em: 23/08/17.

<sup>198</sup>O cartão SIM (Subscriber Identity Module), em português: "módulo de identificação do assinante" é um circuito impresso do tipo [cartão inteligente](#) utilizado para identificar, controlar e armazenar dados de telefones celulares, sendo de uso obrigatório nos equipamentos de tecnologia GSM (Global System for Mobile Communications), como conceitua o European Telecommunications Standards Institute (ETSI):

“The SIM used in Digital Cellular Telecommunications Systems like 3G or GSM is the entity that contains the identity of the subscriber. When the SIM is placed in a terminal or handset, users can register onto a network. The primary function of the SIM is to authenticate the validity of a terminal when accessing the network. It also provides a means to authenticate the user and may also store other subscriber-related information or applications.” Disponível em: <http://www.etsi.org/technologies-clusters/technologies/smart-cards/sim>. Acesso em: 23/08/2017.

**Em livre tradução:** O SIM utilizado em Sistemas Digitais de Telecomunicações Celulares como 3G ou GSM é a entidade que contém a identidade do assinante. Quando o SIM é colocado em um terminal ou aparelho, os usuários podem se registrar em uma rede. A principal função do SIM é autenticar a validade de um terminal ao

ocorrer por meio físico, com a implantação de chip que espelha o telemóvel investigado, podendo ser monitorada toda a atividade do equipamento original à distância. O investigador recebe, em cópia, o tráfego de dados informáticos em tempo real. É possível, também, servir de estação de escuta do tráfego telefónico do aparelho original, e abrir o microfone do aparelho, possibilitando a escuta ambiental por parte do investigador ainda que esteja desligado.

É também possível a instalação de um software que descarrega uma série de arquivos no telemóvel investigado que possibilitam implantar as funcionalidades antes mencionadas, permitindo o seu monitoramento remotamente. Em qualquer dos dois modelos adotados, o *malware*, ao ser acionado, passa a enviar dados confidenciais para o investigador, que de outra maneira a eles não teria acesso. Esses programas permitem acesso aos dados armazenados em sistema informático e em equipamento de telefonia celular, inclusive contam com a funcionalidade da transmissão em tempo real dos dados em trânsito, tendo por origem ou destino o equipamento onde o *malware* estiver instalado.

A utilização do *malware* consiste em uma busca feita no equipamento do investigado, a fim de localizar arquivos e correspondências que estejam armazenados, tanto em sítios que aquele acessa, quanto em transações eventualmente realizadas em determinados sítios. Na busca encoberta, com utilização de *malware*, ou na pesquisa de dados informáticos, o objetivo é apreender informações que estejam de posse do investigado.

A diferença entre ambas reside no fato de que a pesquisa de dados informáticos como previsto no art. 15º da LC<sup>199</sup> é de conhecimento do investigado, que dela é notificado no momento de sua realização. Já a ação encoberta, como seu próprio nome revela, ocorre de maneira velada, sem prévio aviso ao réu, pois, se isso acontece, a investigação perde seu objeto e valor, sendo da natureza deste método de prova o desconhecimento da sua existência pelo investigado.

Um outro aspeto a ser abordado versa sobre o acompanhamento em tempo real aos dados a que o investigado acessa. A inoculação de *malware* no equipamento informático de uso do investigado permite que o investigador visualize simultaneamente as informações e dados aos quais ele está acessando.

---

acessar a rede. Ele também fornece um meio para autenticar o usuário e também pode armazenar outras informações ou aplicativos relacionados ao assinante

<sup>199</sup> Lei nº 109/2009 de 15 de setembro, Lei do Cibercrime (LC).

A partir desses acessos, duas possibilidades podem ocorrer: tanto pode o investigador apenas captar as mesmas informações que o investigado está acessando, e assim produzir prova a ser usada em investigação criminal, como pode o investigador coletar chaves (*passwords*) secretas para posteriormente poder acessar remotamente às informações guardadas pelo investigado no disco rígido e nos sítios eletrônicos.

A escolha do tipo de *malware* a ser utilizado depende do objetivo a ser alcançado, pois a pesquisa pode ser feita no equipamento físico ou no dispositivo informático do investigado, assim como a investigação pode ser feita em ambiente virtual, extraindo informações dos sítios e demais ambientes virtuais sem necessariamente deixar registro no equipamento físico.

Caso seja interesse do investigador fazer uma varredura no equipamento do investigado, pesquisar os registros e arquivos que estejam armazenados no disco rígido, é possível a utilização de *malware* do tipo cavalo de Troia (*trojan horse*), desenhado especificamente para essa finalidade.

O programa pode ser inoculado na máquina do investigado por mais de uma maneira, podendo, por exemplo, ao ler correspondência eletrônica que lhe foi enviada, abrir arquivo que segue em anexo ou aceder a sítio, cujo endereço vem apontado na correspondência em questão, objetivando a atualização do programa que lhe serve de navegação no espaço virtual. No exato momento em que o usuário – neste caso investigado – acedeu ao sítio ou abriu o anexo, ele também instalou um programa, exclusivamente desenhado para copiar-lhe os arquivos e em seguida os enviar ao seu remetente<sup>200</sup>.

---

<sup>200</sup> “The spread of malicious software proves that the installation of software on the computer of an Internet user without his permission is possible. But the main difference between a virus and a remote forensic software is the fact that the remote forensic software needs to be installed on a specific computer system (the suspect’s computer) while a computer virus aims to infect as many computers as possible without need to focus on a specific computer system. There are a number of techniques how the software can be transmitted to the suspect’s computer. For example: the installation with physical access to the computer system; placing the software on a website for download; online access to the computer system by circumventing security measures; and, hiding the software in the data stream that is generated during Internet activities, to mention just a few.” GERCKE, Marco. **Understanding Cybercrime: A Guide for Developing Countries**, Genebra: ITU, 2012. p. 206. Disponível em [ITU Publication on Understanding Cybercrime: A Guide for Developing Countries](#) . Acesso em: 20/09/2021

**Em livre tradução:** A disseminação de softwares maliciosos prova que a instalação de softwares no computador de um usuário da Internet sem sua permissão é possível. Mas a principal diferença entre um vírus e um software forense remoto é o fato de que o software forense remoto precisa ser instalado em um sistema de computador específico (o computador do suspeito), enquanto um vírus de computador visa infectar o maior número possível de computadores sem necessidade de foco em um sistema de computador específico. Existem várias técnicas para transmitir o software ao computador do suspeito. Por exemplo: a instalação com acesso físico ao sistema informático; colocar o software em um site para download; acesso on-line ao sistema de computador, evitando medidas de segurança; e, esconder o software no fluxo de dados que é gerado durante as atividades da Internet,

Nesse caso, o objetivo do investigador é copiar os arquivos armazenados em disco rígido do investigado, podendo tanto ser arquivos pretéritos quanto arquivos futuros. No caso de arquivos já existentes, trata-se propriamente de busca, pois a prova já está constituída, portanto há que se falar em pesquisa de dados informáticos.<sup>201</sup> Mas se o investigador espera, aguarda, tem a expectativa de que o arquivo poderá vir a ser gerado, não se trata propriamente de busca, pois não se pode buscar o que ainda não existe. Não é intercetação, pois o curso dos dados não é desviado, nem acessado em tempo real. Nesse caso é feita uma cópia do arquivo de dados após a regular gravação, como desejado pelo investigador, que pode acessá-la posterior e remotamente. Nesse caso, trata-se de ação encoberta, como será visto no capítulo seguinte.

Assim, usar *malware* é optar por recurso tecnológico para realização de meio oculto de obtenção de prova durante a investigação criminal. Por ser um meio a ser utilizado de maneira oculta, não conhecida pelo investigado, é perfeitamente adequado para os casos de investigação, em especial os casos de criminalidade organizada, tráfico de estupefacientes, tráfico de armas e de pessoas, e nas ocorrências de delitos praticados em ambiente virtual, a exemplo de pedofilia, que exige um maior grau de especialidade do instrumental envolvido na recolha da prova.<sup>202</sup>

---

para mencionar apenas alguns.

<sup>201</sup> Como previsto no art. 15º da Lei nº 109/2009 (LC), nota de rodapé 195

<sup>202</sup>“From February 20 to March 4, 2015, the FBI infected hundreds and maybe thousands of computers with malware, a computer virus designed to help uncover the identity of people who had configured their computers precisely to avoid being identified. The FBI suspected all of the targets of the malware of accessing a website called PlayPen, purportedly the single largest repository of child pornography online at the time. The malware fulfilled the FBI’s intended purpose, leading to hundreds of arrests in the United States and hundreds of referrals to foreign law enforcement partners. The PlayPen case illuminates more than any before it the increasing use by law enforcement of malware—and other forms of government hacking—as an investigative tool. The use of malware is sometimes necessary, the FBI contends, to bring to justice people who use encrypted services such as Tor and Tor-hidden services—the heart of what is colloquially called the darknet or dark web—who cannot otherwise be identified, arrested, or deterred” OHM, Paul. **The Investigative Dynamics of the Use of Malware by Law Enforcement** *In William & Mary Bill of Rights Journal*, v. 26 (2017-2018). Disponível em <https://scholarship.law.wm.edu/wmborj/vol26/iss2/4>. Acesso em 23/09/2021. p.304-305

**Em livre tradução:** De 20 de fevereiro a 4 de março de 2015, o FBI infetou centenas e talvez milhares de computadores com *malware*, um vírus de computador projetado para ajudar a descobrir a identidade de pessoas que configuraram seus computadores precisamente para evitar serem identificadas. O FBI suspeitou que todos os alvos do *malware* acessassem um site chamado PlayPen, supostamente o maior repositório de pornografia infantil online na época. O *malware* cumpriu o propósito pretendido do FBI, levando a centenas de prisões nos Estados Unidos e centenas de referências suspeitas as autoridades policiais estrangeiras. O caso PlayPen ilumina mais do que qualquer outro antes o uso crescente de *malware* - e outras formas de hacking do governo - pelas autoridades policiais - como ferramenta investigativa. O uso de *malware* às vezes é necessário, afirma o FBI, para levar à justiça pessoas que usam serviços criptografados como Tor e serviços ocultos do Tor - o coração do que é coloquialmente chamado de darknet ou dark web - que não podem ser identificadas ou presas outra forma,

O ordenamento jurídico português, em especial o Título III, do Livro III, do Código de Processo Penal, prevê as possibilidades de meios de obtenção de prova, estando ali enumerados alguns desses meios, sem entretanto exaurir seu rol, complementado por leis esparsas<sup>203</sup>. Com o avanço tecnológico, há necessidade de atualização desses meios de obtenção de prova, de forma a acompanharem o novo modo de a sociedade se organizar, comunicar e estabelecer relações<sup>204</sup>. Nessa nova organização social, incluindo aqui a prática de delitos, é imprescindível a utilização de equipamentos eletrônicos, meios informáticos e espaços virtuais, sendo portanto necessária a atualização da execução dos meios de obtenção de prova, para incluir a possibilidade de tal ser feito por meio de programa informático, especialmente desenvolvido para esse fim.

É de se observar que à época da previsão legal dessas estratégias para obtenção de provas, ainda não havia a possibilidade de utilização de dispositivo informático, não físico, para a sua obtenção. Atualmente é possível que um programa informático, devidamente introduzido em um equipamento cibernético, possa extrair prova de um delito já consumado ou ainda em fase de consumação, podendo ocorrer em ambientes virtuais e físicos. Assim, meios de obtenção de prova como a busca, a apreensão, a escuta ambiental, a intercepção telefónica e as ações encobertas<sup>205</sup> podem vir a ser realizadas utilizando programas informáticos específicos para tanto.

Não se trata de pensar que a utilização de programa informático (*malware*) é uma inovação nos meios de obtenção de prova. A ideia apresentada neste trabalho é a possibilidade de atualizar a execução dos meios de obtenção de prova já previstos no ordenamento jurídico português, em especial as ações encobertas. Trata-se do uso de ferramentas mais modernas para a execução de meios ocultos de obtenção de provas, devidamente previstos e delimitados em lei.

Tendo em vista as peculiaridades que os novos dispositivos informáticos apresentam, será necessário promover legislativamente a adequação dos já conhecidos meios de prova,

---

<sup>203</sup> Podemos citar, exemplificativamente, as Leis n.ºs 101/2001 e 109/2009, adequadas a matéria ora em estudo

<sup>204</sup> “Il diritto processuale penale dovrebbe garantire da un lato una persecuzione penale effettiva nell’ambito della tecnica delle informazioni dato che la diffusione e la importanza di questa tecnica aumentano continuamente in tutti i campi della vita.” SIEBER, Ulrich. **La Tutela Penale Dell’Informazione** *In Rivista Trimestrale di Diritto Penale dell’Economia*, anno IV: Padova. Casa Editrice CEDAM, 1991. p. 496

**Em livre tradução:** O direito processual penal deve garantir, por um lado, uma persecução penal eficaz no domínio das tecnologias de informação, uma vez que a difusão e importância desta técnica é cada vez maior em todos os domínios da vida

<sup>205</sup> Lei n.º 101/2001

para possibilitar que sua execução também possa se dar por meio de novos métodos informáticos, utilizando a tecnologia disponível, inclusive amplamente utilizada pela criminalidade organizada. Não se trata de utilização de novos meios de obtenção de prova ou mesmo meio de prova fora do catálogo legal, apenas adequar a legislação vigente para que possa incluir e disciplinar a utilização de novos métodos para a execução de já conhecidos meios de prova.

Os programas informáticos do tipo *malware* apresentam o desenho propício para instrumentalizar os métodos ocultos de obtenção de prova previstos no ordenamento jurídico-penal, tais como a intercepção de comunicações, a escuta ambiental, a vídeo vigilância, a busca em equipamentos informáticos e as ações encobertas, uma vez que, por essência, são de uso oculto, dissimulado, funcionando à revelia do usuário.

A depender do método oculto de obtenção de prova a ser utilizado pelo investigador, é feita a escolha do tipo de *malware* adequado àquela investigação. Se o objetivo for uma intercetação telemática, pode-se inocular um programa cujo objetivo seja se instalar no dispositivo informático do visado e enviar cópia dos dados armazenados, permitindo ao investigador que o mesmo tenha acesso em tempo real à movimentação em ambiente virtual realizada pelo investigado. Pode também ser utilizado na execução de uma ação encoberta, quando o *malware* copia palavras secretas e senhas para posterior envio ao investigador; aqui se consegue revelar códigos protegidos por criptografia ou outro recurso similar, que de outra maneira não poderiam ser conseguidos pelo investigador<sup>206</sup>.

---

<sup>206</sup>Assim como o caso PlayPen, anteriormente citado, encontramos na literatura jurídica internacional outros exemplos de utilização de *malware* para efeitos de investigação criminal. Em cada caso há o desenho de um programa específico, individualmente nominado e que de maneira previamente definida, é utilizado para obter a necessária prova em investigação criminal, como a seguir transcrito:

“The potential of this model for criminal purposes was highlighted by the FBI in August 2013, through the implementation of a form of malware called Magneto in the Freedom Hosting servers, a provider of storage services that contained several hidden services dedicated to child pornography. The malware that was installed exploited a vulnerability in the Firefox browser version 17 and allowed the FBI to identify the MAC address<sup>12</sup> and the Windows administrator user name of the computer system used to access these hidden services, in order to subsequently discover the true IP address. Finally, malware may also be installed in a computer system by downloading certain files, namely by opening some attachments in e-mail messages, either through downloading executable programs (usually pirated or free and obtained through peer-to-peer programs) or even through false legitimate software updates (this was the option chosen by the German police to install the malware known as Bundestrojaner)” VACIAGO, Giuseppe e RAMALHO, David Silva. **Online searches and online surveillance: the use of trojans and other types of malware as means of obtaining evidence in criminal proceedings.** *In Digital Evidence & Elec. Signature L. Rev.*, v. 13, p. 88, 2016. p. 89-90. Disponível em <https://journals.sas.ac.uk/deeslr/article/view/2299/2252>. Acesso em 23/09/2021

**Em livre tradução:** O potencial desse modelo para fins criminosos foi destacado pelo FBI em agosto de 2013, por meio da implementação de uma forma de *malware* denominado Magneto nos servidores da Freedom Hosting, uma provedora de serviços de armazenamento que continha diversos serviços ocultos dedicados à pornografia infantil. O *malware* instalado explorou uma vulnerabilidade no navegador Firefox versão 17 e

Os métodos elencados neste estudo encontram previsão no ordenamento jurídico português, entretanto, a utilização do *malware* para sua operacionalização implica em novas possibilidades cujas peculiaridades ainda não estão contempladas pelo ordenamento. A introdução do *malware* como instrumental hábil para execução de meio de prova, abre lacunas onde havia completude<sup>207</sup>, que necessitam de preenchimento para que o ordenamento volte ao seu necessário equilíbrio, pois se o *malware* está sendo usado para a prática de delito, não é razoável que o ordenamento jurídico dispense tal instrumento para aperfeiçoamento da investigação e, por consequência, combate e prevenção ao crime.

Por outro lado, para o devido uso, os ajustes legais são necessários. Isso não implica em inovação dos meios de provas ou novos métodos de obtenção de prova, apenas regulamentação dos métodos existentes, tendo em vista a introdução de instrumental tecnológico mais sofisticado, sem, contudo, implicar em método outro que não aqueles já conhecidos e devidamente previstos em lei. Cabe ao legislador efetuar as adequações necessárias na pirâmide normativa<sup>208</sup> para que esse instrumental possa ser utilizado, mantendo assim sua completude e coerência<sup>209</sup>, afastando as possíveis lacunas e inconsistências.

---

permitiu ao FBI identificar o endereço MAC12 e o nome de usuário do administrador do Windows do sistema de computador usado para acessar esses serviços ocultos, para posteriormente descobrir o verdadeiro endereço IP. Por último, o *malware* também pode ser instalado num sistema informático através do download de determinados ficheiros, nomeadamente através da abertura de alguns anexos em mensagens de e-mail, quer através do download de programas executáveis (geralmente pirateados ou gratuitos e obtidos através de programas ponto a ponto) ou ainda através de atualizações de software falsas e legítimas (foi a opção escolhida pela polícia alemã para instalar o *malware* conhecido como Bundestrojaner)

<sup>207</sup> “Especificando melhor, a incompletude consiste no fato de que o sistema não compreende nem a norma que proíbe um certo comportamento nem a norma que o permite.” BOBBIO, Norberto. **Teoria do Ordenamento Jurídico**. Trad. Maria Celeste C. J. Santos. 10ª ed. Brasília: Ed. Universidade de Brasília, 1999. p. 115.

<sup>208</sup> “Normalmente representa-se a estrutura hierárquica de um ordenamento através de uma *pirâmide*, donde se falar também de construção em pirâmide do ordenamento jurídico.” BOBBIO, Norberto. **Teoria do Ordenamento Jurídico**. Trad. Maria Celeste C. J. Santos. 10ª ed. Brasília: Ed. Universidade de Brasília, 1999. p. 51.

<sup>209</sup> “Portanto, o nexa entre coerência e completude está em que a coerência significa a exclusão de toda situação na qual pertençam ao sistema ambas as normas que se contradizem; a completude significa a exclusão de toda a situação na qual não pertençam ao sistema nenhuma das duas normas que se contradizem.” BOBBIO, Norberto. **Teoria do Ordenamento Jurídico**. Trad. Maria Celeste C. J. Santos. 10ª ed. Brasília: Ed. Universidade de Brasília, 1999. p. 116.

### 3.5 EXPERIÊNCIA ESTRANGEIRA DO USO DE *MALWARE* EM INVESTIGAÇÃO CRIMINAL

A utilização do *malware* na atividade policial já é um fato em muito países e aos poucos está sendo introduzida nos ordenamentos jurídicos. Podemos encontrar exemplos de sua utilização na literatura jurídica internacional, tanto visando a prevenção de delitos, como a recolha de prova em processo criminal<sup>210</sup>.

A primeira aprovação de uso de programas informáticos para vigilância eletrónica se deu nos Estados Unidos, com a autorização de utilização dos *malware* denominados Magic Lantern e CIPAV, com capacidade para gravar as informações digitadas no dispositivo informático onde o mesmo estivesse instalado, bem como gravar o conteúdo do disco rígido e envio destas informações remotamente, ao equipamento do investigador.

No continente europeu, o primeiro país a legislar sobre a utilização de *malware* em vigilância e investigação foi a Alemanha, por meio da Lei de Defesa contra os Perigos do Terrorismo Internacional, de 25 de dezembro de 2008<sup>211</sup>. A necessidade dessa lei se deu após decisão do Tribunal Constitucional Federal Alemão, datada de 27 de fevereiro de 2008<sup>212</sup>, que

<sup>210</sup> “FBI remotely installs spyware to trace bomb threat, News.com, 18.07.2007, available at: [http://www.news.com/8301-10784\\_3-9746451-7.html](http://www.news.com/8301-10784_3-9746451-7.html); Popa, FBI Fights against terrorists with computer viruses, 19.07.2007, available at: <http://news.softpedia.com/newsPDF/FBI-Fights-Against-Terrorists-With-Computer-Viruses-60417.pdf>; Secret online search warrant: FBI uses CIPAV for the first time, Heise News, 19.07.2007, available at: <http://www.heise-security.co.uk/news/92950>.” Casos apontados no texto, na nota de rodapé nr.1506. GERCKE, Marco. **Understanding Cybercrime: A Guide for Developing Countries**, Genebra: ITU, 2012. Disponível em [ITU Publication on Understanding Cybercrime: A Guide for Developing Countries](#) pág. 204. Acesso em 18.11.2021.

<sup>211</sup> [Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt, Bundesgesetzblatt Teil I, 2008, Nr. 66, vom 31.12.2008](#) Íntegra da lei disponível no endereço: [https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger\\_BGBl&start=//%5B@attr\\_id=%27bgbl108s3083.pdf%27%5D#\\_bgbl\\_%2F%2F%5B%40attr\\_id%3D%27bgbl108s3083.pdf%27%5D\\_1637761543909](https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&start=//%5B@attr_id=%27bgbl108s3083.pdf%27%5D#_bgbl_%2F%2F%5B%40attr_id%3D%27bgbl108s3083.pdf%27%5D_1637761543909). Acesso em 19.11.2021

<sup>212</sup> “2. Die heimliche Infiltration eines informationstechnischen Systems, mittels derer die Nutzung des Systems überwacht und seine Speichermedien ausgelesen werden können, ist verfassungsrechtlich nur zulässig, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen. Überragend wichtig sind Leib, Leben und Freiheit der Person oder solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt.” “Die in § 5a Abs. 1 VSG vorgesehenen Maßnahmen greifen in das Recht auf informationelle Selbstbestimmung ein. Dabei kommt es nicht darauf an, ob sich der Regelungsgehalt der angegriffenen Norm in einer Befugnis der Verfassungsschutzbehörde erschöpft, ein Auskunftersuchen an ein Kreditinstitut zu richten, oder ob sie implizit eine Auskunftspflicht des jeweiligen Kreditinstituts enthält. In jedem Fall ermächtigt die Vorschrift die Behörde zu Datenerhebungen, die bereits als solche einen Grundrechtseingriff bewirken.” BVerfG, Urteil des Ersten Senats vom 27. Februar 2008 - 1 BvR 370/07 -, Rn. 1-333. Trechos da decisão, que pode ser encontrada na íntegra no endereço: [https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2008/02/rs20080227\\_1bvr037007.html](https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2008/02/rs20080227_1bvr037007.html). Acesso em 19.11.2021

declarou inconstitucional a Lei do Estado federado da Renânia do Norte-Westfália, por considerar que tal lei violava o direito a autodeterminação informativa<sup>213</sup>, já que autorizava o controle remoto de equipamentos informáticos, para efeitos de investigação policial e prevenção de delitos.

A seguir serão apresentados alguns exemplos de casos onde houve a utilização de *malware* na investigação criminal e recolha de provas, bem como a atual situação na legislação estrangeira:

### 3.5.1. Estados Unidos:

Durante uma investigação sobre operação ilegal de jogo e agiotagem no ano de 1999, o FBI teve sua atuação frustrada quando descobriu que o investigado Nicodemo Scarfo, havia instalado o *software* Pretty Good Privacy (PGP)<sup>214</sup> para codificar os arquivos onde estavam os dados relacionados ao negócio sob investigação. Assim, a agência de investigação instalou no computador de Scarfo um *malware* do tipo *keylogger*, projetado para atuar quando o computador não estava funcionando em rede, ou seja, sem comunicação com um modem,

---

**Em livre tradução:** 2. A infiltração clandestina de um sistema informático, através do qual se possa monitorizar a utilização do sistema e ler os seus suportes, só é constitucionalmente admissível se existirem indícios reais de um perigo concreto para um bem jurídico vital. De suma importância são o corpo, a vida e a liberdade da pessoa ou dos bens do público em geral, cuja ameaça afeta os fundamentos ou a existência do Estado ou os fundamentos da existência humana.

As medidas previstas na Seção 5a, Parágrafo 1 da Lei de Proteção à Constituição da Renânia do Norte-Vestfália interferem com o direito à autodeterminação informativa. Pouco importa se o conteúdo regulamentar da norma impugnada se esgota na faculdade da autoridade de tutela da constituição de solicitar informações a uma instituição de crédito, ou se contém implicitamente uma obrigação de informação por parte da respetiva instituição de crédito. Em qualquer caso, o regulamento autoriza a autoridade a recolher dados que, como tal, já resultem na violação dos direitos fundamentais. BVerfG, sentença do Primeiro Senado de 27 de fevereiro de 2008- 1 BvR 370/07 -, Rn. 1-333.

<sup>213</sup>“De nuevo, fueron los EE.UU. los que primero aprobaron el uso de programas informáticos de vigilancia electrónica basados en la idea de programas “troyanos” (...). Y en Europa, ha sido Alemania el primer país en legislar sobre la utilización de esta nueva tecnología como medida excepcional de investigación de delitos (...)” PRADILLO, Juan Carlos Ortiz. **“Hacking” legal al servicio de la investigación criminal: nuevos instrumentos para la investigación y prueba de la delincuencia informática in Delincuencia informática.** Tiempos de cautela y amparo: Cizur Menor (Espanha). Thomson Reuters Editorial Aranzadi, 2012. págs. 191 e 192

<sup>214</sup>“In one case involving Nicodemo S. Scarfo, the alleged mastermind of a loan shark operation in New Jersey, the FBI found itself thwarted when Scarfo used Pretty Good Privacy software (PGP) to encode confidential business data.” MCCULLAGH, Declan. **FBI taps cell phone mic as eavesdropping tool.** Disponível em: [http://news.com.com/2102-1029\\_3-6140191.html?tag=st.util.print](http://news.com.com/2102-1029_3-6140191.html?tag=st.util.print) (1 of 4)12/5/2006 8:20:16, acesso em 18.11.2021

**Em livre tradução:** Em um caso envolvendo Nicodemo S. Scarfo, o suposto mentor de uma operação de agiotagem em Nova Jersey, o FBI se viu frustrado quando Scarfo usou o software Pretty Good Privacy (PGP) para codificar dados confidenciais de negócios.

para gravar as teclas pressionadas pelo investigado e assim obter palavra passe que permitia acesso aos arquivos criptografados<sup>215</sup>.

Em análise desse caso, a Corte Distrital de New Jersey decidiu que a Lei de Escuta Telefônica (Wiretap) e a Quarta Emenda, permitiam a utilização desse tipo de *software* em investigação criminal, validando as provas assim obtidas.<sup>216 217 218 219</sup>

Em 2001 há o registo do desenvolvimento pelo FBI do Magic Lantern, um *malware*

---

<sup>215</sup>“While the message is being drafted, it can be captured by keystroke capture software, as was the case when the F.B.I. surreptitiously placed such software on the computer of Nicodemo S. Scarfo to search for evidence of an illegal gambling and loan sharking operation. The software was designed to record keystrokes only when the computer was not using its modem to communicate with other computers. The court held that such capture was not a violation of the Wiretap Act. Thus, capture during the creation phase is arguably not an intercept.” RYAN, Daniel J., SHPANTZER, Gal. **Legal Aspects of Digital Forensics**. Disponível em <http://euro.ecom.cmu.edu/program/law/08-732/Evidence/RyanShpantzer.pdf>, acesso em 18.11.2021

**Em livre tradução:** Enquanto a mensagem está sendo redigida, ela pode ser capturada por um software de captura de pressionamento de tecla, como foi o caso quando o F. B. I. sub-repticiamente colocou esse software no computador de Nicodemo S. Scarfo em busca de evidências de uma operação ilegal de jogo e agiotagem. O software foi projetado para registrar pressionamentos de tecla apenas quando o computador não estava usando o modem para se comunicar com outros computadores. O tribunal considerou que tal captura não foi uma violação da Lei de escuta telefônica. Assim, a captura durante a fase de criação não é indiscutivelmente uma intercetação.

<sup>216</sup>“Commenters have pointed to the use by the government of key logging software, for example, in the investigation of Nicky Scarfo in 1999.” OHM, Paul. **The Investigative Dynamics of the Use of Malware by Law Enforcement In William & Mary Bill of Rights Journal**, v. 26 (2017-2018). Disponível em <https://scholarship.law.wm.edu/wmboj/vol26/iss2/4> p. 311. Acesso em 18.11.2021

**Em livre tradução:** Os comentários apontaram para o uso pelo governo de software de registo de chaves, por exemplo, na investigação de Nicky Scarfo em 1999

<sup>217</sup>“U.S. v Scarfo 180 F.Supp.2d 572 (D.N.J. 2001). While this may not tell you who depressed the keys (thus proving who had control), it would provide access to the encrypted material, which, by itself, is likely to assist the wider investigation.” MASON, Stephen; SENG, Daniel. **Electronic Evidence and Electronic Signatures**. Fifth edition published by the Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2021 Disponível em: <https://humanities-digital-library.org/index.php/hdl/catalog/view/electronic-evidence-and-electronic-signatures/214/408-1> p. 398. Acesso em 18.11.2021

**Em livre tradução:** Embora isso possa não dizer quem pressionou as chaves (provando assim quem tinha o controle), forneceria acesso ao material criptografado, o que, por si só, provavelmente ajudará na investigação mais ampla

<sup>218</sup>“This topic was discussed in the decision of the United States District Court of New Jersey in the case United States v. Scarfo. The District Court decided that the federal wiretapping law and the Fourth Amendment allow the law enforcement agencies to make use of a software to record the key strokes on the suspects computer (key logger) in order to intercept a passphrase to an encrypted file (if the system does not operate while the computer is communicating with other computers).” GERCKE, Marco. **Understanding Cybercrime: A Guide for Developing Countries**, Genebra: ITU, 2012. Disponível em [ITU Publication on Understanding Cybercrime: A Guide for Developing Countries](http://ITU.Publication.on.Understanding.Cybercrime:A.Guide.for.Developing.Countries) p. 200. Acesso em 18.11.2021

**Em livre tradução:** Este assunto foi discutido na decisão do Tribunal Distrital dos Estados Unidos de New Jersey no caso Estados Unidos vs. Scarfo. O Tribunal Distrital decidiu que a lei federal de escuta telefônica e a Quarta Emenda permitem que as agências de aplicação da lei façam uso de um software para registrar os pressionamentos de chave no computador do suspeito (key logger), a fim de interceptar uma frase secreta para um arquivo criptografado (se o o sistema não funciona enquanto o computador está se comunicando com outros computadores)

<sup>219</sup>Trecho da decisão de negativa de exclusão das provas coletadas por meio do keylogger: “In this day and age, it appears that on a daily basis we are overwhelmed with new and exciting, technologically-advanced gadgetry. Indeed, the amazing capabilities bestowed upon us by science are at times mind-boggling. As a result, we must

também do tipo *keylogger*<sup>220</sup>, que podia ser inoculado em computadores por via remota, tendo por alvo os dispositivos que estavam sendo utilizados por suspeitos de estarem envolvidos com ações terroristas<sup>221</sup>. O aperfeiçoamento deste *malware* originou o CIPAV (Computer and Internal Protocol Address Verifier) que conseguia identificar a localização do sujeito, bem como os programas por ele em uso em determinado momento e ainda o último site por ele visitado.<sup>222 223</sup>

Um outro caso de difusão proposital de *malware* por meio de agência investigativa, aconteceu nos primeiros meses de 2015, quando o FBI desenhou e difundiu determinado programa visando identificar usuários que propositalmente ocultavam sua identidade quando

---

be ever vigilant against the evisceration of Constitutional rights at the hands of modern technology. Yet, at the same time, it is likewise true that modern-day criminals have also embraced technological advances and used them to further their felonious purposes. Each day, advanced computer technologies and the increased accessibility to the Internet means criminal behavior is becoming more sophisticated and complex. This includes the ability to find new ways to commit old crimes, as well as new crimes beyond the comprehension of courts.”  
*In* United States v. Nicodemo S. Scarfo, et al. Criminal Action No. 00-404 (NHP), Nicholas H. Politan District Judge, 26.12.2001. Disponível em <https://archive.epic.org/crypto/scarfo/opinion.html>. Acesso e 18.11.2021

**Em livre tradução:** Nos dias de hoje, parece que diariamente somos sobrecarregados com dispositivos novos e emocionantes, tecnologicamente avançados. Na verdade, as incríveis capacidades que a ciência nos concede às vezes são estonteantes. Como resultado, devemos estar sempre vigilantes contra a evisceração dos direitos constitucionais nas mãos da tecnologia moderna. No entanto, ao mesmo tempo, é igualmente verdade que os criminosos modernos também adotaram os avanços tecnológicos e os usaram para promover seus propósitos criminosos. A cada dia, tecnologias de computador avançadas e o aumento da acessibilidade à Internet significam que o comportamento criminoso está se tornando mais sofisticado e complexo. Isso inclui a capacidade de encontrar novas maneiras de cometer crimes antigos, bem como novos crimes além da compreensão dos tribunais.

<sup>220</sup>“Already in 2001 reports pointed out that the United States FBI was developing a key-logger tool for Internet-related investigations called the “magic lantern””. GERCKE, Marco. **Understanding Cybercrime: A Guide for Developing Countries**, Genebra: ITU, 2012. Disponível em [ITU Publication on Understanding Cybercrime: A Guide for Developing Countries](#) p. 204

**Em livre tradução:** Já em 2001, relatórios apontavam que o FBI dos Estados Unidos estava desenvolvendo uma ferramenta keylogger para investigações relacionadas à Internet, chamada de "lanterna mágica"

<sup>221</sup>“O primeiro registro do uso regular dessa tecnologia data de 2001 e refere-se ao *Magic Lantern*, um *keylogger* concebido para poder ser instalado sub-reptícia e remotamente via Internet no sistema informático visado – localizado ou não nos EUA – quando este pertencesse a indivíduos suspeitos de estarem envolvidos com atividades criminosas, em particular de natureza terrorista.” RAMALHO, David Silva. **Métodos Ocultos de Investigação Criminal em Ambiente Digital**. Coimbra: Edições Almedina, 2017 p. 396-398

<sup>222</sup>“In 2007 reports were published that law enforcement agencies in the United States were using software to trace back suspects that use means of anonymous communication. The reports were referring to a search warrant where the use of a tool called CIPAV was requested.” GERCKE, Marco. **Understanding Cybercrime: A Guide for Developing Countries**, Genebra: ITU, 2012. Disponível em [ITU Publication on Understanding Cybercrime: A Guide for Developing Countries](#) p. 204. Acesso em 18.11.2021

**Em livre tradução:** Em 2007, foram publicados relatórios de que agências de aplicação da lei nos Estados Unidos estavam usando software para rastrear suspeitos que usam meios de comunicação anônima. Os relatórios se referiam a um mandado de busca onde o uso de uma ferramenta chamada CIPAV foi solicitado

<sup>223</sup>“O *Magic Lantern* viria a dar lugar ao *Computer and Internal Protocol Address Verifier* (CIPAV), um tipo de *malware*” RAMALHO, David Silva. **Métodos Ocultos de Investigação Criminal em Ambiente Digital**. Coimbra: Edições Almedina, 2017 p. 398

em navegação pela Internet. Tais usuários em regra acessavam ao sítio PlayPen, que difundia pornografia infantil.

Essa ação resultou em centenas de prisões nos EUA e identificação de usuários em outros países, cujas autoridades receberam essas informações para as ações investigativas correspondentes<sup>224</sup>.

Entre as ações deflagradas após a investigação do caso Playpen, houve a Operação Pacifier<sup>225</sup>, que impactou a rede de distribuição de pornografia infantil em vários países, como

---

<sup>224</sup>“From February 20 to March 4, 2015, the FBI infected hundreds and maybe thousands of computers with malware, a computer virus designed to help uncover the identity of people who had configured their computers precisely to avoid being identified. The FBI suspected all of the targets of the malware of accessing a website called PlayPen, purportedly the single largest repository of child pornography online at the time. The malware fulfilled the FBI’s intended purpose, leading to hundreds of arrests in the United States and hundreds of referrals to foreign law enforcement partners. The PlayPen case illuminates more than any before it the increasing use by law enforcement of malware—and other forms of government hacking—as an investigative tool. The use of malware is sometimes necessary, the FBI contends, to bring to justice people who use encrypted services such as Tor and Tor-hidden services—the heart of what is colloquially called the darknet or dark web—who cannot otherwise be identified, arrested, or deterred.” OHM, Paul. **The Investigative Dynamics of the Use of Malware by Law Enforcement** *In William & Mary Bill of Rights Journal*, v. 26 (2017-2018). Disponível em <https://scholarship.law.wm.edu/wmboj/vol26/iss2/4> p. 304. Acesso em 18.11.2021

**Em livre tradução:** De 20 de fevereiro a 4 de março de 2015, o FBI infetou centenas e talvez milhares de computadores com *malware*, um vírus de computador projetado para ajudar a descobrir a identidade de pessoas que configuraram seus computadores precisamente para evitar serem identificadas. O FBI suspeitou de todos os alvos do *malware* de acesso a um site chamado PlayPen, supostamente o maior repositório de pornografia infantil online na época. O *malware* atendeu ao objetivo pretendido do FBI, levando a centenas de prisões nos Estados Unidos e centenas de referências a parceiros estrangeiros de aplicação da lei. O caso PlayPen ilumina mais do que qualquer outro o uso crescente de *malware* - e outras formas de hack do governo - pelas autoridades policiais - como ferramenta investigativa. O uso de *malware* às vezes é necessário, afirma o FBI, para levar à justiça pessoas que usam serviços criptografados como Tor e serviços ocultos do Tor - o coração do que é coloquialmente chamado de darknet ou dark web - que não podem ser identificados, presos, ou dissuadido.

<sup>225</sup>“In early 2015, the FBI carried out an unprecedented hacking campaign, deploying malware on at least one thousand computers that had been used to visit a certain child pornography site. That move, Motherboard has learned, is part of Operation Pacifier, a large multi-agency investigation into child pornography on the so-called dark web. The truly global nature of the operation is now coming to light. Media reports as far afield as Greece and Chile covered related arrests, and a Europol presentation discovered by Motherboard indicates that Danish authorities have arrested dozens of people as part of the investigation. In August of last year, Greece’s Cyber Crime Unit arrested a 21-year-old man on charges of possession and distribution of child pornography. The man, who wasn’t named in reports, was picked up in a hotel in Ilia, Peloponnese, as part of an investigation “international authorities code-named Pacifier,” according to Greek outlet *Ekathimerini.com*. That investigation, the article continues, was based on information obtained by the FBI and Europol, which was then provided to countries where suspects resided. The site in question was a Tor hidden service, according to another Greek report, the server of which was seized by US authorities. Reports from Chile name that site as Playpen, where a man was arrested last week for child pornography crimes as part of Operation Pacifier.” COX, Joseph. **"Operation Pacifier" is larger in scope than most anyone believed**. Disponível em <https://perma.cc/WG6R-TEGU>. Acesso em 18.11.2021

**Em livre tradução:** No início de 2015, o FBI realizou uma campanha de hacking sem precedentes, implantando *malware* em pelo menos mil computadores que haviam sido usados para visitar um determinado site de pornografia infantil. Esse movimento, o Motherboard descobriu, é parte da Operação Pacifier, uma grande investigação multi-agência sobre pornografia infantil na chamada dark web. A natureza verdadeiramente global da operação está agora vindo à tona. Reportagens da mídia em lugares distantes como Grécia e Chile cobriram detenções relacionadas, e uma apresentação da Europol descoberta pelo Motherboard indica que as autoridades

também colocou em questão a utilização de *malware* por agência investigativa. Nesse caso especificamente, após a apreensão do site pelo FBI, houve incremento no número de novos usuários, sugerindo falha no *malware* e, portanto, a validade da técnica utilizada pela agência.

A defesa de um dos acusados, Jay Michaud, que foi preso na operação Pacifier, requereu em juízo o código do *malware* utilizado para identificar seu cliente, mas o FBI não o entregou preferindo retirar a prova dos autos e assim desistir do caso<sup>226</sup>.

### 3.5.2. Alemanha:

Na Alemanha foi pensado o *Bundestrojaner*, um *malware* desenhado para ser enviado ao dispositivo informático suspeito, sob o disfarce de atualização de *software*, que após instalado permitia monitorar todas as atividades do investigado na Internet.<sup>227</sup>

---

dinamarquesas prenderam dezenas de pessoas como parte da investigação. Em agosto do ano passado, a Unidade de Crime Cibernético da Grécia prendeu um homem de 21 anos sob a acusação de posse e distribuição de pornografia infantil. O homem, que não foi citado nos relatórios, foi pego em um hotel em Ilia, Peloponeso, como parte de uma investigação de "codinome de autoridades internacionais Pacifier", segundo o outlet grego Ekathimerini.com. Essa investigação, prossegue o artigo, baseou-se em informações obtidas pelo FBI e pela Europol, que foram então fornecidas aos países onde residiam os suspeitos. O site em questão era um serviço oculto do Tor, de acordo com outro relatório grego, cujo servidor foi apreendido pelas autoridades americanas. Reportagens do Chile chamam esse site de Playpen, onde um homem foi preso na semana passada por crimes de pornografia infantil como parte da Operação Pacifier

<sup>226</sup> “The US Department of Justice (DoJ) has decided to drop its case against Jay Michaud, accused of accessing the notorious and now defunct dark web child pornography website Playpen, instead of sharing the classified technology used to locate thousands of suspects visiting the site.

The DoJ is prosecuting 135 suspects across America for having allegedly accessed Playpen. During investigations, the FBI reportedly used a Tor exploit called NIT (network investigative technique) that most security experts deem a malware. It was this exploit that helped them locate IP addresses of those who visited the site.” ASHOK, India. **Playpen: US DoJ drops child porn case against Jay Michaud to keep Tor hack source code secret.** Disponível em: <https://www.ibtimes.co.uk/playpen-us-doj-drops-child-porn-case-against-jay-michaud-keep-tor-hack-source-code-secret-1609919>. Acesso em 18.11.2021

**Em livre tradução:** O Departamento de Justiça dos Estados Unidos (DoJ) decidiu retirar o caso contra Jay Michaud, acusado de acessar o notório e agora extinto site de pornografia infantil dark web Playpen, em vez de compartilhar a tecnologia secreta usada para localizar milhares de suspeitos que visitam o site. O DoJ está processando 135 suspeitos em toda a América por supostamente terem acessado o Playpen. Durante as investigações, o FBI supostamente usou uma exploração do Tor, chamada NIT (técnica de investigação de rede), que a maioria dos especialistas em segurança considera um *malware*. Foi esse exploit que os ajudou a localizar os endereços IP de quem visitou o site.

<sup>227</sup> “O *Bundestrojaner* consiste numa espécie de *malware* enviado para o computador do suspeito sob a forma de uma comum actualização de *software* e que, após instalação, permite, entre outras funcionalidades, gravar as chamadas *Skype*, monitorizar toda a actividade do suspeito na Internet, gravar as palavras-passe por ele inseridas e até activar o *hardware* do computador do visado, utilizando os seus microfones e a *webcam* para gravar sons e tirar fotografias que virão a ser enviadas para as autoridades responsáveis pela investigação.” RAMALHO, David Silva. **A recolha de Prova Penal em Sistemas de Computação em Nuvem.** pág. 143 *In: Revista de Direito Intelectual*, Coimbra: Almedina, nº 02, dezembro de 2014. p. 159/160

Em 27.02.2008, o Tribunal Constitucional Federal Alemão (1 BvR 370/07; 1 BvR 595/07), ao declarar a inconstitucionalidade da Lei do Estado federado da Renânia do Norte-Westfalia, decidiu também pela possibilidade da utilização do método de infiltração em sistema informático, permitindo assim o monitoramento remoto de investigados, desde que estejam presentes fortes indícios de um perigo concreto para um bem jurídico de relevada importância. Na mesma decisão consta, que a confidencialidade e a integridade dos sistemas informáticos fazem parte do direito geral de personalidade, no entanto, desde que precedida de autorização judicial e regulada por uma lei que restrinja seu uso, tendo por medida o respeito a vida privada, é possível a infiltração em sistemas informáticos.<sup>228</sup>

<sup>228</sup> “1. Das allgemeine Persönlichkeitsrecht (Art.2 Abs. 1 i.V.m. Art.1 Abs. 1 GG) umfasst das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.

2. Die heimliche Infiltration eines informationstechnischen Systems, mittels derer die Nutzung des Systems überwacht und seine Speichermedien ausgelesen werden können, ist verfassungsrechtlich nur zulässig, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen. Überragend wichtig sind Leib, Leben und Freiheit der Person oder solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt. Die Maßnahme kann schon dann gerechtfertigt sein, wenn sich noch nicht mit hinreichender Wahrscheinlichkeit feststellen lässt, dass die Gefahr in näherer Zukunft eintritt, sofern bestimmte Tatsachen auf eine im Einzelfall durch bestimmte Personen drohende Gefahr für das überragend wichtige Rechtsgut hinweisen.

3. Die heimliche Infiltration eines informationstechnischen Systems ist grundsätzlich unter den Vorbehalt richterlicher Anordnung zu stellen. Das Gesetz, das zu einem solchen Eingriff ermächtigt, muss Vorkehrungen enthalten, um den Kernbereich privater Lebensgestaltung zu schützen.

4. Soweit eine Ermächtigung sich auf eine staatliche Maßnahme beschränkt, durch welche die Inhalte und Umstände der laufenden Telekommunikation im Rechnernetz erhoben oder darauf bezogene Daten ausgewertet werden, ist der Eingriff an Art.10 Abs.1 GG zu messen.

5. Verschafft der Staat sich Kenntnis von Inhalten der Internetkommunikation auf dem dafür technisch vorgesehenen Weg, so liegt darin nur dann ein Eingriff in Art.10 Abs.1 GG, wenn die staatliche Stelle nicht durch Kommunikationsbeteiligte zur Kenntnisnahme autorisiert ist. Nimmt der Staat im Internet öffentlich zugängliche Kommunikationsinhalte wahr oder beteiligt er sich an öffentlich zugänglichen Kommunikationsvorgängen, greift er grundsätzlich nicht in Grundrechte ein.” Leitsatz e zum Urteil des Ersten Senats vom 27. Februar 2008; 1 BvR 370/07; 1 BvR 595/07. Disponível em [https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2008/02/rs20080227\\_1bvr037007.html](https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2008/02/rs20080227_1bvr037007.html) Acessado em 19.11.2021

**Em livre tradução:** 1. O direito geral da personalidade (artigo 2.º, n.º 1 em conjugação com o artigo 1.º, n.º 1, da Lei Básica) compreende o direito fundamental de garantir a confidencialidade e integridade dos sistemas informáticos.

2. A infiltração clandestina de um sistema de informática, por meio do qual o uso do sistema possa ser monitorado e sua mídia de armazenamento lida, só é constitucionalmente admissível se houver indícios reais de um perigo concreto para um bem jurídico de extrema importância. De suma importância são o corpo, a vida e a liberdade da pessoa ou os bens do público em geral cuja ameaça afeta os fundamentos ou a existência do Estado ou os fundamentos da existência humana. A medida pode ser justificada se ainda não puder ser determinado com probabilidade suficiente que o perigo ocorrerá em um futuro próximo, desde que certos fatos apontem para um perigo iminente para o ativo jurídico extremamente importante de certas pessoas em um caso individual.

3. A infiltração clandestina de um sistema de tecnologia da informação geralmente está sujeita a uma ordem judicial. A lei que autoriza tal interferência deve conter precauções para proteger a área central da vida privada.

4. Na medida em que a autorização se limite a uma medida estatal por meio da qual o conteúdo e as circunstâncias das telecomunicações em curso na rede de computadores são coletados ou os dados relacionados são avaliados, a intervenção deve ser medida em face do artigo 10, parágrafo 1º da Lei Fundamental da República Federal da Alemanha

5. Se o estado adquiere conhecimento do conteúdo da comunicação pela Internet da forma tecnicamente pretendida, isso só infringe o artigo 10, § 1º da Lei Fundamental da República Federal da Alemanha se a

Apesar de abrir essa brecha de possibilidade para utilização da vigilância eletrônica, declarou que o monitoramento eletrônico, como previsto na lei em questão, violava o direito de autodeterminação informativa, por isso a sua inconstitucionalidade.

Na Alemanha, desde 2008, foram utilizados variados tipos de *malware*<sup>229</sup> para investigação de delitos, apesar de à época não haver ainda definição de catálogo próprio dos crimes que poderiam ser investigados por esse método, nem também regulamentação de como tal método poderia ser efetivado. Tal prática gerou severas críticas, colocando em discussão o

autoridade estadual não estiver autorizada a tomá-lo pelos envolvidos na comunicação. Se o estado percebe conteúdo de comunicação acessível ao público na Internet ou se participa de processos de comunicação acessíveis ao público, isso não interfere nos direitos fundamentais.

<sup>229</sup> “Bereits im Juni 2018 hat das Magazin [Netzpolitik.org](https://www.netzpolitik.org) geleakte Dokumente der Bundesregierung veröffentlicht, die einen Überblick der bisherigen Geschichte der Staatstrojaner in Deutschland bieten:

- 2007 setzte der Zoll eine Software des Unternehmens Era-IT Solutions als Trojaner ein.
- Ab 2008 nutzten Behörden eine Software der Firma DigiTask aus Hessen. Dies war den Dokumenten zufolge der bisher am häufigsten eingesetzte Staatstrojaner. Da die Software mehr konnte, als die Rechtslage zuließ, schlugen Datenschutzbeauftragte Alarm und DigiTask ist nicht mehr im Einsatz.
- DigiTask ging 2018 in den Besitz des Unternehmens Rohde & Schwarz über. Netzpolitik vermutet, dass hier die Entwicklung eines neuen Staatstrojaners geplant ist, doch darüber ist nichts Konkretes bekannt.
- Im Jahr 2015 stellte das BKA einen selbst entwickelten Staatstrojaner fertig, der den Namen RCIS trägt. Dies steht für „Remote Communication Interception Software“. Darauf folgte eine aktualisierte Fassung namens „RCIS 2.0 Mobile“, die auch zur Telekommunikationsüberwachung von Tablets und Smartphones dienen kann. RCIS dient offenbar hauptsächlich oder sogar ausschließlich zum Abhören von Skype-Gesprächen.
- Anfang 2013 **sickerte durch**, dass das BKA die kommerzielle Trojaner-Software „FinFisher“ gekauft hatte, die auch als „FinSpy“ bekannt ist. Hersteller ist das deutsch-britische Unternehmen Gamma mit Sitz in München. FinFisher gilt als ultimatives Schweizer Messer der Online-Überwachung. Deshalb musste das BKA wohl eine abgespeckte Version bestellen, um im Rahmen des Erlaubten zu bleiben. Die Bundesregierung **bezahlte für ihre Lizenz 147.000 Euro**– nicht schlecht für ein Stück Software.“ MAURICIO. **Staatstrojaner erkennen & entfernen 2021: Was hilft gegen Überwachungssoftware?** Disponível em: [https://www-sonntagmorgen-com.translate.goog/staatstrojaner-erkennen/?\\_x\\_tr\\_sl=de&\\_x\\_tr\\_tl=pt&\\_x\\_tr\\_hl=pt-BR&\\_x\\_tr\\_pto=nui,sc](https://www-sonntagmorgen-com.translate.goog/staatstrojaner-erkennen/?_x_tr_sl=de&_x_tr_tl=pt&_x_tr_hl=pt-BR&_x_tr_pto=nui,sc) Acesso em 19.11.2021

**Em livre tradução:** Em junho de 2018, a revista [Netzpolitik.org](https://www.netzpolitik.org) publicou documentos vazados do governo federal que fornecem uma visão geral da história dos cavalos de Troia estaduais na Alemanha até o momento:

- Em 2007, a alfândega implantou o software da Era-IT Solutions como um cavalo de Tróia.
- A partir de 2008, as autoridades usaram software da DigiTask de Hessen. De acordo com os documentos, este foi o cavalo de Tróia estadual usado com mais frequência até o momento. Como o software poderia fazer mais do que a situação legal permitia, o oficial de proteção de dados soou o alarme e o DigiTask não está mais em uso.
- DigiTask se tornou propriedade da Rohde & Schwarz em 2018. A Netzpolitik presume que o desenvolvimento de um novo cavalo de Tróia está planejado aqui, mas nada específico é conhecido sobre ele.
- Em 2015, o BKA concluiu um cavalo de Troia autodesenvolvido, denominado RCIS. Isso significa "Software de intercetação de comunicação remota". Isso foi seguido por uma versão atualizada chamada "RCIS 2.0 Mobile", que também pode ser usada para monitoramento de telecomunicações de tablets e smartphones. O RCIS é aparentemente usado principalmente ou exclusivamente para espionar conversas do Skype.
- Começando 2013 vazou a informação que o BKA comprou o software Trojan comercial "FinFisher", também conhecido como "FinSpy". O fabricante é a empresa alemã-britânica Gamma, com sede em Munique. FinFisher é considerado o canivete suíço definitivo para vigilância online. Portanto, o BKA teve que solicitar uma versão enxuta para se manter dentro do permitido. O governo federal [pagou 147.000 euros pela licença](#) - nada mal para um software.

custo do desenvolvimento ou compra desse tipo de *malware*, o risco de que as vulnerabilidades exploradas pelo Estado pudessem também ser acessadas por interesses privados e ainda a legitimidade do Estado em utilizar métodos próprios da criminalidade, como meio do seu combate.<sup>230</sup>

Atualmente a nova redação do § 100b StPO<sup>231</sup>, regulamenta a *Online-Durchsuchung* (pesquisa on line), ali incluindo o catálogo de crimes que podem ser investigados com a utilização deste método, bem como os limites para sua implementação.

