Instituto Superior de Ciências Policiais e Segurança Interna - ISCPSI

Diana Calazans Mann

Dissertação do VII Mestrado Não Integrado em Ciências Policiais, Especialização em Criminologia e Investigação Criminal

INFILTRAÇÃO DIGITAL: A VALIDADE COMO MEIO DE PROVA E OS LIMITES ÉTICOS DO ESTADO-INVESTIGADOR

Orientador:

Professor Doutor Manuel Monteiro Guedes Valente

Lisboa - Portugal

Dissertação apresentada como requisito parcial para a obtenção do grau de Mestre em Ciências Policiais, na especialização de criminologia e investigação criminal do Mestrado em Ciências Policiais, do Instituto Superior de Ciências Policiais e Segurança Interna, sob orientação científica do Professor Doutor Manuel Monteiro Guedes Valente.

DEDICATÓRIA

Dedico esse trabalho aos meus pais, Rudi Ivo Mann e Vera Calazans Mann, pois a finalização dessa dissertação de mestrado é fruto das sementes que eles plantaram em mim.

AGRADECIMENTOS

Em primeiro lugar, agradeço à Polícia Federal, órgão para qual eu trabalho e sem o qual eu não teria entrado em contato com o apaixonante tema da investigação criminal e produção da prova. Agradeço pelos ensinamentos diários e pela grandeza de sempre incentivar o aprofundamento dos conhecimentos teórico de seus servidores por meio da licença capacitação, recurso indispensável à frequência das aulas na cidade de Lisboa em Portugal.

Agradeço ao Instituto Superior de Ciências Policiais e Segurança Interna que me acolheu, servindo de morada nos três meses em que estive distante da minha.

Ao meu orientador, Professor Doutor Manuel Monteiro Guedes Valente, que me apontou o caminho a seguir.

Aos meus colegas de mestrado pela caminhada em conjunto e apoio nos momentos de insegurança.

E, por fim, a Rafael e Júlia que souberam compreender os períodos de ausência, fornecendo apoio e carinho, um agradecimento especial.

RESUMO

O principal objetivo dessa dissertação de mestrado consiste em aprofundar os conhecimentos sobre a infiltração digital como meio de recolha de provas nos delitos cibernéticos. Para tanto, será feita uma comparação entre o instituto já consagrado da infiltração policial e o novo instituto infiltração digital, surgido com a massificação do uso da internet e em resposta a criminalidade informática com o propósito de construir uma definição da infiltração digital. Para diferenciar os dois institutos, algumas palavras são ditas sobre as figuras assemelhadas à figura do agente infiltrado. Os princípios constitucionais e supraconstitucionais aplicáveis ao processo penal são analisados visando a edificação de limitações ao Estado-Investigação na utilização da infiltração digital. Por fim, é feita menção aos regimes jurídicos do Brasil e Portugal, no sentido de verificar se possuem densidade normativa suficiente para regular a utilização da infiltração digital como método oculto de investigação.

Palavras-chave: crimes cibernéticos, infiltração digital, infiltração policial, princípios, lei penal.

ABSTRACT

The main objective of this master's degree dissertation is intensify the knowledge about *online* undercover operation to collecting evidence against cybercrime. So, a comparison will be made between the established institute of undercover operation and the new digital one, which emerged with the mass usage of the internet and in response to cybercrime, in order to build a definition of "cyber-undercover operation". To differentiate the institutes, some words are about the resembling types to undercover agent. The constitutional and supra-constitutional principles applicable to criminal proceedings are analyzed with a view to constructing limitations to the State in the use of *on-line* undercover operation. Finally, reference is made to the law of Brazil and Portugal, in an effort to verify if they have strength enough in criminal law to regulate *online* undercover operation as a hidden method of investigation.

Key words: criminal law, cybercrimes, online undercover operation; principles.

LISTA DE SIGLAS E ABREVIATURAS

ARPA – *Advanced Research Projects Agency*

ARPANET – Rede de computadores criada pela ARPA

Art. - Artigo

CFB – Constituição Federal do Brasil

CPP – Código de Processo Penal

CRP - Constituição da República Portuguesa

JAI – Decisão Quadro do Conselho da União Européia

Orcrim – Organização Criminosa

RJAE – Regime Jurídico das Ações Encobertas

TOR - The *Onion Router Project*

ÍNDICE

DEDICATÓRIA..... i
AGRADECIMENTOS..... ii
RESUMO..... iii
ABSTRACT..... iv
LISTA DE SIGLAS E ABREVIATURAS..... v
ÍNDICE..... vi
INTRODUÇÃO..... 1
1 - A INFILTRAÇÃO DE POLICIAS NOS CRIMES DIGITAS..... 3
1.1 - Infiltração Policial Clássica..... 4
1.2 - A infiltração digital..... 11
2 - OS FUNDAMENTOS POLÍTICO-CRIMINAIS DA INFILTRAÇÃO DIGITAL..... 21
2.1 - A legislação em Portugal..... 26
2.2 - A legislação no Brasil..... 29
2.3 - Será a infiltração digital uma decorrência do Direito Penal do Inimigo?..... 35
3 - OS LIMITES IMPOSTOS AO ESTADO PELOS PRINCÍPIOS ESTRUTURANTES SUPRACONSTITUCIONAIS..... 38
3.1 - O princípio da superioridade ética do Estado..... 40
3.2 - Princípio da Lealdade ou boa-fé..... 42
3.3 - Princípio da Reserva de Constituição..... 44
3.4 - O princípio da proibição da autoincriminação ou *nemo tenetur* se *detegere*..... 46

3.5 Princípio da proporcionalidade *Lato Sensu* 47
4 - OS LIMITES IMPOSTOS AO ESTADO PELOS PRINCÍPIOS PROCESSUAIS CONSTITUCIONAIS 51
4.1 - Princípio da Reserva Legal 51
4.2 - Reserva de catálogo 52
4.3 - Princípio da Reserva de Juiz ou Reserva Jurisdicional 54
4.4 - Princípio da subsidiariedade 55
4.5 - Princípio de indispensabilidade do recurso ao meio oculto de prova para a descoberta da verdade e para a obtenção da prova 57
4.6 - Princípio da vinculação ao fim 59
5 - A ADMISSIBILIDADE DA INFILTRAÇÃO DIGITAL COMO MEIO DE PRODUÇÃO DE PROVA VÁLIDO 62
6 – CONCLUSÃO 74
7 – BIBLIOGRAFIA 76

INTRODUÇÃO

O advento da era digital trouxe consigo um mundo novo a ser explorado. A rede mundial de computadores passou a ser utilizada por todos os cidadãos com possibilidade de interação em escala planetária. Organizações criminosas e os governos, cada um com seus propósitos, passaram a atuar nesse mesmo espaço, ainda que sem o pleno domínio desse novo território, carente de regras e regulamentações jurídicas.