<sup>230</sup> “Die Vorstellung, dass staatliche Stellen Gelder der öffentlichen Hand direkt oder indirekt in kriminelle Strukturen investieren, ist schwer erträglich und mit Demokratie eigentlich unvereinbar.” GNAUER, Herbert **Weshalb der sogenannte Bundestrojaner eine schlechte Idee ist Gedanken angesichts eines zunehmenden Überwachungspopulismus**. Medienimpulse ISSN 2307-3187 Jg. 55, Nr. 3, 2017 Lizenz: CC-BY-NC-ND-3.0-AT . Disponível em: <file:///C:/Users/visitante/Downloads/1722-Artikeltext-1330-1-10-20190502.pdf>. Acesso em 26.11.2021

**Em livre tradução:** A ideia de que agências governamentais investem dinheiro público direta ou indiretamente em estruturas criminosas é difícil de suportar e, na verdade, incompatível com a democracia.

<sup>231</sup> Strafprozeßordnung (StPO)

§ 100b Online-Durchsuchung

(1) Auch ohne Wissen des Betroffenen darf mit technischen Mitteln in ein von dem Betroffenen genutztes informationstechnisches System eingegriffen und dürfen Daten daraus erhoben werden (Online-Durchsuchung), wenn

1. bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine in Absatz 2 bezeichnete besonders schwere Straftat begangen oder in Fällen, in denen der Versuch strafbar ist, zu begehen versucht hat,

2. die Tat auch im Einzelfall besonders schwer wiegt und

3. die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre.

(2) Besonders schwere Straftaten im Sinne des Absatzes 1 Nummer 1 sind:

1. aus dem Strafgesetzbuch:

a) Straftaten des Hochverrats und der Gefährdung des demokratischen Rechtsstaates sowie des Landesverrats und der Gefährdung der äußeren Sicherheit nach den §§ 81, 82, 89a, 89c Absatz 1 bis 4, nach den §§ 94, 95 Absatz 3 und § 96 Absatz 1, jeweils auch in Verbindung mit § 97b, sowie nach den §§ 97a, 98 Absatz 1 Satz 2, § 99 Absatz 2 und den §§ 100, 100a Absatz 4,

b) Betreiben krimineller Handelsplattformen im Internet in den Fällen des § 127 Absatz 3 und 4, sofern der Zweck der Handelsplattform im Internet darauf ausgerichtet ist, in den Buchstaben a und c bis o sowie in den Nummern 2 bis 10 genannte besonders schwere Straftaten zu ermöglichen oder zu fördern,

c) Bildung krimineller Vereinigungen nach § 129 Absatz 1 in Verbindung mit Absatz 5 Satz 3 und Bildung terroristischer Vereinigungen nach § 129a Absatz 1, 2, 4, 5 Satz 1 erste Alternative, jeweils auch in Verbindung mit § 129b Absatz 1,

d) Geld- und Wertzeichenfälschung nach den §§ 146 und 151, jeweils auch in Verbindung mit § 152, sowie nach § 152a Absatz 3 und § 152b Absatz 1 bis 4,

e) Straftaten gegen die sexuelle Selbstbestimmung in den Fällen des § 176 Absatz 1 und der §§ 176c, 176d und, unter den in § 177 Absatz 6 Satz 2 Nummer 2 genannten Voraussetzungen, des § 177,

f) Verbreitung, Erwerb und Besitz kinderpornografischer Inhalte in den Fällen des § 184b Absatz 1 Satz 1 und Absatz 2,

g) Mord und Totschlag nach den §§ 211, 212,

h) Straftaten gegen die persönliche Freiheit in den Fällen des § 232 Absatz 2 und 3, des § 232a Absatz 1, 3, 4 und 5 zweiter Halbsatz, des § 232b Absatz 1 und 3 sowie Absatz 4, dieser in Verbindung mit § 232a Absatz 4 und 5 zweiter Halbsatz, des § 233 Absatz 2, des § 233a Absatz 1, 3 und 4 zweiter Halbsatz, der §§ 234 und 234a Absatz 1 und 2 sowie der §§ 239a und 239b,

i) Bandendiebstahl nach § 244 Absatz 1 Nummer 2 und schwerer Bandendiebstahl nach § 244a,

j) schwerer Raub und Raub mit Todesfolge nach § 250 Absatz 1 oder Absatz 2, § 251,

### 3.5.3. Itália:

A Itália com a nova redação do art. 266 do Código de Processo Penal (artigo alterado pelo D.L n. 161, de 30 de dezembro de 2019, convertido, com alterações, pela Lei n. 7, de 28 de fevereiro de 2020<sup>232</sup>), incluiu a possibilidade de utilização do *captatore informatico* como método de obtenção de prova, podendo o mesmo ser utilizado para intercetação de e-mail, a ativação do microfone do aparelho, a captura imediata das imagens da câmera e acesso total a

- 
- k) räuberische Erpressung nach § 255 und besonders schwerer Fall einer Erpressung nach § 253 unter den in § 253 Absatz 4 Satz 2 genannten Voraussetzungen,
  - l) gewerbsmäßige Hehlerei, Bandenhehlerei und gewerbsmäßige Bandenhehlerei nach den §§ 260, 260a,
  - m) besonders schwerer Fall der Geldwäsche nach § 261 unter den in § 261 Absatz 5 Satz 2 genannten Voraussetzungen, wenn die Vortat eine der in den Nummern 1 bis 7 genannten besonders schweren Straftaten ist,
  - n) Computerbetrug in den Fällen des § 263a Absatz 2 in Verbindung mit § 263 Absatz 5,
  - o) besonders schwerer Fall der Bestechlichkeit und Bestechung nach § 335 Absatz 1 unter den in § 335 Absatz 2 Nummer 1 bis 3 genannten Voraussetzungen,
2. aus dem Asylgesetz:
    - a) Verleitung zur missbräuchlichen Asylantragstellung nach § 84 Absatz 3,
    - b) gewerbs- und bandenmäßige Verleitung zur missbräuchlichen Asylantragstellung nach § 84a Absatz 1,
  3. aus dem Aufenthaltsgesetz:
    - a) Einschleusen von Ausländern nach § 96 Absatz 2,
    - b) Einschleusen mit Todesfolge oder gewerbs- und bandenmäßiges Einschleusen nach § 97,
  4. aus dem Außenwirtschaftsgesetz:
    - a) Straftaten nach § 17 Absatz 1, 2 und 3, jeweils auch in Verbindung mit Absatz 6 oder 7,
    - b) Straftaten nach § 18 Absatz 7 und 8, jeweils auch in Verbindung mit Absatz 10,
  5. aus dem Betäubungsmittelgesetz:
    - a) besonders schwerer Fall einer Straftat nach § 29 Absatz 1 Satz 1 Nummer 1, 5, 6, 10, 11 oder 13, Absatz 3 unter der in § 29 Absatz 3 Satz 2 Nummer 1 genannten Voraussetzung,
    - b) eine Straftat nach den §§ 29a, 30 Absatz 1 Nummer 1, 2, 4, § 30a,
  6. aus dem Gesetz über die Kontrolle von Kriegswaffen:
    - a) eine Straftat nach § 19 Absatz 2 oder § 20 Absatz 1, jeweils auch in Verbindung mit § 21,
    - b) besonders schwerer Fall einer Straftat nach § 22a Absatz 1 in Verbindung mit Absatz 2,
  7. aus dem Grundstoffüberwachungsgesetz:
    - Straftaten nach § 19 Absatz 3,
  8. aus dem Neue-psychoaktive-Stoffe-Gesetz:
    - Straftaten nach § 4 Absatz 3 Nummer 1,
  9. aus dem Völkerstrafgesetzbuch:
    - a) Völkermord nach § 6,
    - b) Verbrechen gegen die Menschlichkeit nach § 7,
    - c) Kriegsverbrechen nach den §§ 8 bis 12,
    - d) Verbrechen der Aggression nach § 13,
  10. aus dem Waffengesetz:
    - a) besonders schwerer Fall einer Straftat nach § 51 Absatz 1 in Verbindung mit Absatz 2,
    - b) besonders schwerer Fall einer Straftat nach § 52 Absatz 1 Nummer 1 in Verbindung mit Absatz 5.
- (3) Die Maßnahme darf sich nur gegen den Beschuldigten richten. Ein Eingriff in informationstechnische Systeme anderer Personen ist nur zulässig, wenn auf Grund bestimmter Tatsachen anzunehmen ist, dass
1. der in der Anordnung nach § 100e Absatz 3 bezeichnete Beschuldigte informationstechnische Systeme der anderen Person benutzt, und
  2. die Durchführung des Eingriffs in informationstechnische Systeme des Beschuldigten allein nicht zur Erforschung des Sachverhalts oder zur Ermittlung des Aufenthaltsortes eines Mitbeschuldigten führen wird. Die Maßnahme darf auch durchgeführt werden, wenn andere Personen unvermeidbar betroffen werden.

documentos e imagens salvos em computador ou telefone digital, limitada essa utilização para investigação em casos de crimes previstos em catálogo previamente estabelecido, e em conformidade com procedimento ali previsto.

Assim o *malware*, na Itália denominado *captatore informatico*, permite que o investigador tanto tenha acesso a exibição imediata do que está sendo digitado no teclado do aparelho infetado por meio de um *keylogger*, como acesso imediato ao que aparece em sua

---

(4) § 100a Absatz 5 und 6 gilt mit Ausnahme von Absatz 5 Satz 1 Nummer 1 entsprechend.“ Strafprozeßordnung (StPO). Disponível em [https://www.gesetze-im-internet.de/stpo/\\_100b.html#:~:text=bestimmte%20Tatsachen%20den%20Verdacht%20begr%C3%BCnden,2](https://www.gesetze-im-internet.de/stpo/_100b.html#:~:text=bestimmte%20Tatsachen%20den%20Verdacht%20begr%C3%BCnden,2). Acesso em 26.11.2021

**Em livre tradução:**

Código de Processo Penal (StPO)

§ 100b Pesquisa online

(1) Mesmo sem o conhecimento do interessado, meios técnicos podem intervir em um sistema de tecnologia da informação utilizado pelo interessado e os dados podem ser coletados a partir dele (pesquisa online), se

1 Certos factos suscitam a suspeita de que alguém, como autor ou participante, cometeu um crime particularmente grave referido no n.º 2 ou, nos casos em que a tentativa é punível, tentou cometê-la,

2 o ato pesa particularmente em casos individuais e

3 a investigação dos fatos ou a determinação do paradeiro do acusado seria de outra forma significativamente mais difícil ou fútil.

(2) Delitos particularmente graves, na acepção do parágrafo 1 número 1, são:

1 do Código Penal:

a) Crimes de alta traição e que põem em perigo o estado constitucional democrático, bem como traição e põem em perigo a segurança externa de acordo com os §§ 81, 82, 89a, 89c parágrafos 1 a 4, de acordo com os §§ 94, 95, parágrafo 3 e § 96, parágrafo 1, respetivamente também em conexão com § 97b, bem como de acordo com §§ 97a, 98 parágrafo 1 frase 2, § 99 parágrafo 2 e §§ 100, 100a parágrafo 4,

b) Operação de plataformas de negociação criminosa na Internet nos casos do Artigo 127 (3) e (4), desde que o objetivo da plataforma de negociação na Internet seja permitir ou permitir crimes particularmente graves especificados nas letras “a” e “c” a o bem como nos números 2 a 10 apoiam financeiramente,

c) Formação de grupos criminosos de acordo com a Seção 129 (1) em conjunto com o Parágrafo 5 (3) e formação de grupos terroristas de acordo com a Seção 129a (1), (2), (4) e (5) primeira alternativa, em cada caso também em conjunto com a Seção 129b (1),

d) Falsificação de dinheiro e selos de acordo com as Seções 146 e 151, em cada caso também em conjunto com a Seção 152, bem como de acordo com a Seção 152a, Parágrafo 3 e Seção 152b, Parágrafos 1 a 4,

e) Ofensas contra a autodeterminação sexual nos casos da Seção 176 (1) e das Seções 176c, 176d e, nas condições especificadas na Seção 177 (6), sentença 2 número 2, da Seção 177,

f) Divulgação, aquisição e posse de conteúdo pornográfico infantil nos casos da Seção 184b, Parágrafo 1, Cláusula 1 e Parágrafo 2,

g) Assassinato e homicídio culposo de acordo com §§ 211, 212,

h) Ofensas contra a liberdade pessoal nos casos da Seção 232, Parágrafos 2 e 3, Seção 232a Parágrafos 1, 3, 4 e 5, segunda metade da frase, Seção 232b Parágrafos 1 e 3 e Parágrafo 4, isto em conjunto com a Seção 232a Parágrafos 4 e 5 segunda meia frase, da Seção 233 (2), Seção 233a (1), 3 e 4, segunda meia frase, Seções 234 e 234a (1) e (2) e Seções 239a e 239b,

i) Roubo de gangue de acordo com a seção 244 parágrafo 1 número 2 e roubo de gangue grave de acordo com a seção 244a,

j) roubo grave e roubo resultando em morte de acordo com a Seção 250 (1) ou (2), Seção 251,

k) Extorsão predatória de acordo com a Seção 255 e um caso particularmente grave de extorsão de acordo com a Seção 253 nas condições especificadas na Seção 253 (4), sentença 2,

l) Roubo comercial, roubo de gangue e roubo de gangue comercial de acordo com §§ 260, 260a,

m) um caso particularmente grave de lavagem de dinheiro de acordo com a seção 261 sob as condições especificadas na seção 261 (5), sentença 2, se o crime anterior for um dos crimes particularmente graves

tela por meio de um *screenshot*.

A primeira decisão que trata da utilização de *malware*, e que o nomeou como *captatore informatico*, é datada de 14.10.2009<sup>233</sup>, decidindo a Suprema Corte de Cassação pela possibilidade de utilização de *malware* em investigação criminal, por não considerar seu uso violação aos arts. 14 e 15 da Constituição Federal Italiana, que dispõem sobre

- 
- especificados nos números 1 a 7,
  - n) Fraude de computador nos casos da Seção 263a (2) em conjunto com a Seção 263 (5),
  - o) caso particularmente grave de corrupção e suborno de acordo com a seção 335, parágrafo 1, nas condições especificadas na seção 335, parágrafo 2, números 1 a 3,
- 2 da Lei de Asilo:
- a) Indução a pedidos abusivos de asilo de acordo com a Seção 84 (3),
  - b) indução comercial e de gangues a pedidos abusivos de asilo de acordo com § 84a parágrafo 1,
- 3 da Lei de Residência:
- a) Contrabando de estrangeiros de acordo com a Seção 96 (2),
  - b) O contrabando resulta em morte ou o contrabando em regime comercial ou de gangue, de acordo com a Seção 97,
- 4 da Lei de Comércio Exterior:
- a) Ofensas criminais nos termos da Seção 17 (1), (2) e (3), também em conjunto com (6) ou (7),
  - b) Ofensas criminais de acordo com a Seção 18 (7) e (8), também em conjunto com a Seção 10,
- 5 da Lei de Narcóticos:
- a) caso particularmente grave de um crime de acordo com a Seção 29 (1), sentença 1, número 1, 5, 6, 10, 11 ou 13, parágrafo 3, sob a condição especificada na Seção 29 (3), sentença 2 número 1,
  - b) uma infração penal de acordo com §§ 29a, 30 parágrafo 1 números 1, 2, 4, § 30a,
- 6 da Lei sobre o Controle de Armas Militares:
- a) uma ofensa criminal de acordo com a Seção 19 (2) ou Seção 20 (1), em cada caso também em conjunto com a Seção 21,
  - b) caso particularmente grave de uma ofensa criminal nos termos da Seção 22a (1) em conjunto com (2),
- 7 da Lei de Monitoramento de Substâncias Básicas:
- Ofensas criminais nos termos da Seção 19 (3),
- 8 da Nova Lei de Substâncias Psicoativas:
- Ofensas criminais de acordo com a seção 4 (3) número 1,
- 9 do Código Penal Internacional:
- a) Genocídio de acordo com § 6,
  - b) Crimes contra a humanidade de acordo com o § 7,
  - c) Crimes de guerra de acordo com os §§ 8 a 12,
  - d) Crimes de agressão de acordo com § 13,
- 10 da Lei de Armas:
- a) um caso particularmente grave de uma ofensa criminal nos termos da Seção 51 (1) em conjunto com (2),
  - b) caso particularmente grave de uma infração penal nos termos da Seção 52 (1) número 1 em conjunto com (5).
- (3) A medida só pode ser dirigida contra o acusado. A intervenção nos sistemas de tecnologia da informação de outras pessoas só é permitida se, com base em certos fatos, se puder presumir que
- 1 o acusado nomeado na ordem de acordo com a Seção 100e, parágrafo 3 usa os sistemas de tecnologia da informação da outra pessoa, e
  - 2 a intervenção nos sistemas informáticos dos arguidos, por si só, não conduzirá à investigação dos factos nem à determinação do paradeiro do co-arguido.
- A medida também pode ser realizada se outras pessoas forem inevitavelmente afetadas.
- (4) Os n.os 5 e 6 da secção 100-A aplicam-se em conformidade, com excepção do n.º 5, frase 1, número 1

<sup>232</sup> “**Codice di Procedura Penale**

inviolabilidade de domicílio e de sigilo de correspondência e das comunicações<sup>234</sup>

Seis anos após, em nova decisão sobre utilização de *malware* em investigação criminal, a Suprema Corte de Cassação nomeando dessa vez o *malware* de agente *intrusore*<sup>235</sup>, mais uma vez valida a possibilidade de utilização dessa técnica de obtenção de prova<sup>236</sup>, apenas disciplinando os limites de sua utilização naquele caso colocado *sub judice*.

Com a atual redação do art. 266 do CPP Italiano, a utilização de *malware*, ali

---

#### Capo IV

##### Intercettazioni di conversazioni o comunicazioni

Art. 266.

Limiti di ammissibilità.

1. L'intercettazione di conversazioni o comunicazioni telefoniche e di altre forme di telecomunicazione è consentita nei procedimenti relativi ai seguenti reati:

a) delitti non colposi per i quali è prevista la pena dell'ergastolo o della reclusione superiore nel massimo a cinque anni determinata a norma dell'articolo 4;

b) delitti contro la pubblica amministrazione per i quali è prevista la pena della reclusione non inferiore nel massimo a cinque anni determinata a norma dell'articolo 4;

c) delitti concernenti sostanze stupefacenti o psicotrope;

d) delitti concernenti le armi e le sostanze esplosive;

e) delitti di contrabbando;

f) reati di ingiuria, minaccia, usura, abusiva attività finanziaria, abuso di informazioni privilegiate, manipolazione del mercato, molestia o disturbo alle persone col mezzo del telefono;

f-bis) delitti previsti dall'articolo 600-ter, terzo comma, del codice penale, anche se relativi al materiale pornografico di cui all'articolo 600-quater.1 del medesimo codice, nonché dall'art. 609-undecies;

f-ter) delitti previsti dagli articoli 444, 473, 474, 515, 516, 517-quater e 633, secondo comma, del codice penale;

f-quater) delitto previsto dall'articolo 612-bis del codice penale;

f-quinquies) delitti commessi avvalendosi delle condizioni previste dall'articolo 416-bis del codice penale ovvero al fine di agevolare l'attività delle associazioni previste dallo stesso articolo.

2. Negli stessi casi è consentita l'intercettazione di comunicazioni tra presenti, che può essere eseguita anche mediante l'inserimento di un captatore informatico su un dispositivo elettronico portatile. Tuttavia, qualora queste avvengano nei luoghi indicati dall'articolo 614 del codice penale, l'intercettazione è consentita solo se vi è fondato motivo di ritenere che ivi si stia svolgendo l'attività criminosa.

2-bis. L'intercettazione di comunicazioni tra presenti mediante inserimento di captatore informatico su dispositivo elettronico portatile è sempre consentita nei procedimenti per i delitti di cui all'articolo 51, commi 3-bis e 3-quater, e, previa indicazione delle ragioni che ne giustificano l'utilizzo anche nei luoghi indicati dall'articolo 614 del codice penale, per i delitti dei pubblici ufficiali o degli incaricati di pubblico servizio contro la pubblica amministrazione per i quali è prevista la pena della reclusione non inferiore nel massimo a cinque anni, determinata a norma dell'articolo 4.

Art. 266-bis.

Intercettazioni di comunicazioni informatiche o telematiche.

1. Nei procedimenti relativi ai reati indicati nell'articolo 266, nonché a quelli commessi mediante l'impiego di tecnologie informatiche o telematiche, è consentita l'intercettazione del flusso di comunicazioni relativo a sistemi informatici o telematici ovvero intercorrente tra più sistemi.

Art. 267.

Presupposti e forme del provvedimento.

1. Il pubblico ministero richiede al giudice per le indagini preliminari l'autorizzazione a disporre le operazioni previste dall'art. 266. L'autorizzazione è data con decreto motivato quando vi sono gravi indizi di reato e l'intercettazione è assolutamente indispensabile ai fini della prosecuzione delle indagini. Il decreto che autorizza l'intercettazione tra presenti mediante inserimento di captatore informatico su dispositivo elettronico portatile indica le ragioni che rendono necessaria tale modalità per lo svolgimento delle indagini; nonché, se si procede per delitti diversi da quelli di cui all'articolo 51, commi 3-bis e 3-quater, e dai delitti dei pubblici ufficiali o degli incaricati di pubblico servizio contro la pubblica amministrazione per i quali è prevista la pena della reclusione

denominado *captatore informatico*, já encontra catálogo próprio, bem como os limites e o modo de sua utilização.

As disposições procedimentais da legislação italiana quanto a utilização de *malware* em investigação criminal, também estão de acordo com as normativas da Comunidade Europeia que por sua vez, não estabelece limites rígidos para a interceptação ambiental, deixando que cada Estado estabeleça suas regras, desde que respeitando as garantias acusatórias mínimas, como se pode ver de alguns julgados do Tribunal Europeu dos Direitos

---

non inferiore nel massimo a cinque anni, determinata a norma dell'articolo 4, i luoghi e il tempo, anche indirettamente determinati, in relazione ai quali è consentita l'attivazione del microfono.

1-bis. Nella valutazione dei gravi indizi di reato si applica l'articolo 203.

2. Nei casi di urgenza, quando vi è fondato motivo di ritenere che dal ritardo possa derivare grave pregiudizio alle indagini, il pubblico ministero dispone l'intercettazione con decreto motivato, che va comunicato immediatamente e comunque non oltre le ventiquattro ore al giudice indicato nel comma 1. Il giudice, entro quarantotto ore dal provvedimento, decide sulla convalida con decreto motivato. Se il decreto del pubblico ministero non viene convalidato nel termine stabilito, l'intercettazione non può essere proseguita e i risultati di essa non possono essere utilizzati.

2-bis. Nei casi di cui al comma 2, il pubblico ministero può disporre, con decreto motivato, l'intercettazione tra presenti mediante inserimento di captatore informatico su dispositivo elettronico portatile soltanto nei procedimenti per i delitti di cui all'articolo 51, commi 3-bis e 3-quater e per i delitti dei pubblici ufficiali o degli incaricati di pubblico servizio contro la pubblica amministrazione per i quali è prevista la pena della reclusione non inferiore nel massimo a cinque anni, determinata a norma dell'articolo 4. A tal fine indica, oltre a quanto previsto dal comma 1, secondo periodo, le ragioni di urgenza che rendono impossibile attendere il provvedimento del giudice. Il decreto è trasmesso al giudice che decide sulla convalida nei termini, con le modalità e gli effetti indicati al comma 2.

3. Il decreto del pubblico ministero che dispone l'intercettazione indica le modalità e la durata delle operazioni. Tale durata non può superare i quindici giorni, ma può essere prorogata dal giudice con decreto motivato per periodi successivi di quindici giorni, qualora permangano i presupposti indicati nel comma 1.

4. Il pubblico ministero procede alle operazioni personalmente ovvero avvalendosi di un ufficiale di polizia giudiziaria.

5. In apposito registro riservato gestito, anche con modalità informatiche, e tenuto sotto la direzione e la sorveglianza del Procuratore della Repubblica, sono annotati, secondo un ordine cronologico, i decreti che dispongono, autorizzano, convalidano o prorogano le intercettazioni e, per ciascuna intercettazione, l'inizio e il termine delle operazioni.”

Codice di Procedura Penale. Disponível em <https://www.altalex.com/documents/news/2014/03/26/mezzi-di-ricerca-della-prova>. Acesso em 23.11.2021

**Em livre tradução:**

Capítulo IV

Escutas telefônicas de conversas ou comunicações

Art. 266.

Limites de elegibilidade.

1. A interceptação de conversas ou comunicações telefônicas e outras formas de telecomunicação é permitida em processos relativos aos seguintes crimes:

- a) Os crimes não culposos para os quais se preveja a pena de prisão perpétua ou superior a cinco anos, determinada nos termos do artigo 4.º;
- b) Os crimes contra a administração pública para os quais se prevê pena de prisão não inferior a cinco anos, determinada nos termos do artigo 4.º;
- c) crimes envolvendo entorpecentes ou substâncias psicotrópicas;
- d) crimes envolvendo armas e substâncias explosivas;
- e) crimes de contrabando;
- f) crimes de injúria, ameaça, usura, atividade financeira abusiva, abuso de informação privilegiada, manipulação de mercado, assédio ou perturbação telefônica;

Humanos, sendo certo que o mesmo ainda não enfrentou a questão da utilização de *malware* para investigação criminal.<sup>237</sup>

### 3.5.4 Espanha:

#### As diversas e constantes inovações tecnológicas e a possibilidade de sua utilização

f-bis) os crimes previstos no artigo 600-ter, parágrafo terceiro, do código penal, ainda que relativos a material pornográfico a que se refere o artigo 600-quater.1 do mesmo código, bem como no art. 609-undecies;

f-ter) os crimes previstos nos artigos 444, 473, 474, 515, 516, 517-quater e 633, parágrafo segundo, do código penal;

f-quater) crime previsto no artigo 612-bis do código penal;

f-quinques) os crimes cometidos com recurso às condições previstas no artigo 416-bis do código penal ou para facilitar as actividades das associações previstas no mesmo artigo.

2. Nos mesmos casos, é permitida a interceptação de comunicações entre os presentes, o que também pode ser efectuado inserindo um *captatore informatico* num dispositivo electrónico portátil. No entanto, se estas ocorrerem nos locais indicados no artigo 614 do Código Penal, a interceptação só é permitida se houver uma razão fundamentada para crer que aí se desenvolve a actividade criminosa.

2-bis. A interceptação de comunicações entre os presentes através da inserção de *captatore informatico* em dispositivo electrónico portátil é sempre permitida no processo dos crimes referidos no artigo 51.º, n.ºs 3-bis e 3-quater, e, após indicação dos motivos que justificam a utilização também nos locais indicados no artigo 614 do código penal, para os crimes de funcionários públicos ou encarregados da função pública contra a administração pública para os quais a pena de prisão não inferior a cinco anos, fixada nos termos com do artigo 4.

Art. 266-bis.

Intercepção de comunicações por computador ou telemática.

1. Nos processos relativos aos crimes indicados no artigo 266.º, bem como nos cometidos com a utilização de tecnologias da informação ou telemática, é permitida a interceptação do fluxo de comunicações relativas a sistemas de informação ou telemática ou entre vários sistemas.

Art. 267.

Premissas e formas da medida.

1. O Ministério Público pede ao juiz a realização de diligências preliminares para autorização para ordenar as operações previstas no art. 266. A autorização é dada por decreto fundamentado quando existem indícios graves de prática de crime e a interceptação é absolutamente imprescindível para o prosseguimento da investigação. O decreto que autoriza a interceptação entre os presentes por meio da inserção de *captatore informatico* em dispositivo electrónico portátil indica os motivos que tornam esse procedimento necessário para a realização das investigações; bem como, se proceder a crimes diversos dos referidos no artigo 51.º, n.ºs 3-bis e 3-quater, e dos crimes de funcionários públicos ou responsáveis de uma função pública contra a administração pública para os quais a pena de reclusão não seja inferior a cinco anos, fixada nos termos do art. 4º, os locais e os horários, mesmo que indiretamente determinados, em relação aos quais é permitido o acionamento do microfone.

1-bis. Na avaliação de provas graves de um crime, aplica-se o Artigo 203.

2. Em casos de urgência, quando existam motivos fundamentados para crer que o atraso pode causar sérios prejuízos às investigações, o Ministério Público ordena a interceptação por meio de decreto fundamentado, que deve ser comunicado de imediato e em qualquer caso o mais tardar vinte e quatro horas para o juiz indicado no nº 1. O juiz, no prazo de quarenta e oito horas a contar da disposição, delibera sobre a validação com decreto motivado. Se o decreto do Ministério Público não for validado no prazo estabelecido, a interceptação não pode ser continuada e o seu resultado não pode ser aproveitado.

2-bis. Nos casos a que se refere o n.º 2, o Ministério Público pode ordenar, mediante decreto motivado, a interceptação dos presentes, mediante a inserção de *captatore informatico* em dispositivo electrónico portátil, apenas no processo pelos crimes de nos termos do artigo 51.º, n.ºs 3-bis e 3-quartos e para os crimes de funcionários públicos ou responsáveis de uma função pública contra a administração pública para os quais se prevê pena de prisão não inferior a cinco anos, determinado nos termos do artigo 4.º. Para o efeito, indica, para além do disposto no n.º 1, segunda frase, os motivos da urgência que impossibilitam o aguardar a decisão do

para a investigação criminal, encontraram na Espanha demora para sua disciplina e inclusão, seja em decisões, seja em diplomas legislativos<sup>238</sup>, o que levou o Tribunal Europeu de Direito Humanos (TEDH), por mais de uma vez, a condenar os Tribunais espanhóis a regulamentarem a intervenção em comunicações, ante a ausência de regulamentação legislativa específica.<sup>239</sup>

O Tribunal Superior e o Tribunal Constitucional, ante a ausência de legislação específica, passaram a disciplinar os casos onde a utilização de métodos informáticos foram

juiz. O decreto é enviado ao juiz que decide sobre a validação nos termos, com os métodos e efeitos indicados no n.º 2.

3. O decreto do representante do Ministério Público que ordena a interceptação indica os métodos e a duração das operações. Esta duração não pode ultrapassar quinze dias, mas pode ser prorrogada pelo juiz, mediante decreto motivado, por períodos subsequentes de quinze dias, se se mantiverem as condições indicadas no n.º 1.

4. O Ministério Público realiza as operações pessoalmente ou com a ajuda de um agente da polícia judiciária.

5. Num registo especial confidencial gerido, também por meios informáticos, e mantido sob a direcção e supervisão do Ministério Público, são anotados, segundo uma ordem cronológica, os decretos que ordenam, autorizam, validam ou prorrogam as interceptações e, para cada interceptação, o início e o fim das operações.

<sup>233</sup>“Confermerebbero tale tesi le concrete modalità esecutive del decreto de quo, consistite nella installazione, all'interno del sistema operativo del personal computer, di un **captatore informatico** (gosth) in grado di memorizzare i files già esistenti e di registrare in tempo reale tutti i files elaborandi, in tal modo innescando un monitoraggio occulto e continuativo del detto computer (protrattosi per oltre otto mesi).” Destaquei. Corte de Cassazoni, sezione V penale, sentenza 14 ottobre 2009, n. 16556. Disponível em <https://www.penale.it/page.asp?mode=1&IDPag=1228>. Acesso em 23.11.2021

**Em livre tradução:** Esta tese é confirmada pelos métodos executivos concretos do decreto, que consiste na instalação, dentro do sistema operacional do computador pessoal, de um **captatore informatico** (gosth) capaz de armazenar os arquivos existentes e registrar todos os arquivos em tempo real, desencadeando assim um monitoramento oculto e contínuo do referido computador (que durou mais de oito meses). Destaquei

<sup>234</sup> “Detta corte ha ritenuto, correttamente, che l'attività captativa non avesse violato nè l'art. 14 Cost. nè l'art. 15 Cost.. Invero, l'apparecchio monitorato con l'installazione del **captatore informatico** non era collocato in un luogo domiciliare ovvero in un luogo di privata dimora, ancorchè intesa nella sua più ampia accezione, bensì in un luogo aperto al pubblico. Il personal computer, infatti, "si trovava nei locali sede di un ufficio pubblico comunale, ove sia l'imputato sia gli altri impiegati avevano accesso per svolgere le loro mansioni ed ove potevano fare ingresso, sia pure in determinate condizioni temporali, il pubblico degli utenti ed il personale delle pulizie, insomma una comunità di soggetti non particolarmente estesa, ma nemmeno limitata o determinabile a priori in ragione di una determinazione personale dell'imputato". D'altra parte, nel caso di specie, non poteva essere invocata la tutela costituzionale della riservatezza della corrispondenza ed in genere delle comunicazioni, giacchè "quanto riprodotto in copia non era un testo inoltrato e trasmesso col sistema informatico, ma soltanto predisposto per essere stampato su supporto cartaceo e successivamente consegnato sino al suo destinatario".” Destaquei. Corte de Cassazoni, sezione V penale, sentenza 14 ottobre 2009, n. 16556. Disponível em <https://www.penale.it/page.asp?mode=1&IDPag=1228>. Acesso em 23.11.2021

**Em livre tradução:** Este tribunal considerou, corretamente, que a atividade captativa não violou nem o art. 14 da Constituição nem o art. 15. Com efeito, o dispositivo monitorado com a instalação do **captatore informatico** não se localizava em local domiciliar ou em local de residência particular, ainda que entendido em seu sentido mais amplo, mas em local aberto ao público. O computador pessoal, aliás, “localizava-se nas dependências de uma repartição pública municipal, onde tanto o arguido como os restantes funcionários tinham acesso para o exercício das suas funções e onde o público dos utentes e pessoal de limpeza, enfim, uma comunidade de assuntos não particularmente extensos, mas nem mesmo limitados ou determináveis a priori com base em uma determinação pessoal do acusado”. Por outro lado, no caso em apreço, não se poderia invocar a tutela constitucional do sigilo da correspondência e das comunicações em geral, uma vez que “o que foi reproduzido em cópia não foi um texto encaminhado e transmitido em sistema informático, mas apenas preparado para ser impressa em papel e posteriormente entregue ao seu destinatário”. Destaquei

<sup>235</sup> “R. e G.S., ha disposto sia l'intercettazione d'urgenza telematica, tramite **agente intrusore** (virus informatico), di tutto il traffico dati, in relazione agli apparecchi utilizzati dai predetti, sia di tutte le conversazioni tra presenti,

utilizados para obtenção de provas, utilizando analogicamente os princípios e a legislação processual base que disciplinavam as escutas telefônicas, em concerto com a Constituição Espanhola<sup>240 241 242</sup>

A Lei Orgânica de 13/2015, introduziu significativas alterações na Ley de Enjuiciamiento Criminal (LEcrim), trazendo em seu Capítulo IV “Disposições comuns à interceptação de comunicações telefônicas e telemáticas, a captura e gravação de comunicações orais através da utilização de dispositivos eletrônicos, a utilização de dispositivos técnicos de

mediante l'attivazione, attraverso il predetto virus, del microfono e della videocamera dei relativi Smartphone.” (sem destaque no original) Corte de Cassazoni, sezione V penale, sentenza 26 maggio 2015, n. 27100. Disponível em: <https://www.penale.it/page.asp?IDPag=1201>. Acesso em 23.11.2021

**Em livre tradução:** R. e G.S. ordenou tanto a intercetção eletrônica de emergência, por meio de um **agente intrusore** (vírus de computador), de todo o tráfego de dados, em relação aos dispositivos utilizados pelos citados, e de todas as conversas entre os presentes, por acionamento, por meio do vírus mencionado, do microfone e câmara de vídeo dos smartphones relacionados.

<sup>236</sup> “Si tratta infatti di una questione non di legittimità della tecnica di acquisizione probatoria, in sè considerata, ma di utilizzabilità delle relative risultanze.” Corte de Cassazoni, sezione V penale, sentenza 26 maggio 2015, n. 27100. Disponível em: <https://www.penale.it/page.asp?IDPag=1201>. Acesso em 23.11.2021

**Em livre tradução:** Na verdade, é uma questão não da legitimidade da técnica de aquisição do material probatório considerada em si mesma, mas da usabilidade do material dela resultante.

<sup>237</sup> “Quindi, tale comma 2 Art. 266 Cpp limita le intercettazioni ambientali nelle dimore private, ma non viene stabilita alcuna limitazione per la legittimità, o meno, dell'uso del trojan horse in luoghi pubblici, in luoghi aperti al pubblico o, ognimmodo, in qualsivoglia luogo che non sia un domicilio privato. Anche nel Diritto Comunitario europeo, la Normativa UE si limita a fornire delle direttive generali, ma, in definitiva, lascia ai singoli Legislatori nazionali un ampio margine di autonomia de jure condito. P.e., Corte EDU 31/05/2005 Vetter vs. Francia (ripreso poi da Corte EDU 18/05/2010 Kennedy vs. Regno Unito) afferma, in maniera lata e generica, che occorre “statuire garanzie minime, [ ... ] la legge nazionale deve apprestare garanzie nella materia delle intercettazioni [ ... ]. Bisogna predeterminare la tipologia delle comunicazioni oggetto di intercettazione, [ nonché ] le modalità della ricognizione dei reati che giustificano tale mezzo di intrusione nella privacy [ ed è necessario ] predefinire la qualificazione delle categorie di persone che possono essere intercettate ed i limiti di durata delle intercettazioni “ Come si può notare, Corte EDU 31/05/2005 Vetter vs. Francia, nonché Corte EDU 18/05/2010 Kennedy vs. Regno Unito giuridificano la tematica delle intercettazioni in modo financo eccessivamente vago, con la prevedibile conseguenza che ciascun Legislatore comunitario reca un notevole margine di autonomia dispositiva. Tantomeno, la Corte EDU non si è mai addentrata nella spinosa tematica dell'intrusore informatico, salvo imporre alcuna minime garanzie accusatorie, che, comunque, sono analoghe a ciò che risulta statuito negli ottimi e ben nitidi Artt. 14 e 15 della vigente Costituzione italiana. Pertanto, Cass., SS.UU., 28 aprile 2016, n. 26889 conclude che la Giurisprudenza dell'UE è perfettamente compatibile con il comma 2 Art. 266 Cpp, ma ciò non risolve la problematica “dell'intercettazione per mezzo del virus informatico, [perché] la caratteristica tecnica di tale modalità di captazione prescinde dal riferimento al luogo [della dimora privata], trattandosi di un'intercettazione ambientale per sua natura itinerante “.” ALTIERI, Andrea Baiguera. **Le intercettazioni a mezzo captatore informatico** - 4 ottobre 2021. Disponível em <https://www.diritto.it/le-intercettazioni-a-mezzo-captatore-informatico/> Acesso em 23.11.2021

**Em livre tradução:** Portanto, este parágrafo 2 Art. 266 Cpp limita as interceptações ambientais em residências privadas, mas nenhuma limitação é estabelecida para a legitimidade, ou não, do uso do *trojan horse* em locais públicos, em locais abertos ao público ou, em qualquer caso, em qualquer lugar que não seja uma residência particular. Mesmo no direito da Comunidade Europeia, a legislação da UE limita-se a fornecer diretivas gerais, mas, em última análise, deixa aos legisladores nacionais individuais uma ampla margem de autonomia para legislar. Por exemplo, TEDH 31/05/2005 Vetter vs. A França (posteriormente retomada pela CEDH 18/05/2010 Kennedy vs. Reino Unido) afirma, de forma ampla e genérica, que é necessário “estabelecer garantias mínimas, [...] o direito nacional deve fornecer garantias na matéria de escuta telefônica [...]. É necessário predeterminar o tipo de comunicação objeto de interceptação, [bem como] os métodos de reconhecimento dos crimes que justificam este meio de intrusão na privacidade [e é necessário] pré-definir a qualificação das categorias de pessoas quem pode ser interceptado e os limites de duração das interceptações”. Como se pode ver, o TEDH

monitorização, localização e captura de imagens, o registo de dispositivos de armazenamento massivo de informação e registos remotos em computador equipamento”.

Os dispositivos que se encontram no Capítulo IV e nos capítulos que se seguem, estão incorporados ao artigo 588 da LECrim, agrupados de acordo com o método de obtenção de prova a ser utilizado, disciplinando várias possibilidades de interceptação, mas também de utilização de recursos tecnológicos a serem utilizados na recolha de material probatório<sup>243</sup>

---

31/05/2005 Vetter vs. França, bem como TEDH 18/05/2010 Kennedy vs. Reino Unido juridifica o assunto das escutas telefónicas de uma forma excessivamente vaga, com a consequência previsível de que cada legislador comunitário dispõe de uma margem considerável de autonomia dispositiva. Nem o TEDH nunca entrou na espinhosa questão do *intruso informático* exceto para impor algumas garantias acusatórias mínimas, que, em qualquer caso, são semelhantes ao que se estabelece nos excelentes e claros artigos 14 e 15 da atual Constituição italiana. Portanto, Cass., SS.UU., 28 de abril de 2016, n. 26889 conclui que a jurisprudência da UE é perfeitamente compatível com o parágrafo 2 Art. 266 CPP, mas isso não resolve o problema "de interceptação por meio de vírus de computador, [porque] a característica técnica deste método de coleta é independente da referência ao local [da residência privada], por se tratar de uma interceptação ambiental pelo seu caráter itinerante”.

<sup>238</sup> “For several years the Spanish Code of Criminal Procedure was highly criticized due to its inability to keep pace with the evolution of technology.<sup>30</sup> The Spanish legislator’s general lack of activity confronted law enforcement and jurisprudence with a choice between conformity with ineffectiveness or the use of new tools for collecting evidence without specific legal basis. The choice fell on the latter. Thus, gradually the Spanish courts began compensating for the inadequacy of its legislation by allowing the use of new investigative technologies, with a broad legal interpretation of the existing legislation and the Spanish Constitution.” VACIAGO, Giuseppe e RAMALHO, David Silva. **Online searches and online surveillance: the use of trojans and other types of malware as means of obtaining evidence in criminal proceedings.** *In Digital Evidence & Elec. Signature L. Rev.*, v. 13, p. 93, 2016. p. 89-90. Disponível em <https://journals.sas.ac.uk/deeslr/article/view/2299/2252>. Acesso em 23/09/2021

**Em livre tradução:** Durante vários anos, o Código de Processo Penal espanhol foi muito criticado devido à sua incapacidade de acompanhar a evolução da tecnologia. A falta geral de atividade do legislador espanhol confrontou a aplicação da lei e a jurisprudência com uma escolha entre a conformidade com a inefetividade ou a utilização de novos instrumentos de coleta de provas sem embasamento jurídico específico. A escolha recaiu sobre este último. Assim, gradualmente os tribunais espanhóis começaram a compensar o inadequação de sua legislação ao permitir o uso de novas tecnologias investigativas, com ampla interpretação jurídica da legislação existente e da Constituição Espanhola

<sup>239</sup>“Sin embargo, en España aún no se ha llevado a cabo la necesaria y urgente actualización de la LECRIM que recoja, con los debidos márgenes de apreciación judicial en función de las circunstancias de cada caso, las modernas técnicas de investigación que la Informática proporciona (...) Como sabemos, la deficiente regulación procesal española en materia de intervención de las comunicaciones, denunciada de manera reiterada tanto por la doctrina como por el Tribunal Supremo y el Tribunal Constitucional, y motivo por el cual el TEDH condenó en dos ocasiones a España, ha obligado a que sean los tribunales quienes se hayan encargado de establecer y concretar los requisitos necesarios para legitimar la intervención de las telecomunicaciones y su valides probatoria” PRADILLO, Juan Carlos Ortiz. **“Hacking” legal al servicio de la investigación criminal: nuevos instrumentos para la investigación y prueba de la delincuencia informática in Delincuencia informática.** *Tiempos de cautela y amparo: Cizur Menor (Espanha).* Thomson Reuters Editorial Aranzadi, 2012. págs. 195 e 196

<sup>240</sup> “A estas apreciaciones, habría de añadirse que la actuación policial respetó el principio de proporcionalidad, pues se trata de una medida idónea para la investigación del delito (del terminal informático se podían extraer – como así fue– pruebas incriminatorias y nuevos datos para la investigación), imprescindible en el caso concreto (no existían otras menos gravosas) y fue ejecutada de tal modo que el sacrificio del derecho fundamental a la intimidad no resultó desmedido en relación con la gravedad de los hechos y las evidencias existentes. En este punto, merece subrayarse que el órgano judicial no estuvo durante un espacio prolongado de tiempo al margen de la iniciativa adoptada por la Policía, pues ésta inmediatamente (a los dos días) dio cuenta al Juez de

O Capítulo IX, tem por *nomen iuris* “Registros remotos sobre equipos informáticos”, onde está regulada no artigo 588 septies a., a utilização de *software* como método de recolha de prova, com previsão do catálogo de crimes onde tal recurso investigativo pode ser utilizado, bem como os pressupostos e requisitos para sua aplicação<sup>244</sup>

Com essa alteração da LECrim, a legislação espanhola passa a prever expressamente a utilização de *software* como método de obtenção de prova, sendo mais um Estado a regulamentar seu uso, o fazendo de forma detalhada, usando a terminologia convencional, em

Instrucción, pudiendo entonces éste hacer la conveniente ponderación sobre si dicha diligencia estaba o no justificada, después de oír, como hemos visto, al instructor del atestado instruido. De todo lo cual cabe concluir que, siendo la actuación policial constitucionalmente legítima, el sacrificio del derecho fundamental afectado estaba justificado por la presencia de otros intereses constitucionalmente relevantes, no pudiendo apreciarse vulneración alguna del derecho a la intimidad personal del recurrente.” Sentencia Tribunal Constitucional núm. 173/2011 (Sala Segunda), de 7 noviembre. análisis policial de portátil de pedófilo sin autorización judicial. Recurso de Amparo núm. 5928/2009. BOE 7 diciembre 2011, núm. 294 (suplemento). **Delincuencia informática**. Tiempos de cautela y amparo: Cizur Menor (Espanha). Thomson Reuters Editorial Aranzadi, 2012. CD-ROM, pasta 6

<sup>241</sup> “En estas circunstancias, en las que se pone de manifiesto que la policía judicial intentó la investigación de los hechos por otras vías alternativas menos gravosas sin éxito, durante cinco meses –del 24 de marzo al 31 de agosto de 2000–, y en las que la utilización de las tecnologías de la información a la vez que facilitan la comisión del delito dificultan su persecución, no puede sostenerse que la investigación de un delito contra la propiedad intelectual cometido mediante la utilización de las tecnologías de la información carezca de la entidad necesaria para considerar desproporcionada la intervención de la línea del teléfono móvil de contacto que aparecía en la página *web* en la que se ofertaban los productos informáticos. En definitiva, en el juicio de proporcionalidad de la interceptación de las comunicaciones telefónicas, además de la gravedad de la pena, del bien jurídico protegido y de la comisión del delito por organizaciones criminales, también puede ponderarse la incidencia del uso de las tecnologías de la información, pues su abuso facilita la perpetración del delito y dificulta su persecución.” Sentencia Tribunal Constitucional núm. 104/2006 (Sala Primera), de 3 abril. Recurso de Amparo núm. 7224/2002. BOE 9 mayo 2006, núm. 110 (suplemento). **Delincuencia informática**. Tiempos de cautela y amparo: Cizur Menor (Espanha). Thomson Reuters Editorial Aranzadi, 2012. CD-ROM, pasta 9

<sup>242</sup> “I) Uno de los requisitos que ha de observarse en la intervención judicial de las conversaciones telefónicas es la justificación de la medida, que se desdobra en una triple vertiente de: A) Proporcionalidad de la misma; B) Existencia de indicios de un delito y de la intervención en él de una o varias personas y de que por la observación telefónica se podrán conseguir datos importantes para acreditar el delito o la participación en el mismo del delincuente; y C) Explicitación de la justificación mediante la pertinente motivación. A) Según criterio expuesto en la STC de 16-12-1996 (RTC 1996\207) , para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad es necesario constatar si cumple estos tres requisitos: a) si la medida acordada puede conseguir el objetivo propuesto (juicio de idoneidad); b) si es necesaria, en el sentido que no exista otro medio más moderado para conseguir el fin propuesto con igual eficacia (juicio de necesidad); y c) si la medida es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto). La jurisprudencia (SS. 239/1997 de 25-2 [RJ 1997\1376] ) ha entendido que no cabe acordar la intervención telefónica cuando se trate de infracciones penales de menor gravedad, debiendo medirse tal dato no sólo con relación a la pena con la que la Ley las sanciona, sino teniendo en cuenta también el reproche social que determinados delitos pueden merecer. B) En relación a la concurrencia de indicios delictivos, ha de tenerse en cuenta que el art. 579.2 de la LECrim (LEG 1882\16) , condiciona la autorización de la intervención telefónica a que se haya procesado alguna persona y a que existan indicios de que por este medio de investigación se puede obtener algún dato importante para la causa penal. El mismo artículo, en el apartado 3 condiciona la intervención telefónica, no ya a que haya un procesamiento, sino a que existan indicios de criminalidad contra una persona. Según razona la citada sentencia 239/1997, cuando el proceso judicial se inicia a raíz de la petición policial de las escuchas, los indicios en tal caso no podrán consistir más que en sospechas fundadas en datos concretos, que es lo que la Policía comunica al Juez para que éste autorice la grabación de las conversaciones. C) En cuanto a la motivación de la autorización judicial que habilita la intervención, aparte de exigirse expresamente en el art. 579

inglês, sem criar nome próprio para tal método.

A utilização de *software* para obtenção de prova se trata de manejo de aparato tecnológico disponível para uso pelo Estado, sendo certo que tal aparato já vem sendo utilizado em larga escala por organizações criminosas, sem, ainda, o correspondente uso estatal para seu combate.