O conhecimento sobre o uso da internet está disponível na própria rede, entretanto, a absorção desse conhecimento não se opera de forma linear entre os usuários, os quais se diferenciam entre usuários avançados, capazes de dominar os demais, e usuários leigos, inaptos a entender o funcionamento da internet e por via de consequência proteger a si mesmos dos novos riscos.

Essa temática nova traz uma série de questionamentos aos operadores do direito penal e processual penal, sejam eles servidores do sistema de justiça, juristas ou advogados. Quais das condutas praticadas no ciberespaço podem ser chanceladas como crimes? Existiriam bens jurídicos dignos da tutela penal no mundo virtual? Considerando o caráter virtual desses crimes, existem vítimas e danos reais? É possível ao estado investigar crimes ocorridos no ciberespaço? Quais os limites dessa investigação? Todos os atos praticados no ciberespaço são passíveis de investigação pelo estado? Uma investigação digital viola a garantia ao sigilo dos atos da vida privada? A infiltração digital se confunde com a infiltração real? Valem os mesmos normativos? Os direitos fundamentais restringidos são os mesmos? O cometimento de crimes pelo infiltrado é admissível? Como controlar a atividade do policial infiltrado no ciberespaço? A infiltração digital consiste em meio legal e ético de obtenção de prova inobstante a existência de lei específica? Os atos praticados pelos investigadores durante a infiltração geram responsabilização penal?

Entre todas essas questões, decidiu-se pesquisar a possibilidade de utilização da infiltração digital para investigação dos crimes cibernéticos. O presente trabalho pretende contribuir com o aprofundamento do debate sobre os limites da infiltração digital, pois o estudo aprofundado do instituto é extremamente relevante para a construção e definição mais concreta dos parâmetros jurídicos e éticos, bem como para a construção de uma legislação mais adequada à infiltração digital, que contemple uma boa técnica policial, com respeito e garantia dos direitos e liberdades fundamentais da pessoa humana, requisitos essenciais para a construção do justo processo penal, alicerce do Estado Democrático de Direito.

Sendo assim, a presente dissertação tratará no primeiro capítulo das diferenças e aproximações entre os conceitos de infiltração tradicional e infiltração digital, visando construir a definição do novo instituto, A presente investigação pretende aprofundar os estudos sobre a utilização da técnica da infiltração para a investigação dos crimes cibernéticos, transmutando o “agente infiltrado” em uma “infiltração digital”, com a criação de um perfil fictício construído e utilizado por uma equipe de investigação. No segundo capítulo serão abordados os contextos políticos determinantes para a criação e justificação quanto à infiltração digital como técnica especial de investigação.

No terceiro e quarto capítulos serão abordados os princípios que atuam como balizas à atividade probatória, especialmente à atividade de recolha de provas em meio virtual por meio da infiltração digital.

Por fim, no quinto e último capítulo será questionada a admissibilidade da utilização da técnica de infiltração como meio de prova admissível e passível de valoração no âmbito do processo penal justo e democrático, evidenciando-se os problemas da legislação em vigor quando confrontadas com os princípios gerais do processo penal.

1 - A INFILTRAÇÃO DE POLICIAS NOS CRIMES DIGITAS

A infiltração de agentes pelo Estado não consiste em novidade. A utilização de uma pessoa para a recolha de informações restritas a determinados grupos, após estabelecimento de vínculo de confiança, tem sido relatada desde a idade média, estando incluído por exemplo no Manual da Santa Inquisição na forma de informantes anônimos, na época em que não havia uma clara separação entre as figuras do investigador e do Juiz a este cabendo toda a produção probatória e o julgamento (Gontijo, 2016). Ademais, os objetivos não consistiam tanto em perseguição do crime como, sobretudo, para descoberta e perseguição de inimigos e dissidentes políticos (Andrade, 2009, p. 532b).

Entretanto, o instrumento em questão, utilizado em procedimentos inquisitivos inconcebíveis em face do estado democrático de direito vigente, ganha novos contornos ao serem utilizados como um dos instrumentos para o enfrentamento a criminalidade organizada. Nesse contexto, a infiltração digital constitui técnica deveras atual, ensejada pelo fenômeno dos crimes cibernéticos[1],

[1] Os crimes cibernéticos ou crimes digitais podem ser entendidos como aquelas condutas contrárias ao direito praticadas nesse ambiente e que tenham uma prévia definição legal como crime (tipicidade). Os primeiros esforços para conceituar crimes cibernéticos propuseram uma classificação a partir da análise do bem jurídico tutelado pela norma penal incriminadora. De acordo com esse enfoque, existem duas espécies de crimes cibernéticos, crimes cibernéticos puros ou próprios e crimes cibernéticos impuros ou impróprios. Os crimes cibernéticos puros são aqueles que tem como finalidade uma violação ao próprio sistema computacional, como por exemplo a invasão de sites, disseminação de vírus, ataques de negação de serviço, apropriação de perfis virtuais, entre outros (STENIO 2016: 52). Os crimes cibernéticos impuros ou impróprios são aqueles por meio ou com o auxílio do computador ou hardware equivalente. A existência de um computador conectado à internet facilita a empreitada criminosa, mas não se coloca como *conditio sine qua non* para a prática de crime. Como exemplo desse tipo de delito estão as fraudes bancárias e a disseminação de pornografia infantil. No caso desses delitos, os bens jurídicos violados já eram tutelados pelo legislador antes mesmo do advento da internet, quais sejam a dignidade sexual e o patrimônio. Marcel Colli apresenta uma crítica à referida classificação. No entendimento desse doutrinador, a classificação entre crimes cibernéticos próprios e impróprios não teria como eixo de análise somente o bem jurídico, mas em alguns casos o objeto material do crime. Em face dessa imprecisão entre bem jurídico tutelado e objeto do crime, Colli propõe outras duas categorias: quando o computador é utilizado como meio-fim para a consecução de um crime informático comum ou um crime informático especifico e quando o computador, ou algo nele constante ou inerente, é o próprio objeto material da conduta criminalizada (2010, p. 44). Acrescenta o referido autor mais

derivados da massificação do uso da internet. Embora a infiltração policial seja largamente utilizada e sedimentada como meio de obtenção de prova pelos tribunais de diversas partes do mundo moderno, com especial relevo para as cortes norte-americanas, em que pese os questionamentos de ordem ética, a infiltração digital está apenas no início de sua existência como ferramenta de investigação, apta a ser utilizada em um estado democrático de direito.

1.1 - Infiltração policial clássica

A infiltração de agentes como forma de investigação configura um meio de obtenção de prova previsto tanto no Direito Brasileiro quanto no Português, bem como nos mais diversos ordenamentos jurídicos e nos tratados internacionais.

A infiltração policial e mais recentemente a infiltração digital, são utilizados para fazer frente à expansão da criminalidade organizada, a qual possui como características principais a estrutura logística e *modus operandi* mantidos em segredo por seus membros, dificultando, sobremaneira a atuação das instituições policiais (Pereira, 2008b, pp. 13-54). Existem diversos conceitos sobre a infiltração policial propostos pelos diversos autores que estudam o tema. A maior parte deles trazem os mesmos elementos para a definição, variando com relação a finalidade. O agente infiltrado seria aquele membro da polícia judiciária que se infiltra em uma organização criminosa participando da trama organizativa, utilizando-se de uma identidade falsa, concedida pelo Estado, e que possui como finalidade detectar a comissão de delitos e informar sobre suas atividades às autoridades competentes,

uma divisão, os crimes informáticos como gênero dos quais os cibernéticos seriam espécie, e para a ocorrência de um cibercrime exigiria o envolvimento de mais de um computador ou dispositivo telemático ou eletrônico, conectados entre si por uma rede material ou imaterial. Embora as definições sobre crimes cibernéticos sejam importantes para a construção de uma dogmática penal do direito digital, estamos mais de acordo com Pedro Dias Venâncio (2011, p. 17) ao afirmar que a criminalidade informática engloba toda a panóplia de atividade criminosa que pode ser levada a cabo por meios informáticos, ainda que estes não sejam mais que um instrumento para a sua prática. Essa conclusão é bastante adequada e suficiente para o recorte do presente estudo, cujo viés é mais próximo das temáticas processualistas.

com o escopo de obter provas para a detenção dos autores (Pereira, 2008a, p. 176).

Não está entre os objetivos da presente investigação cunhar um novo e mais apropriado conceito de agente infiltrado, apenas reforçar alguns elementos que foram encontrados na maioria dos conceitos propostos pelos doutrinadores mais abalizados.

Em primeiro lugar, o objetivo da infiltração consiste na recolha de provas acerca das atividades criminosas que motivaram a realização da infiltração. A detenção dos envolvidos será a consequência da persecução criminal para a qual as provas são elementos indispensáveis.

Em segundo lugar, é essencial que o agente infiltrado seja necessariamente um servidor público da carreira policial. Isso porque, no plano ideal, a realização da infiltração demandará uma série de capacidades desenvolvidas em face de rigoroso treinamento prévio, bem como da seleção dos agentes mais aptos para a missão. Também porque a principal motivação para a infiltração, conforme referido acima, consiste na recolha de provas. Essa sensibilidade para identificar quais são os elementos de prova que servirão ao processo penal é tarefa desempenhada pelos funcionários da polícia judiciária, os quais são capacitados para essa tarefa desde o ingresso em suas instituições.

A infiltração encerra enormes riscos, que em face de imperativos de ordem ética, não devem ser suportados pelo cidadão não policial. O risco nesse caso é assumido pelo Estado, através da polícia judiciária, não podendo ser transferido a terceiros. Ademais, o risco é inerente a atividade policial. O que não desincumbe as autoridades de fazer um planejamento minucioso que inclua as estratégias utilizadas para minimizar o risco para o infiltrado, motivo pelo qual deverá necessariamente ser realizada não por um policial, mas por uma equipe dedicada integralmente a essa tarefa (missão).

Nesse sentido é a opinião de Valente (2017b, p. 589) ao asseverar que a legitimidade ético-jurídica da ação de infiltração será posta em causa ao se recorrer

a um terceiro para atuar de forma encoberta. A utilização de um terceiro que porventura tenha interesses pessoais no objeto da investigação (para facilita-la ou dificultá-la) aumenta a dificuldade da polícia judiciária a exercer o devido controle sobre os atos praticados pelo infiltrado. Assim, a infiltração policial consistiria em técnica especial de investigação operacionalizada por meio da introdução de um agente público, devidamente treinado, com ocultação de sua condição de policial e utilização de identidade fictícia com o escopo de obter provas dos atos ilícitos praticados após conquistar a confiança dos visados (Carlos & Reis, 2014, p. 16).

Conforme dito assim, constitui-se em técnica excepcional de investigação que exigirá para sua utilização um balizamento pelos princípios limitadores da atuação estatal e somente quando todos os demais meios de obtenção de prova não forem suficientemente capazes e eficazes para descoberta da verdade e obtenção de prova. (Valente, 2017b, p. 567).

Conforme Valente (2017b, p. 565) a busca de mecanismos para “prevenir e investigar a criminalidade mais grave e altamente organizada, complexa, violenta, transnacional, internacional”, responsável por impedir o desenvolvimento humano “impele o legislador a decidir ampliar o âmbito das acções encobertas, vulgo agente infiltrado”. Entretanto, as infiltrações somente podem ser admitidas quando subordinadas ao regime estabelecido pelos princípios norteadores da administração da justiça, “ajustando a lei ao tempo dos nossos dias e dando à sociedade a segurança jurídica no sentido de legalizar um meio de investigação excepcional”.

O recurso a figura do agente infiltrado tem sido colocado pela doutrina entre os meios ocultos de investigação criminal e consubstancia uma técnica de investigação de moral duvidosa na qual o próprio suspeito produz involuntariamente a prova de sua própria condenação (Valente, 2017b, p. 576).