O argumento que o Estado estaria se valendo das mesmas armas que o crime organizado para combatê-lo, portanto praticando um ilícito com o pretexto de evitar ou perseguir e punir outro crime, é falacioso e não merece prosperar.

---

de la LECrim, la jurisprudencia la ha considerado necesaria a nivel constitucional, como elemento de la tutela judicial efectiva, en las resoluciones limitadoras o eliminadoras de derechos fundamentales ( STC 56/1987 de 14-5 [ RTC 1987\56] ). La motivación supone la expresión tanto de la existencia de los presupuestos materiales de la intervención –investigación, delito grave, conexión de las personas con los hechos–, como de la necesidad y adecuación de la medida, en cuyo caso, además, deben ponderarse las concretas circunstancias concurrentes en cada momento y el conocimiento adquirido a través de la ejecución de la medida inicialmente prevista. En orden a la debida motivación de las resoluciones judiciales que autorizan las intromisiones en los derechos constitucionales que protegen la intimidad y el secreto de las comunicaciones y la inviolabilidad del domicilio, tiene declarado el Tribunal Constitucional, así en las sentencias 200/1997 de 24-11 ( RTC 1997\200) , 49/1999 [ RTC 1999\49] , 139/1999 [ RTC 1999\139] , 166/1999 de 27-9 [ RTC 1999\166] , 171/1999 [ RTC 1999\171] y 14/2000 de 26-5, que la resolución puede estar motivada si, integrada con la solicitud a que se remite, contiene los elementos necesarios para considerar satisfechas las exigencias de ponderación de la restricción de derechos fundamentales que la proporcionalidad de la medida conlleva. II) Otro principio que debe regir la intervención judicial de las conversaciones telefónicas es el de especialidad, que significa que, concedida la autorización de las escuchas para la averiguación de un determinado hecho delictivo, no cabe que a través de la intervención se investiguen acciones criminales distintas, por lo que de surgir nuevos hechos, no previstos en la solicitud inicial, deberá extenderse la licencia judicial de escucha a los mismos de un modo formal. Por la jurisprudencia ( SS. 2-7-1993 [ RJ 1993\5692] y 21-1-1994) se ha matizado el principio de especialidad, entendiéndose que sólo se vulnera el mismo cuando se produce una novación del tipo penal investigado, pero no cuando exista una adicción o suma porque, aparte de las conversaciones sobre los hechos investigados, se produzcan otras sobre otros distintos. III) Un tercer requisito de la intervención telefónica procesal es el control judicial en el desarrollo de la misma. Por una parte, supone una supervisión procesal mientras tiene lugar la intervención telefónica, para constatar si hay razones –por las conversaciones escuchadas– para el mantenimiento de la medida, y por otra parte implica la actuación de selección de las conversaciones con utilidad probatoria, y la eliminación de las no relacionadas con los hechos investigados, y la incorporación de las primeras al proceso. Sentencia Tribunal Supremo núm. 1844/2002 (Sala de lo Penal), de 30 enero 2003. Recurso de Casación núm. 249/2001. **Delincuencia informática.** Tiempos de cautela y amparo: Cizur Menor (Espanha). Thomson Reuters Editorial Aranzadi, 2012. CD-ROM, pasta 9

<sup>243</sup> Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica. Disponible em <https://www.boe.es/buscar/pdf/2015/BOE-A-2015-10725-consolidado.pdf>. Acesso em 24.11.2021

<sup>244</sup> “Artículo 588 septies a. Presupuestos. 1. El juez competente podrá autorizar la utilización de datos de identificación y códigos, así como la instalación de un software, que permitan, de forma remota y telemática, el examen a distancia y sin conocimiento de su titular o usuario del contenido de un ordenador, dispositivo electrónico, sistema informático, instrumento de almacenamiento masivo de datos informáticos o base de datos, siempre que persiga la investigación de alguno de los siguientes delitos: a) Delitos cometidos en el seno de organizaciones criminales. b) Delitos de terrorismo. c) Delitos cometidos contra menores o personas con capacidad modificada judicialmente. d) Delitos contra la Constitución, de traición y relativos a la defensa nacional. e) Delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación o servicio de comunicación.” Disponible em <https://www.boe.es/buscar/pdf/2015/BOE-A-2015-10725-consolidado.pdf>. Acesso em 24.11.2021

Não seria justo com os integrantes das forças de segurança do Estado, ser-lhes fornecidos revólveres para combaterem criminosos armados com fuzis. Aqui, municiar os representantes do Estado com as mesmas ferramentas que o agressor, além de equilibrar a disputa de forças, pode fazer a diferença entre a vida e morte dos seus agentes.

A igualdade de armas, tão cara ao processo penal, deve ser também assegurada durante a investigação criminal, sob pena de não se poder falar em paridade durante o processo. Se há inadequação entre os métodos de prática do delito e aqueles destinados a coleta da prova para apuração desse mesmo delito, impossível ao Estado exercer com a eficiência desejada e devida, seu dever de persecução penal.

Esse descompasso entre a forma tecnológica como os delitos são praticados e os métodos obsoletos para a colheita de provas, coloca o Estado em posição débil e ineficiente ante a criminalidade que se organiza de maneira cada vez mais rápida, utilizando todos os meios disponíveis para alcançar seus objetivos.

Assim como em outras áreas de atuação do Estado se deseja e fomenta que ele esteja atento as novas tecnologias e se reclama sua utilização para que possa bem desempenhar sua função, o mesmo raciocínio deve ser utilizado para o seu desempenho na segurança pública - aí incluída a persecução e investigação criminal - onde se torna um imperativo a utilização das ferramentas tecnológicas disponíveis, em especial no combate a criminalidade mais sofisticada, que causa grandes danos sociais, como é o caso do crime organizado.

O universo de possibilidades para uso de tecnologias na investigação criminal é imenso, sendo fundamental estabelecer os limites que se pretende vencer nesta pesquisa. O objetivo encetado é o estudo do uso de *malware*, especificamente no caso de ações encobertas, como agente infiltrado virtual, visando a investigação e recolha de provas em casos de criminalidade organizada e altamente organizada.

#### 4. UTILIZAÇÃO DO *MALWARE* COMO AGENTE INFILTRADO VIRTUAL

O ordenamento português prevê a utilização de métodos de produção de prova que se desenvolvem em ambiente virtual ou relacionados a transmissão de dados por meio telemático, entretanto, as possibilidades presentes no ordenamento ainda encontram barreiras que a criminalidade tem buscado, muitas vezes com êxito, transpor.

Para avançar no aperfeiçoamento das técnicas de investigação e produção de provas, necessário delimitar as que já existem, para se delinear aquelas que ainda estão por ser construídas.

##### 4.1 BUSCAS *ON-LINE*

A doutrina tem utilizado o termo buscas *on-line* despidido de precisão técnica e univocidade de significado. É possível encontrar o termo buscas *on-line* como sinónimo de utilização de *malware*<sup>245</sup> para realização de qualquer operação em ambiente virtual, seja ela *verbi gratia*, de localização, cópia ou apreensão de dados. Tal busca é considerada método oculto de obtenção de prova.

Por outro viés, insere-se acertadamente aqueles que enveredam por fazer distinção entre buscas *on-line* e métodos ocultos de obtenção de prova<sup>246 247</sup>, entendendo que a busca *on-line* é apenas um dentre os métodos ocultos de obtenção de prova, podendo utilizar-se do

<sup>245</sup>“...conceito de *buscas on-line*. Um conceito compreensivo e abrangente, porventura mesmo não inteiramente rigoroso, a que se reconduz um conjunto de intromissões nos sistemas informáticos, feitas através da *internet* e que se atualizam na observação, busca, cópia, vigilância, etc., dos dados presentes naqueles sistemas informáticos.” ANDRADE, Manuel da Costa. **Bruscamente no Verão Passado**. Coimbra: Coimbra Editora, 2009. p. 166.

<sup>246</sup>“Quanto a nós, porquanto entendemos que se trata de um conceito novo no plano jurídico e que merece destacamento de outros conceitos com contornos e propósitos diferentes, optámos por nos referir exclusivamente ao conceito de *malware*, ou a cada uma de suas subespécies, nas suas vertentes de instalação, de pesquisa e de recolha de informação e não – salvo quando estritamente necessário – ao de *busca on-line*.” RAMALHO, Davi Silva. O uso de *malware* como meio de obtenção de prova em processo penal. In: **Revista de Concorrência e Regulação**. Ano IV, número 16. Coimbra: Almedina, 2013. p. 199.

<sup>247</sup>“Julgamos, contudo, que o conceito de busca já não permite abarcar as situações em que a utilização de *malware* se traduz, por exemplo, na observação oculta da actividade que o utilizador desenvolve no sistema informático ou, através dele, na *Internet*. Assim, julgamos ser pertinente, no contexto do presente estudo, a autonomização dos conceitos.” 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**. Disponível em: <http://repositorio.ucp.pt/bitstream/10400.14/21854/1/Tese%20final%2028%20Mar%C3%A7o.pdf>. Acesso em: 06/07/17.

*malware* para sua execução, que, como já anteriormente apresentado, é apenas um tipo de programa informático, portanto indiferente ao mundo jurídico-penal. Desse modo, não pode ser referenciado por si só como método de obtenção de prova.

É necessário avançar nesta reflexão para se discutir o conteúdo do termo buscas *on-line*, delimitar seu alcance, questionar se ainda cabe falar sobre buscas *on-line* como termo genérico de conteúdo indeterminado no ordenamento jurídico português, após a previsão de novos métodos de obtenção de prova na Lei 109/2009 (LC).

Distinguindo-se buscas *on-line* de utilização de *malware*, como versa a doutrina neste momento, constata-se que o conteúdo que animava o primeiro termo foi fragmentado em diversos e específicos métodos de prova, esvaziando assim o conceito primevo de buscas *on-line*, que agora parece ser inócuo e vazio, pois as várias possibilidades que se enfeixavam no termo, tornaram-se independentes e adquiriram nomenclatura e regulamentação próprias na LC.

Esse diploma legal introduz a regulamentação da recolha da prova em ambiente digital, disciplinando questões que até então eram concebidas apenas com uso estendido da disciplina prevista no CPP para diversos métodos de obtenção da prova. Em tal regulamentação, a LC não se refere ao termo buscas *on-line*, mas estabelece nomenclatura própria para tais métodos de obtenção de prova, o que tem levado a doutrina e a jurisprudência a entenderem que a disciplina trazida pelos artigos 11º a 19º desta Lei refere-se, em verdade, a um novo capítulo a ser considerado pelo CPP, inserido no título que trata dos métodos de obtenção da prova<sup>248</sup>.

<sup>248</sup>1. O regime processual das comunicações telefónicas previsto nos artigos 187º a 190º do Código de Processo Penal deixou de ser aplicável por extensão às «telecomunicações electrónicas», «crimes informáticos» e «recolha de prova electrónica (informática)» desde a entrada em vigor da Lei 109/2009, de 15-09 (Lei do Cibercrime) como regime regra. 2. Esse mesmo regime processual das comunicações telefónicas deixara de ser aplicável à recolha de prova por «localização celular conservada» - uma forma de «recolha de prova electrónica - desde a entrada em vigor da Lei 32/2008, de 17-07. 3. Para a prova electrónica preservada ou conservada em sistemas informáticos existe um novo sistema processual penal, o previsto nos artigos 11º a 19º da Lei 109/2009, de 15-09, Lei do Cibercrime, coadjuvado pela Lei nº 32/2008, neste caso se estivermos face à prova por «localização celular conservada». 4. Nessa Lei do Cibercrime coexistem dois regimes processuais: o regime dos artigos 11º a 17º e o regime dos artigos 18º e 19º do mesmo diploma. O regime processual dos artigos 11º a 17º surge como o regime processual «geral» do cibercrime e da prova electrónica. Isto porquanto existe um segundo catálogo na Lei n. 109/2009, o do artigo 18º, n. 1 do mesmo diploma a que corresponde um segundo regime processual de autorização e regulação probatória. Só a este segundo regime - o dos artigos 18º e 19º - são aplicáveis por remissão expressa os artigos 187º, 188º e 190º do C.P.P. e sob condição de não contrariarem e Lei 109/2009. 5. As normas contidas nos artigos 12º a 17º da supramencionada Lei contêm um completo regime processual penal para os crimes que, nos termos das alíneas do n. 1 do artigo 11º, estão (a) previstos na lei nº 109/2009, (b) são ou foram cometidos por meio de um sistema informático ou (c) em relação aos quais seja necessário proceder à recolha de prova em suporte electrónico. 6. A diferenciação de regimes assenta na circunstância de os dados preservados nos termos dos artigos 12º a 17º se referirem à pesquisa e recolha, para prova, de dados já

Tratando-se de buscas em ambiente digital, o método de obtenção de prova é a pesquisa de dados informáticos prevista no art. 15º LC<sup>249</sup>. Caso seja necessário apreender os referidos dados, o método é a apreensão, como previsto no art. 16º da LC. Quando são feitas *on-line*, significa que são intercepções como método previsto no art. 18º LC. Na hipóteses das operações ocorrerem de maneira encoberta, há previsão no art. 19º da LC. Nos dois últimos métodos, como são operados de forma oculta, há a possibilidade de utilização de *malware* em sua execução<sup>250</sup>.

## 4.2 PESQUISA DE DADOS INFORMÁTICOS

A busca é meio de obtenção de prova previsto no CPP, em seu artigo 174º<sup>251</sup> e

---

produzidos mas preservados, armazenados, enquanto o artigo 18º do diploma se refere à intercepção de comunicações electrónicas, em tempo real, de dados de tráfego e de conteúdo associados a comunicações específicas transmitidas através de um sistema informático. 7. **Assim, o Capítulo III da Lei 109/2009, relativo às disposições processuais, deve ser encarado como um «escondido Capítulo V («Da prova electrónica»), do Título III («Meios de obtenção de prova») do Livro III («Da prova») do Código de Processo Penal» (Dá Mesquita) (...)**”. (Ac. TRE de 20-01-2015, Processo nº 648/14.6GCFAR-A.E1; Relator: João Gomes de Sousa; Tribunal da Relação de Évora. Disponível em: <http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/2fbdd21285478f5f80257de10056ff7a?OpenDocument>. Acesso em: 21/05/2018). Inserir destaque na citação.

<sup>249</sup>É possível encontrar na doutrina posicionamento que entende que, após o advento da LC (Lei do Cibercrime), se trata de busca *on-line* a hipótese prevista no item 5 do art. 15º (Pesquisa de dados informáticos) de tal diploma: “Previstas no artigo 15º, n.º 5 da LC, as buscas *online* encontram-se consagradas legislativamente para situações em que surjam razões, durante a pesquisa, “*para crer que os dados procurados se encontram noutra sistema informático ou numa parte diferente do sistema pesquisado*”, e que sejam acessíveis a partir do sistema inicial, estendendo a pesquisa mediante “*autorização ou ordem da entidade competente*”. Assim, não estamos perante uma diligência oculta, desconhecida pelo visado, permitindo que o acesso ao primeiro sistema informático ponha em causa o secretismo da diligência e o assentando o controlo da legalidade pelo visado.” CANCELA, Alberto Gil Lima. **A Prova Digital: Os Meios de Obtenção de Prova na Lei do Cibercrime**. Disponível em: <https://estudogeral.sib.uc.pt/jspui/bitstream/10316/31398/1/A%20prova%20digital.pdf>. Acesso em: 08/05/2018.

<sup>250</sup>Entendo que a hipótese prevista no n.º 5 do art. 15, antes mencionado, não perde a denominação atribuída à cabeça do artigo, de pesquisa de dados informáticos, configurando o método de buscas *on line*. Não há justificativa lógica nem vantagem técnica em assumir nomenclatura diversa daquela atribuída ao *caput*, especialmente porque como já visto, buscas *on line* apresenta conceituação problemática.

<sup>251</sup>Artigo 174º (Pressupostos) 1 - Quando houver indícios de que alguém oculta na sua pessoa quaisquer animais, coisas ou objetos relacionados com um crime ou que possam servir de prova, é ordenada revista. 2 - Quando houver indícios de que os animais, as coisas ou os objetos referidos no número anterior, ou o arguido ou outra pessoa que deva ser detida, se encontram em lugar reservado ou não livremente acessível ao público, é ordenada busca. 3 - As revistas e as buscas são autorizadas ou ordenadas por despacho pela autoridade judiciária competente, devendo esta, sempre que possível, presidir à diligência. 4 - O despacho previsto no número anterior tem um prazo de validade máxima de 30 dias, sob pena de nulidade. 5 - Ressalvam-se das exigências contidas no n.º 3 as revistas e as buscas efectuadas por órgão de polícia criminal nos casos: a) 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; b) Em que os visados consentam, desde que o consentimento prestado fique, por qualquer forma, documentado; ou c) Aquando de detenção em flagrante por crime a que corresponda pena de prisão. 6 - Nos casos referidos na alínea a) do número anterior, a realização da

seguintes, que trata da recolha de objetos relacionados com um crime e que podem servir de elementos de prova para compor processos. O objetivo do dispositivo foi a procura e localização de objetos infungíveis, materiais, que guardam relação com o crime. Neste contexto, não estão previstos os dados telemáticos, nem qualquer outro elemento que esteja presente apenas na virtualidade, visto que carecem de tangibilidade, portanto passível de ser buscado, conforme estabelece o cânone legal<sup>252</sup>.

No art. 15º, a LC introduziu a pesquisa de dados informáticos como meio de obtenção de prova, especificamente para os casos previstos naquele diploma legal, que em verdade é a busca já prevista no CPP, assim nominada na Convenção do Cibercrime em seu art. 19º<sup>253</sup>. A LC, no entanto, optou por estabelecer nomenclatura própria e diversa para esse meio de obtenção de prova.

A pesquisa de dados informáticos equivale à tradicional busca, já prevista no CPP, com ela guardando pontos de convergência, mas também apresentando peculiaridades referentes à prova que se encontra em suporte digital, como a busca à distância que permite aceder a computadores de maneira remota, desde que seja acessado via computador, legitimamente autorizado<sup>254 255</sup>

---

diligência é, sob pena de nulidade, imediatamente comunicada ao juiz de instrução e por este apreciada em ordem à sua validação. Disponível em: <https://dre.pt/web/guest/legislacao-consolidada/-/lc/169645979/202109291859/74225362/diploma/indice>.

Acesso em: 29/09/2021

<sup>252</sup>“Apesar dos ordenamentos jurídicos preverem regimes de buscas e apreensões como meios de obtenção de prova, esses regimes estão pensados apenas para objetos tangíveis, não abrangendo assim os dados informáticos, que são intangíveis, o que conseqüentemente leva a que os mesmos não possam ser obtidos no âmbito de investigações criminais e ações penais nos mesmos moldes que os objetos tangíveis”. SEQUEIRA, Cláudia Sofia Dias. **Os Meios de Obtenção de Prova na Lei do Cibercrime: Pesquisa de Dados Informáticos**. Disponível em: <https://repositorio.ucp.pt/bitstream/10400.14/21980/1/Disserta%C3%A7%C3%A3o%20Mestrado%20Direito%20Criminal%20Cl%C3%A1udia%20Sequeira%20-%20vers%C3%A3o%20final.pdf>. Acesso em: 09/04/2018.

<sup>253</sup>“Artigo 19º - Busca e apreensão de dados informáticos armazenados”

<sup>254</sup>“Esta *pesquisa de dados* é, operacionalmente, em termos processuais penais, uma verdadeira busca, sendo-lhe aliás aplicáveis, subsidiariamente, as regras previstas para as buscas em processo penal (cfr. Artigo 15º, nº 6). (...). Nela se permitem as buscas, ou pesquisas, à distância. Esta será, porventura, a norma mais arrojada da lei, ao permitir que se acedam, por via de busca informática, computadores remotos, desde que esse acesso se faça a partir de um computador que, legitimamente, possa aceder a outro.” VERDELHO, Pedro. **Obtenção de prova online**. In: DUPUY, Daniela; KIEFER, Mariana, **Cibercrimen**. Madrid: B de F Ltda, 2016. p. 444/445.

<sup>255</sup>“...a pesquisa informática e, conseqüentemente, a apreensão de dados informáticos, por parte das autoridades portuguesas, a sistemas informáticos acessíveis através de outro sistema localizado em território português não encontra qualquer limitação territorial, sendo genericamente admitida, desde que, naturalmente, o acesso ao outro sistema informático seja lícito.” RAMALHO, David Silva. **A recolha de Prova Penal em Sistemas de Computação em Nuvem**. p. 143 In: **Revista de Direito Intelectual**, Coimbra, nº 02, p. 123 a 162, dezembro de 2014

Tanto a busca quanto a pesquisa de dados informáticos têm objetivo pré-estabelecido, conhecido da autoridade policial quando é feito o requerimento de autorização judicial para realização da diligência. A pesquisa também ocorre em momento certo, em diligência única<sup>256</sup>, com comunicação imediata ao juiz da instrução assim que ocorre seu término.

Em regra, esse método de obtenção de prova refere-se a delitos cuja consumação já aconteceu ou, no máximo, para delitos que possam estar acontecendo ou na iminência de acontecer<sup>257</sup>. Sua utilização se dá diferentemente de outros métodos de obtenção de prova<sup>258</sup>, que são utilizados para investigar tantos delitos já consumados como para delitos planejados a acontecer no futuro. Assim, não se fala em busca quando o objetivo for a recolha de dados referentes a delito cuja execução é um fato previsto a acontecer no futuro, mas que o agente ainda não tenha ingressado no núcleo do tipo penal do delito a ser executado.

É formalidade da busca, assim como da pesquisa de dados informáticos, o conhecimento do que deve ser realizado por parte de “quem tiver a disponibilidade do lugar em que a diligência se realiza”<sup>259</sup>. Por isso, a busca, em regra, é realizada com o conhecimento do investigado, podendo ser inclusive mediante seu consentimento<sup>260</sup>.

Questiona-se, no entanto, a validade do consentimento dado por pessoa que não o investigado, mas que tenha o controle ou disponibilidade dos dados que se quer pesquisar. Há

---

<sup>256</sup>O artigo 15º da LC se refere no item 1 e na alínea a) do item 4 a “diligência”, sempre com uso do termo no singular. Apesar de ser evento único, não implica que seja breve, pois aplicando subsidiariamente a regra insculpida no item 4 do artigo 174º do CPP (“4 - O despacho previsto no número anterior tem um prazo de validade máxima de 30 dias, sob pena de nulidade.”), tal diligência pode demorar horas ou até mesmo dias, desde que seu cumprimento se inicie antes de findo o prazo fixado no mandado judicial.

<sup>257</sup>Art. 15º, item 3, alínea b) da LC (“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.”); Art. 174º, item 5, alínea a) do CPP (“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.”)

<sup>258</sup>Escutas telefônicas, artigo 187º e ss do CPP; Intercepção de comunicações, artigo 18º da LC, Ações encobertas, artigo 19º da LC.

<sup>259</sup>Art. 176º, item 1 do CPP (“Antes de se proceder a busca, é entregue, salvo nos casos do n.º 5 do artigo 174.º, a quem tiver a disponibilidade do lugar em que a diligência se realiza, cópia do despacho que a determinou, na qual se faz menção de que pode assistir à diligência e fazer-se acompanhar ou substituir por pessoa da sua confiança e que se apresente sem delonga”), valendo essas mesmas regras para a pesquisa de dados, como reza o item 6, do artigo 15º da LC (“À pesquisa a que se refere este artigo são aplicáveis, com as necessárias adaptações, as regras de execução das buscas previstas no Código de Processo Penal e no Estatuto do Jornalista.”)

<sup>260</sup>Art. 174º, item 5, alínea b) do CPP (“Em que os visados consentam, desde que o consentimento prestado fique, por qualquer forma, documentado;”), assim como a pesquisa de dados pode se dar com consentimento de quem estiver na posse dos dados, como se vê no item 3 alínea a) art. 15º da LC (“A mesma for voluntariamente consentida por quem tiver a disponibilidade ou controlo desses dados, desde que o consentimento prestado fique, por qualquer forma, documentado;”)

resistência na doutrina<sup>261</sup> sob o argumento de que a autorização para a pesquisa não pode ser dada por quem não é titular dos dados, apesar de ter o controle ou disponibilidade das informações, pois trata-se de violação da intimidade do visado. O titular dos dados, ao autorizar, explícita ou tacitamente, terceiro a ter à sua disposição dados que lhe pertencem e integram a sua vida privada, abre mão de parcela da sua intimidade, transferindo parte dessa disposição de dados para este terceiro, sendo válido, portanto, o consentimento do detentor dos dados, ainda que não seja seu titular.

Ao usuário de sistemas informáticos, cada dia menos, é ofertada a possibilidade de se negar conhecimento da volatilidade dos dados e da facilidade com que os mesmos se disseminam. Ao permitir a transferência de dados a uma ou mais pessoas, o titular dos dados consente que podem ser colocados à disposição das autoridades judiciárias, considerando que podem, inclusive, estar ao alcance de qualquer usuário do ambiente virtual. Assim, o consentimento para disposição dos dados foi deferido por seu titular a um terceiro, não se tratando então de desvalorização do direito à intimidade da pessoa visada pela diligência, mas sim de aquiescência antecipada, apenas consequência conhecida e aceita por todos aqueles que utilizam o ambiente virtual de trânsito e armazenamento de dados.

#### 4.3 AGENTE INFILTRADO VIRTUAL

A investigação de delitos praticados com intervenção tecnológica é pontuada por grandes desafios a serem superados pelas forças públicas de segurança. Os delinquentes estão cada vez mais informados a respeito das técnicas anti forenses<sup>262</sup>, inclusive sobre estratégias

---

<sup>261</sup>“Só o portador concreto daquele bem jurídico (reserva da intimidade privada) poderá, validamente, prescindir dele.” CORREIA, João Conde, **Prova Digital: as leis que temos e a lei que devíamos ter**. Lisboa: Revista do Ministério Público nº 139, Ano 35, Junho- Setembro 2014, p. 51.

<sup>262</sup>O objetivo das técnicas anti forenses é ocultar ou alterar os arquivos e registos eletrónicos, de modo que se tornem inservíveis ao uso em processos legais ou que sua recuperação se torne muito demorada ou dispendiosa “...the main aim of computer anti-forensics is to hide or alter electronic evidence so that it cannot be used in legal proceedings or it is too costly and time consuming to retrieve and examine” PAJEK, Przemyslaw; PIMENIDIS, Elias. Computer Anti-Forensics Methods and their impact on Computer Forensic Investigation. p. 145. In: JAHANKHANI H., HESSAMI A.G., HSU F. (eds) **Global Security, Safety, and Sustainability**. Communications in Computer and Information Science. vol. 45. Springer, Berlin: Heidelberg, 2009.

que dificultam a localização e a identificação<sup>263</sup> da origem do material a ser apreendido<sup>264</sup>, dificultando a apreensão e a análise do material a ser constituído como prova.

No campo do crime organizado, as dificuldades são ainda maiores e mais complexas, haja vista o encadeamento de condutas que são consideradas como indiferentes penais, pois são assemelhadas à ordinária atividade empresarial, aliadas ao fato de que são praticadas por várias pessoas concertadamente, dificultando a identificação e a localização da atividade criminosa. Reconhece-se que há auxílio em rede virtual para os criminosos que querem dificultar a atividade policial, com a sugestão de técnicas, utilização de recursos e estratégias que auxiliam a escamotear a identificação do autor do fato delitivo, bem como para inutilizar possível meio de prova a ser produzida contra si<sup>265</sup>

A investigação e recolha de provas em sede de crime organizado reclama ordenamento próprio e métodos especializados, que consigam dar conta da complexidade que este tipo de atividade criminosa desenvolve. Quando os agentes dessa atividade criminosa se utilizam das redes virtuais, é importante que o investigador direcione sua atenção também para o mesmo ambiente. A busca do investigador resultará infrutífera na hipótese de restringir-se apenas ao âmbito do mundo real e se optar por ater-se aos métodos de prova próprios da criminalidade comum. Para que a investigação e a instrução do processo penal se estabeleçam em juízo, como instrumentos de enfrentamento aos criminosos, identificando o

<sup>263</sup>Alerta RAMALHO, que as definições de medidas anti forenses, em regra, excluem parte importante das técnicas utilizadas pelos delinquentes, voltadas para dificultar a localização e identificação da origem do conteúdo que irá se constituir em prova. Para este autor estas técnicas também devem estar incluídas na definição de medidas anti forenses.

“Com efeito, a generalidade das definições avançadas neste domínio pecam por delimitar como objecto destas medidas a actividade do procedimento forense correspondente às acima identificadas etapas de exame e análise. Esquecem, porém, que uma parte significativa das medidas anti-forenses incide na fase da identificação da origem e da localização da prova digital, incluídas ainda na primeira etapa do processo, acima qualificada como recolha.” RAMALHO, David Silva. **Métodos Ocultos de Investigação Criminal em Ambiente Digital**. Coimbra: Edições Almedina, 2017. p. 166.

<sup>264</sup>“A modo genérico diremos que las técnicas antirrastros son todas aquellas que se utilizan con la finalidad de evitar dejar rastros de las acciones realizadas por los delincuentes, imposibilitando o al menos dificultando el “trackeo” por las fuerzas de seguridad. En cambio, las técnicas antiforenses buscan que ante el caso de que las fuerzas de seguridad obtuvieran los dispositivos (*notebooks*, celulares, discos rígidos, pendrives, etc.), la información que se encuentra en ellos no puedan ser accedida o analizada en el marco de una pericia informática, por ejemplo por contar con procesos como cifrado o borrado seguro (*Wiping*).” TEMPERINI, Marcelo; MACEDO, Maximiliano. **Nuevas Herramientas de Investigación Penal: El Agente Encubierto Digital**. In: DUPUY, Daniela e KIEFER, Mariana, **Cibercrimen**. Madrid: B de F Ltda, 2016. p. 487/488.

<sup>265</sup>“En la práctica, estas técnicas son explicadas en distintos foros y sitios, como por ejemplo en un conocido sitio de “soporte” para pedófilos, en donde se aconseja tener dos *notebooks*, una para trabajo y otra exclusiva para el intercambio de pornografía infantil, que tenga el disco rígido completamente cifrado con algún algoritmo tipo AES, con contraseña de 64 caracteres, y para navegar, usar máquinas virtuales dedicadas, con conexiones por VPN y navegación por TOR o *Freenet*.” TEMPERINI, Marcelo; MACEDO, Maximiliano. **Nuevas Herramientas de Investigación Penal: El Agente Encubierto Digital**. In: DUPUY, Daniela e KIEFER, Mariana, **Cibercrimen**. Madrid: B de F Ltda, 2016. p. 488.

ato delitivo e a autoria, é necessário que a investigação aconteça de maneira velada, nos mesmos moldes que acontece a prática delitiva, pois a peculiaridade desse tipo criminal é operar com o engano, a ocultação e o embuste.

A utilização de métodos ocultos de obtenção de prova ganha relevo, pois coloca as forças estatais em situação de igualdade com aqueles que se dedicam à criminalidade organizada, não podendo o Estado prescindir desse importante recurso sem ser acusado de omissão no dever constitucional de manter a paz e a segurança dos cidadãos.

Ao dispor dos mesmos métodos utilizados pelos criminosos, visando combater o crime e lograr êxito nas investigações, o Estado não tem o objetivo de nivelar-se aos delinquentes, apenas dispor de armas mais adequadas para o combate efetivo do crime organizado.

O acesso a dados sigilosos armazenados em dispositivo informático do investigado e a dados que trafegam em rede de comunicação virtual, não se configura como intromissão maior do que aquela já registada e autorizada nas escutas telefônicas. Os direitos fundamentais expostos são os mesmos em ambos os métodos de obtenção da prova, sem que atualmente se discuta a respeito da indispensabilidade das escutas telefônicas, quando se trata de investigação de crime organizado.

#### **4.3.1 Ação Encoberta**

Entre os métodos ocultos de obtenção de prova estão aqueles que se desenvolvem em ambiente digital e que podem ser praticados com a utilização de *malware*, objeto desta pesquisa. As ações encobertas ganham relevo, tendo em vista o aspeto de novidade no sistema jurídico, fazendo jus, portanto, a estudo mais específico e detalhado. Esse tipo de atuação foi ampliada para os crimes cometidos em ambiente virtual por força do estabelecido no art. 19º da LC. Assim, para tecer reflexões sobre o agente infiltrado virtual, é fundamental entender, a princípio, como a legislação e a doutrina tratam do tema das ações encobertas, para em seguida dimensionar o alcance que foi dado com a extensão a tais ações pela LC.

A possibilidade de atuação do agente infiltrado já encontra previsão na Lei 101/2001

(Regime jurídico das ações encobertas)<sup>266</sup>, que autoriza a realização de ações encobertas para prevenção e investigação criminal de certo catálogo de delitos, estando incluídos aqueles considerados como de criminalidade organizada e altamente organizada.

Desse modo, o agente infiltrado é participante de uma ação encoberta cuja verdadeira identidade fica em estado de sigilo, não sendo imprescindível que o agente seja funcionário público, mas esteja submetido ao controle de agentes da polícia judiciária, partícipes da ação.

O agente é apenas um dos participantes da ação encoberta, nunca atuando sozinho por sua conta e risco, ao contrário, agindo sempre sob supervisão e acompanhamento de autoridade policial, a quem deve prestar contas sobre todas as atividades atinentes aos casos em que atua.

Quando voltada para o crime organizado, o objetivo de uma ação encoberta é conseguir informações suficientes para entender o funcionamento da empresa criminosa, identificar seus principais mentores e reunir material probatório, apto a conduzir o caso ao desfecho de uma condenação criminal.

Ela não mira o crime que acontece na ponta da atividade, não tem por finalidade o último ator da cadeia criminosa. Seu objetivo é ingressar no núcleo duro da empresa, ir até a chefia da empresa, descobrir a rede criminosa da qual aquela empresa faz parte. Por isso, é necessário ao agente infiltrado, muitas vezes, ignorar a prática de vários delitos que ele presencia, mesmo se comportando como co-autor<sup>267 268</sup>, até que o objetivo final da ação encoberta seja atendido<sup>269</sup>.

---

<sup>266</sup>“Artigo 1º, 2- Consideram-se ações encobertas aquelas que sejam desenvolvidas por funcionários de investigação criminal ou por terceiro atuando sob o controlo da Política Judiciária para prevenção ou repressão dos crimes indicados nesta lei, com ocultação da sua qualidade e identidade.” (Lei 101/2001)

<sup>267</sup>“No resulta difícil imaginar que puede verse durante su actuación, compelido a cometer un ilícito, ya sea para ganar la confianza de los integrantes de la organización delictiva o incluso como una manera de que su vida no corra riesgo, pues el implemento de una orden de los integrantes de estas bandas delictivas le puede significar un serio peligro a su identidad física. (...) cuanto mayor es la integración, mayor la posibilidad del riesgo de verse obligado a realizar actos para ganarse la confianza de sus miembros.” PEREIRA, Flávio Cardoso. **El Agente Infiltrado desde el Punto de Vista del Garantismo Procesal Penal**. Curitiba: Juruá Editora, 2016. pág. 423

<sup>268</sup>“São, contudo, a co-autoria e a cumplicidade as formas de comparticipação que a conduta do agente infiltrado mais frequentemente pode assumir, quer no âmbito *light cover*, quer nas modalidades que consubstanciam as operações *deep cover*.” ONETO, Isabel. **O Agente Infiltrado**. Coimbra: Coimbra Editora, 2005. pág. 150

<sup>269</sup>“A ação do agente infiltrado não pode limitar-se à procura de material probatório que incrimine operadores criminais de primeiro nível operativo de uma organização criminosa, cuja fungibilidade é elevadíssima. Significa que estes devem ficar impunes? Claro que não. A sua detenção insere-se no âmbito da prossecução penal, mas cai fora da admissibilidade de uma ação encoberta, se não tiver por objectivo o desmantelamento de uma organização criminosa...” ONETO, Isabel. **O Agente Infiltrado**. Coimbra: Coimbra Editora, 2005. pág. 143.

### 4.3.2 Agente Infiltrado ou Encoberto

É importante estabelecer o conceito a ser utilizado para se referir a agente infiltrado, pois a doutrina é fértil em classificações e diferenciações entre tipos de agentes participantes de uma ação encoberta<sup>270</sup>. Em alguns autores, é possível encontrar uma subtil distinção entre agente encoberto e infiltrado<sup>271</sup>, sendo considerado infiltrado o agente destacado, com o objetivo de adquirir a confiança do suspeito, visando ingressar em organização criminosa específica, sendo sua ação voltada para o fim pré-determinado pela autoridade policial. O agente encoberto, todavia, é aquele que frequenta lugares identificados com a prática delitiva, para que empreenda a prisão do autor caso presencie um flagrante, ou possa recolher informações sobre um suposto delito ocorrido<sup>272</sup>.

Em se adotando esta distinção, no caso de agente encoberto é preciso comunicar às autoridades superiores o ocorrido para adoção das providências investigativas necessárias, não estando sua ação ligada previamente a alguma atividade criminosa que se queira apurar, sendo por isso considerado uma sub-espécie do agente infiltrado<sup>273</sup>.

Nesse contexto de análise, há também aqueles que entendem tratar-se da mesma

---

<sup>270</sup>Podemos encontrar a classificação de agente ‘à paisana’ ONETO, Isabel. **O Agente Infiltrado**. Coimbra: Coimbra Editora, 2005. pág. 137 a 141. Referência a *homens de confiança*. ANDRADE, Manuel da Costa. **Bruscamente no Verão Passado**. Coimbra: Coimbra Editora, 2009. pág. 127. “Agente Meramente Encubierto”, “Agente Encubierto Infiltrado”, “Agente Encubierto Infiltrado com Identidad Supuesta” e “Agente Provocador”, classificação feita por Joaquin Delgado, *apud* MEDRONI, Marcelo Batlouni. **Comentários à lei de combate ao crime organizado**. São Paulo: Editora Atlas S.A., 2014. págs. 74 e 75.

<sup>271</sup>JESUS, Francisco Marcolino de. **Os Meios de Obtenção da Prova em Processo Penal**. Coimbra: Edições Almedina S.A., 2011. pág. 133. PEREIRA, Sandra. A Recolha da Prova por Agente Infiltrado. *In: Prova Criminal e Direito de Defesa*. Coimbra: Edições Almedina S.A., 2013. págs. 140 a 143. GONZALEZ-CASTELL, Adán Carrizo. El Agente Infiltrado en España y Portugal. *In: VALENTE, Manuel Monteiro Guedes. Criminalidade Organizada e Criminalidade de Massa*. Coimbra: Edições Almedina S.A., 2009. pág. 194. VALENTE, Manuel Monteiro Guedes. A Investigação do Crime Organizado. *In: VALENTE, Manuel Monteiro Guedes. Criminalidade Organizada e Criminalidade de Massa*. Coimbra: Edições Almedina S.A., 2009. págs. 169 e 170.

<sup>272</sup> Conforme distinção recolhida na doutrina e compilada em ONETO, Isabel. **O Agente Infiltrado**. Coimbra: Coimbra Editora, 2005. págs. 12 a 127

<sup>273</sup>“A proceder-se uma distinção entre agente infiltrado e agente encoberto, esta haveria de operar-se no âmbito do conceito de agente infiltrado, atribuindo ao agente encoberto as operações *light cover*, que precisamente se caracterizam pelo facto de não durarem mais de seis meses, exigirem um menor grau de planeamento, de supervisão e de experiência por parte do agente, mantendo este a sua identidade e o seu lugar na estrutura policial. Estas operações implicam um menor risco para o agente e têm um objectivo preciso, que pode consistir numa transacção ou tão só um encontro para recolha de informações. Nelas se enquadram as modalidades *decoy operation*, a *pseudo-achat*, a *pseudo-vente*, o *flash-roll*, a *livraison surveillée* e a *livraison contrôlée*. Desta forma poderíamos entender o agente encoberto com uma sub-espécie do agente infiltrado.” ONETO, Isabel. **O Agente Infiltrado**. Coimbra: Coimbra Editora, 2005. pág. 140.

figura<sup>274</sup>, por estarem ambos acolhidos pelo mesmo dispositivo legal, sujeitos às mesmas restrições e controle por parte da autoridade judicial. Destaca-se que a legislação que regula a matéria adota a nomenclatura de agente encoberto para, ao defini-lo, ajustar vestimenta onde cabem os dois conceitos<sup>275</sup>, como também será tratado neste trabalho.

A distinção encontrada consensualmente na doutrina e na jurisprudência<sup>276 277</sup>, e também a mais útil a ser estudada, trata de separar agente infiltrado de agente provocador<sup>278</sup>, pois cada um participa em momento distinto da empreitada criminosa, e o resultado da sua

<sup>274</sup>Não estabelece distinção entre os termos agente infiltrado e encoberto, usando-os indistintamente. SILVA, Germano Marques da. **Curso de Processo Penal vol. II**. Lisboa: Babel, 2011. pág. 232; PEREIRA, Flávio Cardoso. **El Agente Infiltrado desde el Punto de Vista del Garantismo Procesal Penal**. Curitiba: Juruá Editora, 2016. pág. 390; RAMALHO, David Silva. **Métodos Ocultos de Investigação Criminal em Ambiente Digital**. Coimbra: Edições Almedina, 2017. pág. 346.

<sup>275</sup> Nega distinção entre as duas figuras, destacando que: “Parece que o legislador optou pela expressão “agente encoberto” ao invés de utilizar o termo “agente infiltrado”, nela se incluindo a realidade que pode comportar as duas figuras.”. ONETO, Isabel. **O Agente Infiltrado**. Coimbra: Coimbra Editora, 2005. pág. 141

<sup>276</sup> “I -Agente provocador é aquele que de alguma forma precipita o crime, instigando-o, induzindo-o - Costa Andrade, Sobre as Proibições de Prova em Processo Penal - ou, como refere Germano Marques da Silva, acerca do tema da provocação, para o qual esta não é apenas informativa, mas sobretudo formativa, não revela o crime e o criminoso, mas cria o próprio crime e o criminoso, e, por isso, é contrária à própria finalidade da investigação criminal, uma vez que gera o seu próprio objecto. II -Agente infiltrado é o funcionário de investigação criminal ou terceiro, por exemplo, o cidadão particular, que actue sob controlo da polícia, que, com ocultação da sua qualidade e identidade, e com o fim de obter provas para a incriminação do suspeito, ganha confiança pessoal, para melhor o observar, em ordem a obter informações relativas às actividades criminosas de que é suspeito e provas contra ele(s), com finalidades exclusivas de prevenção ou repressão criminal, sem contudo o(s) determinar à prática de novos crimes.” ACRL de 30-10-2002. Proc. 5810/02 3ª Secção Desembargadores: Carlos Sousa - Teresa Féria - Clemente Lima - Sumário elaborado por José Rita. Disponível em: [http://www.pgdlisboa.pt/jurel/jur\\_busca.php?busca=assunto&buscajur=agente+provocador&areas=000&buscaprocesso=&buscaseccao=&pagina=1&ficha=1](http://www.pgdlisboa.pt/jurel/jur_busca.php?busca=assunto&buscajur=agente+provocador&areas=000&buscaprocesso=&buscaseccao=&pagina=1&ficha=1). Acesso em: 24/05/2018.

<sup>277</sup>“II - A ilegitimidade e inadmissibilidade da prova obtida por via do agente provocador - o agente policial ou o particular por ele comandado que induz outrem à prática do crime para facilitar a recolha de provas da ocorrência do acto criminoso - «é inquestionável... pois seria imoral que, num Estado de Direito, se fosse punir aquele que um agente estadual induziu ou instigou a delinquir». Uma «tal desonestidade seria de todo incompatível com o que, num Estado de Direito, se espera que seja o comportamento das autoridades e agentes da justiça penal, que deve pautar-se pelas regras gerais da ética». Nada terá de ilegítimo, no entanto, a conduta do funcionário de investigação criminal, desde que não induza ou instigue o agente à prática de um crime que de outro modo não praticaria ou que já não estivesse disposto a praticar, porquanto em tais situações não se vê em que é que essa actuação represente grave limitação da liberdade de formação e manifestação da vontade do arguido (Vital Moreira e Gomes Canotilho, Constituição da República Portuguesa, 3.ª ed., pág. 207, e Costa Andrade, Sobre as Proibições de Prova em Processo Penal, pág. 216) - cf. o Ac. TC n.º 76/01, de 14.02, proc. n.º 508/99. III - Neste sentido decidiu o STJ, entre outros nos Acs. de 09-06-05, proc. n.º 1015/05-3, de 06-05-04, proc. n.º 1138/04-5, de 30-10-02, proc. n.º 2118/02-3, de 20-02-03, proc. 4510/02-5, sendo pacífica aquela ideia de que é preciso distinguir os casos em que a actuação do agente provocador cria uma intenção criminosa até então inexistente, dos casos em que o sujeito já está implícita ou potencialmente inclinado a delinquir e a actuação do agente apenas põe em marcha aquela decisão. Isto é, importa distinguir entre a criação de uma oportunidade com vista à realização de uma intenção criminosa, e a criação dessa mesma intenção. ACSTJ de 30-11-2005 Proc. n.º 3349/05 - 3.ª Secção Sousa Fonte (relator. Tem voto de vencido quanto aos pontos VI e VII) Oliveira Mendes João Bernardo Pires Salpico. Disponível em [https://www.pgdlisboa.pt/jurel/stj\\_busca.php?busca=assunto&buscajur=agente+provocador&areas=2&buscaprocesso=&buscaseccao=&pagina=1&ficha=1](https://www.pgdlisboa.pt/jurel/stj_busca.php?busca=assunto&buscajur=agente+provocador&areas=2&buscaprocesso=&buscaseccao=&pagina=1&ficha=1). Acesso em 01/10/2021

<sup>278</sup>JESUS, Francisco Marcolino de. **Os Meios de Obtenção da Prova em Processo Penal**. Coimbra: Edições Almedina S.A., 2011. págs. 132 e 133; PEREIRA, Sandra. A Recolha da Prova por Agente Infiltrado. *In: Prova*

conduta traz resultados opostos ao processo penal, sendo necessário estabelecer a linha divisória entre os dois<sup>279</sup>.

O agente provocador atua antes da prática do delito, não ingressando necessariamente na fase executória. É provocador quem incita, quem faz nascer a vontade de agir, aquele que desperta no autor do delito a vontade de cometê-lo. Sua atividade é, por tudo isso, fundamental para a prática do delito, pois sem ela o autor sequer pensaria nele, portanto reduzindo a margem de propensão ao crime. A ação do agente provocador é também causa do delito, pois sem ela o resultado não teria acontecido, não podendo por isso se valer de uma causa de exclusão de ilicitude para justificar sua conduta<sup>280</sup>.

Seu posicionamento é questionável e o suposto material probatório que o mesmo venha a produzir deve ser repudiado, pois o seu intento é flagrar o autor do delito que ele mesmo deu causa e provocou, com o único objetivo de conseguir uma condenação. O fim almejado pelo provocador não é investigativo nem repressivo, pois não perquire sobre um delito em andamento e nem busca provas de um crime já cometido. Sua finalidade não está aliada aos objetivos do processo penal, e por isso sua admissibilidade é uma afronta ao princípio da lealdade<sup>281</sup> e ao direito a um processo justo, regras básicas que devem nortear o Estado nas suas relações com o particular, especialmente quando o ameaça com a perda da sua liberdade<sup>282</sup>.

---

**Criminal e Direito de Defesa.** Coimbra: Edições Almedina S.A., 2013. pág.143; GONZALEZ-CASTELL, Adán Carrizo. **El Agente Infiltrado en España y Portugal.** In: VALENTE, Manuel Monteiro Guedes. **Criminalidade Organizada e Criminalidade de Massa.** Coimbra: Edições Almedina S.A., 2009. págs. 194 e 195; RAMALHO, David Silva. **Métodos Ocultos de Investigação Criminal em Ambiente Digital.** Coimbra: Edições Almedina, 2017. págs. 348 e 349; RAMÍREZ, Paula Andrea. Nuevas Tendencias Político-Criminales en la Lucha contra la Criminalidad Organizada. In: **Crimen Organizado.** Lima: ARA Editores, 2009. pág. 125.

<sup>279</sup>Vale aqui destacar a afirmativa que delimita com precisão a diferença entre agente provocador e infiltrado, “É que a provocação não é apenas *informativa*, mas é *formativa*; não revela o crime e o criminoso, mas *cria* o próprio crime e o próprio criminoso” SILVA, Germano Marques da. **Curso de Processo Penal** vol. II. Lisboa: Babel, 2011. pág. 233.

<sup>280</sup>“El *agent provocateur*, al instigar o inducir otra persona a cometer un delito con el fin de que este pueda ser detenido e puesto a disposición de la Justicia, no puede en consecuencia, al contrario del agente encubierto, invocar para si la posibilidad de plantear la concurrencia de una causa de justificación.” PEREIRA, Flávio Cardoso. **El Agente Infiltrado desde el Punto de Vista del Garantismo Procesal Penal.** Curitiba: Juruá Editora, 2016. pág. 375.

<sup>281</sup>“Alguns autores e a jurisprudência de certos países socorrem-se também do *princípio da lealdade* para fundamentar a ilegitimidade do recurso aos agentes provocadores e conseqüente proibição da prova obtida por esses meios.” SILVA, Germano Marques da. **Curso de Processo Penal** vol. II. Lisboa: Babel, 2011. pág. 234.

<sup>282</sup>“Por esto se puede afirmar que el agente provocador en razón de ser representado por un individuo que conduce su actividad de forma a inducir o instigar la persona sospechosa a practicar actos delictuosos por los cuales habrá de responder penalmente, con el objetivo principal de obtención de pruebas que vengán a perjudicar el mismo, acaba por violar las garantías esenciales de un Estado social y democrático de Derecho.” PEREIRA, Flávio Cardoso. **El Agente Infiltrado desde el Punto de Vista del Garantismo Procesal Penal.** Curitiba: Juruá Editora, 2016. pág. 375.

Por outro lado, o agente que encoraja um desejo prévio de outrem de cometer um delito, inclusive podendo participar de atos preparatórios e executórios, não se enquadra na figura de provocador. A circunstância descrita se aplica ao agente infiltrado, uma vez que sua atuação na empreitada criminosa incentiva, ainda que de forma silenciosa, a prática do delito<sup>283</sup>, sem entretanto ter sido dele a ideia da prática delituosa.

A dificuldade em desenhar a linha divisória entre os dois agentes está no âmbito da subjetividade do sujeito ativo que pratica o delito, ou seja, em identificar, por meio do compêndio probatório recolhido durante a investigação, que o infrator já trazia dentro de si a vontade de praticar o delito, tendo apenas encontrado no agente infiltrado o incentivo para concretizá-lo.

O TEDH, ao apreciar o caso *Teixeira de Castro v. Portugal*<sup>284</sup>, posiciona com clareza o papel determinante do elemento subjetivo para definir a responsabilidade do agente, como também traça a linha divisória entre agente infiltrado e agente provocador, dirimindo qualquer dúvida, e afastando do ordenamento legal a atividade do provocador como apta a constituir prova no processo penal de um Estado Democrático de Direito.

Para esta Corte, foi a atividade dos policiais que fez nascer no arguido a vontade da prática do delito, pois estes não agiram de forma passiva, ao contrário, incitaram o autor à prática do delito<sup>285</sup>. O Tribunal chegou à etapa de conclusão analisando as demais provas trazidas ao processo<sup>286</sup>, pois nenhuma delas informa, ou ao menos traz alguma indicação, que o autor dos fatos havia outrora praticado condutas dessa mesma natureza<sup>287</sup>.

---

<sup>283</sup>“O agente infiltrado é mais do que um simples observador, é um participante activo na atividade criminosa. Insere-se no mundo do crime, convive com criminosos, ganha sua confiança e comete crimes, quer na forma de cumplicidade, que como co-autor ou mesmo simples autor. Apenas lhe está vedado agir como instigador e como autor mediato. (...) agente infiltrado como o agente policial, ou terceiro sob a orientação daquele, que, no âmbito da prevenção ou repressão criminal, e com o fim de obter provas incriminatórias sobre determinadas actividades criminosas, oculta a sua identidade e qualidade, podendo praticar factos típicos sem, contudo, os poder determinar.” ONETO, Isabel. **O Agente Infiltrado**. Coimbra: Coimbra Editora, 2005. pág. 137 e 150.