Preocupa-se a doutrina em diferenciar a figura do agente infiltrado de outras técnicas de investigação que com ele não se confundem, tampouco no âmbito da infiltração digital, são elas: o informador, o agente à civil, o agente encoberto e o

agente provocador. O recurso a informadores é uma prática tão antiga quanto à existência de agentes provocadores e infiltrados, embora a literatura sobre essa figura seja mais escassa (Oneto, 2015, p. 90)[2]. O informador é a pessoa que fornece subsídios informativos para as investigações da polícia judiciária, mediante cláusula de confidencialidade. A contribuição pode ser graciosa ou mediante pagamento de quantias, estipuladas de acordo com a legislação ou regulamentos internos das Polícias. O informador ou colaborador tem, em regra, certa proximidade com os quadros policiais, prestando sua colaboração na obtenção de dados que possam auxiliar em uma possível investigação e posterior persecução penal. As informações são recolhidas no ambiente criminoso e repassadas à polícia. O resultado dessa observação e colheita de dados se dá sob o manto da garantia da confidencialidade e com expectativa de uma contraprestação material ou imaterial (Pereira, 2007, p 177).

A figura do informador tampouco se confunde com a do "delator" ou "réu colaborador". O delator é um réu ou investigado que ao ser interrogado em juízo ou ouvido pela polícia, além de confessar a autoria de um fato criminoso, atribui a um terceiro a participação como seu comparsa (Aranha *apud* Anselmo, 2016, p. 33). A principal diferença entre o informador e o infiltrado consiste no fato de que o primeiro não pertence aos quadros policiais e não precisará conquistar a confiança dos investigados, pois, para que sua contribuição tenha valor para a investigação, pressupõe-se que já esteja nessa condição, a partir da qual obteve as informações julgadas relevantes para a polícia.

[2] Oneto (2015, p. 90) traz algumas considerações sobremaneira importantes quanto a utilização dos informantes ou informadores. A primeira delas consiste nas quantias despendidas com o pagamento de informantes, muitas vezes superiores aos pagamentos recebidos pelos funcionários das polícias. Destaca a autora a falta de transparência no processo de recrutamento de informadores, o qual é totalmente subjetivo, podendo ser um cidadão com informações em face de sua atuação profissional ou mesmo um alguém do próprio meio criminoso, pessoa que dificilmente se pauta pelas regras da licitude. Preocupa-se a doutrinadora com eventual negociação da polícia com o informante, também autor de crimes, visando a não punição desse, contrariando o sistema penal português fulcrado no princípio da legalidade e da oficialidade dos atos.

O agente à civil consiste naquele policial que pertence aos quadros das polícias fardadas e que não se encontra ostensivamente trajado. A utilização desse recurso poderá ser admitida em certos casos, mas dificilmente será legítima como técnica de recolha de provas. Como exemplo de atuação legítima e lícita de policial à civil pode ser citado o policial que não está em serviço e se depara com a ocorrência de um crime, nesse caso poderá intervir e efetuar a prisão dos criminosos[3]. Também existe possibilidade de utilização do policial à civil para observação em locais específicos, com o intento de prevenção criminal, como em grandes manifestações ou em face de uma denúncia de crime em andamento.

A participação velada de policiais em manifestações para identificar pessoas ou grupos de pessoas que estejam cometendo infrações penais não se confunde com a infiltração. Primeiro porque o policial, em tais situações, não tem como meta a aceitação no grupo investigado por parte de seus membros, seu intuito é simplesmente se utilizar da oportunidade em que poderá ou não haver a ocorrência do delito. Ademais, o policial à civil, em tais casos terá sido designado pela autoridade superior para acompanhar a manifestação, devendo somente efetuar a identificação dos autores e colheita de evidências quanto aos crimes que eventualmente presenciar (Sousa, 2015, pp. 42-43).

A atividade do policial à civil não se refere a uma investigação específica, motivo pelo qual não necessita do prévio e concomitante controle judicial. Ademais, não poderia o policial encarregado do policiamento preventivo atuar como agente encoberto ou agente infiltrado, pois essas atividades são exclusivas da polícia judiciária. Também não se confunde o policial à civil com o agente de inteligência. As atividades de inteligência não se prestam à produção de provas em processo

[3] Importante lembrar que tanto no Brasil como em Portugal qualquer do povo pode efetuar uma prisão ao deparar-se com o flagrante delito, quanto mais o policial. Esse dever de agir significa, portanto, que diante de uma situação de flagrante delito, agentes e autoridades policiais têm a obrigação de atuar imediatamente, prendendo em flagrante delito o autor do crime.

penal, bem como os levantamentos feitos por policiais à civil, que posteriormente possam originar uma investigação policial, como os levantamentos de inteligência.[4]

A figura do agente encoberto consiste na mais debatida pelas divergências de entendimento e conceituação. Especialmente porque muitos diplomas legais utilizam a expressão "ação encoberta" para designar as atividades do agente infiltrado. O Regime Jurídico das Ações Encobertas definido na Lei 101/2001 de Portugal, por exemplo, utiliza a denominação ações encobertas, embora esteja tratando verdadeiramente do agente infiltrado (Valente, 2017, p. 570). [5]

O agente encoberto consiste em técnica e tática policial na qual um policial, sem revelar a sua identidade, frequenta lugares conotados com o crime com a finalidade de identificar e eventualmente deter possíveis suspeitos da prática de crimes, para tanto não determina a ocorrência do crime tampouco conquista a confiança de alguém. Quanto à competência objetiva, o agente encoberto não pode proceder a investigações em locais cujo acesso careça de prévia autorização e não se cinge a um catálogo de crimes, divergindo do que prescreve o art. 2º da Lei 101/2001. Tem como características fundamentais passividade relativamente à decisão criminosa e inexistência de relação pessoal com o agente do crime. A presença do policial no local não determina o rumo dos acontecimentos, poderia

[4] A sistemática constitucional brasileira relativa à segurança pública definiu que as atividades de polícia judiciária são inerentes à Polícia Federal e às Polícia Civis dos Estados. A legislação anterior à atual Lei do crime organizado previa a possibilidade de infiltração por agentes de inteligências, entretanto, o dispositivo não foi mantido na Lei atualmente em vigor (Lei 12850/2013). No Brasil, as atividades de inteligência estão definidas no art. 1º da Lei 9883/1999, que instituiu o Sistema Brasileiro de Inteligência e consistem em atividades que objetivam a obtenção, análise e disseminação de conhecimento dentro e fora do território nacional sobre fatos e situações de imediata ou potencial influência no processo decisório da ação governamental e sobre a salvaguarda e a segurança da sociedade e do Estado. Portanto, diversas das diligências atinentes à polícia judiciária, cujo objetivo precípuo reside na produção de prova em processo penal.