<sup>284</sup>Tribunal Europeu dos Direitos Humanos. Causa *Teixeira de Castro vs. Portugal* (44/1997/828/1034), julgado em 09.06.1998. Disponível em: <http://hudoc.echr.coe.int/eng?i=001-58193>. Acesso em: 17/052018.

<sup>285</sup>O TEDH destaca a conduta dos agentes de incitar o acusado a prática do delito, assumindo postura ativa na prática do mesmo, não se limitando a investigar a existência de possível atividade criminosa por parte do acusado.

<sup>286</sup>Não foi juntada aos autos nenhuma prova ou indício que sem a atividade dos agentes o delito teria sido praticado, levando a Corte a concluir que o agente foi privado de um julgamento justo.

<sup>287</sup>“The necessary inference from these circumstances is that the two police officers did not confine themselves to investigating Mr Teixeira de Castro’s criminal activity in an essentially passive manner, but exercised an influence such as to incite the commission of the offence. (...) In the light of all these considerations, the Court concludes that the two police officers’ actions went beyond those of undercover agents because they instigated the offence and there is nothing to suggest that without their intervention it would have been committed. That intervention and its use in the impugned criminal proceedings meant that, right from the outset, the applicant was

Conclui-se, portanto, que a análise do elemento subjetivo que motivou o investigado a praticar o delito deve ser feita antes da atuação do agente infiltrado<sup>288</sup>, aliás, sendo esta a motivação que autoriza a infiltração do agente na empreitada criminosa. Não se justifica a ação de agente infiltrado antes de existir uma razão baseada em indícios substantivos que evidenciem a ocorrência da prática delitiva ou pelo menos a evidência desta.

A ação encoberta que se inicia sem uma justificada suspeita da existência de uma organização criminosa em plena atividade, a partir da utilização de agente infiltrado, é irregular desde o início, pois está desabrigada de amparo legal para conseguir autorização judicial. No ordenamento brasileiro está afastada a possibilidade da prova resultante da atividade do agente provocador<sup>289</sup>, em especial quanto a preparação da situação de flagrante, cristalizado tal posicionamento no teor da Súmula 145 do Supremo Tribunal Federal, a qual determina que “não há crime, quando a preparação do flagrante pela polícia torna impossível sua consumação”.

Assim, o material produzido em virtude da ação do agente provocador não pode ser considerado como elemento de prova, pois a vontade do autor estava viciada desde o início, maculando assim a própria estrutura do crime, tirando o imprescindível elemento subjetivo necessário à prática daquele delito.

---

definitively deprived of a fair trial.” Tribunal Europeu dos Direitos Humanos, causa Teixeira de Castro vs. Portugal (44/1997/828/1034), julgado em 09/06/1998. Disponível em: <http://hudoc.echr.coe.int/eng?i=001-58193>. Acessado em: 17/05/2018. pág. 10 e 11.

**Em livre tradução:** A inferência necessária destas circunstâncias é que os dois policiais não se limitaram a investigar a actividade criminosa do senhor Teixeira de Castro de forma essencialmente passiva, mas exerceram uma influência que incita à prática da infracção. (...) À luz de todas essas considerações, a Corte conclui que as ações dos dois policiais foram além das dos agentes encobertos porque eles instigaram o delito e não há nada que sugira que sem sua intervenção ele teria sido cometido. Esta intervenção e a sua utilização no processo penal impugnado significou que, desde o início, o recorrente foi definitivamente privado de um julgamento justo.

<sup>288</sup>“A análise das intenções do provocado é feita previamente, isto é, o agente já devia ter a intenção de cometer o crime antes do contato com os agentes provocadores.” ALVES, Catarina Abegão. Agente Infiltrado ou Provocador? Um Problema de Proibição de Prova à Luz do Caso Teixeira de Castro v. Portugal. In: **Revista de Concorrência e Regulação**. Ano IV, número 16. Coimbra: Almedina, 2013. pág. 365.

<sup>289</sup>“Ao menos em nosso ordenamento jurídico, em razão da indução à prática de infração penal, sem que tal propósito existisse previamente na mente do autor, e, sobretudo, da preparação da situação de flagrância, a atuação do **agente provocador (teoria da armadilha ou entrapment defense)** redundará na formação de prova viciada.” MASSON, Cleber; MARÇAL, Vinícius. **Crime Organizado**. São Paulo: Editora Método, 2017. págs. 304 e 305.

### 4.3.3 Elementos de admissibilidade de uma ação encoberta

A autorização judicial do recurso às ações encobertas deve ser precedida da análise da necessidade, proporcionalidade e idoneidade<sup>290</sup> da medida, para o fim a que se destina, pois as mesmas são de uso subsidiário<sup>291</sup>, extraordinário<sup>292</sup> e excecional<sup>293 294</sup>, só a elas recorrendo-se quando os métodos de obtenção de prova, previstos no CPP, não forem suficientes para investigar aquele tipo de delito. Este método de obtenção de prova especial, tem legislação própria que o regula<sup>295</sup>, estabelecendo o âmbito de aplicação previamente fixado por catálogo, e os fins para os quais pode ser utilizado.

O atual desenho legal das ações encobertas as admite tanto para investigação quanto para a prevenção dos delitos do catálogo estabelecido, sendo certo que esse catálogo vai além da investigação e prevenção da criminalidade organizada para permitir alcançar delitos menos complexos, alguns com envolvimento de apenas um agente, como nos casos de homicídio voluntário<sup>296</sup>. O extenso catálogo permissivo para uso das ações encobertas, previsto na

<sup>290</sup>“Debemos, (...) alabar la precisión con la que tanto la regulación portuguesa como la española delimitan el ámbito de aplicación de esta figura y los requisitos necesarios para poder utilizarla: necesidad, proporcionalidad e idoneidad...”. Tais requisitos podem ser extraídos do art. 3º, 1 da Lei 101/01, como observa GONZALEZ-CASTELL, Adán Carrizo. **El Agente Infiltrado en España y Portugal**. In: VALENTE, Manuel Monteiro Guedes. **Criminalidade Organizada e Criminalidade de Massa**. Coimbra: Edições Almedina S.A., 2009. pág. 217.

<sup>291</sup>“O regime jurídico-processual dos meios ocultos de investigação deve,(...), obedecer a um estrito princípio de *subsidiaridade*. (...) Assim, não deve recorrer-se a meios ocultos quando for possível alcançar os mesmos resultados de investigação com a aplicação de meios “descobertos”. ANDRADE, Manuel da Costa. **Bruscamente no Verão Passado**. Coimbra: Coimbra Editora, 2009. págs. 114 e 115.

<sup>292</sup>“Esta figura merece el calificativo de medio de control extraordinario, al conllevar una alteración de principios constitucionales básicos y una fuerte restricción de derechos fundamentales...”. PEREIRA, Flávio Cardoso. **El Agente Infiltrado desde el Punto de Vista del Garantismo Procesal Penal**. Curitiba: Juruá Editora, 2016. pág. 519.

<sup>293</sup>“O recurso ao agente infiltrado está vinculado a quesitos especiais. Desde logo, se impõe que só se recorre a este meio ou técnica excepcional de investigação quando outros meios ou técnicas menos onerosas para o cidadão se mostram inadequadas e incapazes de produzirem prova real e pessoal...” VALENTE, **A Investigação do Crime Organizado**, In: VALENTE, Manuel Monteiro Guedes. **Criminalidade Organizada e Criminalidade de Massa**. Coimbra: Edições Almedina S.A., 2009, pág. 173 e 174.

<sup>294</sup>“...la utilización del agente encubierto es un medio excepcional de investigación restrictivo de derechos fundamentales...” GONZALEZ-CASTELL, Adán Carrizo. **El Agente Infiltrado en España y Portugal**. In: VALENTE, Manuel Monteiro Guedes. **Criminalidade Organizada e Criminalidade de Massa**. Coimbra: Edições Almedina S.A., 2009. pág. 201

<sup>295</sup>A legislação referência para as ações encobertas, Lei nº 101 de 25.08.2001, regulamenta este tipo de método de recolha de provas, fazendo a ela referência a Lei do Cibercrime (Lei nº 109/2009) no seu Artigo 19º “Acções encobertas 1 - É admissível o recurso às acções encobertas previstas na Lei n.º 101/2001, de 25 de Agosto, nos termos aí previstos, no decurso de inquérito relativo aos seguintes crimes:”

<sup>296</sup>“Artigo 2º da Lei 101/2001.

Âmbito de aplicação

As ações encobertas são admissíveis no âmbito da prevenção e repressão dos seguintes crimes:

a) Homicídio voluntário, desde que o agente não seja conhecido;

legislação de base, foi ainda ampliado pela Lei do Cibercrime que incluiu nova lista de delitos que podem ser tanto prevenidos quanto investigados com utilização desse método de obtenção de prova<sup>297</sup>.

Diferentemente de outras legislações<sup>298</sup> como, v.g., a espanhola<sup>299</sup> e a brasileira<sup>300</sup>, que optaram por restringir a admissão do agente infiltrado apenas para a investigação da criminalidade organizada, a moldura que enquadra os crimes que admite a utilização deste método de obtenção de provas na legislação portuguesa é ampla.

- b) Contra a liberdade e contra a autodeterminação sexual a que corresponda, em abstrato, pena superior a 5 anos de prisão, desde que o agente não seja conhecido, ou sempre que sejam expressamente referidos ofendidos menores de 16 anos ou outros incapazes;
- c) Relativos ao tráfico e viciação de veículos furtados ou roubados;
- d) Escravidão, sequestro e rapto ou tomada de reféns;
- e) Tráfico de pessoas;
- f) Organizações terroristas, terrorismo, terrorismo internacional e financiamento do terrorismo;
- g) Captura ou atentado à segurança de transporte por ar, água, caminho-de-ferro ou rodovia a que corresponda, em abstrato, pena igual ou superior a 8 anos de prisão;
- h) Executados com bombas, granadas, matérias ou engenhos explosivos, armas de fogo e objetos armadilhados, armas nucleares, químicas ou radioativas;
- i) Roubo em instituições de crédito, repartições da Fazenda Pública e correios;
- j) Associações criminosas;
- l) Relativos ao tráfico de estupefacientes e de substâncias psicotrópicas;
- m) Branqueamento de capitais, outros bens ou produtos;
- n) Corrupção, peculato e participação económica em negócio e tráfico de influências;
- o) Fraude na obtenção ou desvio de subsídio ou subvenção;
- p) Infracções económico-financeiras cometidas de forma organizada ou com recurso à tecnologia informática;
- q) Infracções económico-financeiras de dimensão internacional ou transnacional;
- r) Contrafação de moeda, títulos de créditos, valores selados, selos e outros valores equiparados ou a respectiva passagem;
- s) Relativos ao mercado de valores mobiliários.”

Disponível em [https://www.pgdlisboa.pt/leis/lei\\_mostra\\_articulado.php?nid=89&tabela=leis&ficha=1&pagina=1&so\\_miolo=&](https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=89&tabela=leis&ficha=1&pagina=1&so_miolo=&). Acesso em 01/10/2021

<sup>297</sup>“Artigo 19º da Lei 109/2009:

Ações encobertas

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, a discriminação racial, religiosa ou sexual, as infracções económico-financeiras, bem como os crimes consagrados no Título IV do Código do Direito de Autor e dos Direitos Conexos.

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

Disponível em [https://www.pgdlisboa.pt/leis/lei\\_mostra\\_articulado.php?nid=1137&tabela=leis&so\\_miolo=](https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1137&tabela=leis&so_miolo=). Acesso em 01/10/2021

<sup>298</sup>A Regulamentação do Agente Infiltrado na Europa, está minuciosamente detalhada em ONETO, Isabel. **O Agente Infiltrado**. Coimbra: Coimbra Editora, 2005. pág. 95 a 105.

<sup>299</sup>“En el artículo 282 bis de la Ley de Enjuiciamiento Criminal española, aparte de proporcionarse habilitación legal a la figura del agente encubierto en el marco de una investigación, posibilitándose en otorgamiento y la utilización de una identidad supuesta a funcionarios de la Policía Judicial, se delimita el concepto de delincuencia organizada, la única para cuya investigación se prevé infiltración policial.” GONZALEZ-

Tal amplitude de admissibilidade exige do aplicador da lei crivo criterioso, *cum grano salis*, no que se refere à análise do pedido de uso de agente infiltrado, para que de exceção não passe a ser regra, ameaçando desnecessariamente os limites dos direitos fundamentais que ele invade<sup>301</sup>. A elasticidade do quadro de delitos, aliada à possibilidade de terceiros atuando como agente infiltrado<sup>302 303</sup>, são permissivos que não poupam o ordenamento de justificadas críticas desferidas em razão de invasão e violação desmedidas de caros direitos fundamentais<sup>304</sup>.

A inclusão de meios ocultos de obtenção de prova na legislação penal esparsa e a necessidade de tratá-los de maneira transparente<sup>305</sup> e uniforme reclamam uma sistematização,

---

CASTELL, Adán Carrizo. **El Agente Infiltrado en España y Portugal**. In: VALENTE, Manuel Monteiro Guedes. **Criminalidade Organizada e Criminalidade de Massa**. Coimbra: Edições Almedina S.A., 2009. pág. 197.

<sup>300</sup>“A Lei 12.850/13 que define organização criminosa e disciplina sua investigação, assim estabelece:

(...) Art. 3º Em qualquer fase da persecução penal, serão permitidos, sem prejuízo de outros já previstos em lei, os seguintes meios de obtenção da prova:

(...)

VII - infiltração, por policiais, em atividade de investigação, na forma do art. 11;” Disponível em <https://www2.camara.leg.br/legin/fed/lei/2013/lei-12850-2-agosto-2013-776714-norma-actualizada-pl.pdf>. Acesso em 01/10/2021

<sup>301</sup>“Apesar de compreender o impulso atual de reforçar as possibilidades da investigação criminal, a verdade é que este elenco parece dar um sinal preocupante: o de tornar este método como algo banal e generalizado. Tendo em conta as fortes limitações a direitos fundamentais que ele acarreta, a sua utilização deveria cingir-se àqueles crimes que, de outra forma, dificilmente seriam revelados.” PEREIRA, Sandra. **A Recolha da Prova por Agente Infiltrado**. In: **Prova Criminal e Direito de Defesa**. Coimbra: Edições Almedina S.A., 2013. pág. 149.

<sup>302</sup>“Não nos repugna que seja infiltrado um elemento de outra polícia. Mas, infiltrar um cidadão já levanta problemas éticos e jurídicos. Se o agente infiltrado é uma técnica excepcional, não faz sentido que o legislador tenha aberto a possibilidade da PJ poder infiltrar um terceiro, sem que tenha limitado a qualidade do terceiro (...). A eticidade deste meio excepcional de obtenção de prova é duvidosa, muita mais se o agente infiltrado for um cidadão oriundo ou ligado ao mundo do crime.” VALENTE, **A Investigação do Crime Organizado**, In: VALENTE, Manuel Monteiro Guedes. **Criminalidade Organizada e Criminalidade de Massa**. Coimbra: Edições Almedina S.A., 2009, pág. 171.

<sup>303</sup>“Maiores dificuldades suscitam ainda, neste contexto, a atuação do terceiro que atua sob o controlo da Polícia Judiciária, em particular porque a lei não define quem pode ser terceiro (ou quem não pode ser terceiro) nem dá indicações sobre o tipo de controlo que será efetuado...” ONETO, Isabel. **O Agente Infiltrado**. Coimbra: Coimbra Editora, 2005. pág. 198.

<sup>304</sup>“É que uma sociedade organizada na base do respeito pelos valores da dignidade humana, que respeite e promova os valores da amizade e da solidariedade, que vise *a construção de um país mais livre, mais justo e mais fraterno*, não pode consentir que o exercício de uma função soberana possa constituir a causa da quebra da solidariedade entre os seus membros, possa ser motivo de desconfiança no próximo, conduzir ao egoísmo e ao isolamento. A sociedade que assim se organize, que consinta a delação organizada e a estimule, tem na sua própria estrutura os germes da sua destruição.” SILVA, Germano Marques da. **Curso de Processo Penal** vol. II. Lisboa: Babel, 2011. pág. 235

<sup>305</sup> “Com efeito continua a verificar-se uma tendencial opacidade da investigação criminal em ambiente digital no ordenamento jurídico português, que se manifesta, desde logo, na dificuldade de o arguido ou defensor saberem se os procedimentos, cada vez mais exigentes, de investigação criminal e subsequente recolha de prova digital são executados pelos órgãos de polícia criminal na sua actividade investigatória, em termos compatíveis com os requisitos legais e as normas técnicas adequadas e relevantes, ou mesmo em que termos tais procedimentos são impostos internamente.” RAMALHO, David Silva. **A recolha de Prova Penal em Sistemas de Computação em Nuvem**. p. 143 In: **Revista de Direito Intelectual**, Coimbra: Almedina, nº 02, dezembro de 2014. P. 156/157

com urgência, estabelecendo um catálogo restrito e comum, próprio para esses meios, tendo como foco a criminalidade organizada, os delitos cibernéticos, a pedofilia, os transnacionais e aqueles que atentam contra a defesa nacional, como é o caso do terrorismo.

Além de estabelecer as bases para a aplicação desses métodos, a sistematização também servirá para estabelecer procedimento judicial específico para processamento e autorização judicial, bem como cuidados com a preservação do sigilo que esse tipo de coleta de prova exige. A jurisprudência já vem sinalizando nessa senda, entendendo que está formado novo capítulo tratando da prova eletrónica<sup>306</sup> na legislação esparsa, restando ao legislador abrigá-lo no Código de Processo Penal, onde poderia ser incluída a regulamentação da utilização do *malware* como instrumental para diferentes meios de obtenção de prova.

#### 4.3.4 A utilização do *malware* como agente infiltrado virtual

O desenvolvimento e a aceitação das ações encobertas justificam-se no ordenamento jurídico pela sofisticação do *modus operandi* de determinado tipo de criminalidade, cujas investigação e prevenção previstas na legislação processual penal não conseguiam apresentar resposta eficaz.

O recurso ao agente infiltrado, ainda que excepcionalmente, é de profunda importância na investigação da criminalidade organizada que se caracteriza por uma atividade contínua, empresarial, com encadeamento da linha de comando, similar a uma atividade comercial de fins lícitos, cujos atos isolados dos seus agentes podem incluir-se entre aqueles indiferentes ao alcance da norma penal, mas que, vistos em conjunto, desenham o mapa da engrenagem empresarial criminoso.

Para ter essa noção de conjunto, para visualizar tal engrenagem e quem ocupa cada posição dentro da empresa, bem como entender o mecanismo de substituição em caso de vacância de postos-chave e como ocorre a aquisição e entrega de mercadorias (que pode variar entre armas, drogas, material pornográfico infantil e até pessoas), por vezes torna-se

<sup>306</sup>...7. Assim, o Capítulo III da Lei 109/2009, relativo às disposições processuais, deve ser encarado como um «escondido Capítulo V («Da prova electrónica»), do Título III («Meios de obtenção de prova») do Livro III («Da prova») do Código de Processo Penal» (Dá Mesquita).”(Ac. TRE de 20-01-2015, Processo nº 648/14.6GCFAR-A.E1; Relator: João Gomes de Sousa; Tribunal da Relação de Évora. Disponível em: <http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/2fbdd21285478f5f80257de10056ff7a?OpenDocument>. Acesso em: 21/05/2018.

imprescindível a utilização do agente infiltrado que, ao ganhar a confiança dos integrantes da organização, acede ao detalhamento das operações, conseguindo reunir material probatório que os métodos à descoberto não conseguiriam alcançar.

Como uma empresa comum, o objetivo da empresa criminosa é a obtenção rápida de lucros, valendo-se, para tanto, de todas as ferramentas tecnológicas disponíveis, transitando no espaço virtual, ainda que dissimuladamente, e visando ampliar o alcance do seu mercado consumidor, bem como fidelizar e facilitar a execução dos atos comuns do seu comércio.

Algumas dessas empresas podem inclusive ter a maior parte das suas operações apenas em ambiente virtual, tendo em vista a maior facilidade para ocultação tanto da identidade dos seus agentes como dos rastros do caminho criminoso (*iter criminis*) percorrido, sendo, nesses casos, de pouca ou nenhuma utilidade o agente infiltrado físico como é convencionalmente conhecido. Para que se conheça a empresa criminosa, é necessário atuar em ambiente virtual, onde as regras de convivência e a aquisição de confiança exigem atuação diferenciada daquela esperada no ambiente convencional.

Partindo dessa constatação e atentos à velocidade com que a atividade criminosa se adapta às novas formas de ocultar sua atividade, os órgãos de investigação policial perceberam a necessidade de ingressar de maneira oculta também em ambiente virtual, exigindo dos agentes de segurança a aquisição de novas habilidades, bem como de regulamentação própria para atuação em ambiente virtual<sup>307</sup>.

Esses órgãos recorrem à analogia para esboçarem o agente infiltrado virtual, considerado como uma modalidade do já regulamentado agente infiltrado, mas que em

---

<sup>307</sup>“Undercover policing is certainly not a new or novel method of policing and online undercover policing has also been used for some time in cyber investigations. However, the ability of police to infiltrate online forums in order to obtain evidence required for a successful prosecution is essential when tracking anonymous users on the dark web. Infiltrating online forums requires police to establish a controlled surveillance operation in which officers covertly act as administrators or moderators of illicit forums. Online undercover operations require a significant degree of skill as officers must learn to mimic the patterns and style of online personas they are impersonating...” DAVIES, Gemma. **Shining a Light on Policing of the Dark Web: An Analysis of UK Investigatory Powers**. The Journal of Criminal Law 2020, Vol. 84 (5) 407–426. pág. 411. Disponível em [Shining a Light on Policing of the Dark Web: An Analysis of UK Investigatory Powers \(sagepub.com\)](https://www.sagepub.com). Acesso em 01/10/2021

**Em livre tradução:** O policiamento disfarçado certamente não é um método novo ou inovador de policiamento, e o policiamento disfarçado online também tem sido usado há algum tempo em investigações cibernéticas. No entanto, a capacidade da polícia de se infiltrar em fóruns online a fim de obter as evidências necessárias para um processo bem-sucedido é essencial ao rastrear usuários anônimos na dark web. A infiltração em fóruns online exige que a polícia estabeleça uma operação de vigilância controlada na qual os policiais atuam secretamente como administradores ou moderadores de fóruns ilícitos. As operações secretas online exigem um grau significativo de habilidade, pois os oficiais devem aprender a imitar os padrões e o estilo das pessoas online que estão se passando...

verdade ainda carente de regulamentação própria<sup>308</sup>. É necessário que o ordenamento jurídico estabeleça limites claros para a utilização desse método, não podendo tal uso se dar por analogia ou por construção jurisprudencial ou doutrinária. Como se trata de severa invasão da privacidade, da intimidade mesmo, os contornos dessa utilização devem estar explícitos e balizados em legislação específica.

O agente encoberto virtual pode assumir uma identidade fictícia e a partir dela estabelecer relação comercial de troca, entrega, compra e venda de material ilícito, com um ou mais investigados, mantendo contacto em salas de conversa ou por endereços de *e-mail* de difícil rastreamento<sup>309</sup>. Nesse caso, o agente se comunica diretamente com o investigado, ainda que escondido sob uma identidade falsa, sendo seu rosto desconhecido dos envolvidos com a atividade criminosa, diferentemente do agente infiltrado físico cuja identidade é falsa, mas sua imagem é conhecida da organização criminosa.

É possível a realização de outros tipos de ação encoberta em ambiente digital sem necessidade de comunicação direta com o investigado, portanto sem necessidade de criação de uma identidade fictícia. Isso acontece em casos como a intercetação telemática, situação em que a autoridade policial, mediante autorização judicial, inocula secreta e disfarçadamente programa informático (*malware*) desenhado com o objetivo de transmitir, em tempo real, as comunicações do investigado para a autoridade investigante, como previsto no artigo 18º da LC, situação que está fora do âmbito desta pesquisa, pois se trata de intercetação telemática, já prevista no dispositivo antes citado.

O *malware* também pode ser utilizado para converter o equipamento informático

---

<sup>308</sup>Ao se referir a utilização das mesmas regras da ação encoberta para a modalidade de ação encoberta virtual, Ramalho se posiciona: “Não cremos que seja assim. E não cremos que assim seja porque a redução de uma realidade complexa a um núcleo simples, vago, abstrato, com o objetivo de nele *encaixar* uma realidade semelhante mas com diferenças relevantes, é susceptível de revelar insuficiências ao nível de densificação, do detalhe e da regulamentação específica de aspectos diferentes decorrentes da natureza dos contextos respectivos.” RAMALHO, David Silva. **Métodos Ocultos de Investigação Criminal em Ambiente Digital**. Coimbra: Edições Almedina, 2017. pág. 341.

<sup>309</sup>“The example of DarkMarket is given. The site required prospective members to provide details of 100 compromised credit cards, which would then be tested by two reviewers who would report on whether the individual should be trusted to join the organisation. A controversial aspect of undercover work surrounds the extent to which an undercover officer can engage in activity that would otherwise be illegal.” DAVIES, Gemma. **Shining a Light on Policing of the Dark Web: An Analysis of UK Investigatory Powers**. The Journal of Criminal Law 2020, Vol. 84 (5) 407–426. pág. 412. Disponível em [Shining a Light on Policing of the Dark Web: An Analysis of UK Investigatory Powers \(sagepub.com\)](https://www.sagepub.com/journalsPermissions.nav?lang=en&path=/journals/criminal-law/vol84/iss5/407-426.davies). Acesso em 01/10/2021

**Em livre tradução:** Dando o exemplo do DarkMarket. O site exigia que os membros em potencial fornecessem detalhes de 100 cartões de crédito comprometidos, que seriam então testados por dois revisores que relatariam se o indivíduo deveria ser confiável para ingressar na organização. Um aspeto controverso do trabalho disfarçado envolve a extensão em que um policial disfarçado pode se envolver em atividades que, de outra forma, seriam ilegais.

onde for instalado em um dispositivo de vigilância, podendo transmitir a localização do investigado em tempo real, bem como captando sons e imagens do ambiente onde o mesmo estiver.<sup>310</sup>

A utilização do *malware* passa a ser do interesse deste trabalho quando é pensado para atuar como agente infiltrado virtual ao interagir com o investigado, tanto em atividade preventiva como investigativa, sugerindo visita a sítios com assuntos variados, inclusive de conteúdos ilícitos que podem ou não ser visitados pelo seu destinatário.

Quando sugeridos sítios que são ambientes próprios para a prática de delitos, como tráfico de armas, de pessoas ou de drogas, cabe ao usuário a decisão de a eles aceder, sendo que, caso ele prossiga e venha a firmar acordo comercial em alguns desses ambientes virtuais de existência real, voltados para a prática delitiva, o próprio *malware* capta toda a negociação e coleta meios de prova aptos a sustentar uma ação penal, tanto contra o usuário como contra o proprietário do sítio.

Nesse caso, o *malware* é utilizado como agente encoberto virtual, dispensando o agente físico da atividade de vigília da prática delitiva. Ele facilita o tratamento de dados, pois atua em tempo real, com evidente economia de tempo, evitando, dentro do limite possível, o contacto do agente físico com o investigado, ainda que em ambiente virtual, fator que reduz o risco inerente à atividade do agente infiltrado.

Nesse contexto, pode-se falar em ação encoberta virtual, cujo agente não é um policial, e sim um *malware*. Ao identificar atividade do investigado própria daquela ligada à prática de delitos, em especial daqueles tipicamente praticados em ambiente de organização

---

<sup>310</sup>“In order to unmask a device’s identifying information, which will lead to its physical location, and then potentially the user’s identity, LEA’s (Law Enforcement Agencies) use hacking tools which enable them to remotely access and install malware on a computer without its owners’ permission. Frequently this is done with the intention of accessing the target computer and converting it into a surveillance device thus circumventing the need to know a target’s location. Once installed the malware can cause a computer to perform any task, even forcing it to covertly upload files to a server controlled by law enforcement or instruct the computer’s camera or microphone to collect sound and images.” DAVIES, Gemma. **Shining a Light on Policing of the Dark Web: An Analysis of UK Investigatory Powers**. The Journal of Criminal Law 2020, Vol. 84 (5) 407–426. págs. 418 e 419. Disponível em [Shining a Light on Policing of the Dark Web: An Analysis of UK Investigatory Powers \(sagepub.com\)](https://www.sagepub.com). Acesso em 01/10/2021

**Em livre tradução:** A fim de desmascarar as informações de identificação de um dispositivo, que levarão à sua localização física e, em seguida, potencialmente à identidade do usuário, as LEA’s (autoridades policiais) usam ferramentas de hacking que lhes permitem acessar remotamente e instalar *malware* em um computador sem a permissão de seus proprietários. Frequentemente, isso é feito com a intenção de acessar o computador alvo e convertê-lo em um dispositivo de vigilância, evitando assim a necessidade de saber a localização de um alvo. Uma vez instalado, o *malware* pode fazer com que um computador execute qualquer tarefa, até mesmo forçando-o a enviar arquivos secretamente para um servidor controlado pela aplicação da lei ou instruir a câmera ou microfone do computador a coletar som e imagens

criminosa (tráfico de drogas, de armas, de pessoas, pedofilia, terrorismo, lavagem de capitais, etc.), o próprio *malware* está desenhado para disparar, dentro do ambiente virtual que o investigado está utilizando, anúncio de endereço virtual apto à prática de transações criminosas. O acesso ao ambiente virtual pode se dar por qualquer dispositivo informático seja um computador, *tablet* ou *smartphone*. Desde que o investigado aceda à esse endereço, o *malware* capta a movimentação produzida pelo investigado dentro daquele sítio virtual, que poderá vir a ser utilizada pela autoridade policial como material probatório em investigação e posterior processo judicial.

A proposta apresentada neste trabalho é de um outro tipo de agente infiltrado virtual além daquele já previsto na doutrina. Ao lado do agente infiltrado virtual, que se dá por meio de identidade fictícia atribuída a agente físico infiltrado que atuará em ambiente virtual, haveria o *malware*, funcionando como agente infiltrado controlado à distância pela autoridade investigativa, sem necessidade de assunção de identidade fictícia, pois não entrará em contacto com o investigado. Nesse hipótese, cabe a autoridade policial que dirige a investigação, o controle do disparo do *malware*, a recolha e custódia do material probatório produzido .

Pelo que foi aqui exposto, constata-se que o trabalho feito pelo *malware* de mapeamento da atividade do investigado não pode ser considerado como simples atividade de intercetação telemática. Com base no mapa das atividades do investigado, é possível ao agente monitorador apresentar catálogo de sugestões de sites com conteúdo criminoso ao usuário e aguardar que aceda a eles e passe a se comunicar ou consumir os produtos ofertados.

Na intercetação telemática, o provedor do sistema informático desvia o fluxo de dados de maneira que o investigador os receba em tempo real. No caso do agente infiltrado virtual, o objetivo do *malware* não é desviar a comunicação entre dois usuários, mas coletar dados, tais como senhas, palavras-chave, histórico de acessos e demais dados que transitem nas contas virtuais do investigado e que possam ser úteis à investigação.

O monitoramento de atividades dentro do espaço virtual é ferramenta conhecida e utilizada de forma habitual pelas empresas para apresentar seus produtos e sugerir seu consumo. Para tanto, utilizam de *softwares* devidamente projetados para tanto, inclusive para “ouvir” as conversas do usuário de *smartphone*, para em seguida sugerir a venda de produtos a ela relacionados. Além disso, toda movimentação feita em ambiente virtual, é rigorosamente

registada e utilizada como parâmetro para movimentação do mercado da publicidade na Internet<sup>311</sup>.

Se a movimentação dos usuários da Internet é monitorada, catalogada e inclusive comercializada servindo como indicativo para transações comerciais, aí incluindo o disparo de propagandas de produtos específicos de acordo com as preferências de cada consumidor, a mesma lógica e tecnologia pode/deve ser utilizada pelo Estado com o objetivo de repressão e prevenção de criminalidade organizada.

A inoculação de programa oculto visando mapear a atividade dos usuários, captar dados (*spyware*) para, por exemplo, orientar publicidade, tendo por base pesquisa nos sites que os mesmos visitam, já é prática usual em ambiente virtual.<sup>312</sup> Esses programas são conhecidos como *adware*<sup>313 314</sup> e funcionam abrindo janelas, independentemente da vontade do usuário, visando promover a venda de produtos, serviços e informar os hábitos de navegação de usuários a servidores remotos que definem quais os produtos a serem oferecidos, por meio de análise cruzada de dados.

Os diversos programas que sugerem a visita a sites de compra de vestuário, passagens aéreas, ingressos para espetáculos, com base na atividade usual do usuário, utilizam ferramenta própria de marketing que pode ou não vir a surtir efeito, pois não se pode alegar que a sugestão de acesso a determinados sites é a causa de falência ou de maus hábitos

---

<sup>311</sup>“Conocemos que cada click en un aviso, cada búsqueda realizada, cada página visitada, cada “Me gusta”, son registrados por algún sistema y forman parte del gran circuito comercial que son la razón de la economía por publicidad en Internet.” TEMPERINI, Marcelo; MACEDO, Maximiliano. **Nuevas Herramientas de Investigación Penal. El Agente Encubierto Digital**. In: DUPUY, Daniela; KIEFER, Mariana, **Cibercrimen**. Madrid: B de F Ltda, 2016. p. 486.

<sup>312</sup>“Podría argumentarse que un programa oculto es em sí mismo ilícito. No es de recibo este argumento porque, en primer lugar, hay aplicaciones informáticas que tienen estas características y no están absolutamente proscritas (p. ej., los que dirigen a orientar la publicidad a partir de las búsquedas en internet o las páginas visitadas por el usuario) (HAIRABEDIÁN, Maximiliano. **El Acceso a Información y Datos de Teléfonos Celulares**. In: DUPUY, Daniela e KIEFER, Mariana. **Cibercrimen**: Madrid. Editorial B de f, 2016, p. 470)

<sup>313</sup>O termo *adware* vem do inglês e se forma pela partícula “ad”, anúncio, e “ware”, programa, e se referem a programas que exibem anúncio sem a autorização do usuário.

<sup>314</sup>“Adware is a program that independently opens windows of the browser in order to promote merchandising and services. This program presents some risks. Some adware can slow down your computer, others can change the html of the pages you are browsing, just to include links and advertisements. In addition, many types of adware communicate your browsing habits to remote servers, thus violating your privacy” MANGIAMELLI, Agata C. Amato. **"Theory of Law and Computer Crimes – Teoria do Direito e Crimes Informáticos"** *Duc In Altum-Cadernos de Direito* v. 8, n.16, set-dez 2016, (2017). Disponível em: <http://www.faculdedamas.edu.br/revistafd/index.php/cihjur/article/view/395/379>. Acesso em: 06/07/17.

**Em livre tradução:** Adware é um programa que abre janelas do navegador de forma independente para promover merchandising e serviços. Este programa apresenta alguns riscos. Alguns *adwares* podem tornar seu computador lento, outros podem alterar o html das páginas que você está navegando, apenas para incluir links e anúncios. Além disso, muitos tipos de *adware* comunicam seus hábitos de navegação a servidores remotos, violando assim sua privacidade

financeiros do usuário. Esses casos decorrem de escolha própria dos usuários e por opções de consumo equivocadas que porventura tenham feito.

A atividade do *malware* como agente encoberto virtual segue a mesma lógica que aquela que orienta a atividade comercial de marketing, ou seja: o *malware* recolhe a atividade do usuário, faz cruzamento de seus diversos acessos e interesses em rede, para em seguida apresentar sugestão dos sites que podem vir a ser visitados. A atividade do programa malicioso fica todo tempo sob a supervisão da autoridade policial, que embora não esteja se comunicando com o investigado, vigia sua atividade com base em informações em tempo real que são fornecidas pelo *malware*.

A sugestão dos sites só é apresentada ao investigado após passar pelo crivo da autoridade policial. Esta chancela o início do trabalho de monitoramento da atividade daquele, que a partir deste ponto acompanha sua atividade. O *malware*, devidamente programado para tanto, registra, grava e encaminha a atividade do observado para o dispositivo informático da autoridade policial, como se fora a atividade de *phishing*<sup>315</sup>, a fim de utilizá-la no direcionamento de investigações.

Ante a ausência de comunicação entre o agente policial que monitora a atuação e o investigado, não há necessidade de uma identidade fictícia, como no caso do agente infiltrado

---

<sup>315</sup>“Phishing is a technique that aims at obtaining confidential information, by addressing the victims directly. For example, in an e-mail, seemingly signed by a lending institution, a user is asked to enter his personal information under the guise of a security check. By using this information, the offender enters the victim’s account and, carries out various operations. This criminal activity is based on the techniques called social engineering. In addition to random emails, phishing can also be carried out by telephone or by sending text messages. Usually, the email asks the user to click on a link in the message to avoid a charge and/or to regularize his position with an institution or company. Sometimes, the e-mail contains an offer of working opportunities, for example, positions as financial operator. By providing their bank details, users will receive a credit. This has a lot to do with recycling activities – cyberlaundering, money-laundering, is particularly important for phishers. By dispersing stolen money in many current accounts and spreading them in different countries, it becomes extremely difficult to discover the criminals’ identities.” MANGIAMELI, Agata C. Amato. "**Theory of Law and Computer Crimes – Teoria do Direito e Crimes Informáticos**" *Duc In Altum-Cadernos de Direito* v. 8, n.16, set-dez 2016, p. 28. Disponível em: <http://www.faculdedamas.edu.br/revistafd/index.php/cihjur/article/view/395/379>. Acesso em 05/10/2021

**Em livre tradução:** Phishing é uma técnica que visa obter informações confidenciais, abordando diretamente as vítimas. Por exemplo, em um e-mail, aparentemente assinado por uma instituição de crédito, um usuário é solicitado a inserir suas informações pessoais sob o pretexto de uma verificação de segurança. Ao usar essas informações, o agressor entra na conta da vítima e realiza várias operações. Essa atividade criminosa é baseada nas técnicas chamadas de engenharia social. Além de e-mails aleatórios, o phishing também pode ser realizado por telefone ou enviando mensagens de texto. Normalmente, o e-mail pede ao usuário que clique em um link da mensagem para evitar cobrança e/ou regularizar sua situação junto a uma instituição ou empresa. Às vezes, o e-mail contém uma oferta de oportunidades de trabalho, por exemplo, cargos como operador financeiro. Ao fornecer seus dados bancários, os usuários receberão um crédito. Essa atividade tem muito a ver com atividades lavagem de dinheiro física e em espaço virtual, sendo elas particularmente importantes para os phishers. Ao dispersar o dinheiro roubado em muitas contas correntes e distribuí-lo em diferentes países, torna-se extremamente difícil descobrir a identidade dos criminosos.

virtual. O investigado não tem conhecimento que sua atividade está sendo monitorada, nem há qualquer comunicação entre ele e o agente policial. Apesar disso, o agente policial, ao avaliar os sites a serem sugeridos pelo *malware*, tem controle da investigação, agindo de maneira encoberta, ocultada pelo programa informático que captura as informações, monitora a atividade do usuário e sugere o acesso a espaços próprios para a prática de delitos.

O *malware*, assim desenhado, trabalha com sugestões, apresentando possibilidades de endereços maliciosos por meio de *adware*, com base nas pesquisas usuais do investigado feita por *spywares*. Caso o arguido aceda a tais sites, usualmente de comércio de armas, de drogas, de pornografia infantil, de tráfico de pessoas, as visitas aos endereços que correspondem a esses conteúdos são registados e monitorados por meio de *trojans*<sup>316</sup>. Desse modo, é possível a captação de senhas, de endereços de outros contactos e o mapeamento de uma rede de comércio ilícito que tanto pode levar a incriminações individuais como a descobrir uma ou mais organizações criminosas.

Importante destacar que, ao sugerir e apresentar possibilidades ao investigado, a autoridade policial, por intermédio do *malware*, apenas facilita a prática do delito, como de resto o agente infiltrado físico também o faz. A atuação do *malware* não tem por objetivo induzir a prática de delito, não operando como agente provocador. Ele apenas sugere para em seguida observar e registar as ações do investigado.

O agente provocador induz o desejo de delinquir em quem não o tem. O agente infiltrado tanto investiga um delito que já aconteceu e busca reunir provas do cometimento deste, como pode atuar preventivamente, visando identificar a organização criminosa e impedindo a prática de novos delitos.

Quando visando a prevenção, pode, por exemplo, monitorar um crime de entrega regular, de consumação constante, como é o caso do tráfico ilícito de estupefacientes. Diferentemente do agente provocador que é responsável pelo delito, é seu coautor, o agente infiltrado reúne provas podendo até mesmo praticar atos preparatórios, mas a decisão da

---

<sup>316</sup>“Trojan horse is a seemingly harmless program that hides dangerous commands for the computer. Typically, a Trojan horse is used to send spam or steal personal data. In any case, it is a program which aims at taking control of a computer.”MANGIAMELI, Agata C. Amato. "Theory of Law and Computer Crimes – Teoria do Direito e Crimes Informáticos" *Duc In Altum-Cadernos de Direito* v. 8, n.16, set-dez 2016, p. 23. Disponível em: <http://www.faculdedamas.edu.br/revistafd/index.php/cihjur/article/view/395/379>. Acesso em 05/10/2021

**Em livre tradução:** O cavalo de Tróia é um programa aparentemente inofensivo que oculta comandos perigosos para o computador. Normalmente, um cavalo de Tróia é usado para enviar spam ou roubar dados pessoais. Em qualquer caso, é um programa que visa assumir o controle de um computador.

prática do delito é do investigado, não tendo o agente policial induzido-o à prática do delito, como o faz o agente provocador.

A sugestão feita pelo *malware* ao investigado, apresentando sites que contenham conteúdo de prática de ato delitivo, não se classifica como indução à prática de delito. Se uma investigação está em andamento é porque já estão reunidos indícios suficientes do envolvimento do investigado em organização criminosa, restando apenas a reunião dos elementos de provas incriminatórias.

Considere-se que a autoridade policial consiga inocular o programa no dispositivo informático do investigado, e tal programa sugira sites de conteúdo não confiável, com base na regular atividade do investigado, e aguarde que o mesmo acesse a ambientes virtuais comprometedores e lá atue criminosamente, para então registrar tais condutas. Essa estratégia não pode ser analisada como uma ação que teria induzido o investigado a praticar o delito. Muito menos é possível determinar que as sugestões de visita a sites de procedência duvidosa tenham retirado dele a capacidade de autodeterminação ou de atuação de maneira diversa.

É fundamental observar que a escolha sempre estará à disposição do usuário, não podendo ser classificada como uma ação de incitação, porque a atividade sugerida é similar àquela já desenvolvida pelo investigado no âmbito das redes virtuais. Não se trata, portanto, de provocar no agente a vontade de delinquir, pois considera-se que exista a pré-disposição para o ato criminoso, comprovada por relatórios elaborados e documentados antes do início da autorização judicial para atividade policial. A identificação do usuário pode ocorrer, inclusive, porque o mesmo acessou um desses sites, não sendo sua existência conhecida previamente pela autoridade policial.

Assim, tanto o *malware* pode atuar após a autoridade policial identificar um determinado suspeito que passará a ser investigado, portanto a jusante, como o *malware* pode ser utilizado para identificar os suspeitos, que a princípio são desconhecidos da autoridade policial e, após sua identificação, passar a registrar sua atividade e coletar provas. Em ambos os casos, para que se inicie a investigação, é necessária uma fundada suspeita da existência de uma organização criminosa, podendo ou não já se iniciar a investigação com algum suspeito identificado.

Como requisito para a autorização judicial da utilização da ação encoberta virtual, é necessária a prévia identificação do sujeito a ser investigado, ainda que essa identificação seja

precária, utilizada apenas em ambiente virtual, como um apelido (*nickname*) ou endereço de IP<sup>317</sup>. Essa identificação, a princípio incipiente, vai se delineando e densificando com o desenvolver da investigação, até chegar a pessoa física por trás do código (*nickname* ou IP)

Nos casos de delitos praticados em ambiente virtual, muitas vezes, suspeita-se da prática do delito. Pode até mesmo ser comprovada a atividade delitativa, mas é possível que não se tenha ideia de quem são os autores. O *malware* é de grande valia nesses casos, pois pode atuar se ocultando em um sítio dedicado à prática de atividade criminosa e ali ficar à espreita, como que de tocaia, aguardando que os agentes compareçam para a prática do delito.

A atividade dentro desse ambiente virtual, portanto local do crime, pode ser monitorada e seguido o rastro deixado por meios das ações praticadas virtualmente. Entretanto, nem sempre é fácil identificar o local do crime, bem como alcançar tanto o proprietário do sítio virtual, como aqueles que ali frequentam. A investigação, portanto, pode partir de um crime determinado em busca da sua autoria ou da suspeita de um indivíduo que supostamente pratica delitos, e assim seguir passando da suspeita à confirmação do caso concreto.

No caso de criminalidade organizada, a investigação apresenta determinadas peculiaridades que precisam ser observadas. No crime comum, o objeto da atividade investigativa é identificável como resultado de uma atividade criminosa, e a investigação parte para a recolha de material probatório visando comprovar materialidade e autoria do delito.

No crime organizado, a identificação do resultado criminoso e do seu autor imediato, em regra, está muito distante do principal responsável pelas ações criminosas, do chefe da organização, daquele que tem o domínio do fato e que é quem de fato interessa à investigação desse tipo de criminalidade. Por isso, identificar quem entregou a droga e recebeu o valor correspondente não causa impacto significativo à estrutura organizacional da empresa criminosa. É importante atuar na repressão do crime no varejo, mas a tarefa de maior envergadura é identificar a organização criminosa e quem está no topo da pirâmide gerencial.

---

<sup>317</sup>“Internet Protocol” or “IP” address, which is a series of numbers that computers connected to the Internet understand as an address akin to a phone number” KERR, Orin S. **The Problem of Perspective in Internet Law.** *In Georgetown Law Journal*, Vol. 91, p. 357-405, February 2003, p. 363. Disponível em <https://heinonline.org/HOL/LandingPage?handle=hein.journals/glj91&div=17&id=&page=>, Acesso em 05/10/2021

**Em livre tradução:** Endereço de “protocolo da Internet” ou “IP”, é uma série de números que os computadores conectados à Internet entendem como um endereço semelhante a um número de telefone

Com base em pequenos delitos de tráfico de drogas, por exemplo, pode-se estabelecer uma conexão entre eles, embora com conhecimento rudimentar sobre as especificidades de funcionamento e alcance dessa conexão. O investigador tem os fatos que até podem ser punidos isoladamente, mas não detém o conhecimento sobre a conexão entre eles, a organização de maior complexidade que os sustenta, que dá suporte à prática diária de diversos fatos idênticos, sobretudo se ele tiver à sua disposição apenas os métodos tradicionais de investigação. Nesse contexto, o *malware* pode agregar maior alcance e efetividade ao trabalho investigativo.

Os requisitos para escolha do sujeito a ser investigado no ambiente virtual são similares àqueles que se utilizam para escolher um alvo de investigação com agente infiltrado, por exemplo. Em toda organização criminosa, como na vida, sempre existem os mais espalhafatosos, que costumam vangloriar-se de suas façanhas, ávidos por palco e plateia que lhes afague o ego.

No ambiente virtual não é diferente, podendo o *malware*, devidamente programado e parametrizado previamente pelo investigador, servir para a identificação do suposto autor de delitos com base em análise de milhares de atividades em ambiente virtual e consequente cruzamento dos dados colhidos nesta análise. Em seguida, é possível acompanhar o caminho que ele vai trilhar, os sites que acessará, com quem estabelecerá comunicação, aguardando, por fim, pela sua livre atividade delitiva nas redes virtuais, quando será colhido o material probatório necessário para instruir a devida ação penal.

As possibilidades de utilização do *malware* como um tipo de agente infiltrado virtual são promissoras e pretende aumentar a eficácia de quem se dedica a investigação e ao combate ao crime organizado. Entretanto, a sua inclusão no ordenamento processual penal, como propõe este trabalho, necessita ser submetida ao crivo dos Princípios Constitucionais indagando os mesmos quanto ao cabimento de tal método oculto de obtenção de prova.

No capítulo a seguir será estabelecido esse diálogo, tanto com Princípios Constitucionais, como aqueles que servem de esteio ao ordenamento processual penal.

## 5. ESTEIO CONSTITUCIONAL

É na Constituição, usada como *ultima ratio*, que busca-se encontrar justificativa tanto para os limites e direitos insertos no catálogo ofertado aos participantes do processo penal, como para solucionar as questões não suficientemente resolvidas pelo código de ritos que o disciplina. A relação do cidadão com o processo penal é assim, em última instância, uma relação constitucional, sendo necessário entendê-la no limite em que ela influencia o embate do cidadão com o poder punitivo estatal.<sup>318</sup>

São os instrumentos do processo penal, na maior parte das vezes, o primeiro ponto de comunicação que a maioria dos cidadãos tem de confrontação com o poder estatal, em especial num Estado que apresenta índices de violência só comparados aos de países conflagrados por guerras<sup>319 320</sup>.

Da tensão gerada entre o dever do Estado em aplicar com o rigor da lei a sanção devida e a expectativa do cidadão, recorrentemente frustrada, de ver devidamente punido o autor do homicídio do seu ente querido, vem a necessidade do estabelecimento de regras explícitas, a exigência da delimitação exata dos poderes estatais, bem como dos direitos e deveres não só do arguido, mas de todos os participantes do processo penal, incluídos desde o perito, a testemunha, até o Estado-Juiz.

Esse cardápio de direitos e obrigações oferecido aos atores chamados a atuar nos diversos cenários, desenhados pelo código de ritos penal, e ainda as questões surgidas das falhas comunicativas entre a situação posta no cenário da vida real e a solução (não)

<sup>318</sup>“Para a maioria dos cidadãos, o processo penal representa a confrontação mais intensa com o poder soberano estatal que existe. (...) ...para a compreensão e para o funcionamento do processo penal e a relação deste com o Direito Constitucional, sendo a situação de conflito mencionada entre o cidadão e poder estatal, em última instância, um problema de Direito Constitucional.” TIEDEMANN, Klaus. *In*: ROXIN, Claus; ARTZ, Gunther e TIEDEMANN, Klaus. **Introdução ao Direito Penal e ao Direito Processual Penal**. Belo Horizonte: Del Rey, 2007. p. 145 e 146.

<sup>319</sup>FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. **Atlas da Violência**, [http://www.forumseguranca.org.br/wp-content/uploads/2018/06/FBSP\\_atlas\\_violencia\\_2108\\_Infografico.pdf](http://www.forumseguranca.org.br/wp-content/uploads/2018/06/FBSP_atlas_violencia_2108_Infografico.pdf). Disponível em: <https://infograficos.oglobo.globo.com/brasil/a-guerra-do-brasil.html>. Acesso em: 19/06/2018.

<sup>320</sup>“O Brasil mata. Mata muito. Entre 2001 e 2015 houve 786.870 homicídios, a enorme maioria (70%) causados por arma de fogo e [contra jovens negros](#). Os números da violência no maior país da América Latina atingem dimensões ainda mais preocupantes ao se compararem com guerras internacionais deste século. Desde que começou o conflito sírio, em março de 2011, morreram 330.000 pessoas. A guerra de Iraque soma 268.000 mortes desde 2003. Brasil, com 210 milhões de habitantes, é o país que mais mata no século XXI. (...) Segundo os números do jornal, o Brasil matou nos últimos 15 anos o equivalente à população de Frankfurt, Sevilha ou João Pessoa”. Disponível em: [https://brasil.elpais.com/brasil/2017/12/11/politica/1513002815\\_459310.html](https://brasil.elpais.com/brasil/2017/12/11/politica/1513002815_459310.html). Acesso em: 19/06/2018.

apresentada por aqueles cenários, previstos neste mesmo código de ritos, exige que o intérprete, o aplicador da lei, recorra de pronto à Constituição.

## 5.1 PRINCÍPIOS E POSTULADOS CONSTITUCIONAIS

A intercessão entre processo penal e Constituição pode ser identificada nos princípios processuais penais insertos na carta constitucional. Localiza-se aqui a abertura cognitiva, o ponto de comunicação entre os dois diplomas legais, onde se busca a autorização para aplicar a constrição das liberdades impostas pelo processo ao cidadão. Por outro lado, é nesse mesmo *locus* que o imperativo estatal de garantia da segurança encontra a possibilidade de sua realização e adquire corpo e concretude, vestindo a roupagem das regras processuais penais.

O processo penal é regido e sustentado por princípios próprios e tem por finalidade instrumentalizar a aplicação da lei penal, ou seja, servir de chave tradutora que possibilite o encaixe entre o código restritivo estatal (lei penal) e o fato da vida (fato penalmente relevante). Sem essa chave, esse instrumento de adequação, a lei penal será uma carta de intenções que não conseguirá ultrapassar a barreira do simbólico-intimidatório.

Por sua vez, a elaboração e o manuseio dessa chave leitora, como metaforicamente aqui proposto, não acontece desvinculada de qualquer parâmetro. Deve estar de acordo com os princípios constitucionais gerais, que são a ossatura de todo texto constitucional e dão forma ao Estado de acordo com os princípios específicos do processo penal, por eleição constitucional, acusatório<sup>321</sup>, entre eles o direito ao processo equitativo<sup>322</sup>, ao contraditório<sup>323</sup>

---

<sup>321</sup>“Precisamente, se puede llamar *acusatorio* a todo sistema procesal que concibe al juez como un sujeto pasivo rígidamente separado de las partes y al juicio como una contienda entre iguales iniciada por la acusación, a la que compete la carga de la prueba, enfrentada a la defensa em un juicio contradictorio, oral y público y resuelta por el juez según su libre convicción.” FERRAJOLI, Luigi. **Derecho y Razón**. Madrid: Editorial Trotta, 2000, pág. 564

<sup>322</sup>“Art. 20º da CRP (...) 4. Todos têm direito a que uma causa em que intervenham seja objecto de decisão em prazo razoável e mediante processo equitativo.”

<sup>323</sup>“Art. 32º da CRP (...) 5. O processo criminal tem estrutura acusatória, estando a audiência de julgamento e os actos instrutórios que a lei determinar subordinados ao princípio do contraditório.”

<sup>324</sup>e a ampla defesa<sup>325</sup>. Esses princípios gerais informam outros tantos que, mesmo não estando inscritos literalmente na Carta Magna, adquirem tal *status*, como é o caso do direito ao silêncio, por alguns considerado como direito a não autoincriminação (autoinculpação), mas que não se confundem por apresentarem conteúdos distintos, e que de perto interessa ao estudo desenvolvido neste trabalho.

Os diversos princípios, que por sua própria estrutura normativa apenas contém fundamentos, podem entrar em colisão, e por isso é necessário que o sistema jurídico estabeleça técnicas próprias para avaliação e definição de qual ou quais princípios devem ser utilizados em casos concretos e em que medida.

Quando se defrontam em um caso concreto, por possuírem dimensão de peso e de importância<sup>326</sup>, os princípios, diferentemente das regras, não necessariamente se excluem. Pode ser usado mais de um princípio para uma mesma situação, embora seja fundamental avaliar em qual medida cada um interferirá para resolução da questão. Para efetuar essa avaliação, é necessária a utilização de postulados, como a proporcionalidade e a ponderação, que não se confundem com os princípios. Nesse ponto, faz-se importante fixar os conceitos a serem utilizados, e o referencial teórico eleito para sustentar o entendimento aqui escolhido para conceituar regras, princípios e postulados.

A primeira distinção que merece destaque é a que trata de regras e princípios. Ambas são normas, porque dizem exatamente o que deve ser.<sup>327 328</sup> Essa divisão não se baseia em critérios como generalidade e especialidade da norma, mas em estrutura e forma de aplicação, sendo portanto uma distinção qualitativa e não uma distinção de grau. São consideradas regras

---

<sup>324</sup>Apesar da literalidade da escolha do modelo acusatório feito pelo legislador Constituinte, encontramos na doutrina posicionamento afirmando que o processo penal adota modelo híbrido: “Embora o nº 5 do art. 32º da Constituição da República Portuguesa (CRP) se refira apenas à estrutura acusatória, entende a doutrina que ela é mitigada por um princípio de investigação.” MENEZES, Sofia Saraiva de. **O Direito ao Silêncio: A Verdade por Trás do Mito** in BELEZA, Tereza Pizarro e PINTO, Frederico de Lacerda Costa. **Prova Criminal e Direito de Defesa**. Coimbra: Almedina, 2013, pág. 120

<sup>325</sup> “Art. 32º da CRP (...) 1. O processo criminal assegura todas as garantias de defesa, incluindo o recurso.”

<sup>326</sup>“Os princípios possuem uma dimensão que as regras não têm – a dimensão do peso ou importância.” DWORKIN, Ronald. **Levando os Direitos a Sério**. Trad. Nelson Boeira. 2 ed. São Paulo: Martins Fontes, 2007. p. 42.

<sup>327</sup>“Com frequência, não são regra e princípio, mas norma e princípio ou norma e máxima, que são contrapostos. Aqui, regras e princípios serão reunidos sob o conceito de norma. Tanto regras quanto princípios são normas, porque ambos dizem o que deve ser.” ALEXYS, Robert. **Teoria dos Direitos Fundamentais**. Trad. Virgílio Afonso da Silva. São Paulo: Malheiros Editores, 2008. p. 87.

<sup>328</sup>“(1) as regras e princípios são duas espécies de normas; (2) a distinção entre regras e princípios é uma distinção entre duas espécies de normas.” CANOTILHO, José Joaquim Gomes. **Direito Constitucional e Teoria da Constituição**. Coimbra: Ed. Almedina, 2003. p. 1160.

as normas que são sempre satisfeitas ou não satisfeitas, ou seja, se tem validade é coercitivo, que seja feito aquilo que ela manda<sup>329</sup>.

Princípios, por sua vez, expressam deveres *prima facie*, cujo conteúdo definitivo somente é fixado após sopesamento com princípios colidentes. Eles são normas que obrigam que algo seja realizado em determinada medida, desde que dentro do universo de possibilidade fática e jurídica existente. Assim, enquanto as regras contém determinações a serem integralmente cumpridas, os princípios se apresentam como mandamentos de otimização cuja satisfação pode se efetivar em variados graus<sup>330 331</sup>.

No caso de conflitos entre regras, uma será considerada válida em detrimento das outras e será aplicada ao caso concreto, mas tal solução não se apresenta assim quando o conflito é entre princípios. A colisão entre princípios não exclui necessariamente nenhum dos colidentes, apenas aponta que será necessário decidir em qual medida cada um deles deve ser aplicado, qual terá prevalência, sendo certo que essa prevalência não é absoluta, pois se restringe apenas ao caso em análise.

Mudadas as circunstâncias e o balizamento, pode ser o contrário, bem como invertida a ordem de prevalência entre os mesmos princípios, se outra vez em colisão<sup>332</sup>. É fundamental, portanto, definir como será estabelecido o parâmetro a ser utilizado para decidir qual o princípio e em que medida ele deverá prevalecer, visando reduzir ao mínimo o espaço da subjetividade do julgador. Isso porque quanto mais objetivo for o critério adotado, maior será

---

<sup>329</sup>“ Já as *regras* são normas que são sempre ou satisfeitas ou não satisfeitas. Se uma regra vale, então, deve se fazer exatamente aquilo que ela exige; nem mais, nem menos. (...) Isso significa que a distinção entre regras e princípios é uma distinção qualitativa, e não uma distinção de grau.” ALEXY, Robert. **Teoria dos Direitos Fundamentais**. Trad. Virgílio Afonso da Silva. São Paulo: Malheiros Editores, 2008. p. 91.

<sup>330</sup>“Princípios são, por conseguinte, *mandamentos de otimização*, que são caracterizados por poderem ser satisfeitos em graus variados e pelo fato de que a medida devida da sua satisfação não depende somente das possibilidades fáticas, mas também das possibilidades jurídicas ALEXY, Robert. **Teoria dos Direitos Fundamentais**. Tradução Virgílio Afonso da Silva. São Paulo: Malheiros Editores, 2008. p. 90.

<sup>331</sup>“**Regras** – insista-se neste ponto – são normas que, verificados determinados pressupostos, exigem, proíbem ou permitem algo em termos definitivos, sem qualquer exceção (*direito definitivo*). (...) **Princípios** são normas que exigem a realização de algo, da melhor forma possível, de acordo com as possibilidades fáticas e jurídicas. Os princípios não proíbem, permitem ou exigem algo em termos de “tudo ou nada”; impõem a otimização de um direito ou de um bem jurídico, tendo em conta a “reserva do possível”, fática ou jurídica.” CANOTILHO, José Joaquim Gomes. **Direito Constitucional e Teoria da Constituição**. Coimbra: Ed. Almedina, 2003. p. 1255.

<sup>332</sup> “Se dois princípios colidem (...) um dos princípios terá que ceder. Isso não significa, contudo, nem que o princípio cedente deva ser declarado inválido, nem que nele deva ser introduzida uma cláusula de exceção. Na verdade, o que ocorre é que um dos princípios tem precedência em face do outro sob determinadas condições. Sob outras condições a questão da precedência pode ser resolvida de forma oposta.” ALEXY, Robert. **Teoria dos Direitos Fundamentais**. Trad. Virgílio Afonso da Silva. São Paulo: Malheiros Editores, 2008. p. 93.

a garantia do respeito ao direito fundamental<sup>333</sup> que será mitigado. Como aos princípios cabe a tarefa de promover a realização de direitos fundamentais, é necessário definir como tal promoção será efetivada.

Para o estabelecimento da resolução do conflito entre princípios, são invocadas outras normas que possuem a única finalidade de estruturar a aplicação dos princípios e das regras, resolvendo, por consequência, possíveis conflitos que venham a ocorrer. Tais normas são estruturantes e não guardam conteúdo de promoção de um determinado fim, nem descrevem comportamento a ser observado. Elas apenas estruturam a aplicação das normas que assim o fazem, ou seja, servem de parâmetro para aplicação dos princípios e das regras.

É possível afirmar que esses postulados normativos aplicativos localizam-se em patamar distinto daquele em que se situam as normas, em que residem os princípios e as regras, podendo ser chamadas de normas de segundo grau ou metanormas, e que funcionam apenas como estruturantes para aplicação de outras normas<sup>334</sup>.

Por apresentarem caráter estruturante, vazios de comando para realização de um fim, os postulados podem indiretamente ser violados, como é o caso da proporcionalidade, geralmente tomada por princípio, mas que em verdade é uma norma estruturante, utilizada para aplicação dos princípios e das regras.

Os postulados normativos, adjetivados aplicativos para melhor destacar sua finalidade, não podem ser aplicados pelo julgador apenas por subsunção, mas reclamam a observância de ordenação e relação entre vários elementos, tais como critério e medida, meio e fim, regra geral e caso individual, não se limitando a uma mera correspondência entre a norma e o fato<sup>335</sup>.

---

<sup>333</sup> “As normas de direitos fundamentais são não raro caracterizadas como ‘princípios’”. ALEXY, Robert. **Teoria dos Direitos Fundamentais**. Trad. Virgílio Afonso da Silva. São Paulo: Malheiros Editores, 2008. p. 86.

<sup>334</sup> “...os postulados normativos situam-se num plano distinto daquele das normas cuja aplicação estruturam. (...) São, por isso, metanormas, ou normas de segundo grau. O qualificativo de *normas de segundo grau*, porém, não deve levar à conclusão de que os postulados normativos funcionam como qualquer norma que fundamenta a aplicação de outras normas (...) os postulados normativos funcionam como estrutura para aplicação de outras normas.” ÁVILA, Humberto. **Teoria dos Princípios**. São Paulo: Malheiros Editores Ltda, 2006. p. 121 a 123.

<sup>335</sup> “A análise dos postulados de razoabilidade e proporcionalidade, por exemplo, está longe de exigir do aplicador uma mera atividade subsuntiva. Eles demandam, em vez disso, a ordenação e a relação entre vários elementos (meio e fim, critério e medida, regra geral e caso individual), e não um mero exame de correspondência entre a hipótese normativa e os elementos de fato.” ÁVILA, Humberto. **Teoria dos Princípios**. São Paulo: Malheiros Editores Ltda, 2006. p. 123 a 124.

## 5.2 DOS PRINCÍPIOS

O recurso, a ação encoberta, seja ela em meio físico ou virtual, como método de produção de prova, recebe à partida crítica referente a violação dos princípios processuais constitucionais da intimidade, da não autoincriminação e do direito ao silêncio<sup>336</sup>. Entretanto, tais princípios, como de regra todos os outros, podem sofrer mitigação, não apresentando validade irrestrita. A necessidade de combate ao crime, especialmente ao crime organizado, o dever do Estado em promover a ordem e a segurança dos cidadãos são também princípios constitucionais a serem avaliados no momento do seu chamamento para dirimir conflitos entre os interesses particulares e os da comunidade.<sup>337</sup>

O confronto que possa vir a surgir entre princípios constitucionais cristalizados em direitos fundamentais deve ser resolvido considerando que os princípios são ponderáveis, e por isso podem ser balanceados, sem necessariamente ser feita a opção por um deles, ignorando os demais na resolução da questão.

A possível violação de direito fundamental para a implementação do método de prova proposto neste trabalho entra em confronto com o dever do Estado em manter a segurança da sociedade<sup>338</sup>, sendo certo que na adoção de políticas públicas, mais que interesses individuais, é necessário ter em mira o interesse coletivo que, respeitando os interesses individuais dentro do possível, deve priorizar atender ao fim social para o qual o Estado foi criado.

<sup>336</sup>“Así, frente a la utilización de la figura del agente encubierto como medio de investigación, se plantea la posibilidad de que el derecho fundamental a la autoincriminación quede prácticamente anulado, debido a que es muy probable que el agente encubierto induzca al investigado para que le declare hechos o cosas autoincriminantes...” PEREIRA, Flávio Cardoso. **El Agente Infiltrado desde el Punto de Vista del Garantismo Procesal Penal**. Curitiba: Juruá Editora, 2016. p. 710

<sup>337</sup>“Desde lo jurídico y como sucede históricamente en el universo jurídico, no existen derechos absolutos, sino limitados precisamente por otros derechos” TEMPERINI, Marcelo; MACEDO, Maximiliano. *Nuevas Herramientas de Investigación Penal. El Agente Encubierto Digital*. In: DUPUY, Daniela; KIEFER, Mariana, **Cibercrimen**. Madrid: B de F Ltda, 2016. p. 487.

<sup>338</sup>“... una política criminal eficiente no puede propiciar seguridad solamente as garantías individuales del investigado en perjuicio del combate a la criminalidad organizada que expone a peligro toda una sociedad. Nos parece que toda regla presenta excepciones, pues deberá por veces, predominar la necesaria salvaguardia a los intereses de la colectividad en detrimento a los derechos individuales de algunos ciudadanos comprometidos con bandas de delincuentes organizados. Se evitaría de este modo la subsistencia de una maléfica y abusiva instrumentalización de las garantías, la cual viene a propiciar una fuerte sensación de inseguridad.” PEREIRA, Flávio Cardoso. **El Agente Infiltrado desde el Punto de Vista del Garantismo Procesal Penal**. Curitiba: Juruá Editora, 2016. p. 514, 515.

### 5.2.1 Direito ao Silêncio

O Código de Processo Penal em seu art. 61º, 1, d) assegura ao arguido o direito de “não responder a perguntas feitas, por qualquer entidade, sobre os fatos que lhe forem imputados e sobre o conteúdo das declarações que acerca deles prestar”.<sup>339</sup> Em assim dispondo, garante a possibilidade de permanecer em silêncio, evitando a hipótese de fazer prova contra si mesmo, em virtude de alguma declaração que venha a prestar. O direito assegurado pela letra da lei é o do silêncio, o de ficar calado, de não prestar depoimento. A extensão dada a esse direito que avança para negativas que extrapolam o limite da omissão declarativa é construção doutrinária e jurisprudencial e assim deve ser analisada.

A garantia de não se autoinculpar, mantendo-se em silêncio, tem origem na necessária proteção contra as torturas praticadas com o objetivo de se obter confissões durante os interrogatórios<sup>340</sup>, prática comum tanto na época inquisitorial quanto mais recentemente, nas ditaduras da era moderna. O fim a que se destina esse direito é assegurar que o arguido possa ficar em silêncio, que não haja obrigatoriedade em falar sobre os fatos que lhe forem imputados ou sobre qualquer outro assunto a eles relacionados, que de tal silêncio não lhe redunde prejuízo, nem consequências.

No modelo acusatório, especificamente sob a ótica garantista, o interrogatório deixa de ser meio de prova para se constituir instrumento de defesa, momento oportuno para o arguido livremente apresentar seus argumentos<sup>341</sup>, inclusive, se quiser, para ali silenciar. O

<sup>339</sup>“O CPP de 1987 corporiza as garantias constitucionais, interpretadas à luz da Convenção Europeia dos Direitos Humanos (CEDH) e da jurisprudência do TEDH. Por essa via, está também associado à prerrogativa contra a auto-incriminação (*privilege against self-incrimination*) da tradição anglo-americana, que abrange o direito ao silêncio.” MENDES, Paulo Sousa. **O Processo Penal entre Eficácia e Garantias. In Direito da Investigação Criminal e da Prova.** Coimbra: Almedina, 2014, pág. 75

<sup>340</sup>“A administração da justiça dos países da Europa continental, por sua vez, foi se ancorando, a partir do século XIII, em um modelo misto de direito romano, canônico e germânico, racionalmente construído e centrado na decisão de juízes. Seu bastião era um sistema de provas que permitisse alcançar a verdade que mais se aproximasse da verdade divina. Valia-se, para tanto, de testemunhos oculares considerados idôneos ou da confissão do réu. Entretanto, dada a dificuldade de obtenção de testemunhos, o sistema centrava-se, de fato, na confissão. E nos casos em que esta não fosse conseguida espontaneamente, ou ainda, se a confissão não satisfizesse o interrogador (geralmente munido de informações anteriores), então empregava-se a tortura (...) Assaltante de banco, Japonês fora enquadrado, durante o Regime Militar, na Lei de Segurança Nacional que não diferenciava, nesses casos, o preso comum do preso político e funcionava como artifício para não permitir o reconhecimento dos crimes de natureza ideológica. Essa e outras formas de tortura relatadas pelo assaltante foram também estendidas, à época, como se sabe, aos presos e militantes políticos.” Vargas, Joana Domingues. **Em Busca da "Verdade Real": Tortura e Confissão no Brasil Ontem e Hoje.** Sociologia & Antropologia [online]. 2012, v. 2, n. 3 , pp. 237-265. Disponível em: <<https://doi.org/10.1590/2238-38752012v2310>>. ISSN 2238-3875. <https://doi.org/10.1590/2238-38752012v2310>. Acesso em: 8/10/2021

<sup>341</sup>“...en el modelo garantista del proceso acusatorio, informado por la presunción de inocencia, el interrogatorio

objetivo do direito ao silêncio é garantir ao réu o direito a sua palavra ou, se assim preferir, a sua não palavra, a sua objeção em falar, ainda que sua versão seja a única a respeito dos fatos. Se isso acontecer, o processo terá que dispor de outras provas para alcançar a verdade possível, mas garantindo ao réu o seu direito ao silêncio.

O direito a permanecer em silêncio não se confunde com a garantia de não produzir prova contra si. Embora ambos guardem próxima relação e embrionariamente tenham surgido juntos, esta é consequência daquele. A garantia de não se autoinculpar é consectário lógico do direito ao silêncio, surgido como reação crítica ao interrogatório, cujas afirmações de culpa feitas pelo acusado produziam, sob a lâmina do algoz, a principal prova para a condenação - a sua confissão<sup>342</sup>.

Foi com o advento do Iluminismo que surgiram propostas para melhorar a proteção do réu, entre elas a de limites ao poder do soberano sobre a vida, a integridade física e a liberdade dos súditos, que ficavam à mercê de julgamentos arbitrários. Entre os limites apresentados, um de grande relevância para o modelo de processo inquisitorial que se desenvolvia naquela época foi o direito ao silêncio do réu, cuja consequência esperada era a de este não fazer prova contra si mesmo no momento do seu interrogatório<sup>343 344</sup>, ocasião em que era buscada a confissão do réu, considerada a rainha das provas<sup>345</sup>.

---

es el principal medio de defensa y tiene la única función de dar materialmente vida al juicio contradictorio y permitir al imputado refutar la acusación o aducir argumentos para justificarse.” FERRAJOLI, Luigi. **Derecho y Razón**. Madrid: Editorial Trotta, 2000. p. 608.

<sup>342</sup> “A tendência era a busca de provas por meio do acusado ou com a sua cooperação. Nesse contexto, justificou-se o emprego da tortura, como meio de obtenção da confissão do acusado. A verdade, extorquida do acusado, era tida como decisiva para o resultado do processo penal. A confissão era a prova máxima.” QUEIJO, Maria Elizabeth. **O Direito de Não Produzir Prova Contra Si Mesmo**. São Paulo: Saraiva, 2012. p. 31.

<sup>343</sup> “Se alguém for interrogado pelo soberano ou por sua autoridade, relativamente a um crime que cometeu, não é obrigado (a não ser que receba garantia de perdão) a confessá-lo, porque ninguém (conforme mostrei no mesmo capítulo) pode ser obrigado por um pacto a recusar-se a si próprio.” MALMESBURY, Thomas Hobbes de. **Leviatã ou matéria, forma e poder de um estado eclesiástico e civil**. Coleção Os pensadores. vol. XIV. Trad. João Paulo Monteiro e Maria Beatriz Nizza da Silva. São Paulo: Abril cultural, 1974. p.75.

<sup>344</sup> “Direi ainda que é monstruoso e absurdo exigir que um homem seja acusador de si mesmo, e procurar fazer nascer a verdade pelos tormentos, como se essa verdade residisse nos músculos e nas fibras do infeliz!” BECCARIA, Cesare. **Dos Delitos e das Penas**. Tradução Paulo M. Oliveira. Ed. Ediouro: Rio de Janeiro, 1992. p. 48.

<sup>345</sup> “No seio destas alterações ideológicas, com repercussão ao nível do direito penal adjectivo, justifica-se assim o direito ao silêncio, enquanto meio de reacção aos processos inquisitórios que viam a confissão como *regina probationum*, utilizando indiscriminadamente o arguido como instrumento da sua própria condenação.” MENEZES, Sofia Saraiva de. O Direito ao Silêncio: A Verdade por Trás do Mito. In: BELEZA, Tereza Pizarro; PINTO, Frederico de Lacerda Costa. **Prova Criminal e Direito de Defesa**. Coimbra: Almedina, 2013. p. 121.

Esse direito, e a consequência dele esperada, veio a se cristalizar no brocardo latino *nemo tenetur se detegere*<sup>346</sup>, que a partir de então passa a ser utilizado como fórmula que sintetiza de uma só vez tanto o direito ao silêncio quanto o resultado que dele se espera. Desse molde inicial do direito a permanecer em silêncio, o processo penal vai avançando, burilando os instrumentos que permitem o seu exercício, para alcançar as situações que se referem ao direito ao silêncio no atual estágio do Processo Penal. Caracteriza-se pelo não uso de violência, drogas ou manipulação da psique para obtenção das declarações do acusado, além do direito do imputado à assistência de um defensor, fazendo-se presente durante o interrogatório para evitar abusos ou qualquer tipo de violação das garantias processuais<sup>347</sup>.

#### 5.2.1.1 - Garantia da não autoincriminação (*nemo tenetur se detegere*)

O direito de permanecer em silêncio, como mostra a sua origem e evolução, cinge-se especificamente das declarações feitas pelo acusado, sejam elas orais ou escritas, e exige que as declarações digam respeito a fatos que lhe são imputados, que guardem relação com a incriminação que lhe é conferida. O objetivo é assegurar ao imputado que sua condenação não decorrerá das suas declarações, limitando-se, este direito, às declarações, às assertivas referentes ao fato considerado criminoso e a sua autoria.

---

<sup>346</sup> “Outros são também utilizados, tais como: *nemo tenetur se ipsum prodere, nemo tenetur se detegere, nemo tenetur edere contra se, nemo tenetur detegere turpidunem suam, nemo testis se ipsum* ou ainda, simplesmente, *nemo tenetur*”. MENEZES, Sofia Saraiva de. O Direito ao Silêncio: A Verdade por Trás do Mito. In: BELEZA, Tereza Pizarro; PINTO, Frederico de Lacerda Costa. **Prova Criminal e Direito de Defesa**. Coimbra: Almedina, 2013. p. 119.

<sup>347</sup> “*Nemo tenetur se detegere* es la primera máxima del garantismo procesal acusatorio, enunciado por Hobbes y recibida a partir del siglo XVII em el derecho inglés. De ell se siguen, como corolarios, la prohibición de esa ‘tortura espiritual’, como la llamó Pagano, que es el juramento del imputado; el “derecho del silencio”, según palabras de Filangieri, así como la facultad del imputado de faltar con a verdad en sus repostas; la prohibición, por el respeto debido a la persona del imputado y por la inviolabilidad de su conciencia, no sólo de arrancar la confesión con violencia, sino también de obtenerla mediante manipulaciones de la psique, con drogas o con prácticas hipnóticas; la consiguiente negación del papel decisivo de la confesión, tanto por el rechazo de cualquier prueba legal como por el carácter indisponible asociado a las situaciones penales; el derecho del imputado a la asistencia y, en todo caso, a la presencia de su defensor en el interrogatorio para impedir abusos o cualesquiera violaciones de las garantías procesales.” FERRAJOLI, Luigi. **Derecho y Razón**. Madrid: Editorial Trotta, 2000. p. 608.

O direito previsto no art. 61º, 1, d) do CPP<sup>348</sup>, albergado em algumas Constituições como a brasileira<sup>349</sup>, a espanhola<sup>350</sup> e a norte americana<sup>351</sup>, é o direito ao silêncio, sendo sua resultante a garantia da não autoincriminação. Entretanto, hodiernamente, passou-se a tomar o fim pelo motivo, a confundir a resultante do direito pelo próprio direito, alargando seu escopo, dando-lhe roupagem maior que àquela que foi desenhada no molde original.

A borda demarcatória que limita o território do direito ao silêncio e ao privilégio<sup>352</sup> da não autoincriminação que dele decorre não é pacífica, nem na doutrina<sup>353</sup> nem na jurisprudência, mas é possível encontrar em ambas as searas tanto quem os distinga como

<sup>348</sup>“Artigo 61.º Direitos e deveres processuais 1 - O arguido goza, em especial, em qualquer fase do processo e salvas as excepções da lei, dos direitos de: (...) d) Não responder a perguntas feitas, por qualquer entidade, sobre os factos que lhe forem imputados e sobre o conteúdo das declarações que acerca deles prestar;” Disponível em [https://www.pgdlisboa.pt/leis/lei\\_mostra\\_articulado.php?nid=199&tabela=leis&ficha=1&pagina=1&so\\_miolo=&](https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=199&tabela=leis&ficha=1&pagina=1&so_miolo=&). Acesso em: 08/10/2021

<sup>349</sup> “Art. 5º (...) LXIII - o preso será informado de seus direitos, entre os quais o de permanecer calado, sendo-lhe assegurada a assistência da família e de advogado” Disponível em: [http://www.planalto.gov.br/ccivil\\_03/Constituicao/Constituicao.htm](http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm). Acesso em: 20/06/2018.

<sup>350</sup> “Artículo 17, 3. Toda persona detenida debe ser informada de forma inmediata, y de modo que le sea comprensible, de sus derechos y de las razones de su detención, no pudiendo ser obligada a declarar. Se garantiza la asistencia de abogado al detenido en las diligencias policiales y judiciales, en los términos que la ley establezca”. Disponível em: <https://www.tribunalconstitucional.es/es/tribunal/normativa/Normativa/Ceportugués.pdf>. Acesso em: 20/06/2018.

<sup>351</sup> “**Amendment V (1791)** No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offence to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.” Disponível em: [https://www.senate.gov/civics/constitution\\_item/constitution.htm](https://www.senate.gov/civics/constitution_item/constitution.htm). Acesso em: 20/06/2018.

**Em livre tradução:** Emenda V (1791) Nenhuma pessoa será responsabilizada por um crime capital ou de outra forma infame, a menos que seja apresentada ou indiciada por um Grande Júri, exceto em casos decorrentes das forças terrestres ou navais, ou na Milícia, quando em serviço efetivo em tempo de Guerra ou perigo público; nem qualquer pessoa estará sujeita pelo mesmo crime a ser duas vezes colocada em risco de vida ou integridade física; nem será compelido em qualquer processo criminal a ser testemunha contra si mesmo, nem será privado da vida, liberdade ou propriedade, sem o devido processo legal; nem a propriedade privada será tomada para uso público, sem justa indenização.

<sup>352</sup> O termo privilégio é utilizado por MENEZES quando diz: “...parece resultar que o privilégio contra a auto-incriminação e o direito ao silêncio são sinónimos para descrever uma mesma realidade. Como veremos de seguida, tal entendimento mostra-se equivocado”, a meu sentir, com absoluta propriedade. O direito é conquistado, é fruto do processo evolutivo da sociedade, conseguido de maneira custosa para aqueles que o defenderam e lutaram por ele; já o privilégio é a benesse decorrente deste direito, usufruída pelas gerações futuras àquela que lutou para conquistar e fazer valer aquele direito. MENEZES, Sofia Saraiva de. *O Direito ao Silêncio: A Verdade por Trás do Mito*. In: BELEZA, Tereza Pizarro; PINTO, Frederico de Lacerda Costa. **Prova Criminal e Direito de Defesa**. Coimbra: Almedina, 2013. p. 118

<sup>353</sup> ANDRADE, Manuel da Costa. **Sobre as Proibições de Prova em Processo Penal**. Coimbra: Coimbra Editora, 2006; DIAS, Jorge Figueiredo; ANDRADE, Manuel da Costa. **Supervisão, direito ao silêncio e legalidade da prova**. Coimbra: Ed. Almedina, 2006; RAMOS, Vânia Costa. *Corpus Iuris 2000* Imposição ao arguido de entrega de documentos para provas e *nemo tenetur se ipsum accusare* Parte I in Revista do Ministério Público, nº 108; DIAS, Augusto Silva e RAMOS, Vânia Costa **O direito à não auto-inculpação (nemo tenetur se ipsum accusare) no processo penal e contra-ordenacional português**. Coimbra: Coimbra Editora, 2009.

quem os tome um pelo outro, ou ainda quem entenda que ambos integram um *tertium genus*, o princípio do *nemo tenetur*<sup>354</sup>. À partida, é mister observar o uso adequado da terminologia conceitual para enquadrar cada um dos termos aqui empregados. Não se deve confundir direitos com garantias ou com princípios, razão porque está sendo destacado neste trabalho o direito ao silêncio, como o faz a lei.

Impende salientar que a não autoincriminação trata de uma garantia do arguido deduzida do comando legal, sendo que essa garantia está atrelada ao direito ao silêncio que a corporifica, ou seja, a garantia existe na exata medida do direito que ela acompanha<sup>355 356</sup>.

Feita a necessária fixação terminológica e axiológica que pontua o silêncio como direito albergado pelo ordenamento processual penal e acolhido pelos princípios constitucionais do processo equitativo e da ampla defesa, torna-se necessário estabelecer qual o limite do direito ao silêncio: se restrito às declarações do imputado ou se abrange todo e qualquer outro ato que o mesmo venha a praticar e que possa constituir eventual prova contra si.

A discussão tem assim dois polos: um que considera cabível uma interpretação extensiva da garantia, eximindo o arguido do dever de colaboração na atividade probatória; e o que entende que a garantia se limita apenas ao silêncio do acusado, quanto às informações que vier a ser solicitado a prestar, não reconhecendo sua aplicação em relação a provas que dependam da sua colaboração.

---

<sup>354</sup>“Para aferir da extensão do princípio *nemo tenetur* é preciso aferir a extensão das suas componentes (o privilégio contra a auto-incriminação e o direito ao silêncio), sendo que este terá a extensão que suas componentes tiverem.” PINTO, Lara Sofia. Privilégio Contra a Auto-Incriminação Versus Colaboração do Arguido. In: BELEZA, Tereza Pizarro; PINTO, Frederico de Lacerda Costa. **Prova Criminal e Direito de Defesa**. Coimbra: Ed. Almedina, 2013. p. 108. Entendo que o *nemo tenetur* é uma garantia atrelada ao direito ao silêncio, sendo a relação entre eles de acessório e principal. Assim, a garantia do *nemo tenetur* tem seu alcance limitado pela extensão do direito ao silêncio.

<sup>355</sup>“Os direitos representam só por si certos bens, as garantias destinam-se a assegurar condições para a fruição desses bens; os direitos são principais, as garantias são acessórias e, muitas delas adjetivas (ainda que possam ser objeto de um regime constitucional substantivo); os direitos permitem a realização das pessoas e inserem-se direta e imediatamente, por isso, nas respectivas esferas jurídicas, as garantias só nelas se projetam pelo nexo que possuem com os direitos; na acepção jusracionalista inicial, os direitos *declaram-se*, as garantias *estabelecem-se*.” MIRANDA, Jorge. **Manual de Direito Constitucional**. Tomo IV. Coimbra: Coimbra Editora, 2008. p. 113.

<sup>356</sup>“Rigorosamente, as clássicas garantias são também direitos, embora muitas vezes se salientasse nelas o *carácter instrumental* de protecção dos direitos. As garantias traduziam-se quer no direito dos cidadãos a exigir dos poderes públicos a protecção dos seus direitos, que no reconhecimento de meios processuais adequados a essa finalidade” CANOTILHO, José Joaquim Gomes. **Direito Constitucional e Teoria da Constituição**. Coimbra: Ed. Almedina, 2003. p. 396.

Para a primeira corrente, também chamada maximalista, a garantia contra a autoincriminação vai para além do direito ao silêncio na investigação e no interrogatório, abrangendo a proibição de que o acusado seja compelido a auxiliar na recolha de material probatório que possa vir a incriminá-lo.

Ela interpreta a mencionada garantia defendendo a ideia de que o sujeito passivo não pode ser obrigado a participar, prestando qualquer forma mínima de colaboração, de atividade probatória cujo resultado lhe possa ser, eventualmente, prejudicial, seja tal colaboração ativa, como entrega de documentos e recolha de autógrafos, ou passiva, como a sujeição a exames, por exemplo.<sup>357</sup>

A outra interpretação recusa-se a reconhecer que o direito ao silêncio conceda ao sujeito passivo de uma investigação ou de um processo penal o direito de não participar da atividade probatória. Essa corrente reconhece a incidência do *nemo tenetur se detegere* no interrogatório e demais formas de inquirição do acusado, garantindo o direito ao silêncio com todas as implicações derivadas deste, contudo não concorda com a extensão da garantia à possibilidade de recusa do acusado à contribuição na produção de outras provas, tendo por fundamento o disposto no art. 60º do CPP<sup>358</sup>, que estabelece um rol de deveres ao qual o arguido deve sujeição.<sup>359</sup>

A garantia de não produzir prova contra si encontra limite na lida forense diária. É na construção do procedimento penal, no prosseguimento do processo, que vai surgindo a necessidade de estabelecer-se, no caso concreto, o limite de contribuição do arguido para produção da prova. No momento da faina diária, o confronto dessa garantia, com um ou mais princípios que informam o processo, vem à tona e reclama do julgador sua apreciação.

---

<sup>357</sup>“...embora admita a possibilidade de limitar estes direitos, entende que o direito ao silêncio e o direito à não auto-incriminação se estendem a outras formas de cooperação do arguido na produção de prova, passíveis de o incriminar, que não apenas as declarações orais.(...) Daqui decorre que se teria que distinguir a exigibilidade da sujeição passiva a diligências de prova, como é o caso da maior parte dos exames, da inexigibilidade de um comportamento activo do arguido, como as declarações, a entrega de documentos ou a recolha de autógrafos.” MENEZES, Sofia Saraiva de. O Direito ao Silêncio: A Verdade por Trás do Mito. In: BELEZA, Tereza Pizarro; PINTO, Frederico de Lacerda Costa. **Prova Criminal e Direito de Defesa**. Coimbra: Almedina, 2013. p. 134.

<sup>358</sup>“Artigo 60.º Posição processual Desde o momento em que uma pessoa adquirir a qualidade de arguido é-lhe assegurado o exercício de direitos e de deveres processuais, sem prejuízo da aplicação de medidas de coacção e de garantia patrimonial e da efectivação de diligências probatórias, nos termos especificados na lei.” Disponível em [https://www.pgdlisboa.pt/leis/lei\\_mostra\\_articulado.php?nid=199&tabela=leis&ficha=1&pagina=1&so\\_miolo=&](https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=199&tabela=leis&ficha=1&pagina=1&so_miolo=&). Acesso em: 08/10/2021

<sup>359</sup>“Uma extensão minimalista, incidindo apenas sobre as declarações do arguido em sentido estrito (‘prova por declarações’) e sobre os fatos que lhe são imputados.” PINTO, Lara Sofia. Privilégio Contra a Auto-Incriminação Versus Colaboração do Arguido. In: BELEZA, Tereza Pizarro; PINTO, Frederico de Lacerda Costa. **Prova Criminal e Direito de Defesa**. Coimbra: Ed. Almedina, 2013. p. 108.

A garantia do *nemo tenetur* não autoriza ao arguido, por exemplo, impedir a atuação dos órgãos de persecução penal, fornecendo informações falsas, o que importaria em falta de lealdade processual, em clara violação ao princípio do contraditório. Não se deve esperar do Estado, cuja tarefa é garantir o respeito aos princípios do Estado Democrático e de Direito<sup>360</sup>, incluindo o de defender a sociedade e garantir sua segurança, que permita a esdrúxula possibilidade de ter o objetivo de toda a coletividade sacrificado para atender ao interesse de apenas um de seus membros.<sup>361 362</sup>

Após enfrentar a questão do limite do direito ao silêncio, o Supremo Tribunal de Justiça, em recente fixação de jurisprudência uniformizadora, decidiu incorrer em crime de desobediência àquele que descumprir ordem de prestar autógrafos para submissão a exame e perícia<sup>363</sup>. A construção da decisão foi estabelecida em um processo dialético, em que dialogaram a garantia do arguido de não se autoinculpar e o direito do Estado de aplicar a punição, atendendo a expectativa da sociedade de que as leis serão cumpridas<sup>364</sup>.

A decisão do STJ aqui mencionada, seguindo a corrente denominada minimalista, sufraga entendimento que tem prevalecido no âmbito da Suprema Corte dos Estados Unidos da América, no sentido de que a garantia refere-se apenas às manifestações testemunhais do acusado, não abrangendo, assim, outras fontes de prova. A garantia contra a autoincriminação no direito norte-americano não tem extensão ilimitada a todo e qualquer ato que venha a ser produzido pelo réu. Ao contrário, o réu pode ser compelido a andar, fornecer padrão gráfico para identificação da escrita, repetir frases e sons para comparação e identificação, fornecer

<sup>360</sup> Art.9º, b) CRP

<sup>361</sup> “...o direito ao silêncio é apenas o direito que assiste ao arguido de não lhe ser extorquida uma confissão. Ao admitirmos o contrário, estaríamos a favorecer um efeito dominó em relação às provas pessoais cujo resultado seria totalmente fraudulento para o sucesso da investigação criminal: a descoberta da verdade material ficaria assim irremediavelmente comprometida.” MENEZES, Sofia Saraiva de. O Direito ao Silêncio: A Verdade por Trás do Mito. In: BELEZA, Tereza Pizarro; PINTO, Frederico de Lacerda Costa. **Prova Criminal e Direito de Defesa**. Coimbra: Almedina, 2013. p. 134, 135.

<sup>362</sup> “Seria uma irônica e incompreensível contradição que o Estado, no exercício de seu mister de combate ao crime, criasse e aparelhasse órgãos de persecução, para depois reconhecer entraves intransponíveis ao seu trabalho, sem que houvesse, por trás de tais empecilhos, uma justificativa plausível, materializada num verdadeiro direito fundamental a ser defendido.” ALBUQUERQUE, Marcelo Schirmer. **A Garantia de Não Auto-Incriminação Extensão e Limites**. Belo Horizonte: Del Rey, 2008. p. 51.

<sup>363</sup> “Os arguidos que se recusarem à prestação de autógrafos, para posterior exame e perícia, ordenados pelo Exm.º Magistrado do M.º P.º, em sede de inquérito, incorrem na prática de um crime desobediência, previsto e punível pelo artigo 348.º, n.º 1 b), do Código Penal, depois de expressamente advertidos, nesse sentido, por aquela autoridade judiciária.” Acórdão STJ, data 28/05/2014, Processo 171/12.3TAFLG.G1-A.S1, Rel. Armindo Monteiro. Disponível em: [www.dgsi.pt](http://www.dgsi.pt). Acesso em: 08/08/2017.

<sup>364</sup> “...uma interpretação demasiado restritiva teria como consequência contradizer princípios fundamentais, como o do direito do Estado à punição, o seu monopólio da punibilidade e de assegurar a tranquilidade dos cidadãos, a sua expectativa contrafáctica, que, como o direito à liberdade do arguido merece, no seu confronto, ser sopesado e não minorizado.” (Ac. 28/05/2014. p. 32)

peças do vestuário, assim como sangue ou outro material orgânico (sêmen, por exemplo) desde que imprescindíveis à obtenção da prova.<sup>365</sup>

Dispensando dúvidas sobre o tema, a Corte Europeia dos Direitos Humanos estabeleceu que a garantia da não autoincriminação não se estende aos casos em que o acusado pode ser compelido legalmente a cooperar com o processo penal, como é o caso do fornecimento de amostras de sangue, urina e tecidos corporais para efeito de teste de DNA<sup>366</sup>. Analisando a jurisprudência do TEDH se pode concluir que o direito ao silêncio não é absoluto, encontrando limite no confronto com outros interesses juridicamente tutelados<sup>367</sup>.

Além da discussão quanto ao alcance material do direito ao silêncio, outra questão que se levanta diz respeito a validade da confissão de delito feita a agente infiltrado, cuja vontade do confesso está viciada, já que desconhece a qualidade de agente estatal do seu confessor.

Tendo assegurado o direito ao silêncio em interrogatório do acusado, assim como a qualquer questionamento que lhe seja diretamente dirigido, resta resolver a questão das informações prestadas pelo investigado ao informante, algumas delas implicando em confissão da prática do delito, pois tais informações podem tanto ser prestadas espontaneamente como podem ser respostas a questionamentos feitos pelo agente estatal infiltrado.

---

<sup>365</sup> O leading case nesse sentido é o julgado *Holt v. United States*, proferido pela Suprema Corte dos Estados Unidos da América em 1910, no qual o acusado alegou violação à garantia contra a auto-incriminação ao ter sido coagido a experimentar uma blusa, que supostamente pertencia ao autor de um homicídio. Nesse caso, o juiz Holmes decidiu que a proibição da não auto incriminação se limita apenas ao uso de coerção física ou moral para obtenção de declaração, mas não a exclusão do seu corpo como evidência material. MORAES, Carla Dias Caldas de. **A garantia contra a auto-incriminação e a produção de provas no Brasil e nos Estados Unidos** In 2º Curso de Introdução ao Direito Americano, *Fundamentals of US Law Course*, volume 1. Brasília: Advocacia Geral da União, 2012.

<sup>366</sup> “123. However, the privilege against self-incrimination does not extend to the use in criminal proceedings of material which may be obtained from the accused through recourse to compulsory powers but which has an existence independent of the will of the suspect, such as documents acquired pursuant to a warrant, breath, blood and urine samples, and bodily tissue for the purpose of DNA testing (*Saunders v. the United Kingdom*, § 69; *O'Halloran and Francis v. the United Kingdom* [GC], § 47).” EUROPEAN COURT OF HUMAN RIGHTS. **Guide on Article 6 of the European Convention on Human Rights**, 2014, pág. 24. Disponível em: [https://www.echr.coe.int/Documents/Guide\\_Art\\_6\\_criminal\\_ENG.pdf](https://www.echr.coe.int/Documents/Guide_Art_6_criminal_ENG.pdf). Acesso em: 20/09/2018.

**Em livre tradução:** No entanto, o privilégio contra a autoincriminação não se estende ao uso em processos criminais de material que pode ser obtido do acusado por meio do recurso a poderes compulsórios, mas que tem uma existência independente da vontade do suspeito, como documentos adquiridos de acordo com um mandado, amostras de respiração, sangue e urina e tecido corporal para fins de teste de DNA

<sup>367</sup> “... a análise da jurisprudência do TEDH autoriza, pelo menos, a conclusão de que o direito de não contribuir para a sua própria incriminação não é um direito absoluto, mas admite ponderações e restrições no confronto com outros interesses juridicamente tutelados, desde que se garanta a preservação do núcleo essencial daquele direito.” MENDES, Paulo Sousa. **Lições de Direito Processual Penal**. Coimbra: Almedina, 2014. pág. 216

O ponto de inflexão que serve para avaliar se a garantia da não autoincriminação foi violada é a voluntariedade das declarações prestadas pelo acusado. Se a iniciativa de prestar informações ao informante parte do investigado, ainda que em razão da relação de confiança estabelecida entre eles, essas declarações podem integrar o corpo probatório do processo, pois foram obtidas livremente, fruto da vontade livre de prestar informações.

Por outro lado, se as declarações são fruto de coação psicológica, de interrogatório adrede preparado pelo informante, que com habilidade conduz o investigado a prestar as informações que ele pretende obter, trata-se de ardil que prejudica a voluntariedade do acusado, inviabilizando, portanto, a licitude da prova que venha a ser constituída.<sup>368</sup>

Para o CEDH, o marco temporal a partir do qual o acusado pode arguir em seu favor o direito ao silêncio, com a consequente garantia de não autoincriminação, é o momento em que ele é inquirido pela polícia<sup>369</sup>. A partir desse momento, torna-se proibido o uso de qualquer artifício enganoso para obtenção de informações ou confissão do investigado.

Partindo dessa afirmação, aliada à premissa que o interesse público deve ser considerado na avaliação das provas, ainda que obtidas sem o consentimento do investigado, e que apenas estão alijadas do processo aquelas provas conseguidas por intermédio de ardil ou coação psicológica<sup>370</sup>, conclui-se que as declarações obtidas por agente infiltrado, desde que

<sup>368</sup> “Si bien es correcto en esta perspectiva que tampoco la CEDH considera suficiente a cada conversación ‘secreta’ impulsada por el Estado a través de un informante como violación al art. 6 CEDH, sino que exige una infracción que ejerza una ‘presión psicológica’ sobre el acusado – sea por tratarse de una relación cercana existente o por la forma de las preguntas – que ponga en cuestión la libre voluntad con que la información fue brindada.” AMBOS, Kai. **Derecho Procesal Penal Contemporáneo**. San Jose C.R.: Editorial Jurídica Continental, 2011. p. 169, 170.

<sup>369</sup> “121. The right to remain silent applies from the point at which the suspect is questioned by the police (*John Murray v. the United Kingdom*, § 45).” EUROPEAN COURT OF HUMAN RIGHTS. EUROPEAN COURT OF HUMAN RIGHTS. **Guide on Article 6 of the European Convention on Human Rights**, 2014. p. 24.

**Em livre tradução:** O direito de permanecer em silêncio aplica-se a partir do momento em que o suspeito é interrogado pela polícia

<sup>370</sup> “132. Furthermore, the weight of the public interest in the investigation and punishment of the particular offence in issue may be taken into consideration and weighed against the individual’s interest in having the evidence against him gathered lawfully. However, public-interest concerns cannot justify measures which extinguish the very essence of an applicant’s defence rights, including the privilege against self-incrimination (*Jalloh v. Germany* [GC], § 97). The public interest cannot be relied on to justify the use of answers compulsorily obtained in a non-judicial investigation to incriminate the accused during the trial proceedings (*Heaney and McGuinness v. Ireland*, § 57).” EUROPEAN COURT OF HUMAN RIGHTS. **Guide on Article 6 of the European Convention on Human Rights**, 2014. p. 26.

**Em livre tradução:** Além disso, o peso do interesse público na investigação e punição do crime específico em questão, pode ser levado em consideração e pesado contra o interesse do indivíduo em ter as provas contra ele coletadas legalmente. No entanto, preocupações de interesse público não podem justificar medidas que extinguem a própria essência dos direitos de defesa de um requerente, incluindo o privilégio contra a autoincriminação (*Jalloh c. Alemanha* [GC], § 97). Não se pode invocar o interesse público para justificar a utilização de respostas obtidas obrigatoriamente em inquérito extrajudicial para incriminar o arguido durante o processo de julgamento

fornecidas voluntariamente pelo investigado, não são consideradas violação ao princípio do direito ao silêncio nem violação da garantia da não autoincriminação.

### 5.2.2 Direito a Intimidade

O art. 26º, 1 da Constituição da República Portuguesa<sup>371</sup> elenca entre os direitos pessoais a reserva da intimidade da vida privada e familiar, garantindo assim proteção a um espaço onde o indivíduo pode livremente se desenvolver sem receio de ser vigiado ou invadido seja por terceiro, seja pelo Estado.

Ao considerar os limites para que o Estado possa invadir a privacidade do indivíduo, o direito norte americano estabelece disciplina em sua Quarta Emenda Constitucional<sup>372</sup>, sem entretanto estabelecer um limite claro e único, mas adjetiva como possível ser violado aquilo que a sociedade entende como razoável<sup>373</sup>, estando excluído da privacidade aqueles dados que foram conscientemente compartilhados com terceiros<sup>374</sup>. Assim, o objetivo principal da

<sup>371</sup>“Artigo 26.º (Outros direitos pessoais) 1. A todos são reconhecidos os direitos à identidade pessoal, ao desenvolvimento da personalidade, à capacidade civil, à cidadania, ao bom nome e reputação, à imagem, à palavra, à reserva da intimidade da vida privada e familiar e à protecção legal contra quaisquer formas de discriminação.” Disponível em [https://www.pgdlisboa.pt/leis/lei\\_mostra\\_articulado.php?artigo\\_id=4A0026&nid=4&tabela=leis&pagina=1&ficha=1&so\\_miolo=&nversao=#artigo](https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?artigo_id=4A0026&nid=4&tabela=leis&pagina=1&ficha=1&so_miolo=&nversao=#artigo). Acesso em 19/10/21

<sup>372</sup> The Fourth Amendment states: “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”

**Em livre tradução:** O direito das pessoas de estarem pessoalmente seguras em suas casas, papéis e pertences, contra buscas e apreensões não razoáveis, não deve ser violado, e nenhum mandado deve ser emitido, apenas com uma causa provável, apoiado por juramento ou afirmação, e particularmente descrevendo o lugar a ser revistado e as pessoas ou coisas a serem apreendidas. Office of Legal Education, Executive Office for United States Attorneys. **Searching and seizing computers and obtaining electronic evidence in criminal investigations**, 2009. Disponível em <https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf>. Acessado em 06.09.2021. p.1

<sup>373</sup>“Furthermore, the Court has held that a ‘search’ occurs when an expectation of privacy that society is prepared to consider reasonable is infringed.” Jacobsen, 466 U.S. at 113. If the government’s conduct does not violate a person’s “reasonable expectation of privacy,” then formally it does not constitute a Fourth Amendment “search” and no warrant is required.” Office of Legal Education, Executive Office for United States Attorneys. **Searching and seizing computers and obtaining electronic evidence in criminal investigations**. 2009. Disponível em <https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf>. Acessado em 06.09.2021. p.2

**Em livre tradução:** Além disso, a Corte considerou que uma “busca” ocorre quando uma expectativa de privacidade que a sociedade está preparada para considerar razoável é infringida”. Jacobsen, 466 U.S. em 113. Se a conduta do governo não violar a “expectativa razoável de privacidade” de uma pessoa, então formalmente não constitui uma “busca” da Quarta Emenda e nenhum mandado é necessário.