[5] Para Oneto (2015, p.139-141), o agente encoberto é uma subespécie do agente infiltrado, sendo aquele que pode ocultar sua qualidade ou identidade ao interagir com terceiros "mantendo-os na ignorância para ganhar a sua confiança". Prossegue afirmando que o agente encoberto está submetido ao regime jurídico das ações encobertas previstos na Lei 101/2001, uma vez que o legislador utiliza a expressão "agente encoberto" no artigo 4º, nº 3, ao tratar do depoimento sob identidade fictícia. Afirma a doutrinadora que caberia ao agente encoberto as ações do tipo light cover, com duração de até seis meses. Também nesse sentido Pereira (2013), para quem a distinção entre agente infiltrado e agente encoberto não tem importância capital visto que a Lei 101/2001 se aplicaria a ambas as figuras.

estar qualquer outra pessoa que a cena se daria da mesma forma (Valente, 2017, p. 570).

Embora situado por razões didáticas no mesmo capítulo que estuda os conceitos de agente à civil, encoberto e infiltrado, o agente provocador não é uma categoria ao lado das demais. Em verdade, a provocação consiste em uma atividade vedada aos agentes do estado, sejam eles à civil, encobertos ou infiltrados. Senão vejamos.

O agente provocador pode ser definido como todo agente que, no desempenho de suas funções, instiga uma conduta criminosa de terceiro, tomando todas as medidas para que o autor seja imediatamente surpreendido em flagrante delito. Na realidade, cuida-se de ato nulo, dando causa ao chamado crime impossível O comportamento do agente provocador somente poderá resultar em um flagrante provocado ou preparado, nome que ficou sedimentado na doutrina e jurisprudência brasileiras para descrever a prisão em flagrante realizada em face de um estímulo para que o investigado ou arguido cometa a infração penal (Sousa, 2015, p. 45).[6] A figura do agente provocador, além de não prevista em Lei, é repudiada por se cuidar de comportamento maquiavélico e desleal, característicos de tempos ditatoriais os quais devem constar apenas na memória para jamais serem permitidos novamente. O flagrante provocado pelo agente dá azo a nulidade do ato, em razão do crime impossível, com a consequente responsabilização do policial. Diferentemente, a prova colhida pelo agente policial infiltrado em organizações criminosas é considerada lícita, e em muitos casos essencial à elucidação dos fatos apurados, desde que atendidos os requisitos legais (Sousa, 2015, p. 46).

[6] O Supremo Tribunal Federal Brasileiro editou a Súmula 145 que dispõe sobre a ilegalidade do flagrante preparado estabelecendo que "não há crime, quando a preparação do flagrante pela polícia torna impossível a sua consumação. Texto da súmula disponível em http://www.stf.jus.br/portal/jurisprudencia/menuSumarioSumulas.asp?sumula=2119

1.2 - A infiltração digital:

No que tange à infiltração digital, tanto Portugal quanto o Brasil têm dispositivos próprios, diversos das Leis que tratam da infiltração real ou *off line*. No Brasil, a Lei 13.441/2016 regulamentou a infiltração para investigação de crimes que atentem contra a dignidade de crianças e adolescentes. Entretanto, silenciou o legislador sobre a infiltração digital para investigação de outros crimes cibernéticos, diversos da pornografia infantil pela internet, somente tendo incluído a invasão de dispositivo informático. Em Portugal a Lei 109/2009, que aprovou a Lei dos Cibercrimes, introduziu o meio de obtenção de prova do agente infiltrado, embora nominando-o de regime de ações encobertas, para a repressão dos crimes nela previstos (crimes do catálogo), cometidos por meios informáticos e através de meios informáticos (Valente, 2017, p. 565). Não se preocupou o legislador brasileiro em construir uma definição para a infiltração digital. Talvez porque, dada a atenção que desperta, a técnica em questão é bastante conhecida por juristas e leigos. Tampouco o fez o legislador português, que apenas remeteu a regulamentação da infiltração digital para o regime jurídico das ações encobertas.

Sendo esse um tema bastante recente, doutrina e jurisprudência também não delinearam os contornos do novo instituto. Predominam as indefinições sobre as diversas atividades de investigação que podem ser realizadas pela polícia no ciberespaço[7], dentre elas algumas que não se confundem com a infiltração policial pois não geram restrição à direitos fundamentais e que, portanto, não se confundem com a infiltração policial (*off line*) e a infiltração digital propriamente dita. Para

[7]O ciberespaço consiste em uma realidade intangível caracterizada pela troca de informações entre pessoas por meio de dispositivos de comunicação eletrônicos, como computadores e sujeitos do materespaço, compreendido esse como a realidade tangível. O ciberespaço não se constitui pelo tempo ou espaço que ocupa, mas pelo intercâmbio de informações. De acordo com Colli (2010, p.31) "não se trata de criar e dicotomizar realidades, uma virtual e outra real [...] para se estabelecer o que é fluxo de informações e o que é movimento corpóreo (ação e presença física) mas sim de agregar e encarar como contínuos os mundos *off-line* (materespaço) e *on-line* (ciberespaço)". Além disso, a definição do ciberespaço impacta em diversos aspectos da persecução penal, especialmente para compreensão do *locus comissi delict* e da jurisdição criminal competente para a apuração do injusto e aplicação da pena.

delinear um conceito de infiltração digital visando diferenciá-la de outras diligências policiais realizadas em ambiente virtual, é de bom alvitre partir dos conceitos construídos acerca da infiltração real. Pois, de fato, a infiltração virtual parecer estar sendo tratada como uma subespécie da infiltração real.

Para fins didáticos utilizaremos o seguinte conceito para a infiltração *off line*: trata-se de uma técnica especial de investigação, mediante a qual um **agente policial**, devidamente treinado, **oculta sua verdadeira identidade** para utilizar outra fornecida pelo estado que viabilize a **introdução em uma organização criminosa** na qual terá como missão **conquistar a confiança** dos verdadeiros membros, passando a atuar com **o fim de obter provas** dos atos ilícitos praticados.

A partir do conceito acima, extraem-se como elementos mínimos necessariamente presentes na ação de infiltração: a execução por um policial, a dissimulação da identidade, o ingresso em organização criminosa, o estabelecimento de relação de confiança e a finalidade de recolha das provas.

A realização da infiltração por policial devidamente treinado deverá ser observada tanto na infiltração real quanto na virtual, não havendo maiores diferenciações ou observações quanto a esse item. Pereira (2017), ao se referir a infiltração “virtual”, destaca que a técnica “deverá ser levada a efeito por agente policial devidamente treinado para tal desígnio, devendo este apresentar aspectos psicológicos condizentes com a complexidade da operação, perfil intelectual adequado para o correto desempenho das tarefas inerentes ao plano operacional, conhecimentos avançados em matéria cibernética e capacidade de inovar em situações de extrema fragilidade no tocante ao sigilo do trabalho encoberto”. Com relação à **dissimulação e ocultação da identidade**, importante observar que não bastará a confecção de um documento com nome e números fictícios devidamente registrado nos bancos de dados oficiais. O agente infiltrado deverá construir uma identidade virtual com alto grau de credibilidade e verossimilhança, capaz de subsistir as pesquisas dos usuários avançados altamente qualificados, aptos a

utilizar ferramentas para proteção de suas atividades ilícitas, como engenharia social[8] e intrusão através de *malwares*[9].

No que concerne à aquisição da confiança do arguido ou investigado, surge uma segunda dificuldade, sempre presente nas investigações cibernéticas mas estranha à infiltração em campo, a qual advém da própria essência da internet, qual seja a anonimidade virtual [10].

É característico da informática o fato de as interações e relações serem feitas entre aparelhos, os quais são operacionalizados via de regra por seres humanos. Isso porque a ideia inicial da computação foi a facilitação das tarefas para os seres humanos, o foco era o aumento constante da capacidade de processamento de dados para permitir a realização de tarefas complexas com o apertar de um botão. Mas o evoluir da tecnologia trouxe o relacionamento entre as pessoas usuárias da informática. Como qualquer pessoa pode utilizar a tecnologia, surgiu a insegurança no que se refere ao usuário conectado, uma vez que a identidade pessoal é presumida (Sydow, 2015, p. 110).

[8] De acordo com o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), a engenharia social é um método de ataque, onde alguém faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores ou informações (disponível em https://cartilha.cert.br/sobre/old/cartilha_seguranca_3.1.pdf)

[9] De acordo com o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), código malicioso ou *malware* (*Malicious Software*) e um termo genérico que abrange todos os tipos de programa especificamente desenvolvidos para executar ações maliciosas em um computador. Na literatura de segurança o termo *malware* também é conhecido por "*software* malicioso" (disponível em https://cartilha.cert.br/sobre/old/cartilha_seguranca_3.1.pdf)

[10] Além da anonimidade, o autor Sydow (2015, pp. 89-112) destaca as características dos delitos informático. As mais relevantes para o presente estudo: a interatividade (para funcionar os computadores necessitam de uma intervenção humana), mobilidade (os dispositivos estão na mão do usuário literalmente, como os *smartphones*), conversibilidade (capacidade dos computadores conversarem entre si, conectividade (capacidade de um equipamento se conectara a internet), mundialização (a internet está disponível em todos os cantos do planeta e continua a se expandir), fracionabilidade (os programas de computador podem ser divididos e armazenados em diferentes plataformas), divisibilidade (os dados podem ser divididos em partes menores, ou pacotes, e percorrer caminhos diferentes até o destinatário final) a intangibilidade (a troca de dados é inerente ao conceito de informática, entretanto, esse doados não são materiais nem são materializáveis por si, os dados tratados pela informática nada mais são dos que bits interpretados por dispositivos, ubiquidade ou simultaneidade (pode-se estar em diversos lugares virtuais ao mesmo tempo.

Essa identificação presumida, feita com base nos dados informados inseridos por cada usuário, ou por um número de IP de uma máquina, gerou o fenômeno da anonimidade. Entende-se por anonimidade a falta de certeza quanto à identidade imediata referente a um usuário, levando-se em conta a impossibilidade de se atribuir o uso de um maquinário a uma pessoa (Sydow, 2015, p. 110). Ademais, o anonimato *on-line* fornece uma liberdade inatingível no mundo real. Seja em *websites* de relacionamentos, seja em conversas através de mensageiros instantâneos (*instant messenger*), seja através de dados armazenados em bancos de dados de quem procura emprego, em qualquer destes ambientes, a liberdade para se assumir características de gênero, idade e religião é ilimitada. Essa ampla liberdade permite a qualquer pessoa adotar uma personalidade ou identidade que poderá corresponder ou não à da pessoa do mundo *off-line* (Colli, 2010, p. 87). Portanto, compete ao agente infiltrado identificar um ser humano real de quem deverá se aproximar, para somente então, conquistar-lhe a confiança.

Para que a atividade de infiltração seja reconhecida como tal, necessário que haja a identificação dos suspeitos ou indícios veementes da prática de crimes, a atividade policial se dará necessariamente com o estabelecimento de uma relação de confiança entre o policial disfarçado e o investigado[11]. Importante observar que inicialmente o investigado poderá estar identificado apenas com um *nickname* ou um e-mail, não sendo possível atribuir-lhe uma qualificação real, ou seja nome, idade, gênero e endereço. Dado que as comunicações na internet se executam entre as máquinas, haverá a identificação de um número IP (protocolo de internet), que não necessariamente levará ao local do crime, mas a um ponto de

[11] Questão de alta sensibilidade ética seria admitir-se o estabelecimento de relação de confiança com familiares dos investigados. É próprio dos roteiros cinematográficos explorarem essa temática. Mas seria ético um policial, para investigar um suspeito, estabelecer um relacionamento (falso) com alguém que não faz parte da organização criminosas?

conexão da internet (um cibercafé, uma biblioteca pública ou um roteador utilizado pela rede TOR[12]).

A investigação dos crimes cibernéticos, geralmente, comporta duas fases distintas, uma virtual e outra de campo. A primeira fase, também designada fase técnica da investigação, na qual serão necessários conhecimentos informáticos avançados, o objetivo único consiste em localizar o computador que foi utilizado para a ação criminosa. Para tanto serão analisadas informações prestadas pelos provedores de conexão e de conteúdo, visando identificar especialmente o IP, data e hora da conexão, pois não existem dois usuários com o mesmo IP durante a navegação na internet no mesmo dia e hora e fuso horário. A partir da identificação e localização do computador que permitiu a conexão e o acesso criminoso na internet surge a denominada fase de campo, quando há necessidade de deslocamento de agentes policiais para realização de diligências com o intuito de promover o reconhecimento operacional no local (Wendt & Jorge, 2013, pp. 67-68). Nesse momento outras técnicas de investigação poderão ser aplicadas, como tomada de depoimentos de testemunha, interrogatórios, buscas e apreensões, ou ainda a continuidade da infiltração dessa vez a partir do formato tradicional.