<sup>374</sup>“But the use of big data through predictive software provides the opportunity to rapidly obtain information that could be used on the basis of the following principle: law enforcement officers may access many of these records without violating the Fourth Amendment, on the basis of the theory that there can be no reasonable expectation

Quarta Emenda não é defender a privacidade, mas sim regular a polícia em suas atividades cotidianas<sup>375</sup>, regulando como se deve operar o fluxo de informações entre o indivíduo e o Estado, sendo a privacidade um subproduto dessa regulação, já que possível o estabelecimento de restrições ao acesso de dados pelo governo<sup>376</sup>

O direito processual penal, autorizadamente, opera invadindo por diversas vezes a esfera da intimidade do acusado, apesar do direito constitucional, tendo em vista que mesmo nesse espaço interior podem existir violações a bens ou interesses de terceiros ou à vida social

of privacy in relation to information that we have knowingly revealed to third parties. This issue was addressed in *People v. Harris*. On January 26, 2012, the New York County District Attorney's Office sent a subpoena to Twitter Inc. seeking to obtain the Twitter records of a user suspected of having taken part in the 'Occupy Wall Street' movement. Twitter refused to provide the law enforcement officers with the information requested and sought to quash the subpoena. Rejecting the arguments put forward by Twitter, the Criminal Court of New York upheld the subpoena, stating that tweets are, by definition, public, and that a warrant is not required in order to compel Twitter to disclose them. The District Attorney's Office argued that the "third party disclosure" principle that had been put forward for the first time in *United States v. Miller* applied." MANTELERO, Alessandro; VACIAGO, Giuseppe. **Data protection in a big data society. Ideas for a future regulation.** *In Digital Investigation*, v. 15, p. 104-109, 2015. Disponível em: [https://d1wqtxts1xzle7.cloudfront.net/41265404/Mantelero-Vaciago\\_Big\\_data\\_privacy\\_PREPRINT-with-cover-page-v2.pdf?Expires=1632434885&Signature=E388VvvZ5VsucMEgqxTruobxDcQSW24AjRQ3uw~MqFK2PUMGddV-2kiaWf5CljaS7DM8gH~PxIJfjK6sGbsudpabChlaAjTE3y8WNIQ0MhB6XwSr9VeTZIADFizAA-VbsRKLiwBPG78UTwNd-RaWRvpBcCDIJtLXuX772NDDwAHYa1yT~Q5F3AdftpiXkwdU8Ki5eBAipcuLkfbzOoQMI45uwbKLi~4MDhGz8dvXRhB5QYluSeXl8HHp0kIMWHhtPM6Xfa5zTINMICRSdkqR-dbKsCy4lAshBP67Qp8~RUHE6JqdNNL0Rn-KzPtTg3VAdAxjqDz1QayR0-OjfpnA\\_&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA](https://d1wqtxts1xzle7.cloudfront.net/41265404/Mantelero-Vaciago_Big_data_privacy_PREPRINT-with-cover-page-v2.pdf?Expires=1632434885&Signature=E388VvvZ5VsucMEgqxTruobxDcQSW24AjRQ3uw~MqFK2PUMGddV-2kiaWf5CljaS7DM8gH~PxIJfjK6sGbsudpabChlaAjTE3y8WNIQ0MhB6XwSr9VeTZIADFizAA-VbsRKLiwBPG78UTwNd-RaWRvpBcCDIJtLXuX772NDDwAHYa1yT~Q5F3AdftpiXkwdU8Ki5eBAipcuLkfbzOoQMI45uwbKLi~4MDhGz8dvXRhB5QYluSeXl8HHp0kIMWHhtPM6Xfa5zTINMICRSdkqR-dbKsCy4lAshBP67Qp8~RUHE6JqdNNL0Rn-KzPtTg3VAdAxjqDz1QayR0-OjfpnA_&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA). Acesso em 23/09/2021

**Em livre tradução:** Mas o uso de big data por meio de software preditivo oferece a oportunidade de obter rapidamente informações que poderiam ser usadas com base no seguinte princípio: policiais podem acessar muitos desses registros sem violar a Quarta Emenda, com base na teoria de que não pode haver expectativa razoável de privacidade em relação às informações que revelamos conscientemente a terceiros. Esse problema foi abordado em *People v. Harris*. Em 26 de janeiro de 2012, o Ministério Público do Condado de Nova York enviou uma intimação ao Twitter Inc. buscando obter os registros do Twitter de um usuário suspeito de ter participado do movimento "Ocupe Wall Street". O Twitter se recusou a fornecer aos policiais as informações solicitadas e procurou anular a intimação. Rejeitando os argumentos apresentados pelo Twitter, o Tribunal Criminal de Nova York manteve a intimação, afirmando que os tweets são, por definição, públicos e que um mandado não é necessário para obrigar o Twitter a divulgá-los. O Gabinete do Promotor Público argumentou que o princípio de "divulgação de terceiros" que havia sido apresentado pela primeira vez em *Estados Unidos v. Miller* se aplicava ao caso.

<sup>375</sup>“According to the Supreme Court, “Fourth Amendment doctrine . . . is primarily intended to regulate the police in their day-to-day activities.” The rules set up a regulatory scheme that limits how the government can collect evidence of crime. Although the underlying purpose of the Fourth Amendment is to protect privacy, Fourth Amendment doctrine protects privacy by regulating how the government investigates crime. In developing that regulatory scheme, the Court strives to create readily administrable rules that the police can follow “on the spur (and in the heat) of the moment.” KERR, Orin S. **The Problem of Perspective in Internet Law.** *In Georgetown Law Journal*, Vol. 91, p. 357-405, February 2003, p. 398. Disponível em <https://heinonline.org/HOL/LandingPage?handle=hein.journals/glj91&div=17&id=&page=>, Acesso em 21/09/2021

**Em livre tradução:** De acordo com a Suprema Corte, “A doutrina da Quarta Emenda. . . tem como objetivo principal regular a polícia em suas atividades cotidianas.” As regras sistematizam um esquema regulatório que limita como o governo pode coletar evidências de crime. Embora o propósito subjacente da Quarta Emenda seja proteger a privacidade, a doutrina da Quarta Emenda protege a privacidade ao regulamentar como o governo investiga o crime. Ao desenvolver esse esquema regulatório, a Corte se esforça para criar regras prontamente

que precisam ser apurados e restabelecidos. Assim, pode-se concluir que apesar da previsão constitucional, esse direito não é intangível, sendo algumas vezes mitigado quando assim o exige o interesse social.

Decidir o que integra ou não o direito à intimidade, bem como o seu limite, é tarefa complexa e que se implementa apenas na análise do caso concreto. Ao lidar com esse nível de complexidade, aos poucos foi-se desenvolvendo na jurisprudência alemã<sup>377</sup> a teoria das esferas<sup>378</sup>, que procura distinguir três esferas de proteção ao direito de liberdade, com intensidade de proteção decrescente: a *esfera mais interior*, que trata do âmbito mais interno, íntimo e inviolável, que merece proteção de forma absoluta; a *esfera privada ampliada*, que inclui o âmbito privado que não pertence a esfera mais interior; e a *esfera social* que, por exclusão, abrange tudo aquilo que sequer foi atribuído à esfera privada ampliada.<sup>379</sup>

administráveis que a polícia possa seguir "no estímulo (e no calor) do momento."

<sup>376</sup>“The concept of privacy doesn’t quite capture the purpose of Fourth Amendment rules, it suggests; privacy is best seen as a vital byproduct of Fourth Amendment rules, not its goal. The perspective of computer search and seizure suggests that the deeper role of Fourth Amendment doctrine is regulating the information flow between individuals and the state. In a sense, the digital world of computer data is a particularly pure platform for the Fourth Amendment to operate: it offers an environment of pure data, and considers how the courts can limit and regulate law enforcement access to that data given the practical dynamics of how the data can be retrieved. Privacy results when the rules restrict access or use of that information, but the broader question is how to regulate government access to information. The dynamics of criminal investigations in physical space support one set of answers to this question. The dynamics of investigations involving digital evidence may support another.” KERR, Orin S. **Searches And Seizures In A Digital World** *In Harvard Law Review*, v. 119, p. 531-585, 2005. p. 585. Disponível em [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=697541](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=697541), Acesso em: 21/09/2021

**Em livre tradução:** O conceito de privacidade não captura bem o propósito das regras da Quarta Emenda, apenas sugere; privacidade é melhor visto como um subproduto vital das regras da Quarta Emenda, não seu objetivo. A perspectiva da busca e apreensão em computador sugere que o papel mais profundo da doutrina da Quarta Emenda é regular o fluxo de informações entre os indivíduos e o Estado. Em certo sentido, o mundo de dados digitais do computador é uma plataforma particularmente pura para a Quarta Emenda operar: oferece um ambiente de dados puros, e considera como os tribunais podem limitar e regular o acesso da aplicação da lei a esses dados, dada a dinâmica prática de como os dados podem ser recuperados. A privacidade ocorre quando as regras restringem o acesso ou uso dessa informação, mas a questão mais ampla é como regular o acesso do governo à informação. A dinâmica das investigações criminais em espaço físico apoia um conjunto de respostas a essa pergunta. A dinâmica das investigações envolvendo evidências digitais pode apoiar outro

<sup>377</sup>“ El criterio definitivo desarrollado por el Tribunal Constitucional es la llamada “doctrina de los dos niveles” (BverfGE 34, 238). De acuerdo con esta teoría, existe una diferencia entre “el área nuclear de un estilo personal de vida” y la privacidad de la persona. Cualquier prueba resultante del rango del núcleo esencial de la personalidad debe ser tenida automáticamente como inadmisibile, mientras que en el problema relativo a la admisión de prueba que comprometa el resto del área de la privacidad el tribunal debe ponderar el interés estatal en la persecución penal contra la protección de la individualidad.” ROXIN, Claus. **Pasado, Presente y Futuro del Derecho Procesal Penal**: Buenos Aires, Rubinzal-Culzoni Editores, 2009. p. 104

<sup>378</sup>“A teoria das esferas pode, nos limites de sua correção e utilidade, ser concebida como o resultado de sopesamentos do princípio da liberdade negativa *em conjunto* com outros princípios contra princípios colidentes.” ALEXY, Robert. **Teoria dos Direitos Fundamentais**. Trad. Virgílio Afonso da Silva. São Paulo: Malheiros Editores, 2008. p. 361.

<sup>379</sup>“É possível distinguir três esferas, com intensidades e proteção decrescente: a *esfera mais interior* (“último e inviolável âmbito de liberdade humana”, “âmbito mais interno (íntimo), “esfera íntima inviolável”, “esfera nuclear da configuração da vida privada, protegida de forma absoluta”), a *esfera privada ampliada*, que inclui o âmbito privado que não pertence à esfera mais interior, e a *esfera social*, que inclui tudo aquilo que não for

Como esfera mais interior, entende o Tribunal Constitucional Federal ser aquela em que a expressão dos interesses e direitos do indivíduo não interfere na vida de terceiros nem no âmbito da vida social. A questão colocada é se de fato existe uma tal esfera, em que o comportamento do indivíduo não afete terceiros ou interesses da vida social e, por suposição que essa esfera exista, qual interesse a mesma tem para o direito, pois se não há conflito de direitos, esse nível não interessa a uma teoria jurídica.

Parece, portanto, que a questão deve ser outra, não de uma esfera em que os direitos não entrem em colisão com nenhum outro, mas de um espaço onde, apesar de existir essa colisão, os interesses do indivíduo deverão prevalecer, ou seja, na ponderação dos interesses em conflito, estes terão um peso maior, sem entretanto abolir a necessidade de sopesamento<sup>380</sup>.

A conclusão à qual se chega é que o objeto do direito, a reserva da intimidade da vida privada, coincide com aquele núcleo essencial delimitado pela teoria dos dois níveis, que diz respeito à personalidade do indivíduo, ao seu estilo pessoal e íntimo de viver. A princípio, tal núcleo é intangível e coincide com a esfera mais interior da teoria das esferas, entretanto ainda é possível sopesamento, pois não existe área da vida do indivíduo em que, em algum momento, seu comportamento não possa vir a colidir com interesse de terceiro ou com aspectos da vida social.

Caso tal conflito exista, é preciso ponderar, não havendo que se falar em núcleos ou espaços onde tal não seja cabível, pois é da essência da atividade jurisdicional a incerteza quanto ao resultado do julgado. É a possibilidade de avaliação, de decisão no caso concreto, que traz o direito do teórico para o prático, dando-lhe vida e contornos de acordo com os sentimentos da sociedade naquele momento. Conceitos fluidos e subjetivos como “intimidade”, “vida privada”, “pessoal”, “particular”, serão definidos e redefinidos de acordo com o movimento próprio da sociedade que os reclama.

---

atribuído nm ao menos à esfera privada ampliada.” ALEXY, Robert. **Teoria dos Direitos Fundamentais**. Trad. Virgílio Afonso da Silva. São Paulo: Malheiros Editores, 2008. p. 360 e 361.

<sup>380</sup> Para Alexy determinados conflitos de tão corriqueiros, poderão dar origem a regras extremamente seguras, que decorrem do estabelecimento de relações de precedências, e que protegem a esfera mais interior. O Tribunal pode assim, lançar mão de tais regras para resolução do caso concreto, sem entretanto excluir a possibilidade de sopesamento quando tais regras não forem suficientes para resolução do conflito. “Mas isso nada muda no fato de que existem circunstâncias sob as quais o resultado de sopesamento é tão certo que se pode falar de *regras* extremamente seguras que protegem um esfera mais interior. O Tribunal Constitucional pode aplicar essas regras sem realizar um sopesamento.” ALEXY, Robert. **Teoria dos Direitos Fundamentais**. Trad. Virgílio Afonso da Silva. São Paulo: Malheiros Editores, 2008. p. 362 e nota de rodapé 83.

Assim a mitigação do direito a intimidade é possível, podendo ser incluído no rol dos métodos de prova legalmente autorizados a ação encoberta, mediante o uso de sistema informático, visando a captação de dados telemáticos.

Caberá a autoridade judiciária avaliar, ponderando e sopesando, ou seja, lançando mão das ferramentas já apresentadas pela doutrina, e aqui apresentadas, se a utilização de método que dispõe do direito a intimidade é cabível no caso concreto.

### 5.3 DOS POSTULADOS

A proporcionalidade e a ponderação postulados que são, em virtude de serem chamadas para estabelecer a aplicação de outras normas, mas não por reclamar comportamento a ser observado, serão sob essa ótica aqui analisadas<sup>381</sup>.

#### 5.3.1 Proporcionalidade

A fixação terminológica quanto à classificação da proporcionalidade se faz necessária, tanto para justificar sua disposição topográfica neste texto quanto para esclarecer a partir de qual base teórica a mesma será analisada. Para tanto, será utilizado o balizamento estabelecido entre princípios e regras, como aplicado por Dworkin e aprofundado o estudo por Alexy<sup>382</sup>.

A proporcionalidade tem sido designada como princípio, em contraposição ao conceito de regra, como estabelecido por Alexy. Entretanto, apesar de partir-se da diferenciação estabelecida por aquele autor entre as duas normas – princípio e regra - a categorização de proporcionalidade como princípio não é esposada pelo mesmo.

---

<sup>381</sup>“Além disso, o funcionamento dos postulados difere muito dos princípios e das regras. (...) os postulados, de um lado, não impõem a promoção de um fim, mas, em vez disso, estruturam a aplicação do dever de promover um fim; de outro, não prescrevem indiretamente comportamentos, mas modos de raciocínio e argumentação relativamente a normas que indiretamente prescrevem comportamentos.” ÁVILA, Humberto. **Teoria dos Princípios**: São Paulo, Malheiros Editores Ltda, 2006. p. 123

<sup>382</sup> DWORKIN, Ronald. **Levando os Direitos a Sério**. Trad. Nelson Boeira. 2 ed. São Paulo: Martins Fontes, 2007. ALEXY, Robert. **Teoria dos Direitos Fundamentais**. Trad. Virgílio Afonso da Silva. São Paulo: Malheiros Editores, 2008.

Ao se referir à proporcionalidade, Alexy a denomina como máxima, que se compõe de três máximas parciais, adequação, necessidade e proporcionalidade em sentido estrito. Ele é claro ao afirmar que a proporcionalidade não é um princípio, como empregado em sua obra, e sim uma regra, já que se trata de um enunciado jurídico cuja aplicação se dá por subsunção – e só as regras se aplicam por subsunção.<sup>383</sup>

Outra questão a se observar é que a proporcionalidade, diferentemente dos princípios em geral, não entra em conflito com outros princípios e não é concretizada em graus de intensidade ou em relação de prevalência a outra norma, mas aplicada de forma constante e sem variações. A proporcionalidade apresenta-se para auxiliar a dirimir conflitos entre princípios, mas não como uma norma que entra em colisão com outra. Ela é chamada para orientar como se deve promover um estado de coisas e não para promover um determinado estado de coisas.

Estabelecida a distinção entre princípio e regra, ainda assim a proporcionalidade segue sendo nominada como princípio<sup>384 385</sup>, assim como suas máximas parciais. Faz-se assim para lhe ser dada a importância que merece<sup>386</sup>, sem a preocupação do seu enquadramento na moldura teórica que lhe cabe, apenas para sublinhar a exigência e a necessidade de observação.

A proporcionalidade, pois, não é um princípio, mas uma norma que serve para estruturar a aplicação de um preceito que impõe o dever de promover um estado ideal de

---

<sup>383</sup>“A máxima da proporcionalidade é com frequência denominada ‘princípio da proporcionalidade’. Nesse caso, no entanto, não se trata de um princípio no sentido aqui empregado. A adequação, a necessidade e a proporcionalidade em sentido estrito não são sopesadas contra algo. Não se pode dizer que ela às vezes tenham precedência, e às vezes não. O que se indaga é, na verdade, se as máximas parciais, foram satisfeitas ou não, e sua não-satisfação tem como consequência lógica uma ilegalidade. As três máximas parciais devem ser, portanto, consideradas como regras.” ALEXY, Robert. **Teoria dos Direitos Fundamentais**. Trad. Virgílio Afonso da Silva. São Paulo: Malheiros Editores, 2008. p. 117.

<sup>384</sup>“... a aplicação dos princípios da proporcionalidade, necessidade e adequação, e, em casos extremos, uma ponderação conducente a soluções diferentes das que resultariam da simples aplicação do princípio da concordância prática...” CANOTILHO, José Joaquim Gomes. **Direito Constitucional e Teoria da Constituição**. Coimbra: Ed. Almedina, 2003. p. 1258 e 1297.

<sup>385</sup>“O princípio da proporcionalidade manifesta-se, na Constituição, nos momentos mais difíceis dos direitos fundamentais”, MIRANDA, Jorge. **Manual de Direito Constitucional, Tomo IV**. Coimbra: Coimbra Editora, 2008. p. 279.

<sup>386</sup>“Quando se fala em *princípio da proporcionalidade*, o termo ‘princípio’ pretende conferir a importância devida ao conceito, isto é, à exigência de proporcionalidade. Em vista disso, e em vista da própria plurivocidade do termo ‘princípio’, não há como esperar que tal termo seja usado somente como contraposto a regra jurídica. Não há como querer, por exemplo, que expressões como ‘princípio da anterioridade’ ou ‘princípio da legalidade’ sejam abandonadas, pois, quando se trata de palavras de forte carga semântica, como é o caso do termo ‘princípio’, qualquer tentativa de uniformidade terminológica está fadada ao insucesso.” SILVA, Virgílio Afonso da. **O proporcional e o razoável**. Revista dos Tribunais 798 (2002): 23-50 p.27.

coisas – o princípio. Ela não descreve um determinado comportamento a ser adotado, mas estrutura a aplicação da norma que o faz<sup>387</sup>. Assim, a proporcionalidade se encaixa melhor na conceituação de postulado normativo, ou seja, uma metanorma, ou uma norma em segundo grau, que serve para estabelecer a estrutura de aplicação de outras normas, sejam elas princípios ou regras<sup>388</sup>.

A introdução de um novo método de obtenção de prova no sistema jurídico levanta dúvidas quanto a sua constitucionalidade, pois há um razoável receio que sua admissão acarretará mitigação de direito fundamental, portanto princípio constitucional. A proposta de admissão como método de obtenção de prova do agente infiltrado virtual também gera desconfiança, pois, assim como todos os outros métodos, ele implica em colocar em conflito dois ou mais princípios constitucionais, sendo imprescindível estabelecer como esses conflitos podem ser resolvidos<sup>389</sup>. É dessa tarefa que se ocupam os postulados normativos, como a proporcionalidade<sup>390</sup>.

Embora adotando nomenclaturas diversas (máximas parciais, subprincípios) a doutrina divide a proporcionalidade em três elementos<sup>391 392 393 394 395</sup>, cujo atendimento deve ser

<sup>387</sup> “Com efeito, os princípios são definidos como normas imediatamente finalísticas, isto é, normas que impõem a promoção de um estado ideal de coisas por meio de prescrição indireta de comportamentos cujos efeitos são havidos como necessários àquela promoção. (...) Distintamente, os postulados não descrevem comportamentos, mas estruturam a aplicação de normas que o fazem.” ÁVILA, Humberto. **Teoria dos Princípios**. São Paulo, Malheiros Editores Ltda, 2006. p. 123.

<sup>388</sup> Como já explicado na nota 284. ÁVILA, Humberto. **Teoria dos Princípios**. São Paulo: Malheiros Editores Ltda, 2006. p. 121

<sup>389</sup> “Pese a las consideraciones precedentes, el principio de proporcionalidad se manifiesta como un criterio para establecer los límites a la intervención estatal en la búsqueda de la verdad, equilibrándose los intereses del Estado y los derechos de las personas objeto de la investigación.” PEREIRA, Flávio Cardoso. **El Agente Infiltrado desde el Punto de Vista del Garantismo Procesal Penal**. Curitiba: Juruá Editora, 2016. pág. 418.

<sup>390</sup> Outros postulados, portanto também deveres estruturantes da aplicação de outras normas, são a ponderação, a igualdade, a razoabilidade, a concordância prática, a proibição de excesso. ÁVILA, Humberto. **Teoria dos Princípios**. São Paulo: Malheiros Editores Ltda, 2006. p. 121.

<sup>391</sup> Além de Alexy, que divide a máxima da proporcionalidade em três máximas parciais, como visto anteriormente. ALEXY, Robert. **Teoria dos Direitos Fundamentais**. Trad. Virgílio Afonso da Silva. São Paulo: Malheiros Editores, 2008. p. 117.

<sup>392</sup> “Requisito que, a sua vez, se desglosa em tres elementos: necesidad, idoneidad y proporcionalidad en sentido estricto.” WINTER, Lorena Bachmaier. Investigación criminal y protección de la privacidad en la doctrina del Tribunal Europeo de Derechos Humanos. In: **2º Congresso de Investigação Científica**. Coimbra. Almedina, 2010. p. 172.

<sup>393</sup> “O princípio da proporcionalidade decompõe-se nos três subprincípios da idoneidade ou adequação, da necessidade e da racionalidade ou proporcionalidade *stricto sensu*” MIRANDA, Jorge. **Manual de Direito Constitucional**. Tomo IV. Coimbra: Coimbra Editora, 2008. p. 284/285.

<sup>394</sup> “Exames inerentes à proporcionalidade: Adequação (...) Necessidade (...) Proporcionalidade em sentido estrito” Assim disserta ÁVILA, Humberto. **Teoria dos Princípios**: São Paulo, Malheiros Editores Ltda, 2006. p. 152 a 161.

<sup>395</sup> “Nos tempos mais recentes, tende-se a reforçar a metódica de controlo do princípio da igualdade através da proporcionalidade (em sentido amplo). (...) O controlo metódico da desigualdade de tratamento tera de testar: (1) a legitimidade do fim do tratamento desigualitário; (2) a adequação e necessidade deste tratamento para a

integral para que se possa afirmar a sua completa aplicação. Além disso, é fundamental também que a situação a ser analisada sob a ótica da proporcionalidade, seja submetida a três exames fundamentais, cuja verificação dá-se por meio de questionamentos específicos feitos ao problema, visando permitir o controle dos atos decisórios, reduzindo substancialmente a margem de subjetividade e, por consequência, evitando a arbitrariedade<sup>396</sup>.

Para o chamamento da proporcionalidade, como raciocínio estruturante para resolução da colisão existente entre princípios, é necessário que haja um meio, um fim concreto e uma relação de causalidade entre eles, em torno dos quais se elaboram questões visando verificar a ocorrência dos três elementos que a compõem; a adequação, a necessidade e a proporcionalidade em sentido estrito<sup>397</sup>.

O processo de verificação da aplicação da proporcionalidade inicia indagando se o meio proposto promove o fim esperado, ou seja, se a medida proposta é adequada para atender a um fim legítimo, para o qual se autoriza a restrição de um direito fundamental. O segundo questionamento concentra-se em saber se, dentre os meios disponíveis e igualmente adequados para promover o fim desejado, não há outro meio menos restritivo dos direitos fundamentais afetados, ou seja, se a utilização daquele meio proposto é necessária.

Por fim, indaga-se se as vantagens trazidas pela promoção do fim correspondem às desvantagens provocadas pela adoção do meio, ou seja, se foi aplicada a justa medida, a mínima restrição possível ao direito fundamental para o alcance do fim colimado com a adoção da medida.

Quanto à adequação e à necessidade, pode-se dizer que ambas podem ser verificadas com base em critérios objetivos, que não encontram grandes dificuldades para sua

---

prossecação do fim; (3) a proporcionalidade do tratamento desigual relativamente aos fins obtidos (ou a obter)" Ao discorrer sobre o princípio da proporcionalidade, Canotilho também se refere ao seu controle por meio de teste em três etapas. CANOTILHO, José Joaquim Gomes. **Direito Constitucional e Teoria da Constituição**. Coimbra: Ed. Almedina, 2003. p. 1298.

<sup>396</sup>“Sua aplicação depende de elementos sem os quais não pode ser aplicada. Sem um meio, um fim concreto e uma relação de causalidade entre eles não há aplicabilidade do postulado da proporcionalidade em seu caráter trifásico.” ÁVILA, Humberto. **Teoria dos Princípios**. São Paulo: Malheiros Editores Ltda, 2006. p. 149.

<sup>397</sup>“O postulado da proporcionalidade não se confunde com a idéia de proporção em suas mais variadas manifestações. Ele se aplica apenas em situações em que há uma relação de causalidade entre dois elementos empiricamente discerníveis, um meio e um fim, de tal sorte que se possa proceder ao três exames fundamentais: o da adequação (o meio promove o fim?), o da necessidade (dentre os meio disponíveis e igualmente adequados para promover o fim, não há outro meio menos restritivo do(s) direito(s) fundamentais afetados?) e o da proporcionalidade em sentido estrito (as vantagens trazidas pela promoção do fim correspondem as desvantagens provocadas pela adoção do meio?)” ÁVILA, Humberto. **Teoria dos Princípios**. São Paulo: Malheiros Editores Ltda, 2006. p. 149.

constatação. Assim, trazendo para o objeto deste trabalho, verifica-se que a utilização do agente infiltrado virtual é adequada quando por seu intermédio é possível obter o conteúdo probatório que se deseja, no caso de uma indicação segura da autoria do delito, assim como do *modus operandi* do agente ou, ainda, onde podem ser localizados os instrumentos ou produtos do delito. Configura-se procedimento necessário, por vezes, não havendo outro meio para se obter os elementos de prova para o processo.

Já quanto à proporcionalidade em sentido estrito, não há um dado específico a ser analisado. São as circunstâncias do caso concreto que vão delinear sua aplicação. Esse princípio não pode ser reproduzido indistintamente em outras situações, sem uma análise criteriosa de suas circunstâncias. Assim, é imprescindível observar a gravidade do delito, a intensidade da suspeita, os tipos de indícios, as possibilidades de êxito da medida, o esforço em sua realização e o resultado a ser obtido, além do prejuízo causado em relação à efetividade do resultado<sup>398</sup>.

Enquanto a adequação e a necessidade se referem à resolução de conflitos entre possibilidades fáticas, a proporcionalidade em sentido estrito refere-se à relativização entre duas ou mais possibilidades jurídicas e ao sopesamento entre elas<sup>399</sup>. Observar a proporcionalidade em sentido estrito implica a correta avaliação da providência adotada não apenas em termos qualitativos, mas também quantitativos, de maneira que encontre a justa medida para se alcançar o resultado pretendido.<sup>400 401</sup>

Ante a impossibilidade de resolução da colisão entre princípios com a utilização de critérios apenas objetivos, matemáticos, e tendo por conta a opção estatal pela utilização de método de prova que viola mais sensivelmente o direito fundamental, é importante que seja

<sup>398</sup> WINTER, Lorena Bachmaier. Investigación criminal y protección de la privacidad en la doctrina del Tribunal Europeo de Derechos Humanos. In: 2º Congresso de Investigação Científica. Coimbra: Almedina, 2010. p. 174.

<sup>399</sup> “A máxima da proporcionalidade em sentido estrito decorre do fato de princípios serem mandamentos de otimização em face das possibilidades *jurídicas*. Já as máximas de necessidade e de adequação decorrem da natureza dos princípios como mandamentos de otimização em face de possibilidades *fáticas*.” ALEXYS, Robert. **Teoria dos Direitos Fundamentais**. Trad. Virgílio Afonso da Silva. São Paulo: Malheiros Editores, 2008. p. 118.

<sup>400</sup> “A *racionalidade* ou proporcionalidade *stricto sensu* equivale justa medida. Implica que o órgão proceda a uma correcta avaliação da providência em termos quantitativos (não só qualitativos), de tal jeito que ela não fique além ou aquém do que importa para se alcançar o resultado devido – nem mais, nem menos.” MIRANDA, Jorge. **Manual de Direito Constitucional**. Tomo IV. Coimbra: Coimbra Editora, 2008. p. 285.

<sup>401</sup> No mesmo sentido: “Para além disso, o regime dos meios ocultos terá de obedecer a um princípio de *proporcionalidade em sentido estrito*. Entendendo-se por tal a exigência de que ‘numa ponderação global, a gravidade da intromissão não seja desproporcionada face ao peso das razões que a justificam’.” ANDRADE, Manuel da Costa. **Bruscamente no Verão Passado**. Coimbra: Coimbra Editora, 2009. p. 116.

possível ao cidadão questionar tal decisão, inquirir sobre os critérios que foram utilizados para decidir pela adoção desse método, bem como ter a sua disposição efetivo mecanismo de controle<sup>402</sup> capaz de conter o Estado dentro de balizamento democrático<sup>403</sup>.

Tal controle pode estar previsto, inclusive, no curso do procedimento que decide pela admissão da utilização desse método no caso concreto. O controle pode ser assim feito de maneira difusa, como no caso de comissão parlamentar voltada para a análise da legislação que trata da admissibilidade de métodos ocultos de provas no sistema jurídico penal, como pode ser concentrado, quando específico para a análise da utilização de método oculto em cada caso particularmente.<sup>404</sup>

### 5.3.2 Ponderação

Assim como a proporcionalidade, a ponderação consiste em um método destinado a atribuir pesos diante de uma situação em que mais de uma norma possa ser aplicada ao caso concreto. A subsunção continua sendo a fórmula fundamental para aplicação do direito, em que a premissa maior, a norma, incide sobre a premissa menor, os fatos, e produz como consequência a aplicação do conteúdo da norma ao caso concreto.

---

<sup>402</sup> Ao tratar da questão da utilização de métodos ocultos na investigação criminal, seja pela polícia, seja pelo serviço secreto, Hassemer leciona a necessidade de “excluir que o Estado intervenha concretamente na liberdade individual de cada cidadão, sem que dele deva ser controlado, corrigido ou admoestado por essa intervenção (...) Um controle genérico e global dos serviços, como eventualmente por uma comissão parlamentar não ajuda aos cidadãos contra a sua lesão concreta. Intervenções, sem controle, na liberdade, em casos individuais são proibidas no Estado democrático de Direito.” HASSEMER, Winfried. **Direito Penal Libertário**. Trad. de Regina Greve. Belo Horizonte: Editora Del Rey, 2007. p. 146.

<sup>403</sup> “Además, debe existir un cauce adecuado para que el ciudadano pueda defenderse frente a posibles abusos en la adopción de medidas restrictivas de derechos fundamentales. La existencia de un mecanismo de control que permita mantener las injerencias dentro de los límites de la ‘necesidad en una sociedad democrática’ deriva de la noción de Estado de derecho” WINTER, Lorena Bachmaier. Investigación criminal y protección de la privacidad en la doctrina del Tribunal Europeo de Derechos Humanos. *In: 2º Congreso de Investigación Científica*. Coimbra: Almedina, 2010. p. 172/183.

<sup>404</sup> “Por último, uma exigência de cariz orgânico-procedimental, atinente à entidade competente para decidir sobre a medida ou autorizar a sua realização. Uma competência que – ressalvadas as situações de ‘perigo na demora’ - deve estar sempre reservada ao Juiz (de Instrução)”. Segue o autor citando decisão do Tribunal Constitucional Federal Alemão: “Uma tal reserva permite o controlo preventivo de um almejado meio oculto de investigação por uma instância independente e neutra. Tal controlo pode ser um elemento significativo de uma efectiva protecção dos direitos fundamentais.”. Finaliza exemplificando como possibilidade de controle a ser feito durante a escolha do método oculto de obtenção de prova, a intervenção de advogado nomeado pela Ordem “Que estaria presente junto do juiz da instrução, sindicando a admissibilidade e legalidade da medida em concreto. Estando, naturalmente, também ele, obrigado a guardar sigilo sobre o procedimento e a sua intervenção”. ANDRADE, Manuel da Costa. **Bruscamente no Verão Passado**. Coimbra: Coimbra Editora, 2009. p. 117 e 119.

Em virtude da expansão dos princípios, o sistema jurídico, especialmente os órgãos de decisão, vêm se deparando com casos em que é possível se identificar mais de uma premissa maior (normas) a incidir sobre uma premissa menor (fatos), sendo que o recurso à subsunção não é suficiente para encontrar uma resposta, pois esta opera segundo uma lógica unidirecional (premissa maior – premissa menor), que implica em trabalhar com apenas uma das normas, desprezando as demais.

Para equacionar essa questão, em que mais de um princípio, todos em um mesmo nível de hierarquia, incidindo sobre um caso concreto, torna-se necessário realizar raciocínio diverso, não mais unidirecional, mas multidirecional, capaz de produzir regra concreta que vai reger a hipótese a partir de uma síntese dos distintos elementos normativos refletidos sobre aquele conjunto de fatos.

De alguma forma, cada um desses elementos deverá ser considerado na medida de sua pertinência para o caso concreto<sup>405</sup>, e nisso consiste a ponderação. A ponderação, portanto, é um método, como já explicado anteriormente, que serve para estruturar o raciocínio da aplicação das diversas normas que incidem sobre o caso concreto, podendo ser descrito em três etapas: preparação da ponderação, realização da ponderação e reconstrução da ponderação, não sendo tal classificação unânime na doutrina<sup>406 407</sup>.

Na etapa da preparação devem ser detetadas e analisadas as normas relevantes para a solução do caso, identificando eventuais conflitos entre elas. Para se proceder à ponderação é

---

<sup>405</sup>“A ponderação consiste, portanto, em uma técnica de decisão jurídica aplicável a casos difíceis, em relação aos quais a subsunção se mostrou insuficiente, especialmente quando uma situação concreta dá ensejo à aplicação de normas de mesma hierarquia que indicam soluções diferenciadas. A estrutura interna do raciocínio ponderativo ainda não é bem conhecida, embora esteja sempre associada às noções difusas de balanceamento e sopesamento de interesses, bens, valores ou normas.” BARROSO, Luís Roberto e BARCELLOS, Ana Paula de. **O começo da história. A nova interpretação constitucional e o papel dos princípios no direito brasileiro**, [http://xa.yimg.com/kq/groups/22830878/36505266/name/texto\\_principios\\_constitucionais\\_barroso.pdf](http://xa.yimg.com/kq/groups/22830878/36505266/name/texto_principios_constitucionais_barroso.pdf). Acesso em: 18/03/2013. p. 17 e 18

<sup>406</sup>“A primeira delas é a da *preparação da ponderação (Abwägungsvorbereitung)*. Nessa fase devem ser analisados todos os elementos e argumentos, o mais exaustivamente possível. (...) A segunda etapa é a da *realização da ponderação (Abwägung)*, em que se vai fundamentar relação estabelecida entre os elementos objeto de sopesamento. (...) A terceira etapa é a da *reconstrução da ponderação (Rekonstruktion der Abwägung)*, mediante a formulação de regras de relação, inclusive de primazia entre os elementos objeto de sopesamento, com pretensão de validade para além do caso.” ÁVILA, Humberto. **Teoria dos Princípios**: São Paulo, Malheiros Editores Ltda, 2006, pág. 132

<sup>407</sup>“Na *primeira* etapa, cabe ao intérprete detectar no sistema as normas relevantes para a solução do caso, identificando eventuais conflitos entre elas. (...) Na *segunda* etapa, cabe examinar os fatos, as circunstâncias concretas do caso e sua interação com os elementos normativos. (...) É na terceira etapa que a ponderação irá singularizar-se, em oposição à subsunção.” BARROSO, Luís Roberto e BARCELLOS, Ana Paula de. **O começo da história. A nova interpretação constitucional e o papel dos princípios no direito brasileiro**, [http://xa.yimg.com/kq/groups/22830878/36505266/name/texto\\_principios\\_constitucionais\\_barroso.pdf](http://xa.yimg.com/kq/groups/22830878/36505266/name/texto_principios_constitucionais_barroso.pdf). Acesso em: 18/03/2013. p. 18 e 19

necessário que sejam citados os princípios em conflito e o que está sendo objeto de sopesamento, agrupando aqueles que indicam soluções semelhantes. Isso facilita o trabalho subsequente de comparação entre os elementos normativos em questão, assim como o exame dos fatos e sua implicação com os elementos normativos antes agrupados.

Na realização da ponderação, são analisados os diferentes grupos de princípios implicados na resolução do caso concreto, de modo a apurar os pesos que serão atribuídos aos diversos elementos em análise com a consequente escolha do grupo de princípios que deverá prevalecer. Em seguida, deve ser decidido qual o grau de intensidade que cada um desses grupos terá em relação aos demais, ou seja, qual a relação de primazia entre um princípio e outro. A reconstrução da ponderação consiste numa formulação de regras de relação, com a pretensão de validade para além do caso concreto.

A ponderação, embora preveja a atribuição de pesos diversos aos vários fatores envolvidos, não oferece critérios materiais ou axiológicos em relação à valoração a ser feita, pois figura como técnica desprovida de características valorativas.

Trazendo a reflexão sobre a ponderação para o caso específico do agente encoberto virtual, o Estado se vale do engano para investigar ou prevenir a prática de delito praticado por criminalidade organizada. A utilização de *malware* para identificação da rede criminoso ou para obter as provas necessárias da sua prática, se dá por meio de inoculação subreptícia, sem autorização nem conhecimento do investigado. Entretanto, na ponderação entre o direito violado do investigado e o bem a ser alcançado, que beneficia toda sociedade, o resultado é pela autorização da utilização dessa possibilidade de obtenção de prova<sup>408</sup>.

---

<sup>408</sup>“La justificación del engaño usado por el agente encubierto radica en una cuestión de política criminal, que llega a justificar las consecuencias desvaliosas que su utilización implica. La solución viene dada por una ponderación de valores, en el que se acaba por dar preponderancia al valor “eficacia”, en el sentido que si se quiere luchar eficazmente contra este delito tan oculto, la mejor manera y la opción idónea es infiltrar a la persona de esta manera para llegar a una situación más favorable para la sociedad. Estamos eligiendo así una solución que reporta más seguridad y bienestar al conjunto de la sociedad y que logra la justicia, objetivo capital en un Estado de Derecho. Sin embargo, debemos matizar que no puede existir un engaño a cualquier precio, por lo que se deben tener siempre presentes los principios de necesidad y proporcionalidad, siempre respetando los principios y las garantías procesales y los Derechos Fundamentales de cualquier persona, incluso los de los presuntos autores.” MATA, Federico Bueno de. **El Agente Encubierto En Internet: Mentiras Virtuales Para Alcanzar La Justicia**. 2012. Disponível em [https://ruc.udc.es/dspace/bitstream/handle/2183/9179/comunicacions\\_01\\_Bueno\\_de\\_Mata\\_295-306.pdf](https://ruc.udc.es/dspace/bitstream/handle/2183/9179/comunicacions_01_Bueno_de_Mata_295-306.pdf). Acesso em 05/10/2021

A utilização da ponderação e da proporcionalidade se fazem imprescindíveis quando necessária intervenção em certo direito fundamental, visando proteger outro direito de igual importância, naquele caso considerado de maior valor<sup>409</sup>.

Essa decisão afeta não apenas as partes de determinado processo penal, pois dentre os fatores a serem sopesados para definir qual o bem de maior valor, constam também as diretrizes de política criminal adotadas pelo Estado, portanto de interesse de toda sociedade, já que impactam diretamente naquilo que ela considera como importante medida de segurança pública

---

<sup>409</sup>“O bem jurídico, de grande valor e ameaçado, é protegido às custas de um bem de valor inferior (...) Evidentemente, ninguém discute que intervenções em um direito fundamental devem ocorrer proporcionalmente. A única pergunta interessante é sobre a maneira como se pretende assegurar a validade do princípio da proporcionalidade” HASSEMER, Winfried. **Direito Penal Libertário**: Belo Horizonte. Editora Del Rey, 2007. p. 136

## 6. O DIREITO À SEGURANÇA PÚBLICA NO ESTADO DEMOCRÁTICO DE DIREITO

*A interdependência humana é hoje tão flagrante que só faz mesmo sentido falar de paz mundial. (...) Ela pode ser vista como uma simples ausência de guerra ou como um estado de tranquilidade baseado em uma profunda sensação de segurança, oriunda da compreensão mútua, da tolerância pelos pontos de vista dos outros e do respeito por seus direitos.<sup>410</sup>*

A garantia da liberdade em um Estado Democrático de Direito é assegurada pelos limites impostos pelo Estado através de ordenamentos legais que ajustam as condutas dos seus integrantes. Na ausência de limites, vigora a lei do mais forte, onde a atuação do indivíduo é determinada pela necessidade de sobrevivência e seu sucesso condicionado a sorte. Nesse estágio, não há que se falar em liberdade, pois apenas a vontade do mais forte é satisfeita, não havendo espaço para vontades ou necessidades que com ela conflitem. O espaço da liberdade corresponde portanto, a resultante entre o exercício da vontade pessoal e o limite da vontade geral.<sup>411</sup>

A liberdade individual se não devidamente limitada, se apresenta como fonte de conflitos tanto entre os indivíduos, como entre os indivíduos e as instituições públicas, sendo necessário que o Estado organize o ordenamento jurídico de maneira a assegurar que as liberdades possam ser exercidas em ambiente de convivência segura a todos.

Assim, é possível concluir que cabe ao Estado a permanente administração da segurança, sendo esta sua principal razão de ser, seja essa segurança externa ou interna. Para tanto lhe cabe impor limites a liberdade individual, estando tais limites consubstanciados em leis, que por sua vez são formuladas e aprovadas por Parlamentos eleitos pelo voto popular. Assim, os limites a liberdade, em última análise, são impostos pelos próprios integrantes da

<sup>410</sup>Sua Santidade, o Dalai Lama: **Uma Ética para o Novo Milênio**. Trad. Maria Luiza Newlands. Rio de Janeiro: Sextante, 2000. p. 219.

<sup>411</sup>“En el reino de la naturaleza no existe la libertad. Existe el azar y la necesidad, pero no la libertad. La libertad no existe nada más que en las sociedades humanas y existe porque nos ponemos límites a nosotros mismos estableciendo normas a las que tenemos que ajustar nuestra conducta.”ROYO, Javier Pérez. **La Democracia Frente al Terrorismo Global**. In ROYO, Javier Pérez e DURÁN, Manuel Carrasco. **Terrorismo, democracia y seguridad, en perspectiva constitucional**. Madrid: Marcial Pons, 2010. p. 8

comunidade.<sup>412</sup>

Falar em segurança encaminha necessariamente para a discussão do tema da criminalidade organizada, fenómeno que constantemente desafia o Estado a garantir a segurança da sociedade. A reação a este fenómeno pode provir das normas que integram o Código Penal e o Código Processual Penal<sup>413</sup>, por essa razão, é possível se pensar em medidas legais que ataquem diretamente a causa que põe em risco a segurança da sociedade. Apesar disso, não se pode olvidar que a causa da insegurança não é única, e que a elaboração de leis e incorporação de novos métodos de investigação e prova, integram apenas uma das diversas áreas que necessitam da atuação do Estado no seu mister de garantir a segurança.

A criminalidade, seja ela de massa ou organizada, e a sensação de insegurança que ela traz, tem motivações que não serão resolvidas apenas com utilização de novos métodos de obtenção de prova, por mais sofisticados que sejam. Suas raízes são mais profundas, e limitar a discussão a esse patamar é garantia de frustração de uma sociedade que busca a resposta para derrotar a criminalidade com o endurecimento do Direito Penal e Processual Penal<sup>414</sup>.

Abordar o fenómeno da criminalidade organizada, ainda que sob o enfoque investigativo e processual, exige observar o que está ao redor, pois esse problema social é sintoma das modificações pelas quais passa a sociedade, refletindo-se na organização política e jurídica do Estado. Em igual sentido, o estudo feito neste trabalho envolve a discussão sobre o crime organizado, as questões práticas referentes a sua investigação, ao respeito de garantias processuais penais e constitucionais, e reclama uma síntese que não está contida apenas no ordenamento penal<sup>415</sup>.

<sup>412</sup>“El Estado es un suministrador permanente de seguridad. Ésta es su razón de ser. Y la única forma que tiene de hacerlo es poniéndonos límites. Límites que nos poneos nosotros mismos, ya que se establecen por ley aprobada por Parlamentos democráticamente elegidos. Justamente por eso, dichos límites son los elementos constitutivos de nuestra libertad. Podemos ser libres porque nos sentimos seguros. Y nos sentimos seguros porque hay un ordenamiento jurídico que ordena la convivencia.” ROYO, Javier Pérez. **La Democracia Frente al Terrorismo Global**. In ROYO, Javier Pérez e DURÁN, Manuel Carrasco. **Terrorismo, democracia y seguridad, en perspectiva constitucional**. Madrid: Marcial Pons, 2010. p. 9

<sup>413</sup>“En realidad, desde esta perspectiva, la reacción al fenómeno terrorista proviene, predominantemente, de las normas que regulan el Código Penal y el proceso criminal.” DURÁN, Manuel Carrasco. **Medidas Antiterroristas y Constitución, tras el 11 de Septiembre de 2001**. In ROYO, Javier Pérez e DURÁN, Manuel Carrasco. **Terrorismo, democracia y seguridad, en perspectiva constitucional**. Madrid: Marcial Pons, 2010. p. 15

<sup>414</sup>“O fracasso da prevenção criminal e da investigação criminal não pode ter como substituto um Processo Penal inquisitorial e uma instrumentalização do conceito de crime numa sociedade.” PALMA, Maria Fernanda. **O Problema Penal do Processo Penal** In PALMA, Maria Fernanda. **Jornadas de direito processual penal e direitos fundamentais**. Coimbra: Almedina, 2004 p. 53

<sup>415</sup>“A função anticriminal do Processo Penal é, na verdade diminuta como, a esse nível, o é a própria solução penal. Veja-se o problema insolúvel do tráfico de estupefacientes e da criminalidade organizada nessa área. A intervenção do Estado deve situar-se a montante do processo, nos mecanismos sociais de mercado que tornam

É o espaço da política de segurança pública que comporta todas as matérias aqui envolvidas, abrangendo desde o ordenamento penal e processual penal, bem como suas intercessões constitucionais, até política criminal e policial, sem descuidar de questões sociais mais amplas como a proteção da juventude, o acesso à educação, saúde, trabalho e geração de renda<sup>416</sup>.

Três variáveis estão umbilicalmente ligadas e relacionadas com a questão da criminalidade organizada, importante vetor de geração de medo e insegurança na sociedade, e que serão analisadas a seguir: a sensação de insegurança proveniente da sociedade de risco, segurança pública como dever do Estado e a relação destas com o direito penal.

## 6.1 SOCIEDADE DE RISCO

Desde meados do século passado, presencia-se uma modificação da percepção da sociedade em relação ao Estado, bem como da imbricação entre ambos. A sociedade passa a operar com um novo código de identificação. Antes marcada pela vigência de uma sociedade de classes<sup>417</sup>, funcionando em uma lógica de divisão interna em virtude da categorização económica dos seus integrantes, agora não é mais o critério económico a definir a feição da sociedade, mas sim a capacidade de gerar e administrar riscos<sup>418</sup>.

A sociedade passa a centrar-se na maior ou menor capacidade de controlar os riscos. Assim, como providência adota a identificação e a catalogação de dois tipos: o risco externo e

---

possível a economia da droga ou nas condições sociais desesperantes que fazem de tantas pessoas recrutas desse exército de inimigos da sociedade. A nós, juristas penais, não nos cabe pensar o Processo Penal como puro instrumento de combate à criminalidade, mas aprender a analisar os modos sociais de controlar os problemas da criminalidade, com os meios de um estudo interdisciplinar e através de uma política social global.” PALMA, Maria Fernanda. **O Problema Penal do Processo Penal** In PALMA, Maria Fernanda. **Jornadas de direito processual penal e direitos fundamentais**. Coimbra: Almedina, 2004 p. 53

<sup>416</sup>“... uma política de segurança pública sem consideração pela juventude, o trabalho, a habitação, os problemas sociais e a educação, converte-se num espetáculo sem esperanças e sem fim previsível.” HASSEMER, Winfried. **A Segurança Pública no Estado de Direito**. Lisboa: Associação Académica da Faculdade de Direito de Lisboa, 1995. p. 109-110.

<sup>417</sup>“ A força impulsionadora da sociedade de classes se resume na frase: “*Tenho fome!*”, enquanto, pelo contrário, o movimento que se põe em marcha com a sociedade de risco se expressa na frase “Tenho medo!””FABRETTI, Humberto Barrionuevo. **Segurança Pública. Fundamentos Jurídicos para uma abordagem Constitucional**. São Paulo: Editora Atlas, 2014. p.26

<sup>418</sup>“Hoy nos encontramos a las puertas de un cambio transcendental en nuestra comprensión de la sociedad, la cual ha evolucionado, sin darnos cuenta, de una sociedad de clases a una sociedad de “riesgos”. SÁNCHEZ, Alfredo Chirino. **La Seguridad como un topos discursivo en la política criminal centroamericana. Perspectivas de una desesperanza**. In: ALFARO, Luis Reyna; TERÁN, Sergio Cuaresma. **Derecho Penal y Estado de Derecho**: Buenos Aires: Editorial B de f, 2008. p. 17-18.

o risco fabricado. O risco externo é o risco do ambiente que pode advir dos costumes ou da natureza, portanto previsíveis, quantificáveis e controláveis, dentro de certa margem. Já o risco fabricado é o que advém do impacto da atividade humana sobre o meio ambiente, portanto sem registo histórico, ainda não quantificável, cujos efeitos não são previsíveis.<sup>419</sup>

Quanto ao primeiro, são desenvolvidos mecanismos de controle e redução de danos, cujas restrições são previamente comunicadas, impostas como consequência à sociedade, portanto consensualmente aceitas ou, ao menos, toleradas. Em relação ao risco fabricado, o Estado, como responsável pelo bem-estar da sociedade (*Welfare State*), já não pode garantir quais as restrições que lhe serão impostas, pois não consegue avaliar os riscos nem suas consequências, podendo ser acusado tanto de alarmista, caso exagere na notícia do fato, quanto de acobertamento, se calcular mal suas consequências.<sup>420</sup>

É desta capacidade humana de gerar riscos e destruição ao ambiente que o cerca - o risco fabricado - e de como essa capacidade de gerar riscos ao ambiente influencia todos sistemas sociais<sup>421</sup>, que passa a fluir o discurso corrente, reproduzido e massificado pela imprensa, assentando de forma sensacionalista a urgência da segurança nas consciências da coletividade, e que esta deve ser proporcionada pelo Estado.