[12] O projeto TOR consiste em um software livre e de código aberto criado para possibilitar a utilização da internet com privacidade e com anonimato garantido e está disponível para download no site https://www.torproject.org. De acordo com a Nota Técnica da Sociedade Civil para a CPI dos crimes cibernéticos 'O Tor ... é o nome tanto de um software mantido por uma organização sem fins lucrativos sediada em Massachussetts, EUA, quanto da rede mundial de relays ("retransmissores"), computadores mantidos por pessoas e organizações voluntárias. Quando alguém usa Tor para acessar um site ou ler e-mails, seu computador escolhe três desses relays para encaminharem seu tráfego de forma que ele saia para a Internet com o IP do último deles, o relay de saída. Como há muitos relays na rede Tor (cerca de 7200 em 15 de fevereiro de 2016), e pessoas utilizando o serviço em todo o mundo (mais de 2 milhões na mesma data), usá-la tem o efeito de anonimizar a sua conexão, impedindo que os seus pacotes de dados trafegados sejam ligados ao seu endereço IP tanto pelo provedor de conexão quanto pelo servidor acessado. Além disso, quando o computador vai enviar uma mensagem ou acessar uma página através da rede Tor, o conteúdo é enviado com três camadas de criptografia, uma para cada relay. Isto e mais algumas técnicas matemáticas garantem que nem mesmo os relays que participam da rede possam saber o que estão encaminhando e ao mesmo tempo quem é o remetente. (Conteúdo disponível em https://cpiciber.codingrights.org/tor-onion/)

Entretanto, embora seja impossível a utilização do mesmo endereço IP no mesmo momento, existem inúmeras formas de maquiar o endereço IP visando a não identificação do local do crime e do usuário atrás da máquina. Existem técnicas bastante simples, como utilização de ponto de acesso à internet em nome de terceiros (seja por não haver exigência de senha pelo roteador, ou seja, em face de invasão da rede por um usuário avançado), e outras mais complexas com utilização do software TOR (*The onion router project*) que produz a sucessiva troca de números IPs ao passar por inúmeros pontos de conexão. Nesses casos, a requisição dos logs de acesso ao provedor de internet não levará a identificação dos suspeitos. Entretanto, consiste em etapa indispensável da investigação, pois sem ela não será possível afirmar que o usuário do IP não tem participação na prática criminosa em investigação.

Diante dessa dificuldade de identificação dos investigados, o agente infiltrado precisará conquistar a confiança no próprio ambiente virtual para somente então, colhidas informações sobre a identidade real atrás do teclado, partir para outras medidas de investigação, esquias os autores antes mencionados classificaram como “fase de campo”.

Igualmente digno de nota e agregador de dificuldades à empreitada do agente infiltrado, o fenômeno da dissociação entre o perfil virtual e a identidade real dos internautas. Muitas vezes a invenção de um perfil possibilita a criação de um ente com personalidade diversa da original (persona), com o único objetivo de aceitação social, pois é mais fácil expressar gostos e preferências socialmente questionáveis em um local em que não existe o confronto físico entre os indivíduos (Faria & Monteiro, 2017, p. 3). De modo que o perfil de um criminoso virtual pode se distanciar muito da pessoa real. Portanto, a tarefa de conquistar a confiança do investigado, mais do que requisito para a configurar a infiltração poderá ser um elemento crucial a permitir a qualificação do investigado ou arguido. No que tange a tarefa de recolha de provas, essa será feita necessariamente no ciberespaço, ao

menos no primeiro momento, enquanto não há um endereço físico no qual possam ser realizadas outras diligências.

Quanto à necessidade de introdução em organização criminosa, existem alguns apontamentos a serem feitos. Na égide da Lei n.º 12.850/2013, a infiltração policial era admitida para investigar crimes cometidos por organização criminosa, assim considerada "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"[13]. Não havia um catálogo de crimes, mas um *modus operandi* a ser identificado, qual seja, a prática de crime por organização criminosa. Mas já nessa época todas os meios de recolha de provas mencionados na referida Lei, entre eles a infiltração, poderiam ser utilizados para a investigação de "infrações penais previstas em tratado ou convenção internacional quando, iniciada a execução no País, o resultado tenha ou devesse ter ocorrido no estrangeiro, ou reciprocamente[14].

Portanto, o requisito introdução em organização criminosa, não era exigido na legislação, tampouco passou a ser na sistemática da nova Lei n.º 13441/2017 que permite a infiltração para investigação de crimes contra a dignidade sexual de crianças e adolescentes e de invasão de dispositivos informáticos.

Quanto as finalidades da infiltração virtual, existem conceitos construídos pela doutrina que mencionam como finalidade "o desmonte da organização criminosa". Entretanto, considerando os textos legais que regem o assunto, que consideram a infiltração como meio de produção de prova, a finalidade de utilização do instrumento não pode ser maior do que essa. Havendo indícios da

[13] Conceito de crime organizado insculpido no Artigo 1º, inciso I, da Lei 12850 (disponível em http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/Lei/l12850.htm)
[14] Art. 1º, inciso II, da Lei 12850. (Disponível em http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/Lei/l12850.htm)

prática de crimes, o estado deve empreender esforços para recolhê-los e mover o devido processo penal. Imputar à investigação criminal a responsabilidade de encerrar a empreitada criminosa de terceiros é extremamente utópico.

No que tange as finalidades da investigação criminal, conforme leciona Guedes Valente a função instrumental do processo penal visa no fundo a realização da justiça, função que somente pode ser alcançada com "uma promissora e bem estruturada investigação criminal que está enquadrada dentro de limites intransponíveis como a liberdade, a integridade e a vida". Conforme o referido doutrinado, a investigação criminal pertence a uma fase preparatória do processo que se preocupa em "efetivar as diligências necessárias na busca de provas (reais e pessoais) que permitam reconstituir os factos que, no 'respeito pelo princípio da verdade material', conduzirão a uma decisão: submeter ou não submeter alguém a julgamento" (Valente, 2017, p. 468).

De modo que a infiltração digital tem por escopo, assim como todas as investigações criminais, a busca da prova. A finalidade de desbaratar a organização criminosa se amolda muito mais aos fins de uma política criminal de prevenção da criminalidade e manutenção da paz social, desbordando, portanto, as finalidades da investigação criminal. Claro está que a investigação criminal é uma das ferramentas de uma política criminal ampla, mas com ela não se confunde[15].