Não que os riscos atuais sejam maiores que os de época anteriores, autorizando por essa razão leis mais duras e invasivas, mas, como também em outras épocas da história<sup>422</sup>, tem

---

<sup>419</sup>“Propõe, assim, a suposição de que o risco seria uma maneira de regular o futuro, de normatizá-lo e de submetê-lo ao nosso domínio. No sentido de explicar essa situação, distingue dois tipos de risco: o risco externo e o risco fabricado. Assim, à medida que o risco fabricado se expande, passa a haver algo de mais arriscado no risco, pois o risco tradicional pode ser calculado de forma atuarial (acidentes automobilísticos, por exemplo), enquanto o risco fabricado não (Não há como calcular os efeitos, a longo prazo, de uma intoxicação nuclear como a que ocorreu em Chernobyl, por exemplo).” FABRETTI, Humberto Barrionuevo. **Segurança Pública. Fundamentos Jurídicos para uma abordagem Constitucional**. São Paulo: Editora Atlas, 2014. p. 27-28.

<sup>420</sup>“Esse tipo de paradoxo torna-se rotina na sociedade contemporânea e não há uma maneira fácil de lidar com ela, principalmente em relação aos riscos fabricados, pois na maioria dessas situações a própria existência do risco é posta em dúvida. Surge, assim, uma grande dúvida em relação aos comportamentos que se devem tomar em relação aos riscos fabricados, pois não se sabe exatamente se existem e, em caso positivo, qual a sua extensão.” FABRETTI, Humberto Barrionuevo. **Segurança Pública. Fundamentos Jurídicos para uma abordagem Constitucional**. São Paulo: Editora Atlas, 2014. p. 28.

<sup>421</sup>“La consecuencia central es que en la modernidad avanzada la sociedad con todos sus sistemas parciales (economía, política, familia, cultura) ya no se puede comprender de una manera “autónoma” respecto de la naturaleza. Los problemas del medio ambiente *no* son problemas del entorno, sino (en su génesis y en sus consecuencias) problemas *sociales*, problemas del ser humano, de su historia, de sus condiciones de vida, de su referencia al mundo y a la realidad, de su ordenamiento económico, cultural y político. (...) A finales del siglo XX hay que decir que la naturaleza *es* sociedad, que la sociedad es (también) *naturaleza*. Quien hoy sigue hablando de la naturaleza como no sociedad habla con las categorías de otro siglo, las cuales ya no captan nuestra realidad.” BECK, Ulrich. **La sociedad del riesgo**. Barcelona: Paidós, 1998. p. 90.

<sup>422</sup>Vale trazer aqui a oportuna reflexão feita por Tiedemann ao discorrer sobre a evolução do uso da tortura no processo penal moderno até sua abolição e o paralelo com o atual recrudescimento da legislação processual penal: “A tortura, instrumento já conhecido: na antiguidade para se obter *confissões*, (...) existia também – o

se apresentado de forma reduzida o equilíbrio entre os riscos e a capacidade de controlá-los, incluída aqui a variável globalização, que removeu as fronteiras também para controle de danos, seja para a disseminação de uma doença ou para venda internacional de drogas, por exemplo.

A sociedade, inundada pelos meios de comunicação com exaustivas notícias que se esforçam em realçar fatos criminosos em cores vibrantes e assustadoras, infundindo a percepção que se vive em uma época com alto grau de insegurança, produzindo convicções a respeito dos riscos que nem sempre correspondem ao grau real de insegurança<sup>423</sup>.

São mais temores subjetivos e dissociados da realidade do que uma ameaça concreta, resultado do discurso dominante que destaca a necessidade de segurança, que é marcado por duas características: por um lado, os riscos devem se realizar e os efeitos são devastadores quando eles se concretizam; por outro lado, esse discurso de segurança convence as pessoas de que os riscos são intransponíveis, que contra eles não há nada a se opor, gerando um sentimento de “desorientação destrutiva”<sup>424</sup>, uma premente necessidade de defesa contra os riscos e perigos supostamente existentes, sendo urgente controlar essas ameaças. Sabe-se que são passíveis de controle, entretanto pouco prováveis de serem de fato afastadas da sociedade, e sobretudo do inconsciente coletivo.

---

que, à primeira vista é surpreendente – no início do processo penal moderno. (...) Naquela época, na guerra contra as “pessoas nocivas ao país” (bandos de ladrões que devastavam o país), admitiram-se todos os instrumentos processuais que pareciam apropriados ao combate dessa criminalidade. Esse procedimento foi acolhido mais tarde no processo penal geral para além da persecução penal específica de “pessoas nocivas ao país”. O paralelismo dessa evolução em relação ao atual problema do processo penal contra supostos terroristas é evidente. Sob esse aspecto também o legislador encontrava-se diante da alternativa de criar regras processuais especiais contra supostos terroristas ou então exarcebar as regras processuais penais gerais, aplicáveis a qualquer acusado. Na República Federal da Alemanha, o legislador escolheu essencialmente o segundo caminho, limitando de modo geral, os direitos de defesa do acusado. Naturalmente, pode-se questionar se esse caminho de evitar leis excepcionais contra terroristas foi razoável. Um outro exemplo para essa problemática é fornecido pela legislação contra o crime organizado (investigação criminal sistemática, investigadores infiltrados, etc.)” TIEDEMANN, Klaus. *In*: ROXIN, Claus; ARTZ, Gunther; TIEDEMANN, Klaus. **Introdução ao Direito Penal e ao Direito Processual Penal**. Belo Horizonte: Del Rey, 2007. p. 150.

<sup>423</sup>“As sociedades ocidentais, têm sido quotidianamente fustigadas por um discurso de hipervalorização de determinados tipos de criminalidade e das supostas ameaças e perigos neles contidos. Uma narrativa ampliada e repetida *ad nauseam*, por alguns órgãos de comunicação social, indutora de elevados níveis de medo e insegurança subjetiva, que não encontram a mínima concordância com a realidade do quotidiano, na generalidade dos países, entre os quais Portugal.” BRAZ, José. **Ciência, tecnologia e Investigação Criminal**. Coimbra: Editora Almedina, 2015. p. 426.

<sup>424</sup>“El resultado de todo ello es una desorientación destructiva, una creciente pero ciega actitud de defensa en contra los disturbios y el peligro, y una urgente necesidad de controlar por lo menos aquellas situaciones problemáticas que aún sean controlables o de las que aún se cree que podrían ser controladas.” HASSEMER, Winfried. *El Derecho Penal del Estado de Derecho en los Tiempos de Terrorismo*. *In*: ALFARO, Luis Reyna; TERÁN, Sergio Cuaresma. **Derecho Penal y Estado de Derecho**: Buenos Aires. Editorial B de f, 2008. p. 190.

## 6.2 SEGURANÇA CIDADÃ

A sensação de medo e insegurança da sociedade impõe ao Estado novo conteúdo ao dever de segurança. Enquanto o dever de segurança historicamente imputado ao Estado era a promoção da segurança externa, exercido na relação Estado-Estado, agora o foco do dever de segurança concentra-se na segurança interna, para os riscos provenientes do próprio sistema social. A exigência deixa de ser exclusivamente defender o Estado de possíveis ataques de outro Estado-Nação, para incluir a defesa também dos riscos internos, muitas vezes, causados pelo próprio Estado ou por suas instituições.<sup>425</sup>

Com o fim da Guerra Fria, os riscos de ataques globais promovidos por uma guerra entre duas ou mais superpotências são minimizados, no entanto surgem os ataques internos à própria sobrevivência e manutenção da organização estatal, fruto da instabilidade pela qual atravessa o Estado em busca de uma nova delimitação de limites de atuação.

As alterações nas relações sociais, antes definidas por classes claramente diferenciadas; o encurtamento das distâncias que permitiu maior mobilidade migratória e, conseqüentemente, menor identificação nacional pelos critérios até então estabelecidos, tais como raça, língua e religião; a relativização das fronteiras, não havendo limites para o comércio e o intercâmbio de mercadorias, sejam elas lícitas ou não. Esses fatores, aliados à incrível velocidade na troca de informações, fragilizaram o conceito de Estado, como até então é reconhecido, sendo posta em dúvida sua capacidade de manter a ordem e a segurança internas.

Isso porque a ordem e a segurança são frágeis, pois em constante comunicação com o ambiente externo. A menor alteração no fluxo migratório, o aparecimento de uma doença

---

<sup>425</sup>“For too long, the concept of security has been shaped by the potential for conflict between states. For too long, security has been equated with the threats to a country's borders. For too long, nations have sought arms to protect their security. For most people today, a feeling of insecurity arises more from worries about daily life than from the dread of a cataclysmic world event. Job security, income security, health security, environmental security, security from crime-these are the emerging concerns of human security all over the world.” UNITED NATION DEVELOPMENT PROGRAMME (UNDP). **Human Development Report 1994**. Nova York: Oxford University Press, 1994. p. 3. Disponível: [http://hdr.undp.org/sites/default/files/reports/255/hdr\\_1994\\_en\\_complete\\_nostats.pdf](http://hdr.undp.org/sites/default/files/reports/255/hdr_1994_en_complete_nostats.pdf). Acesso em: 08/08/2018.

**Em livre tradução:** Por muito tempo, o conceito de segurança foi moldado pelo potencial de conflito entre os Estados. Por muito tempo, a segurança foi equiparada às ameaças às fronteiras de um país. Por muito tempo, as nações buscaram armas para proteger sua segurança. Para a maioria das pessoas hoje, um sentimento de insegurança surge mais das preocupações com a vida cotidiana do que do medo de um evento mundial cataclísmico. Segurança no emprego, segurança na renda, segurança na saúde, segurança ambiental, proteção contra o crime - essas são as preocupações emergentes da segurança humana em todo o mundo.

grave e contagiosa, o surgimento de uma nova empresa criminosa, por exemplo, alteram toda a dinâmica mundial, sem restringirem-se apenas ao Estado diretamente afetado.

A ideia de Estado provedor e assegurador das relações internas da sociedade está em mudança, sendo de relevante importância que ele demonstre sua capacidade de estabilizar a expectativa da sociedade por segurança e paz, e esteja ciente do desafio de que tais valores não dependem apenas da sua política interna, devendo estar aberto ao diálogo e à cooperação com a comunidade internacional, pois sem o equilíbrio da paz entre as nações não lhe será possível garantir a paz e a segurança internas.

Aliada à questão de segurança externa, de possível conflito entre partes, é preciso observar os riscos internos inerentes à própria dinâmica da sociedade. A dificuldade de acesso a atendimento médico e hospitalar, o desemprego e a falta de habitação digna passam a ser riscos muito mais graves e seriamente considerados que a possibilidade de uma guerra ou um evento natural de efeitos globais.

A segurança que se espera do Estado começa a ser cobrada para o bem-estar do indivíduo e não aquela direcionada para a paz entre os Estados, pois a insegurança causada pela possibilidade de uma guerra é infinitamente menor do que o justo receio de ser demitido da empresa ou de ser assaltado na rua. A paz que se deseja é a paz interna, a tranquilidade de ter suas necessidades básicas atendidas, o que levará, por consequência, à redução dos índices de criminalidade urbana, causada mais pela falta de atendimento a necessidades básicas da grande parcela da população do que pelas grandes empresas criminosas.

Essa gradual mudança da percepção de segurança pela sociedade e, por consequência, o crescimento da sua importância para o Estado de Direito, dá início, especialmente a partir da década de 1990, a uma nova delimitação sobre o dever de segurança imposto ao Estado para com a sociedade. O Relatório sobre Desenvolvimento Humano de 1994 da ONU é paradigmático nessa sequência histórica, pois pela primeira vez um documento internacional utiliza o termo segurança humana e o faz estabelecendo um contraponto com segurança militar, cujo propósito era a defesa entre Estados.

Esse novo conteúdo do direito à segurança amplia o seu alcance, superando o limite defensivo bélico cujo beneficiário-segurado era apenas o Estado enquanto pessoa de direito público externo, para estendê-lo, incluindo, em seu conteúdo, a defesa contra todas as ameaças à vida e à dignidade humana, passando a ser beneficiário de tal direito cada um dos

integrantes da comunidade, individualmente.<sup>426</sup>

O dever de proteção do Estado deixa de estar centralizado na defesa da sua manutenção contra as ameaças externas de outros entes de igual estatura jurídico-política para voltar-se para sua manutenção interna, para a garantia da sua estabilidade e inteireza, pois os riscos impostos à sociedade, em última análise, comprometem a higidez política do próprio Estado.

Assegurar paz e ordem internas, tranquilidade no que diz respeito a emprego, saúde, habitação e demais necessidades básicas integram o conceito mais amplo de segurança. A temática sobre as políticas de segurança, por sua vez, para serem consideradas eficazes e legítimas devem estar voltadas para o indivíduo como seu principal beneficiário, identificando as ameaças a que está exposto e elaborando planos de controle e minimização de riscos. A paz interna em cada Estado passa a ser fator de segurança de todos os outros Estados individualmente considerados, pois o conflito interno de um afeta a todos.

A guerra civil, a fome, a doença e a miséria geram consequências que não respeitam fronteiras, produzindo insegurança não apenas no epicentro dessas conflagrações sociais, mas também na comunidade internacional, haja vista a crise migratória que se estabeleceu na Europa, em que multidões abandonam seus países de origem, afligidos por guerra e fome principalmente, para ali buscarem refúgio.

Considera-se irrelevante investir em políticas públicas de saúde e educação apenas para a população interna de cada comunidade internacional, como se fosse possível sua separação ou isolamento do restante do globo. A atual debilidade das fronteiras entre as nações, implica que estas se afetam todo o tempo, mutuamente, podendo haver considerável variação de quantitativo populacional, seja em virtude de um ciclo migratório atípico ou de uma epidemia que a todos atinge, causando uma tragédia em escala global, como a que estamos vivenciando com a COVID-19. Assim pensar em segurança e paz interna, precisa levar em consideração que elas não serão atingidas isoladamente, independente do que

---

<sup>426</sup>“...we need another profound transition in thinking from nuclear security to human security. (...) With the dark shadows of the cold war receding, one can now see that many conflicts are within nations rather than between nations” UNITED NATION DEVELOPMENT PROGRAMME (UNDP). **Human Development Report 1994**. Nova York: Oxford University Press, 1994. p. 22. Disponível em: [http://hdr.undp.org/sites/default/files/reports/255/hdr\\_1994\\_en\\_complete\\_nostats.pdf](http://hdr.undp.org/sites/default/files/reports/255/hdr_1994_en_complete_nostats.pdf). Acesso em: 14/08/2018.

**Em livre tradução:** precisamos de outra transição profunda no pensamento da segurança nuclear para a segurança humana. (...) Com as sombras escuras da guerra fria recuando, pode-se agora ver que muitos conflitos estão dentro das nações e não entre nações

acontece ao restante dos integrantes da comunidade internacional.

Além disso, o dimensionamento de gastos públicos é insuficiente, tendo em vista a chegada de novos usuários do sistema público, egressos de países açoitados por tragédias particulares, com os quais o Estado não contava. A manutenção da segurança interna, então, está intimamente ligada à paz mundial, ao controle e minimização dos riscos fabricados que podem afetar a vida e a dignidade humana em qualquer um dos Estados, pois tal qual uma lemniscata, a segurança interna de cada Estado está umbilicalmente ligada à segurança e à paz dos outros Estados. Do conjunto das seguranças internas dos diversos Estados, resulta a segurança e a paz mundial em uma necessária relação de imbricação e causalidade.

Assim, a paz e a segurança interna de cada Estado estão diretamente relacionadas à prioridade que se pode dar à formulação de políticas públicas que valorizem a vida e a dignidade humana para os integrantes da sociedade. A garantia da segurança pública que se baseie nesse modelo contribui para a construção da segurança e da paz internacional, pois os riscos estarão sob controle, enfraquecendo o potencial lesivo de interferência em outros Estados.

Por outro lado, o desequilíbrio interno da segurança em qualquer dos Estados implica em afetar outros Estados, que inevitavelmente arcarão com as consequências dos riscos fabricados em uma determinada sociedade, alterando sua segurança interna, o que resultará na interferência da segurança de outros Estados e assim sucessivamente. Portanto, não há mais possibilidade de políticas autocentradas que desconsiderem as questões do Estado vizinho, pois o problema de um passa a ser problema de todos. Não existe segurança para um, não existe bem-estar social para um, ou é para todos ou não será para ninguém. A pandemia do coronavírus (COVID-19), causada pelo vírus SARS-CoV-2, é o exemplo atual, que de maneira eloquente deixa essa lição para o mundo. Não haverá saúde, segurança sanitária, normalidade nas relações internacionais, portanto paz, enquanto o governante de um país, de maneira irresponsável, se negar a adotar as medidas necessárias a redução da disseminação do vírus, especialmente negando a importância da vacinação em massa e dificultando a sua efetivação dentro do seu território.

Esse é o outro lado da globalização, a internacionalização dos deveres e dos direitos e, por extensão, da paz. A ajuda e a doação humanitárias são importantes estratégias de sobrevivência e manutenção de privilégios do doador, pois ao minimizar os riscos, ao garantir

a segurança mínima em cada Estado, reduz-se a chance de novo ciclo migratório, por exemplo, que poderá afetar a estabilidade social e económica das nações mais ricas.

Solidariedade e ajuda ao próximo, além de instrumentos de elevação espiritual, deixam de ter apenas o perfume da sacristia para incorporarem-se como estratégias políticas que, se bem conduzidas, poderão garantir a execução de orçamentos com políticas públicas internas de ordem e segurança. A ênfase da segurança deixa de ser limitada pelo território, pelos armamentos, para estar focada na população e no seu desenvolvimento sustentável.

A segurança interna de cada Estado significa compromisso com a segurança humana e esta apresenta algumas características que auxiliam na sua conceituação. A segurança humana está centrada no ser humano, em como ele vive e é respeitado em uma sociedade. Ela é uma preocupação universal, pois as mesmas ameaças afetam tanto países ricos como países pobres. Seus componentes são interdependentes, deixando o risco de ser regionalizado, já que a insegurança de um Estado afetará outros, não podendo ser vista de maneira particular e isolada. A dimensão das consequências e dos riscos que geram insegurança são imprevisíveis, sendo mais fácil e menos oneroso cuidar da segurança preventivamente que tratar dos efeitos posteriores.<sup>427</sup>

---

<sup>427</sup>“The idea of human security, though simple, is likely to revolutionize society in the 21st century. A consideration of the basic concept of human security must focus on four of its essential characteristics:

- Human security is a *universal* concern. It is relevant to people everywhere, in rich nations and poor. There are many threats that are common to all people—such as unemployment, drugs, crime, pollution and human rights violations. Their intensity may differ from one part of the world to another, but all these threats to human security are real and growing.

- The components of human security are *interdependent*. When the security of people is endangered anywhere in the world, all nations are likely to get involved. Famine, disease, pollution, drug trafficking, terrorism, ethnic disputes and social disintegration are no longer isolated events, confined within national borders. Their consequences travel the globe.

- Human security is *easier to ensure through early prevention* than later intervention. It is less costly to meet these threats upstream than downstream. For example, the direct and indirect cost of HIV/AIDS (human immunodeficiency virus/acquired immune deficiency syndrome) was roughly \$240 billion during the 1980s. Even a few billion dollars invested in primary health care and family planning education could have helped contain the spread of this deadly disease.

- Human security is *people-centred*. It is concerned with how people live and breathe in a society, how freely they exercise their many choices, how much access they have to market and social opportunities and whether they live in conflict or in peace.” UNITED NATION DEVELOPMENT PROGRAMME (UNDP). **Human Development Report 1994**. Nova York: Oxford University Press, 1994. p. 22 e 23. Disponível em: [http://hdr.undp.org/sites/default/files/reports/255/hdr\\_1994\\_en\\_complete\\_nostats.pdf](http://hdr.undp.org/sites/default/files/reports/255/hdr_1994_en_complete_nostats.pdf). Acesso em: 14/08/2018.

**Em livre tradução:** A ideia de segurança humana, embora simples, provavelmente revolucionará a sociedade no século 21. Uma consideração do conceito básico de segurança humana deve se concentrar em quatro de suas características essenciais:

- A segurança humana é uma preocupação *universal*. É relevante para pessoas em todos os lugares, em nações ricas e pobres. Existem muitas ameaças que são comuns a todas as pessoas, como desemprego, drogas, crime, poluição e violações dos direitos humanos. Sua intensidade pode variar de uma parte do mundo para outra, mas todas essas ameaças à segurança humana são reais e crescentes.

- Os componentes da segurança humana são *interdependentes*. Quando a segurança das pessoas está em perigo

Pela ampliação do conceito, vê-se que as ameaças à segurança assumem nova feição e podem ser classificadas em económica<sup>428</sup>, alimentar<sup>429</sup>, ambiental<sup>430 431</sup>, referente à saúde<sup>432</sup> da comunidade<sup>433 434</sup>, política<sup>435 436</sup> e pessoal, sendo esta última a que está mais próxima do objeto deste trabalho, pois se relaciona com a criminalidade praticada dentro do território nacional e como o Estado pode atuar para seu controle, pois a violência pessoal é a maior ameaça à vida humana, seja em países pobres ou ricos, e o crime é a principal causa de

---

em qualquer parte do mundo, é provável que todas as nações se envolvam. Fome, doença, poluição, tráfico de drogas, terrorismo, disputas étnicas e desintegração social não são mais eventos isolados, confinados dentro das fronteiras nacionais. Suas consequências viajam pelo mundo.

- A segurança humana é mais fácil de garantir por meio da prevenção precoce do que da intervenção posterior. É menos caro enfrentar essas ameaças a montante do que a jusante. Por exemplo, o custo direto e indireto do HIV / AIDS (vírus da imunodeficiência humana / síndrome da imunodeficiência adquirida) foi de aproximadamente US \$ 240 bilhões durante a década de 1980. Mesmo alguns bilhões de dólares investidos em cuidados básicos de saúde e educação em planejamento familiar poderiam ter ajudado a conter a propagação desta doença mortal.
- A segurança humana é centrada nas pessoas. Preocupa-se com a forma como as pessoas vivem e respiram em uma sociedade, com que liberdade exercem suas muitas escolhas, quanto acesso têm ao mercado e às oportunidades sociais e se vivem em conflito ou em paz.

<sup>428</sup>“Economic security requires an assured basic income-usually from productive and remunerative work, or in the last resort from some publicly financed safety net” UNITED NATION DEVELOPMENT PROGRAMME (UNDP). **Human Development Report 1994**. Nova York: Oxford University Press, 1994. p. 25. Disponível em: [http://hdr.undp.org/sites/default/files/reports/255/hdr\\_1994\\_en\\_complete\\_nostats.pdf](http://hdr.undp.org/sites/default/files/reports/255/hdr_1994_en_complete_nostats.pdf). Acesso em: 14/08/2018.

**Em tradução livre:** A segurança económica exige uma renda básica garantida, geralmente proveniente de trabalho produtivo e remunerado ou, como último recurso, de algum sistema de seguridade financiado com fundos públicos.

<sup>429</sup>“Food security means that all people at all times have both physical and economic access to basic food. This requires not just enough food to go round. It requires that people have ready access to food-that they have an "entitlement" to food, by growing it for themselves, by buying it or by taking advantage of a public food distribution system. UNITED NATION DEVELOPMENT PROGRAMME (UNDP). **Human Development Report 1994**. Nova York: Oxford University Press, 1994. p. 27. Disponível em: [http://hdr.undp.org/sites/default/files/reports/255/hdr\\_1994\\_en\\_complete\\_nostats.pdf](http://hdr.undp.org/sites/default/files/reports/255/hdr_1994_en_complete_nostats.pdf). Acesso em: 14/08/2018.

**Em tradução livre:** A segurança alimentar significa que todas as pessoas, em todos os momentos, têm acesso tanto físico quanto económico aos alimentos básicos. Isso requer que haja alimentos suficientes para todos e também que haja acesso imediato aos alimentos, que haja um "direito" aos alimentos, seja por que o cultiva, o comprando ou aproveita de um sistema público de distribuição de alimentos.

<sup>430</sup>A segurança ambiental diz respeito ao direito a um meio ambiente saudável, ou seja, direito de acesso a água, de fixar moradia em áreas seguras, não expostas a catástrofes naturais. Segundo o Relatório citado, nos últimos anos as grandes catástrofes têm sido provocadas em virtude da ação humana, podendo serem evitadas ou minimizados seus efeitos.

<sup>431</sup>“Many chronic "natural" disasters in recent years have also been provoked by human beings. Deforestation has led to more intense droughts and floods. And population growth has moved people into areas prone to cyclones, earthquakes or floods-areas always considered dangerous and previously uninhabited. Poverty and land shortages are doing the same-driving people onto much more marginal territory and increasing their exposure to natural hazards. The result: disasters are more significant and more frequent.” UNITED NATION DEVELOPMENT PROGRAMME (UNDP). **Human Development Report 1994**. Nova York: Oxford University Press, 1994. p. 30. Disponível em: [http://hdr.undp.org/sites/default/files/reports/255/hdr\\_1994\\_en\\_complete\\_nostats.pdf](http://hdr.undp.org/sites/default/files/reports/255/hdr_1994_en_complete_nostats.pdf). Acesso em: 08/08/2018.

**Em tradução livre:** Muitos desastres "naturais" crónicos nos últimos anos também foram provocados por seres humanos. O desmatamento tem causado secas e inundações mais intensas. E o crescimento populacional levou as pessoas para áreas sujeitas a ciclones, terremotos ou inundações - áreas sempre consideradas perigosas e antes desabitadas. A pobreza e a escassez de terras estão fazendo o mesmo, levando as pessoas para territórios muito

ansiedade para a maioria da população<sup>437</sup>.

Os subseqüentes estudos da ONU referentes à segurança humana aprofundam e refinam seu conceito<sup>438</sup>, bem como adotam como nomenclatura “segurança cidadã” em substituição à “segurança pessoal”, aclarando e melhor delimitando seu contorno<sup>439</sup>. A segurança cidadã trata especificamente de um tipo de risco fabricado pela ação humana - o delito - seja ele *mala in se* ou *mala prohibita*<sup>440</sup>, estando o controle de tal risco ligado primordialmente à atividade legislativa estatal, sem desprezar contudo a fundamental

mais marginais e aumentando sua exposição a perigos naturais. Resultado: os desastres são mais significativos e mais frequentes

<sup>432</sup>“The disparities between rich and poor are similar for access to health services” UNITED NATION DEVELOPMENT PROGRAMME (UNDP). **Human Development Report 1994**. Nova York: Oxford University Press, 1994. p. 28. Disponível em: [http://hdr.undp.org/sites/default/files/reports/255/hdr\\_1994\\_en\\_complete\\_nostats.pdf](http://hdr.undp.org/sites/default/files/reports/255/hdr_1994_en_complete_nostats.pdf). Acesso em: 08/08/2018.

**Em tradução livre:** As disparidades entre ricos e pobres são semelhantes no acesso aos serviços de saúde.

Segurança da saúde refere-se ao acesso aos serviços de saúde, afirmando o relatório que tanto nos países industrializados quanto nos países em desenvolvimentos, o acesso à saúde costuma ser mais difícil para a população mais pobre, especialmente as crianças, mulheres e habitantes das zonas rurais.

<sup>433</sup>Segurança da comunidade trata do direito de estar seguro independentemente do grupo, família, comunidade, etnia, grupo racial ao qual pertença, onde encontra sua identidade cultural ou conjunto de valores que lhe identifica.

<sup>434</sup>“In several nations, ethnic tensions are on the rise, often over limited access to opportunities whether to social services from the state or to jobs from the market. Individual communities lose out, or believe they lose out, in the struggle for such opportunities. As a result, about half of the world's states have recently experienced some interethnic strife. And this has been especially serious where national conflict was exacerbated by cold war rivalry.” UNITED NATION DEVELOPMENT PROGRAMME (UNDP). **Human Development Report 1994**. Nova York: Oxford University Press, 1994. p. 32. Disponível em: [http://hdr.undp.org/sites/default/files/reports/255/hdr\\_1994\\_en\\_complete\\_nostats.pdf](http://hdr.undp.org/sites/default/files/reports/255/hdr_1994_en_complete_nostats.pdf). Acesso em: 08/08/2018.

**Em tradução livre:** Em várias nações, as tensões étnicas estão aumentando, muitas vezes devido ao acesso limitado a oportunidades de serviços sociais do estado ou a empregos no mercado. Comunidades individuais perdem, ou acreditam que perdem, na luta por essas oportunidades. Como resultado, cerca de metade dos estados do mundo experimentaram recentemente algum conflito interétnico. E isso tem sido especialmente sério onde o conflito nacional foi exacerbado pela rivalidade da guerra fria.

<sup>435</sup>“One of the most important aspects of human security is that people should be able to live in a society that honours their basic human rights.” UNITED NATION DEVELOPMENT PROGRAMME (UNDP). **Human Development Report 1994**. Nova York: Oxford University Press, 1994. p. 32. Disponível em: [http://hdr.undp.org/sites/default/files/reports/255/hdr\\_1994\\_en\\_complete\\_nostats.pdf](http://hdr.undp.org/sites/default/files/reports/255/hdr_1994_en_complete_nostats.pdf). Acesso em: 08/08/2018.

**Em tradução livre:** Um dos aspectos mais importantes da segurança humana é que as pessoas devem ser capazes de viver em uma sociedade que honre seus direitos humanos básicos.

<sup>436</sup>A segurança política trata da garantia de viver numa sociedade onde os direitos humanos são respeitados, mesmo em época de conturbações políticas, pois em tempos como estes ocorrem intervenções militares, cujos agentes reprimem indivíduos e grupos, bem como suas ideias e informações.

<sup>437</sup>“Perhaps no other aspect of human security is so vital for people as their security from physical violence. In poor nations and rich, human life is increasingly threatened by sudden, unpredictable violence. (...) In many societies, human lives are at greater risk than ever before. For many people, the greatest source of anxiety is crime, particularly violent crime.” UNITED NATION DEVELOPMENT PROGRAMME (UNDP). **Human Development Report 1994**. Nova York: Oxford University Press, 1994, p. 30. Disponível em: [http://hdr.undp.org/sites/default/files/reports/255/hdr\\_1994\\_en\\_complete\\_nostats.pdf](http://hdr.undp.org/sites/default/files/reports/255/hdr_1994_en_complete_nostats.pdf)

**Em tradução livre:** Talvez nenhum outro aspecto da segurança humana seja tão vital para as pessoas quanto sua proteção contra a violência física. Nas nações pobres e ricas, a vida humana é cada vez mais ameaçada por uma violência repentina e imprevisível. (...) Em muitas sociedades, as vidas humanas estão em maior risco do que nunca. Para muitas pessoas, a maior fonte de ansiedade é o crime, especialmente o crime violento

<sup>438</sup>“La seguridad humana consiste en proteger el núcleo central de todas las vidas humanas contra riesgos graves

importância das políticas de desenvolvimento humano que impactam diretamente na redução da criminalidade e na sensação subjetiva de insegurança.

Infelizmente, a associação imediata que se faz ao tratar de redução de criminalidade é de exacerbação de medidas penais contra o crime, sem se preocupar em cuidar de medidas que evitem que o crime seja cometido, que mais jovens sejam atraídos para a marginalidade, despojados de usufruir dos seus direitos fundamentais e condenados a uma vida pobre e breve.

A urgência por uma resposta rápida e eficaz leva a sociedade a clamar por um direito penal do inimigo<sup>441</sup>, mais invasivo<sup>442</sup>, menos fragmentário, seduzido por discursos mendazes de grupos políticos com interesses escusos, que prometem segurança à custa do incremento de ações violentas e que desrespeitam direitos fundamentais, como a integridade física, a liberdade e a vida.

---

y previsible, de una forma congruente con la realización humana de largo plazo (Alkire, 2003).” PROGRAMA DE LAS NACIONES UNIDAS PARA EL DESARROLLO (PNUD). **Informe sobre Desarrollo Humano para América Central, IDHAC 2009-2010**. Colombia: Dvinni S.A., 2009. p. 30. Disponível em: [http://www.latinamerica.undp.org/content/dam/rblac/docs/Research%20and%20Publications/Central\\_America\\_RHDR\\_2009-10\\_ES.pdf](http://www.latinamerica.undp.org/content/dam/rblac/docs/Research%20and%20Publications/Central_America_RHDR_2009-10_ES.pdf). Acesso em: 14/08/2018.

<sup>439</sup>“...la seguridad ciudadana es una modalidad específica de la seguridad humana, que puede ser definida inicialmente como la *protección universal contra el delito violento o predatorio*. Seguridad ciudadana es la protección de ciertas opciones u oportunidades *de todas las personas* –su vida, su integridad, su patrimonio– contra un tipo específico de riesgo (el delito) que altera en forma “súbita y dolorosa” la vida cotidiana de las víctimas.” PROGRAMA DE LAS NACIONES UNIDAS PARA EL DESARROLLO (PNUD). **Informe sobre Desarrollo Humano para América Central, IDHAC 2009-2010**. Colombia: Dvinni S.A., 2009. p. 31. Disponível em: [http://www.latinamerica.undp.org/content/dam/rblac/docs/Research%20and%20Publications/Central\\_America\\_RHDR\\_2009-10\\_ES.pdf](http://www.latinamerica.undp.org/content/dam/rblac/docs/Research%20and%20Publications/Central_America_RHDR_2009-10_ES.pdf). Acesso em: 14/08/2018.

<sup>440</sup>“ O conceito de “delicta in se” exprime um domínio de condutas genuinamente criminosas, posto que lesivas de valores ou bens respaldados pela experiência normativa do mundo da vida, através das quais a comunidade constrói a sua identidade normativa. Por sua vez, o conceito de “delicta mere prohibita” designa um âmbito de infrações sistémicas criadas pelo “magistério do governo”, porque disfuncionais relativamente à “prosperidade pública”” DIAS, Augusto Silva. **“Delicta in Se” e “Delicta Mere Prohibita”**. Coimbra: Coimbra Editora, 2008. p.211

<sup>441</sup>“O inimigo da contemporaneidade é, para G. JAKOBS e discípulos, o terrorista, o traficante de droga, de armas e de seres humanos, os membros de organizações de crime organizado transnacional; delinquente de elevada perigosidade e ser nefasto à comunidade e, como tal, deve-se submeter à construção jurídico-criminal de *inimigo*.” VALENTE, Manuel Monteiro Guedes. **Direito Penal do Inimigo e o Terrorismo**. Coimbra: Almedina, 2010. p. 19

<sup>442</sup>“Se o debate sobre o conceito do “Direito penal” do inimigo (um setor de regulação em que se adianta ao máximo a barreira da criminalização, elevam-se as penas drasticamente e restringe-se sensivelmente o estatuto processual do imputado) tem mostrado alguma coisa para as infrações em matéria de terrorismo é que a estrela no arsenal argumentativo a favor de regras completamente distintas para os *inimigos* (terroristas) está – de maneira paralela ao que acontece noutros setores de regulação envolvidos nesta evolução político-criminal, embora com maior intensidade – na questão da *periculosidade* dos atos dos terroristas e na consequente necessidade de sua prevenção instrumental, ao se tratar de uma fonte de perigo especialmente significativa.” MELIÁ, Manuel Cancio. **Internacionalização do Direito Penal e da política criminal: algumas reflexões sobre a luta jurídico-penal contra o terrorismo**. PANOPTICA (em reformulação), v. 4, n. 3, 2009. p. 12.

### 6.3 SOCIEDADE DE RISCO, SEGURANÇA PÚBLICA E DIREITO PENAL

A generalizada sensação de insegurança causada pelos riscos que advém do avanço tecnológico traz consigo o sentimento de incompetência do cidadão em se autoprotger, levando-o a direcionar ao Estado sua expectativa de proteção e segurança, apontando o direito penal como âmbito da concretização desses anseios, espaço em que é possível, por meio de instrumento tangível, gerar o sentimento de segurança desejado.

Uma sociedade marcada pelo risco, tende a prever as possíveis consequências da ocorrência de fato considerado perigoso, exigindo do Estado a criação de normas que atuem ainda antes que ele ocorra, especialmente categorizando como crime<sup>443</sup>. Assim, a pressão exercida pela sociedade de risco, tira o direito penal do campo exclusivo da dogmática, portanto de pensar apenas o delito já consumado, e o traz para o âmbito da prevenção, da elaboração de políticas públicas em matéria penal, área específica para pensar como prevenir e evitar que o delito se concretize, antecipando assim a intervenção do direito penal<sup>444</sup>.

A alternativa do direito penal como resposta possível ao desejo de segurança pode ser associada a alguns fatores decorrentes dos riscos fabricados, ou seja, aqueles resultantes da ação humana e que gera sensação de incerteza e insegurança<sup>445</sup>. Entre eles está a dimensão

---

<sup>443</sup>“Assiste-se à criação dos chamados delitos de perigo abstrato, nos quais é suficiente demonstrar a prática de uma ação descrita pelo legislador como perigosa, e não a ocorrência de danos efetivos (...); à tendência de retrocesso na incidência da figura do risco permitido, com uma restrição progressiva das esferas de atuação arriscada (...) A pretensão de satisfazer as necessidades de justiça faz com que haja o surto legislativo, e na medida em que há conflitos de ordem múltipla, vem-se recorrendo ao direito penal como solução *prima ratio*, assumindo uma função eminentemente simbólica, isto é, como forme de tranquilizar a opinião pública.” AZEVEDO, Rodrigo Ghiringhelli. **Sociologia e Justiça Penal. Teoria e Prática da Pesquisa Sociocriminológica**: Rio de Janeiro. Editorial Lumen Juris, 2010. p. 219 e 220

<sup>444</sup>“El paradigma absoluto y dominante es el dela prevención. Del Derecho penal se espera, sobre todo, efectividad en la protección de los bienes jurídicos y en la producción de seguridad frente al delito, y, mucho menos, la protección frente a los derechos fundamentales en peligro, lo que era observado en la década de los años setenta de una manera totalmente distinta.” HASSEMER, Winfried. **El Derecho Penal del Estado de Derecho en los Tiempos de Terrorismo** in ALFARO, Luis Reyna e TERÁN, Sergio Cuaresma. **Derecho Penal y Estado de Derecho**: Buenos Aires. Editorial B de f, 2008. p. 187

<sup>445</sup>“En concordancia con estas solicitudes provenientes de los medios de información y grupos de poder interesados, la política criminal responde con una reacción inmediata consistente en paquetes de leyes que aumentan las penas de los delitos (...) que la opinión pública justifique la construcción de un Estado poderoso que enfrente el problema de la criminalidad con contundencia, ya que ésta es visualizada como un “riesgo social”, en cual, junto a otros “riesgos modernos”, como el temor a los derrames de sustancias químicas venenosas o la contaminación de la población por reactores atómicos (...) Esto significa que, junto a los riesgos surgidos de la ciencia y la industria, aparece el hombre mismo como un riesgo de seguridad y el Estado está listo para utilizar todos los medios para combatir este riesgo.” SÁNCHEZ, Alfredo Chirino. **La Seguridad como un topos discursivo en la política criminal centroamericana**. Perspectivas de una desesperanza in ALFARO, Luis Reyna e TERÁN, Sergio Cuaresma. **Derecho Penal y Estado de Derecho**: Buenos Aires. Editorial B de f, 2008. p. 23 e 24

desses novos riscos e a destruição em massa que eles eventualmente podem vir a causar. Aliado a esse fato, está a desconfiança de que a própria ciência pode vir a controlar ou neutralizar os efeitos das inovações tecnológicas, bem como considerar que os riscos gerados pelas constantes descobertas sejam apenas avaliados e classificados por seus autores, pois tal avaliação pode minimizar os resultados e tender a considerá-los acidentais.

Em uma sociedade de medo e desconfiança, o risco causado por uma conduta humana tende a não ser visto como casualidade, e sim como injustiça, incluindo-o na categoria das ações reprováveis, portanto passíveis de aplicação de pena, ou seja, como categoria de tipo penal, reclamando assim a utilização do lado mais grave do ordenamento jurídico para seu controle.<sup>446</sup>

Do direito penal agora se espera que produza segurança frente ao delito, que impeça o seu cometimento, podendo utilizar para tanto os meios disponíveis, não mais havendo a preocupação que ele garanta o respeito aos direitos fundamentais em perigo. Visando atender essa expectativa, o Estado avança com ações mais enérgicas e invasivas, ora mitigando ora suprimindo direitos e garantias individuais sob a justificativa de estabelecer a ordem pública e o bem-estar da sociedade<sup>447 448</sup>.

O Estado deixa de ser uma ameaça aos direitos individuais do cidadão e passa a com ele se ladear, formando uma dupla contra suposto “inimigo”, essa entidade sem rosto, que custa ao cidadão perceber que, se for encarar o tal inimigo frente a frente, verá que no lugar do seu rosto há um espelho, em que sua face estará refletida.

Apoiado no consenso da sociedade, surge o direito penal da segurança ou direito

---

<sup>446</sup>“Inicialmente, aduz-se que a gravidade e a dimensão dos novos riscos, capazes de causar ondas de destruição massiva, justificam que se recorra ao mais grave instrumento da tutela jurídica, qual seja, o direito penal. (...) Em segundo lugar, identifica-se que a relação de desconfiança estabelecida no que se refere à ciência, responsável pela criação de novos riscos, legitima o abandono das soluções para gestão dos riscos ligados a ela, para se reivindicar a intervenção punitiva do Estado nessa seara. Ademais, se, nos termos da definição de Beck, os riscos tecnológicos podem ser sempre remetidos a decisões humanas, cresce a tendência a deixar de percebê-los como acidentes fortuitos para encará-los como injustos.” MACHADO, Marta Rodriguez de Assis. **Sociedade de Risco e Direito Penal**. São Paulo: IBCCRIM, 2005. p. 93-94.

<sup>447</sup>“De igual modo, ser protegido é também aceitar a diminuição de uma parte de sua segurança, resultante da entrega a outrem – ao Estado de Direito- do direito individual a se autoprotoger” LOURENÇO, Nelson. **Segurança, Sentimento de Insegurança e Estado de Direito**. O Espectro axial da relação Direitos, Liberdades e Garantias e Poderes do Estado. 2009. p. 90. Disponível em: [www.researchgate.net/publication/262874417\\_Seguranca\\_Sentimento\\_de\\_Inseguranca\\_e\\_Estado\\_de\\_Direito\\_O\\_Espectro\\_axial\\_da\\_relacao\\_Direitos\\_Liberdades\\_e\\_Garantias\\_e\\_Poderes\\_do\\_Estado](http://www.researchgate.net/publication/262874417_Seguranca_Sentimento_de_Inseguranca_e_Estado_de_Direito_O_Espectro_axial_da_relacao_Direitos_Liberdades_e_Garantias_e_Poderes_do_Estado). Acesso em: 14/08/2018.

<sup>448</sup>“Lamentavelmente, nós já nos habituamos a uma técnica enganosa de avaliação. Quando uma ameaça nos parece particularmente intensa, nada mais é sagrado para nós, nem mesmo os direitos fundamentais...” HASSEMER, Winfried. **A Segurança Pública no Estado de Direito**. Lisboa: Associação Académica da Faculdade de Direito de Lisboa, 1995. p. 103.

penal dos riscos, que apressa-se em debilitar ou até mesmo eliminar o papel dos direitos fundamentais, admitindo a construção de um direito penal do inimigo, permitindo que o Estado introduza, cada vez com mais frequência, instrumentos agudos e constritores de liberdades e de direitos subjetivos.<sup>449</sup>

O cidadão agora está convencido a cambiar o direito penal baseado na culpabilidade, no fato concreto e pretérito, por um direito penal de segurança, de riscos, projetado para os acontecimentos futuros, concordando em relativizar ou mitigar direitos fundamentais essenciais, como a proteção dos dados ou da privacidade<sup>450</sup>, direitos que têm perdido validade e cuja defesa de preservação já não encontra respaldo em discurso convincente.

Neste ponto se transita por terreno movediço e perigoso sendo necessário traçar com risco forte a necessidade da defesa dos direitos fundamentais, dificultando a inclusão de métodos de prova que os violem, deixando as medidas mais duras e invasivas apenas para os casos mais graves de criminalidade, onde a ordem processual penal geral não consiga apresentar a resposta necessária. Delitos como pedofilia, tráfico de armas, de pessoas, de estupefacientes e aqueles produto de criminalidade organizada, exigem cabedal próprio e específico para seu enfrentamento.

A criminalidade organizada, por imposição de exaustivos discursos mediáticos, assume papel de destaque como geradora de risco atual e iminente, esteja ela organizada no formato de máfias, cartéis ou facções criminosas. Sua atuação, que não dispensa o uso da violência, atinge direitos penais difusos, comuns a toda coletividade, robustecendo o discurso do controle precedente antes mesmo da prática do delito.

Segundo essa linha de raciocínio, faz-se necessária a utilização dos métodos

---

<sup>449</sup>“Con ello el Estado ha cambiado fundamentalmente su papel, de una amenaza a los derechos individuales se há convertido ahora en un garante de la seguridad. La clásica reacción de tensión entre la seguridad y la libertad, que se manifiesta en la experiencia, en donde el aumento de la seguridad frente al delito debe ser organizada mediante el Derecho penal y acompañada de limitaciones a las libertades públicas, ya no constituye algo vivo.” HASSEMER, Winfried. **El Derecho Penal del Estado de Derecho en los Tiempos de Terrorismo**. In: ALFARO, Luis Reyna; TERÁN, Sergio Cuaresma. **Derecho Penal y Estado de Derecho**. Buenos Aires: Editorial B de f, 2008. p. 186-187.

<sup>450</sup>“Whilst it would be an unusual person who placed no value upon privacy, significant difficulties have to be overcome in the attempt to give the concept concrete legal meaning. First, it is undoubtedly the case that different people and societies have widely varying interpretation as to which matters are private and reasonable belong in the public arena.” LLOYD, Ian J. **Information Technology Law**, 9.<sup>a</sup> ed. Oxford: Oxford University Press, 2020. p.15

**Em livre tradução:** Embora seja incomum uma pessoa que não valorizava a privacidade, dificuldades significativas devem ser superadas na tentativa de dar sentido concreto ao conceito. Em primeiro lugar, é sem dúvida o caso, de que diferentes pessoas e sociedades têm interpretações amplamente variadas quanto a quais assuntos são privados e quais pertencem à arena pública.

tecnológicos disponíveis, anterior à conduta criminosa ser praticada, visando coibi-la e assim exercitar o controle possível do risco iminente. É fundamental também a utilização de tais meios durante todo o processo de persecução penal, ou seja, ao apurar um crime que já aconteceu, desde a sua investigação, seguindo pela persecução penal em juízo.

Isso porque, segundo tal discurso, o Estado deve servir-se dos mesmos recursos utilizados pela criminalidade organizada a fim de garantir a eficiência do seu trabalho repressivo<sup>451</sup>, não podendo ser limitado por direitos fundamentais que devem ceder ante o direito à segurança<sup>452</sup>.

Ressalta-se, entretanto, que a violência que desperta o medo e a insegurança é decorrente muito mais da criminalidade de massa do que da criminalidade organizada. É preciso estabelecer o limite do que se considera criminalidade organizada e bem diferenciá-la do seu entorno. A existência e o potencial perigo gerado pelo crime organizado são reais, mas o que deve ser questionado é se são eles que hoje despertam a sensação de insegurança e medo na sociedade.

Sob o pretexto de reduzir a insegurança e de combater o crime organizado, estão sendo ampliadas medidas legislativas interventivas em direitos fundamentais. Ao crime organizado tem sido atribuído, ainda que equivocadamente, o aumento dos índices de violência, quando, em verdade, é o incremento da violência na criminalidade de massa que está influenciando os padrões de comportamento do crime organizado. Criminalidade de massa e crime organizado são conceitos diversos e fenômenos sociais diferentes, como já discutido no Capítulo 1 deste trabalho, mas que não se excluem, ao contrário, se influenciam mutuamente.

A criminalidade de massa pode ser identificada observando-se o incremento dos assaltos a ônibus, do roubo de veículos e de outros delitos praticados em espaço público, especialmente aqueles contra o patrimônio e que se utiliza de violência. Seu combate passa

---

<sup>451</sup>“El argumento se sostiene, de una manera simplificada, en que el Estado de Derecho, antes graves amenazas de nuevo cuño, debe proteger su eficiencia y debe servirse de los mismos medios de los cuales disponen los perpetradores criminales.” HASSEMER, Winfried. *El Derecho Penal del Estado de Derecho en los Tiempos de Terrorismo*. In: ALFARO, Luis Reyna; TERÁN, Sergio Cuaresma. **Derecho Penal y Estado de Derecho**. Buenos Aires: Editorial B de f, 2008. p. 184.

<sup>452</sup>“Este constructo há permitido demoler las últimas conexiones básicas de nuestra concepción democrática y decidir que nuestro derecho a la seguridad bien merece combatir hasta los derechos humanos más esenciales, y reducir, con ello, los últimos espacios de libertad para los seres humanos que viven en sociedad.” SÁNCHEZ, Alfredo Chirino. *La Seguridad como un topos discursivo en la política criminal centroamericana. Perspectivas de una desesperanza*. In: ALFARO, Luis Reyna e TERÁN, Sergio Cuaresma. **Derecho Penal y Estado de Derecho**. Buenos Aires: Editorial B de f, 2008. p. 19.

necessariamente pela adoção de medidas preventivas, que só exceccionalmente ingressam na seara jurídica.

Medidas como escola em tempo integral para os jovens, promoção de atividades culturais, criação de espaços públicos para convivência e prática de atividades desportivas e lúdicas pela comunidade, incentivo à criação de políticas públicas para geração de emprego e renda, especialmente para os egressos do sistema carcerário, entre outras tantas medidas que podem ser postas em prática pelo Poder Público e pela própria sociedade. Tais medidas não guardam qualquer relação com a criação de leis penais ou maior intervenção do sistema penal nas liberdades individuais, mas que podem gerar efeitos exponencialmente maiores na redução da violência do que aqueles que possam ser trazidos pela ordem jurídica penal.<sup>453</sup>

Estando o crime organizado presente em todas as sociedades, seja qual for o nível de desenvolvimento económico ou político, podemos observar que o que diferencia a manifestação externa do crime organizado nos diversos tipos de sociedade é, entre outros, o nível de violência aceite pela comunidade e que se reflete primeiramente nos crimes ordinariamente cometidos. Tal normalização da violência se dá pela banalização das notícias veiculadas, sem qualquer critério de horário, fazendo parecer ser normal o uso regular da violência, a todo tempo e em toda lugar<sup>454</sup>.

Por sua vez, observar as diversas manifestações sociais e culturais de uma determinada sociedade, como os programas de televisão, as notícias diariamente veiculadas, e ainda os abusos e violações interpessoais aceites e considerados toleráveis, como violência de género, intolerância religiosa, desrespeito à garantia de prioridade de determinadas categorias, é possível ter um entendimento mais fidedigno sobre as especificidades da violência manifestada no interior daquela sociedade.

É a tolerância às pequenas violências diárias, consideradas aceitáveis e, portanto,

---

<sup>453</sup>“Na verdade, a população encontra-se realmente sobressaltada e agredida por uma forma de criminalidade que nada tem a ver com a criminalidade organizada: é a criminalidade de massa. Quem mistura ambas dificulta uma política criminal racional. Assaltos de rua, invasões de apartamentos, tráfico de droga, furtos de bicicletas ou delinquência juvenil crescem, ao passo que sua elucidação, bem como a sua real perseguição, tendem para zero. (...) Os efeitos não são apenas físico e económicos, mas sobretudo atingem o nosso equilíbrio emocional e o nosso senso normativo: trata-se da sensação de desprotecção e de debilidade diante de ameaças e perigos desconhecidos, que nos levam a duvidar da força do direito.” HASSEMER, Winfried. **A Segurança Pública no Estado de Direito**. Lisboa: Associação Académica da Faculdade de Direito de Lisboa, 1995. p. 91.

<sup>454</sup>“Por outro lado, fenómenos superficiais como as exhibições de violência na televisão, tidos como responsáveis pelas tendências descritas, são menos as fontes do que já a manifestação mal. Acaso tivéssemos outra concepção de violência, estas exhibições não encontrariam espaço nos programas e a sua eliminação da televisão atingiria menos a mensagem que o mensageiro” HASSEMER, Winfried. **A Segurança Pública no Estado de Direito**. Lisboa: Associação Académica da Faculdade de Direito de Lisboa, 1995. p. 106

sem exigência de reprimenda, que incrementa o grau de violência nas condutas consideradas pela sociedade como reprováveis. Quanto maior o grau de tolerância à violência, mais bárbaros precisam ser os comportamentos criminosos para que sejam considerados reprováveis, intoleráveis.

Chega-se à conclusão de que o risco, a sensação de insegurança e medo hoje impregnados na sociedade são provenientes muito mais do conjunto de vários delitos cometidos sem qualquer organização prévia, sem vínculo subjetivo ou material, por sujeitos que praticam delitos sem qualquer combinação entre si, do que daqueles cometidos por organizações criminosas.

As organizações que desviam verbas da merenda escolar, que adulteram licitações de obras públicas, que retiram medicamentos de postos de saúde, produzem consequências muito mais nefastas ao conjunto da sociedade do que uma sequência de roubo de telemóveis, entretanto sem provocar temor, nem sensação de risco ou sentimento de insegurança.

A necessidade de aperfeiçoamento nos métodos de prova e de investigação da criminalidade organizada, bem como a melhoria das práticas de persecução penal já conhecidas, aliadas a soluções ligadas ao direito administrativo, financeiro e tributário, especialmente no combate à corrupção<sup>455</sup>, seja ela dentro da esfera legislativa, da polícia, do sistema judicial, não provêm do alto risco ou insegurança que ela causa a sociedade, mas do grau de sofisticação na prática dos delitos e da alta danosidade que elas trazem ao corpo social.

---

<sup>455</sup>“Não o direito penal, mas o direito administrativo, o direito do serviço público, o direito tributário e a política financeira, a doutrina administrativa, a psicologia ou a doutrina da administração de empresas seriam as células de referência que deveriam ser questionadas para que o direito penal pudesse representar o papel que lhe foi destinado no Estado de Direito, para que isso restasse como razão última do problema e não se tornasse a primeira ou até mesmo a única razão.” HASSEMER, Winfried. **Direito Penal Libertário**: Belo Horizonte. Editora Del Rey, 2007. p. 97.

## 7. CONSIDERAÇÕES FINAIS

O conceito de Estado passa por uma transformação, cujo formato futuro viceja no terreno das indefinições de funções e prerrogativas, pois o avanço tecnológico, a velocidade das informações e a inserção da comunidade global no mundo virtual tem encurtado distâncias e feito evanescer fronteiras físicas, cada vez mais difíceis de serem identificadas;

O fim da divisão do mundo em dois blocos, em que cada um concentrava Estados que se protegiam e se regulavam internamente, coloca todos no mesmo ambiente negocial. Os Estados menores, com organizações sociais, económicas e jurídicas ainda imberbes, perderam a capacidade de diálogo em paridade de condições com os Estados de organização e estrutura mais antiga e definida. A busca desesperada pelo lucro passa a ser a tônica da atual época, restando aos mais débeis, seja por inferioridade económica, social ou política, submeterem-se aos interesses dos mais fortes. Está em questão, por consequência, o conceito de soberania.

O crime é um fenómeno social que acompanha o movimento de encurtamento de distâncias e de redefinição de fronteiras. Ele começa a se organizar em estruturas complexas, aptas a acompanhar a transformação pela qual atravessa a sociedade e o Estado, que tem por principal objetivo o lucro. Outras atividades ilícitas são acessórias e funcionam como meios para obtenção da conquista de mercados.

No Brasil, o crime organizado surge no interior dos presídios, origem das duas maiores organizações criminosas em atuação no país, classificadas como facções: o Primeiro Comando da Capital (PCC), que se originou em São Paulo, e o Comando Vermelho (CV), mais antigo e articulado, no Rio de Janeiro, tendo por atividade principal o tráfico de drogas.

O crescimento dessas facções deve-se, em grande parte, à ineficiência do Estado em exercer o controle dos presídios, permitindo que as facções se organizem para comandar todo o tráfico de drogas no país.

Nos últimos anos, tem-se desenvolvido o combate à corrupção, especialmente aquela praticada por organizações criminosas que atuam entranhadas na máquina estatal, apoderando-se de toda a estrutura burocrática a ponto de colocar em risco a manutenção e a estabilidade do Estado Democrático de Direito.

A investigação da criminalidade organizada reclama método próprio, não podendo apenas voltar-se para o passado, para os fatos já consumados, mas também para os atuais que estão acontecendo durante o procedimento investigatório, assim como para os atos futuros, cuja preparação já se iniciou.

O acesso à tecnologia de informação está cada dia mais fácil e barato, sendo possível a qualquer pessoa, bastando apenas o acesso a um *smartphone*. Utilizando esses aparelhos é possível arquivar uma infinita quantidade de dados, bem como acessar a sistemas bancários e realizar transações comerciais, inclusive de caráter ilícito.

Chama-se *malware* o programa informático (*software*) introduzido maliciosamente (*malicious*) em um determinado dispositivo eletrónico e que permite ao autor dessa intervenção a realização de diversas operações no sistema informático atingido, independentemente do consentimento e mesmo do conhecimento do seu usuário. Existem vários tipos de *malware* (*keylogger*, *spyware*, *trojan horse*, *adware*, *screenlogger*, etc.) sendo que constantemente surgem novos, cuja classificação tende a ser sempre incompleta.

O *malware* tem sido utilizado para a prática de delitos, especialmente no âmbito da criminalidade organizada, sendo possível tecnicamente o seu uso para auxílio à investigação em crimes que apresentem este grau de organização e complexidade.

É necessário fazer distinção entre *malware* e buscas on-line, pois este é apenas um dentre os métodos ocultos de obtenção de prova possíveis. Para sua execução, é possível fazer uso de *malware*.

Há alguns métodos de obtenção de prova que abrigavam-se sob a nomenclatura de buscas on-line, mas a LC, nos seus artigos 11º a 19º, deu-lhes tratamento próprio e específico: pesquisa de dados informáticos, apreensão de dados informáticos, intercetações de dados informáticos e a possibilidade de ações encobertas, ainda não catalogadas, com utilização de *malware*.

O *malware* pode atuar como agente infiltrado virtual, tanto em atividade preventiva como investigativa, interagindo com o investigado, sugerindo visita a sítios com assuntos variados, inclusive conteúdo ilícito, que podem ou não ser visitados pelo seu destinatário. O *malware*, assim utilizado, dispensa o agente físico do dever de vigiar a prática da atividade delitativa, reduzindo o risco inerente à atividade do agente infiltrado, além de agilizar o tratamento dos dados captados.

A garantia do arguido da não autoincriminação é deduzida do direito ao silêncio ao qual ela está atrelada, ou seja, a garantia existe na exata medida do direito que ela acompanha, não se tratando, portanto, de dois princípios ou dois direitos distintos.

As declarações obtidas por agente infiltrado, desde que fornecidas voluntariamente pelo investigado, não são consideradas violação ao princípio do direito ao silêncio, nem violação da garantia da não autoincriminação.

A LC regula tanto regimes distintos para investigação de crimes cometidos por meio de sistema informático, quanto a recolha de prova em suporte electrónico, sendo que em seus artigos estão previstas as modalidades de acesso a dados armazenados em sistemas informáticos e a interceptação em tempo real de comunicações eletrónicas, de dados de tráfego e do conteúdo associado as comunicações.

Em ambos os casos o investigador se limita a coletar os dados produzidos *sponte propria* pelo investigado, sem adotar mecanismos capazes de interagir com o investigado durante a coleta da prova. É possível, entretanto, que a participação do investigador seja ativa, podendo interagir com o investigado por meio de dispositivo eletrónico, utilizado de maneira remota e encoberta.

Assim como acontece com o agente infiltrado, cuja implementação pelo órgão investigador pode acontecer antes do início do *iter criminis* visando evitar a prática delitiva ou reunir provas que venha a ajudar a descoberta da verdade, a previsão legal para utilização de *malware* na investigação da criminalidade organizada tem a mesma finalidade, parte dos mesmos pressupostos e pode atingir os mesmos fins, de maneira mais eficaz e segura para os agentes do Estado.

A inclusão no Código de Processo Penal Português de capítulo específico, no Livro III que trata da Prova, dentro do Título III que disciplina os Meios de Obtenção de Prova, que trate dos Meios Ocultos de Obtenção de Prova, se apresenta como solução possível para sistematizar esse tipo de método de obtenção de prova, que já vem disciplinado em legislação esparsa, como a Lei do Cibercrime (Lei n.º 109/2009) e a Lei de Acções Encobertas (Lei n.º 101/2001).

Essa inclusão em capítulo próprio, tem ainda a vantagem de poder inserir um novo tipo de método oculto de obtenção de prova - a utilização de *malware* como agente infiltrado -

que reúne características previstas em ambas as leis citadas anteriormente, mas não é por nenhuma delas previsto, nem regulado, exigindo portanto disciplina própria, específica.

Ao questionamento quanto a possibilidade de utilização deste método oculto de obtenção de prova, pois tal violaria direitos fundamentais do cidadão, a construção da resposta passa pelo sopesamento dos interesses que entram em colisão e que são considerados importantes pela sociedade. Para essa análise são utilizados os princípios constitucionais e, instrumentalmente, os postulados da ponderação e da proporcionalidade.

Deste processo de ponderação em virtude da colidência entre princípios constitucionais, ante o risco da criminalidade cada dia mais organizada e que utiliza métodos sofisticados para a prática de delitos, o direito a segurança tem assumido papel de expressivo destaque. A busca por maior segurança, tem justificado a utilização de métodos de prova que estejam em compasso com os avanços tecnológicos, que já são adotados pela criminalidade organizada.

É possível concluir que o risco, a sensação de insegurança e medo hoje impregnados na sociedade são influenciados tanto pela criminalidade de massa, quanto pela constatação da existência de organizações criminosas e seus métodos de atuação.

A adoção pelos agentes estatais de métodos tecnológicos de investigação, hábeis a enfrentar o crime organizado em igualdade de condições, pode evitar a prática de delitos, agilizar o processo de persecução penal, apresentando assim respostas mais efetivas em seu combate.

Não se trata de legitimar o Estado para uso de técnicas criminosas, o que se pretende é atualizar os métodos de obtenção de provas, para adequá-los aos avanços tecnológicos alcançados pela sociedade e que com competência já utilizados pelas organizações criminosas em favor de seus objetivos delitivos.

**REFERÊNCIAS BIBLIOGRÁFICAS**

ADORNO, Sérgio; SALLA, Fernando. **Criminalidade organizada nas prisões e os ataques do PCC**. Estudos avançados, v. 21, n. 61, p. 7-29, 2007. disponível em: <<http://www.scielo.br/pdf/ea/v21n61/a02v2161>>, acessado em 08.08.17

ALESSI, Gil, **Família do Norte, a facção que fez a guerra entre o PCC e o Comando Vermelho**, Jornal El País, publicado em 01.11.2016, disponível em: <[https://brasil.elpais.com/brasil/2016/10/25/politica/1477406310\\_192891.html](https://brasil.elpais.com/brasil/2016/10/25/politica/1477406310_192891.html)>

ALESSI, Gil. **Rebeliões sinalizam fim de pacto entre PCC e CV e espalham tensão em presídios**, Jornal El País, publicado em 20.10.2016, disponível em: <[https://brasil.elpais.com/brasil/2016/10/17/politica/1476734977\\_178370.html](https://brasil.elpais.com/brasil/2016/10/17/politica/1476734977_178370.html)>

ALEXY, Robert. **Teoria dos Direitos Fundamentais**. Tradução Virgílio Afonso da Silva. São Paulo: Malheiros Editores, 2008

ALVES, Catarina Abegão. **Agente Infiltrado ou Provocador? Um Problema de Proibição de Prova à Luz do Caso Teixeira de Castro v. Portugal**. In Revista de Concorrência e Regulação. Coimbra: Almedina, Ano IV, número 16, outubro-dezembro 2013

AMBOS, Kai. **Derecho Procesal Penal Contemporáneo**. San Jose C.R.: Editorial Jurídica Continental, 2011

AMBOS, Kai e ROMERO, Eneas **Crime Organizado**, Análise da Lei 12.850/2013: São Paulo. Ed. Marcial Pons, 2017

AMORIM, Carlos. **CV-PCC: A irmandade do crime**. Rio de Janeiro: Record, 2004.

AMORIM, Carlos. **Comando Vermelho: a estória secreta do crime organizado**, 4ª ed.: Rio de Janeiro Record, 1994

ANDRADE, Manuel da Costa. **Bruscamente no Verão Passado**. Coimbra: Coimbra Editora, 2009

ANDRADE, Manuel da Costa. **Sobre as Proibições de Prova em Processo Penal**. Coimbra: Coimbra Editora, 2006

ALBUQUERQUE, Marcelo Schirmer. **A Garantia de Não Auto-Incriminação Extensão e Limites**. Belo Horizonte: Del Rey, 2008

ALBUQUERQUE, Paulo Pinto. **O Crime de Organização Criminosa no Código Penal Português**. In: AMBOS, Kai e ROMERO, Eneas **Crime Organizado**, Análise da Lei 12.850/2013: São Paulo. Ed. Marcial Pons, 2017

ALTIERI, Andrea Baiguera. **Le intercettazioni a mezzo captatore informatico** - 4 ottobre 2021. Disponível em <https://www.diritto.it/le-intercettazioni-a-mezzo-captatore-informatico/> Acesso em 23.11.2021

ASHOK, India. **Playpen: US DoJ drops child porn case against Jay Michaud to keep Tor hack source code secret.** Disponível em: <https://www.ibtimes.co.uk/playpen-us-doj-drops-child-porn-case-against-jay-michaud-keep-tor-hack-source-code-secret-1609919>. Acesso em 18.11.2021

ÁVILA, Humberto. **Teoria dos Princípios**: São Paulo, Malheiros Editores Ltda, 2006

AZEVEDO, Rodrigo Ghiringhelli. **Sociologia e Justiça Penal. Teoria e Prática da Pesquisa Sociocriminológica**: Rio de Janeiro. Editorial Lumen Juris, 2010

BARBOSA, Paula Andrea. **Nuevas Tendencias Politico-Criminales en La Lucha Contra La Criminalidad Organizada.** in Crimen Organizado: Lima. ARA Editores E.I.R.L, 2009

BARROSO, Luís Roberto e BARCELLOS, Ana Paula de. **O começo da história. A nova interpretação constitucional e o papel dos princípios no direito brasileiro.** Disponível em: <[http://xa.yimg.com/kq/groups/22830878/36505266/name/texto\\_principios\\_constitucionais\\_barroso.pdf](http://xa.yimg.com/kq/groups/22830878/36505266/name/texto_principios_constitucionais_barroso.pdf)>

BAUMAN, Zygmunt, **Globalização: as conseqüências humanas.** Tradução Marcus Penchel. Rio de Janeiro: Jorge Zahar Ed., 1999

BECCARIA, Cesare. **Dos Delitos e das Penas.** Tradução Paulo M. Oliveira. Ed. Ediouro: Rio de Janeiro, 1992

BBC . Ruptura entre PCC e Comando Vermelho pode gerar 'carnificina', diz pesquisadora, publicada em 18.10.2016. Disponível em: <<http://ultimosegundo.ig.com.br/brasil/2016-10-18/pcc-comando-vermelho-ruptura.html>>

BECK, Francis Rafael. **Perspectivas de controle ao crime organizado e crítica à flexibilização das garantias**: São Paulo. IBCCrim, 2004

BECK, Ulrich. **La sociedad del riesgo**: Barcelona. Paidós, 1998

BORGES, Paulo César Corrêa. **Crime Organizado.** São Paulo: Associação Paulista do Ministério Público, 2000

BOSSLER, Adam M., HOLT, Thomas J. **On-line Activities, Guardianship, and Malware Infection: An Examination of Routine Activities Theory** International Journal of Cyber Criminology (IJCC) January - June 2009, Vol 3 (1): 400–420. Disponível em [https://www.researchgate.net/publication/228929213\\_On-line\\_Activities\\_Guardianship\\_and\\_Malware\\_Infection\\_An\\_Examination\\_of\\_Routine\\_Activities\\_Theory](https://www.researchgate.net/publication/228929213_On-line_Activities_Guardianship_and_Malware_Infection_An_Examination_of_Routine_Activities_Theory). Acesso em 15.12.2021

BRANCO, José António. **Criminalidade Organizada, Instrumentos e Mecanismos Legais de Investigação e Recuperação de Activos. “Uma Breve Incursão”**. In Terra de Lei, nº 2. Lisboa: Vigaprintes, 2012

BRAZ, José. **Ciência, Tecnologia e Investigação Criminal**. Interdependências e Limites num Estado de Direito Democrático: Coimbra. Almedina, 2015

BRAZ, José. **Investigação Criminal. A organização, o método e a prova. Os desafios da nova criminalidade**: Coimbra. Almedina, 2013

BRENNER, Susan W. e KOOPS, Bert-Jaap. **Approaches to Cybercrime Jurisdiction**, In **Journal of High Technology Law**, vol. 4, 2005. disponível em [https://www.researchgate.net/publication/228198888\\_Approaches\\_to\\_Cybercrime\\_Jurisdiction](https://www.researchgate.net/publication/228198888_Approaches_to_Cybercrime_Jurisdiction)

BRENNER, Susan W. e SCHWERHA, Joseph J. IV, **Transnational Evidence Gathering and Local Prosecution of International Cybercrime**, 20 J. Marshall J. Computer & Info. L. 347 (2002), disponível em <https://repository.law.uic.edu/cgi/viewcontent.cgi?article=1139&context=jitpl>

BROADHURST, Roderic e CHANG, Lennon. (2013). **Cybercrime in Asia: Trends and Challenges**. In **Asian Handbook of Criminology**. Nova York: Springer, 2013. Disponível em [\(PDF\) Cybercrime in Asia: Trends and Challenges \(researchgate.net\)](#)

CABETTE, Eduardo Luis Santos; NAHUR, Marcius Tadeu Maciel. **Criminalidade organizada & globalização desorganizada**. Rio de Janeiro: Editora Freitas Bastos, 2014

CALDAS, André Moz. **A Magistratura dos Censores e o Combate à Corrupção em Roma**. Lisboa: AAFDL, 2017

CALLEGARI, André Luis. **Control Social y Criminalidad Organizada in Crimen Organizado**: Lima. ARA Editores E.I.R.L, 2009

CANCELA, Alberto Gil Lima. **A Prova Digital: Os Meios de Obtenção de Prova na Lei do Cibercrime**. Disponível em: <<https://estudogeral.sib.uc.pt/jspui/bitstream/10316/31398/1/A%20prova%20digital.pdf>>

CANOTILHO, José Joaquim Gomes. **Direito Constitucional e Teoria da Constituição**. Coimbra: Ed. Almedina, 2003

**CARTILHA DE SEGURANÇA PARA INTERNET**. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT). Disponível em: <https://cartilha.cert.br/malware/#footnote003>

CASTRO, Lola Anyar de. **Formas de Delinquencia Organizada em America Latina**, la Simbologia del Narcotráfico e das Técnicas de Control. São Paulo: Revista Brasileira de Ciências Criminais nº 112, 2015

CLOUGH, Jonathan. **Cybercrime**: Sydney. Commonwealth Law Bulletin, vol. 37, nº 4, December 2011, 671-680. Disponível em <https://heinonline.org/HOL/LandingPage?handle=hein.journals/commwlb37&div=61&id=&page=>

CONSELHO DA UNIÃO EUROPÉIA. **Acção Comum**, 21.12.1998. Disponível em: <<http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:31998F0733>>

CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO. **Ministério Público: um retrato: dados de 2016, Volume IV**. Brasília: CNMP 2017, disponível em: <[http://www.cnmp.mp.br/portal/images/Anu%C3%A1rio\\_um\\_retrato\\_2017\\_internet.pdf](http://www.cnmp.mp.br/portal/images/Anu%C3%A1rio_um_retrato_2017_internet.pdf)>

CORREIA, João Conde. **Prova Digital**: as leis que temos e a lei que devíamos ter. Lisboa: Revista do Ministério Público nº 139, Ano 35, Junho-Setembro 2014

COSTA, Álvaro Mayrink da. **Temas de Direito Penal**: Rio de Janeiro. Editora Lumen Juris, 2011

COSTA, José de Faria. **Direito Penal e Globalização**. Coimbra: Wolters Kluwer Portugal. Coimbra Editora, 2010

COX, Joseph. **"Operation Pacifier" is larger in scope than most anyone believed**. Disponível em <https://perma.cc/WG6R-TEGU>.

CPI – TRÁFICO DE ARMAS, Número: 0871R/06, Câmara dos Deputados, Brasília, em 08.06.2006, disponível em: <[http://www1.folha.uol.com.br/folha/cotidiano/20060708-marcos\\_camacho.pdf](http://www1.folha.uol.com.br/folha/cotidiano/20060708-marcos_camacho.pdf)>

CHRISTINO, Márcio Sérgio: **Rebeliões não estão relacionadas às más condições das cadeias ou superlotação**: Consultor Jurídico, ISSN 1809-2829, <<http://www.conjur.com.br/2017-jan-16/marcio-christino-rebelioes-nao-relacionadas-superlotacao>>

CUNHA, Rogério Sanches e PINTO, Ronaldo Batista. **Crime Organizado**: Salvador, Editora JusPodium, 2015

CRUZ, Elaine Patrícia. **Crimes de maio causaram 564 mortes em 2006; entenda o caso**. Disponível em: <http://agenciabrasil.ebc.com.br/direitos-humanos/noticia/2016-05/crimes-de-maio-causaram-564-mortes-em-2006-entenda-o-caso>

DAMASCENO, Leandro et al. **A Lei nº 9.034/95 e as Organizações Criminosas Brasileiras**. THEMIS: Revista da Esmec, v. 11, p. 267-280, 2016. disponível em: <<http://revistathemis.tjce.jus.br/index.php/THEMIS/article/view/70/69>>

DALLAGNOL, Deltan. **A Luta Contra a Corrupção**: Rio de Janeiro. Editora Primeira Pessoa, 2017

DAVIES, Gemma. **Shining a Light on Policing of the Dark Web: An Analysis of UK Investigatory Powers**. The Journal of Criminal Law 2020, Vol. 84 (5) 407–426. Disponível

em [Shining a Light on Policing of the Dark Web: An Analysis of UK Investigatory Powers \(sagepub.com\)](http://Shining a Light on Policing of the Dark Web: An Analysis of UK Investigatory Powers (sagepub.com))

**DELINCUENCIA informática.** Tiempos de cautela y amparo: Cizur Menor (Espanha). Thomson Reuters Editorial Aranzadi, 2012

DIAS, Augusto Silva. “**Delicta in Se**” e “**Delicta Mere Prohibita**”. Coimbra: Coimbra Editora, 2008

DIAS, Augusto Silva. **Criminalidade Organizada e combate ao lucro ilícito** In 2º Congresso de Investigação Científica: Coimbra. Almedina, 2010

DIAS, Augusto Silva e RAMOS, Vânia Costa. **O direito à não auto-inculpação (nemo tenetur se ipsum accusare) no processo penal e contra-ordenacional português.** Coimbra: Coimbra Editora, 2009

DIAS, Camila Caldeira Nunes. **Ocupando as brechas do direito formal: O PCC como instância alternativa de resolução de conflitos**, in Dilemas Revista de Estudos de Conflito e Controle Social, vol. 2, n. 4: Rio de Janeiro, 2009, disponível em: <<https://revistas.ufrj.br/index.php/dilemas/article/view/7165/5744>>

DIAS, Camila Caldeira Nunes. **Da pulverização ao monopólio da violência: expansão e consolidação do Primeiro Comando da Capital (PCC) no sistema carcerário paulista.** 2011. Tese de Doutorado. Universidade de São Paulo, disponível em: <<http://www.teses.usp.br/teses/disponiveis/8/8132/tde-13062012-164151/en.php>>

DIAS, Jorge de Figueiredo. **Criminalidade Organizada** in Revista Brasileira de Ciências Criminais, n. 71: São Paulo. Editora Revista dos Tribunais, 2008

DIAS, Jorge Figueiredo e ANDRADE, Manuel da Costa. **Supervisão, direito ao silêncio e legalidade da prova.** Coimbra: Ed. Almedina, 2006

DOELITZSCHER, Frank; REICH, Christoph; KNAHL, Martin e CLARKE, Nathan. **Understanding Cloud Audits In Privacy and Security for Cloud Computing.** Londres: Ed. Springer, 2013

DOYLE, Charles. **Cybercrime: An Overview of The Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws.** Congressional Research Service, 2011

DURÁN, Manuel Carrasco. **Medidas Antiterroristas y Constitución, tras el 11 de Septiembre de 2001.** In ROYO, Javier Pérez e DURÁN, Manuel Carrasco. **Terrorismo, democracia y seguridad, en perspectiva constitucional.** Madrid: Marcial Pons, 2010.

DURKHEIM, Émile. **As Regras do Método Sociológico.** São Paulo. Companhia Editora Nacional, 1976

DWORKIN, Ronald. **Levando os Direitos a Sério**. Tradução Nelson Boeira. 2ª edição. São Paulo: Martins Fontes, 2007

EDWARDS, Lilian. **The Fall an the Rise of Intermediary Liability Online** In EDWARDS, Lilian, WAELDE, Charlotte, **Law and the Internet**. Oxford/Portland: Hart Publishing, 2009

ERBSCHELO, Michael. **Trojans, Worms and Spyware. A Computer Security Professional's Guide to Malicious Code**. Burlington (USA): Elsevier Butterworth-Heinemann, 2005

EUROPEAN COURT OF HUMAN RIGHTS. **Guide on Article 6 of the European Convention on Human Rights**, 2014, pág. 24, disponível no endereço eletrônico: <[https://www.echr.coe.int/Documents/Guide\\_Art\\_6\\_criminal\\_ENG.pdf](https://www.echr.coe.int/Documents/Guide_Art_6_criminal_ENG.pdf)>

EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE (ETSI), disponível no sítio: <<http://www.etsi.org/technologies-clusters/technologies/smart-cards/sim>>

FABRETTI, Humberto Barrionuevo. **Segurança Pública**. Fundamentos Jurídicos para uma abordagem Constitucional. São Paulo: Editora Atlas, 2014

FERRAJOLI, Luigi. **A soberania no mundo moderno**. Tradução Carlo Cocciolli e Márcio Lauria, 2ª ed. São Paulo: Martins Fontes, 2007

FERRAJOLI, Luigi. **Derecho y Razón**. Madrid: Editorial Trotta, 2000

FERRO, Ana Luiza Almeida. **Crime Organizado e Organizações Criminosas Mundiais**. Curitiba: Juruá, 2012

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. **Atlas da Violência**. Disponível em: [http://www.forumseguranca.org.br/wpcontent/uploads/2018/06/FBSP\\_atlas\\_violencia\\_2108\\_Infografico.pdf](http://www.forumseguranca.org.br/wpcontent/uploads/2018/06/FBSP_atlas_violencia_2108_Infografico.pdf)

GERCKE, Marco. **Understanding Cybercrime: A Guide for Developing Countries**, Genebra: ITU, 2012. Disponível em [ITU Publication on Understanding Cybercrime: A Guide for Developing Countries](#)

GNAUER, Herbert **Weshalb der sogenannte Bundestrojaner eine schlechte Idee ist Gedanken angesichts eines zunehmenden Überwachungspopulismus**. Medienimpulse ISSN 2307-3187 Jg. 55, Nr. 3, 2017 Lizenz: CC-BY-NC-ND-3.0-AT . Disponível em: <file:///C:/Users/visitante/Downloads/1722-Artikeltext-1330-1-10-20190502.pdf>. Acesso em 26.11.2021

GOMES, José Carlos. **O Estado Democrático de Direito e o Terrorismo**. In Repressão Penal e Crime Organizado: São Paulo. Quartier Latin, 2009

GONZALEZ-CASTELL, Adán Carrizo. **El Agente Infiltrado en España y Portugal**. In VALENTE, Manuel Monteiro Guedes. **Criminalidade Organizada e Criminalidade de Massa**. Coimbra: Edições Almedina S.A., 2009

HANNAN, Mathew. **To revisit: What is forensic computing?**. In Australian Computer, Network & Information Forensics Conference. 2004. p. 103-111. Disponível em: <<https://pdfs.semanticscholar.org/7fc8/d1c9d7fbd7368685368954c24fc20139cc2>>., acessado em 23.08.17

HASSEMER, Winfried. **El Derecho Penal del Estado de Derecho en los Tiempos de Terrorismo** in ALFARO, Luis Reyna e TERÁN, Sergio Cuaresma. **Derecho Penal y Estado de Derecho**: Buenos Aires. Editorial B de f, 2008

HASSEMER, Winfried. **Direito Penal Libertário**: Belo Horizonte. Editora Del Rey, 2007

HASSEMER, Winfried. **A Segurança Pública no Estado de Direito**: Lisboa. Associação Académica da Faculdade de Direito de Lisboa, 1995

JACOBSSON, Andreas; BOLDT, Martin; CARLSSON, Bengt. **Privacy-Invasive Software in Filesharing Tools**. In Information Security Management, Education and Privacy. Springer, Boston, MA, 2004. p. 281-296. disponível no site: <[https://link.springer.com/content/pdf/10.1007%2F1-4020-8145-6\\_22.pdf](https://link.springer.com/content/pdf/10.1007%2F1-4020-8145-6_22.pdf)>

JESUS, Francisco Marcolino de. **Os Meios de Obtenção da Prova em Processo Penal**. Coimbra: Edições Almedina S.A., 2011

JUSTIÇA GLOBAL E CLÍNICA INTERNACIONAL DE DIREITOS HUMANOS DA UNIVERSIDADE DE DIREITO DE HARVARD. **São Paulo sob a chapeleto: Corrupção, Crime Organizado e Violência Institucional em maio de 2006**, disponível no sítio: <<http://hrp.law.harvard.edu/wp-content/uploads/2011/05/full-with-cover.pdf>>

KERR, Orin S. **Searches And Seizures In A Digital World** In *Harvard Law Review*, v. 119, p. 531-585, 2005. Disponível em [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=697541](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=697541)

KERR, Orin S. **The Problem of Perspective in Internet Law**. In *Georgetown Law Journal*, Vol. 91, p. 357-405, February 2003. Disponível em <https://heinonline.org/HOL/LandingPage?handle=hein.journals/glj91&div=17&id=&page=>

LABORATÓRIO DE ANÁLISE DA VIOLÊNCIA DA UNIVERSIDADE ESTADUAL DO RIO DE JANEIRO. **Análise dos Impactos dos Ataques do PCC**. Coordenação CANO, Ignácio. Disponível em: <http://ponte.cartacapital.com.br/crimes-de-maio-completam-9-anos-564-pessoas-morreram/>

LAMA, Dalai: **Uma Ética para o Novo Milênio**. Tradução Maria Luiza Newlands. Rio de Janeiro: Sextante, 2000

LLINARES, Fernando Miró, **El Cibercrimen Fenomenología Y Criminología De La Delincuencia En El Ciberespacio**: Madrid. Marcial Pons, 2012

LLOYD, Ian J. **Information Technology Law**, 9.<sup>a</sup> ed. Oxford: Oxford University Press, 2020

LOURENÇO, Nelson. **Segurança, Sentimento de Insegurança e Estado de Direito. O Espectro axial da relação Direitos, Liberdades e Garantias e Poderes do Estado.** 2009

MACHADO, Marta Rodriguez de Assis. **Sociedade de Risco e Direito Penal:** São Paulo. IBCCRIM, 2005

MALMESBURY, Thomas Hobbes de. **Leviatã ou matéria, forma e poder de um estado eclesiástico e civil.** Coleção **Os pensadores**, vol. XIV. Tradução João Paulo Monteiro e Maria Beatriz Nizza da Silva. São Paulo: Abril cultural, 1974

MANGIAMELI, Agata C. Amato. "Theory of Law and Computer Crimes – Teoria do Direito e Crimes Informáticos" *In* Duc In Altum-Cadernos de Direito v. 8, n.16, set-dez 2016,(2017), pág.6. Disponível em: <<http://www.faculdedamas.edu.br/revistafd/index.php/cihjur/article/view/395/379>> acessado em 06.07.17

MANTELERO, Alessandro; VACIAGO, Giuseppe. **Data protection in a big data society. Ideas for a future regulation.** *In* **Digital Investigation**, v. 15, p. 104-109, 2015. Disponível em: [https://d1wqtxtslxzle7.cloudfront.net/41265404/Mantelero-Vaciago\\_Big\\_data\\_privacy\\_PREPRINT-with-cover-page-v2.pdf?Expires=1632434885&Signature=E388VvvZ5VsucMEgqxTruobxDcQSW24AjRQ3uw~MqFK2PUMGddV-2kiaWf5CijaS7DM8gH~PxIJfpjK6sGbsudpabChlaAjTE3y8WNIQ0MhB6XwSr9VeTZIADdbKsCy4IAshBP67Qp8~RUHE6JqdNNL0Rn-KzPtTg3VAdAxjqDz1QayR0-OjfpnA\\_\\_&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA](https://d1wqtxtslxzle7.cloudfront.net/41265404/Mantelero-Vaciago_Big_data_privacy_PREPRINT-with-cover-page-v2.pdf?Expires=1632434885&Signature=E388VvvZ5VsucMEgqxTruobxDcQSW24AjRQ3uw~MqFK2PUMGddV-2kiaWf5CijaS7DM8gH~PxIJfpjK6sGbsudpabChlaAjTE3y8WNIQ0MhB6XwSr9VeTZIADdbKsCy4IAshBP67Qp8~RUHE6JqdNNL0Rn-KzPtTg3VAdAxjqDz1QayR0-OjfpnA__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA). Acesso em 23/09/2021

MASON, Stephen; SENG, Daniel. **Electronic Evidence and Electronic Signatures.** Fifth edition published by the Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2021 Disponível em: <https://humanities-digital-library.org/index.php/hdl/catalog/view/electronic-evidence-and-electronic-signatures/214/408-1> p. 398. Acesso em 18.11.2021

MASSON, Cleber e MARÇAL, Vinícius. **Crime Organizado.** São Paulo: Editora Método, 2017

MATA, Federico Bueno de. **El Agente Encubierto En Internet: Mentiras Virtuales Para Alcanzar La Justicia.** 2012 Disponível em [https://ruc.udc.es/dspace/bitstream/handle/2183/9179/comunicacions\\_01\\_Bueno\\_de\\_Mata\\_295-306.pdf](https://ruc.udc.es/dspace/bitstream/handle/2183/9179/comunicacions_01_Bueno_de_Mata_295-306.pdf).

MAZZILLI, Hugo Nigro. **Introdução ao Ministério Público.** São Paulo: Saraiva, 2002, 4ª ed.

MCCULLAGH, Declan. **FBI taps cell phone mic as eavesdropping tool.** Disponível em: [http://news.com.com/2102-1029\\_3-6140191.html?tag=st.util.print](http://news.com.com/2102-1029_3-6140191.html?tag=st.util.print) (1 of 4)12/5/2006 8:20:16, acesso em 18.11.2021

MELIÁ, Manuel Cancio. **El Injusto de Los Delitos de Organización: Peligro y Significado** in *Crimen Organizado*: Lima. ARA Editores E.I.R.L, 2009

MELIÁ, Manuel Cancio. **Internacionalização do Direito Penal e da política criminal: algumas reflexões sobre a luta jurídico-penal contra o terrorismo**. PANOPTICA (em reformulação), v. 4, n. 3, p. 01-22, 2009.

MENDRONI, Marcelo Batlouni. **Crime Organizado**: São Paulo. Editora Atlas, 2012

MENDES, Paulo Sousa. **Lições de Direito Processual Penal**. Coimbra: Almedina, 2014

MENDES, Paulo Sousa. **O Processo Penal entre Eficácia e Garantias**. In *Direito da Investigação Criminal e da Prova*. Coimbra: Almedina, 2014,

MENEZES, Sofia Saraiva de. **O Direito ao Silêncio: A Verdade por Trás do Mito**. in BELEZA, Tereza Pizarro; PINTO, Frederico de Lacerda Costa. **Prova Criminal e Direito de Defesa**. Coimbra: Almedina, 2013

MIGUEL, Nuno Gonçalo Caseiro. **Globalização, crime organizado e terrorismo: que relação?**. In *Revista Negócios Estrangeiros*, abril, n. 14, publicação semestral do Instituto Diplomático do Ministério dos Negócios Estrangeiros, 2009

MILLARD, Cristopher. **Cloud Computing Law**: Oxford. Oxford University Press. Disponível em [https://www.researchgate.net/profile/Christopher-Millard-2/publication/269037199\\_Cloud\\_Computing\\_Law/links/5531016d0cf2f2a588ab843b/Cloud-Computing-Law.pdf](https://www.researchgate.net/profile/Christopher-Millard-2/publication/269037199_Cloud_Computing_Law/links/5531016d0cf2f2a588ab843b/Cloud-Computing-Law.pdf).

MINGARDI, Guaracy. **O Estado e o Crime Organizado**: São Paulo. IBCCrim, 1998

MINGARDI, Guaracy. **O trabalho da inteligência no controle do crime organizado. Estudos Avançados**, v. 21, n. 61, p. 55, 2007. Disponível em: <<https://www.revistas.usp.br/eav/article/view/10266/11898>>, acessado em 24.08.17

**MINISTÉRIO PÚBLICO**: um retrato: dados de 2016 Volume IV/ Conselho Nacional do Ministério Público. - Brasília: CNMP 2017, disponível no endereço: <[http://www.cnmp.mp.br/portal/images/Anu%C3%A1rio\\_um\\_retrato\\_2017\\_internet.pdf](http://www.cnmp.mp.br/portal/images/Anu%C3%A1rio_um_retrato_2017_internet.pdf)>

MIRANDA, Jorge. **Manual de Direito Constitucional, Tomo IV**. Coimbra: Coimbra Editora, 2008

MISSE, Michel. **Mercados ilegais, redes de proteção e organização local do crime no Rio de Janeiro**. São Paulo: Instituto de Estudos Avançados da Universidade de São Paulo, v. 21, 2007

MORAES, Carla Dias Caldas de. **A garantia contra a auto-incriminação e a produção de provas no Brasil e nos Estados Unidos** In 2º Curso de Introdução ao Direito Americano, Fundamentals of US Law Course, volume 1. Brasília: Advocacia Geral da União, 2012

MOREIRA, Rômulo de Andrade. **A Nova Lei do Crime Organizado**. Porto Alegre: Editora Magister, 2014

NETO, Mário Furlaneto; DO CARMO, Júlio César Lourenço; SCARMANHÃ Bruna de Oliveira da Silva Guesso. **Cookies: Vulnerabilidade do Direito à Privacidade nos Meios Digitais no Âmbito da Legislação Brasileira**. p.1501. Disponível em : [https://www.cidp.pt/revistas/rjlb/2018/4/2018\\_04\\_1491\\_1517.pdf](https://www.cidp.pt/revistas/rjlb/2018/4/2018_04_1491_1517.pdf).

NUCCI, Guilherme de Souza. **Organização Criminosa**. Rio de Janeiro: Editora Forense, 2017

OHM, Paul. **The Investigative Dynamics of the Use of Malware by Law Enforcement** *In William & Mary Bill of Rights Journal*, v. 26 (2017-2018). Disponível em <https://scholarship.law.wm.edu/wmborj/vol26/iss2/4>.

ONETO, Isabel. **O Agente Infiltrado**. Coimbra: Coimbra Editora, 2005

PAIXÃO, Antônio Luiz. **Recuperar ou Punir? Como o Estado trata o criminoso**: São Paulo. Cortez, 1987

PAJEK, Przemyslaw PIMENIDIS, Elias. **Computer Anti-Forensics Methods and their impact on Computer Forensic Investigation**, pág. 145 *in: JAHANKHANI H., HESSAMI A.G., HSU F. (eds) Global Security, Safety, and Sustainability. Communications in Computer and Information Science, vol 45. Springer, Berlin, Heidelberg, 2009*

PALMA, Maria Fernanda. **Direito Constitucional Penal**: Coimbra. Almedina, 2011

PALMA, Maria Fernanda. **Introdução ao Direito da Investigação Criminal e da Prova**. *In Direito da Investigação Criminal e da Prova*. Coimbra: Almedina, 2014, pág.

PARIZOT, Raphaële. **La Responsabilité Pénale à L'épreuve de La Criminalité Organisée**: Paris. Lextenso éditions, 2010

PEARSON, Siani. **Privacy, Security and Trust in Cloud Computing** *In Privacy and Security for Cloud Computing*. Londres: Ed. Springer, 2013

PELLEGRINI, Angiolo e COSTA, Jr., Paulo José da. **Criminalidade Organizada**. São Paulo: Ed. Atlas, 2008.

PEREIRA, Flávio Cardoso. **Crime Organizado e suas Infiltrações nas Instituições Governamentais**. São Paulo: Editora Atlas, 2015

PEREIRA, Flávio Cardoso. **El Agente Infiltrado desde el Punto de Vista del Garantismo Procesal Penal**. Curitiba: Juruá Editora, 2016

PEREIRA, Sandra. **A Recolha da Prova por Agente Infiltrado**. *In Prova Criminal e Direito de Defesa*. Coimbra: Edições Almedina S.A., 2013

PETRONE, Daniel, BASSO, Marina, EMILIOZZI, Agustina. **Phishing Attacks: Problemáticas de su Recepción en el Ordenamiento Local y Nuevos Desafíos.** In: DUPUY, Daniela e KIEFER, Mariana. **Cibercrimen:** Madrid. Editorial B de f, 2016

PINTO, Lara Sofia. **Privilégio Contra a Auto-Incriminação Versus Colaboração do Arguido** in BELEZA, Tereza Pizarro e PINTO, Frederico de Lacerda Costa. **Prova Criminal e Direito de Defesa.** Coimbra: Ed. Almedina, 2013

PORTO, Roberto. **Crime Organizado e Sistema Prisional:** São Paulo. Editora Atlas, 2008

PRADEL, Jean e DALLEST, Jacques. **La Criminalité Organisée.** Paris: LexisNevis, 2012

PRADILLO, Juan Carlos Ortiz. **“Hacking” legal al servicio de la investigación criminal:** nuevos instrumentos para la investigación y prueba de la delincuencia informática in **Delincuencia informática.** Tiempos de cautela y amparo: Cizur Menor (Espanha). Thomson Reuters Editorial Aranzadi, 2012

PRADO, Antônio Carlos. **Marcola versus Fernandinho Beira Mar.** Revista IstoÉ, publicado em 21.10.16, disponível no endereço: <<http://istoe.com.br/marcola-versus-fernandinho-beira-mar>>

PROGRAMA DE LAS NACIONES UNIDAS PARA EL DESARROLLO (PNUD). **Informe sobre Desarrollo Humano para América Central, IDHAC 2009-2010.** Colombia: Dvinni S.A., 2009, pág. 30, disponível no endereço eletrônico: <[http://www.latinamerica.undp.org/content/dam/rblac/docs/Research%20and%20Publications/Central\\_America\\_RHDR\\_2009-10\\_ES.pdf](http://www.latinamerica.undp.org/content/dam/rblac/docs/Research%20and%20Publications/Central_America_RHDR_2009-10_ES.pdf)>

QUEIJO, Maria Elizabeth. **O Direito de Não Produzir Prova Contra Si Mesmo.** São Paulo: Saraiva, 2012

RAMALHO, David Silva. **A Investigação Criminal na Dark Web** in **Revista de Concorrência e Regulação.** Coimbra, a.4 n.14-15 (Abr.-Set. 2013)

RAMALHO, David Silva. **A recolha de Prova Penal em Sistemas de Computação em Nuvem.** p. 143 In: **Revista de Direito Intelectual,** Coimbra: Almedina, nº 02, dezembro de 2014

RAMALHO, David Silva. **Métodos Ocultos de Investigação Criminal em Ambiente Digital.** Coimbra: Edições Almedina, 2017

RAMALHO, Davi Silva. **O uso de malware como meio de obtenção de prova em processo penal** in **Revista de Concorrência e Regulação.** Coimbra: Almedina, Ano IV, número 16, outubro-dezembro 2013

RAMÍREZ, Paula Andrea. **Nuevas Tendencias Político-Criminales en la Lucha contra la Criminalidad Organizada.** In **Crimen Organizado.** Lima: ARA Editores, 2009

RAMOS, Vânia Costa. **Corpus Iuris 2000** Imposição ao arguido de entrega de documentos para provas e *nemo tenetur se ipsum accusare* Parte I in Revista do Ministério Público, nº 108

REED, Chris. **Internet Law Text and Materials**: Cambridge. Cambridge University Press, 2004

RIBEIRO, Aline e CORREA, Hudson. **O violento plano de expansão no Paraguai da maior facção brasileira**. Revista Época, publicado em 26.06.2017, atualizado em 24.07.2017, disponível no endereço:

<http://epoca.globo.com/brasil/noticia/2017/06/o-violento-plano-de-expansao-no-paraguai-da-maior-faccao-brasileira.html>

ROBLES, Diego Torrente. **La Inseguridad creada por la Delincuencia Económica Transnacional** in PUIG, Santiago Mir e Queralt Joan J. **La Seguridad Pública ante el Derecho Penal**. Buenos Aires: Euros Editores S.R.L, 2010

ROCHA, Lyvia. **PCC acusa Comando Vermelho por fim de pacto de paz**, Tribuna do Ceará, publicado em 19.10.2016, disponível no endereço: <<http://tribunadoceara.uol.com.br/noticias/segurancapublica/pcc-acusa-comando-vermelho-por-fim-de-pacto-de-paz/>>

RODRIGUES, Alan. **Como nasceram as facções**. Revista Istoé, postado em 24.05.2016, disponível no endereço [http://istoe.com.br/22098\\_COMO+NASCERAM+AS+FACCOES/](http://istoe.com.br/22098_COMO+NASCERAM+AS+FACCOES/)

ROYO, Javier Pérez. **La Democracia Frente al Terrorismo Global**. In ROYO, Javier Pérez e DURÁN, Manuel Carrasco. **Terrorismo, democracia y seguridad, en perspectiva constitucional**. Madrid: Marcial Pons, 2010.

RYAN, Daniel J., SHPANTZER, Gal. **Legal Aspects of Digital Forensics**. Disponível em <http://euro.ecom.cmu.edu/program/law/08-732/Evidence/RyanShpantzer.pdf>, acesso em 18.11.2021

SALLA, Fernando. **Considerações Sociológicas sobre o crime organizado no Brasil**. In Revista Brasileira de Ciências Criminais, ano 16 n. 71: São Paulo. Editora Revista dos Tribunais, 2008

SÁNCHEZ, Alfredo Chirino. **La Seguridad como un topos discursivo en la política criminal centroamericana**. Perspectivas de una desesperanza in ALFARO, Luis Reyna e TERÁN, Sergio Cuaresma. **Derecho Penal y Estado de Derecho**: Buenos Aires. Editorial B de f, 2008

SANTOS, Cristina Máximo dos. **As Novas Tecnologias da Informação e o Sigilo das Telecomunicações** In Revista do Ministério Público: Lisboa, Ano 25º, nº 99, (p.89 a 116), julho-setembro 2004

SCHILLING, Flávia. **Corrupção, crime organizado e democracia**. Revista Brasileira de Ciências Criminais, São Paulo, v. 36, 2001.

Scientific Working Group on Digital Evidence – SWGDE, disponível no sítio: <<https://www.swgde.org>>

SEÑA, Jorge F. Malem. **Globalización, comercio internacional y corrupción**. Barcelona: Editorial Gedisa, 2000

SIEBER, Ulrich. **Instruments of International Law: Against Terrorist Use of the Internet** *In* WADE, Marianne e MALJEVIĆ, Almir. **War on Terror?:** New York. Spring, 2010

SIEBER, Ulrich. **La Tutela Penale Dell’Informazione** *In* **Rivista Trimestrale di Diritto Penale dell’Economia**, anno IV: Padova. Casa Editrice CEDAM, 1991.

SIEBER, Ulrich. **Responsabilità Penali per la Circolazione di Dati nelle Reti Internazionali di Computer** *In* **Rivista Trimestrale di Diritto Penale dell’Economia**, anno X: Padova. Casa Editrice CEDAM, 1998

SILVA, Germano Marques da. **Curso de Processo Penal vol. II**. Lisboa: Babel, 2011

SILVA, Virgílio Afonso da. **O proporcional e o razoável**. Revista dos Tribunais 798 (2002): 23-50. Disponível em <https://revistas.unifacs.br/index.php/redu/article/view/1495>

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**. Disponível em: <<http://repositorio.ucp.pt/bitstream/10400.14/21854/1/Tese%20final%2028%20Mar%20C3%A7o.pdf>>, acessado em 06.07.17

STIENNON, Richard. **Surviving Cyber War**: Lanham. The Scarecrow Press, 2010

STOCHERO, Tahiane. **Entenda: o que a disputa nacional entre facções tem a ver com a barbárie no presídio do Amazonas**, postado em 03.01.2017, disponível em: <<http://g1.globo.com/am/amazonas/noticia/entenda-o-que-a-disputa-nacional-entre-faccoes-tem-a-ver-com-a-barbarie-no-presidio-do-amazonas.ghtml>>

TEMPERINI, Marcelo, MACEDO, Maximiliano, **Nuevas Herramientas de Investigación Penal: El Agente Encubierto Digital** *in* DUPUY, Daniela e KIEFER, Mariana, **Cibercrimen**. Madrid: B de F Ltda, 2016

TEUBNER, Gunther. **O Direito como Sistema Autopoiético**. Tradução de José Engrácia Antunes. Lisboa: Fundação Calouste Gulbekian, 1989

TIEDEMANN, Klaus *in* ROXIN, Claus, ARTZ, Gunther e TIEDEMANN, Klaus. **Introdução ao Direito Penal e ao Direito Processual Penal**. Belo Horizonte: Del Rey, 2007

UNITED NATIONS OFFICE ON DRUGS AND CRIME. **United Nations Convention Against Transnational Organized Crime and the Protocols Thereto**, em 15.12.2004, disponível no endereço: <<http://www.unodc.org/documents/treaties/untoc/publications/toc>>

%20convention/tocebook-e.pdf>

UNITED NATION DEVELOPMENT PROGRAMME (UNDP). **Human Development Report 1994**. Nova York: Oxford University Press, 1994, pág. 3, disponível no endereço eletrônico:

<[http://hdr.undp.org/sites/default/files/reports/255/hdr\\_1994\\_en\\_complete\\_nostats.pdf](http://hdr.undp.org/sites/default/files/reports/255/hdr_1994_en_complete_nostats.pdf)>

VACIAGO, Giuseppe e RAMALHO, David Silva. **Online searches and online surveillance: the use of trojans and other types of malware as means of obtaining evidence in criminal proceedings**. In **Digital Evidence & Elec. Signature L. Rev.**, v. 13, págs. 88-96, 2016

VALENTE, Manuel Monteiro Guedes. **Criminalidade Organizada e Criminalidade de Massa**. Coimbra: Edições Almedina S.A., 2009

VALENTE, Manuel Monteiro Guedes. **A Investigação do Crime Organizado** In VALENTE, Manuel Monteiro Guedes. **Criminalidade Organizada e Criminalidade de Massa**. Coimbra: Edições Almedina S.A., 2009

VALENTE, Manuel Monteiro Guedes. **Direito Penal do Inimigo e o Terrorismo**. Coimbra: Almedina, 2010

VERDELHO, Pedro. **A Obtenção de Prova no Ambiente Digital** In **Revista do Ministério Público**: Lisboa, Ano 25º, nº 99, (p.117 a 136), julho-setembro 2004.

VERDELHO, Pedro. **Obtenção de prova online** in DUPUY, Daniela e KIEFER, Mariana, **Cibercrimen**. Madrid: B de F Ltda, 2016

WINTER, Lorena Bachmaier. **Investigación criminal y protección de la privacidad en la doctrina del Tribunal Europeo de Derechos Humanos**. In 2º Congresso de Investigação Científica: Coimbra. Almedina, 2010

ZIEGLER, Jean. **Senhores do Crime**: Rio de Janeiro. Editora Record, 1998

ZIROJEVIĆ, Mina. **Computer Related Crime – Offences Against The Confidentiality, Integrity, And Availability Of Computer Data And Systems** Disponível em [http://medial.naukaidrustvo.org/2015/07/zirojevic\\_computer\\_related\\_crime.pdf](http://medial.naukaidrustvo.org/2015/07/zirojevic_computer_related_crime.pdf)