Dessa forma, estar-se-á diante de uma infiltração virtual quando uma equipe de policiais especificamente designada para a tarefa, em face de indícios da prática de crimes cibernéticos – próprios ou impróprios, obtém uma autorização judicial e estabelece uma relação de confiança com um usuário da internet ainda não

[15] A política criminal, como ciência não jurídica, mas que desenha o conteúdo e os fins do Direito penal, ciência jurídica, é a ciência que, subordinada aos vectores da legitimidade e da eficácia e aos princípios ético-filosófico-jurídicos da legalidade, da culpabilidade, da ressocialização e da humanidade, deve debruçar-se sobre as causas do crime, sobre a correta redação dos tipos legais de crime de modo a corresponderem à realidade delituosa, sobre os efeitos das sanções penais, sobre o limite de extensão da aplicação do Direito penal de que dispõe o legislador penal face à liberdade do cidadão e, ainda, sobre a adequação do Direito penal material ao Direito processual penal, cujo desafio é orientar o Direto penal no cumprimento da missão de proteção da sociedade sem niilificar as liberdades individuais

qualificado, mediante ocultação da condição de policial e criação de uma identidade fictícia, visando com isso, obter a qualificação do investigado e provas dos crimes praticados. Considera-se necessário inserir no conceito de infiltração digital o requisito da autorização judicial, uma vez que, presentes todos os elementos do conceito cunhado acima, haverá restrição a direitos fundamentais do investigado, restrições de tal ordem que somente se admitem com a vênia judicial, em face do princípio da reserva de juiz conforme se verá adiante.

Presentes todos esses elementos, a atividade policial poderá ser considerada uma infiltração digital. É preciso ter a clareza de que a infiltração digital não contém em seu núcleo todas as diligências veladas que a polícia possa praticar no mundo virtual. Importante referir que nem todas as atividades realizadas na internet, podem ser consideradas atividades privadas. Tome-se como exemplo as publicações em redes sociais. Essas publicações têm um caráter eminentemente público, salvo restrição de acesso realizada pelo próprio autor das postagens.

Por via de consequência, não poderá o autor de uma postagem de conteúdo ofensivo ou ilegal, alegar violação à sua privacidade para impedir uma investigação policial. Do mesmo modo, não se poderia invocar o manto constitucional de proteção à privacidade em face da publicação de pornografia infantil em um sítio qualquer, que não possua restrições de acesso.

Questão um pouco mais tormentosa, mas que também não se confunde com a infiltração, pois não restringe direitos fundamentais tampouco exige o estabelecimento de vínculo de confiança, são as investigações sobre pornografia infantil e pirataria a partir das redes *peer to peer* ou P2P. Essas redes criadas para permitir o compartilhamento de arquivos na web têm como característica o fato de serem redes abertas, todos os seus usuários são clientes e servidores da referida rede. Quando um dos usuários requisita um arquivo, faz uma busca por um arquivo, esse pedido é enviado a todas as máquinas da referida rede, que disparam uma resposta automática. Ao instalar um software para compartilhamento de arquivos, o internauta está disponibilizando o conteúdo de suas pastas e fazendo requisições

a um incontável número de computadores de forma explícita e pública. Se um desses computadores estiver sendo operado pela Polícia, não há que se falar em violação de privacidade, mas em atuação encoberta da polícia para identificar criminosos virtuais. Além disso, a identificação será de um número IP e não de um investigado devidamente qualificado, motivo pelo qual ainda precisarão ser realizadas outras diligências para a identificação do criminoso, especialmente a requisição dos dados cadastrais para o provedor de acesso, identificado a partir do log (IP, data, hora).[16] [17] As ações encobertas não se confundem com a atividade de infiltração, pois naquela não estão incluídos todos os elementos do conceito de agente infiltrado. A ação encoberta é uma técnica utilizada pela polícia e situada no campo dos poderes cautelares da polícia os quais por não apresentarem restrição a direitos fundamentais não se submetem ao controle jurisdicional.

[16] No Brasil, por força do Marco Civil da Internet, a requisição dos logs de acesso aos provedores de acesso à internet é necessariamente precedida de ordem judicial.

[17] Não é esse o entendimento de Marcel Colli, referido doutrinador considera as investigações de rede P2P como verdadeiras interceptações telemáticas, a exigem autorização judicial para sua realização. De acordo com Colli uma investigação preliminar na qual incida uma interceptação de dados lesa direitos e garantias constitucionais. A vigilância de atos na rede mundial seria um limite a liberdade de expressão e adentraria nos limites do direito à privacidade constitucionalmente protegidos. Inobstante a correção dos argumentos colocados pelo ilustre doutrinador no que tange à proteção do direito à privacidade, data vênia, equivoca-se ao considerar a técnica de investigação de redes P2P como interceptação telemática. A interceptação telemática somente se processa quando o fluxo de dados é copiado ou desviado por e para um terceiro que não seu destinatário, ou seja, quando “A” envia um determinado fluxo de dados para “B” e esse é lidos por “C”. Seja através de correio eletrônico ou outro software de comunicação instantânea. No caso das redes P2P todos os usuários estão “autorizados” pelo software a acessar reciprocamente as pastas de compartilhamento uns dos outros. O fato de um dos usuários do programa ser um computador da polícia e estar a serviço de uma investigação não configura uma interceptação, mas sim uma ação encoberta. A dúvida reside em saber se para esse tipo de ação encoberta aplica-se o regime jurídico das infiltrações, exigindo-se autorização judicial.

2 - OS FUNDAMENTOS POLÍTICO-CRIMINAIS DA INFILTRAÇÃO DIGITAL

A internet, mais do que uma ferramenta de comunicação da era moderna, tornou-se um emulador da vida social, a ponto de os estudiosos do tema não falarem em mundo virtual, mas considerar a internet, em si mesma, como uma das faces da realidade, uma vez que o virtual não se oporia ao real, mas sim ao atual (Lévy, 1999, p. 15).

A massificação do uso da rede mundial determinou a transferência de diversos serviços públicos e privados para o ambiente virtual. Em decorrência disso, o ciberespaço se tornou palco de significativas transferências de capital, bens e valores. Essa nova forma de circulação de riquezas aguçou a cobiça de muitos e transferiu atividades criminosas para o mundo virtual. Contribuíram para a mudança de escopo de muitas organizações criminosas a sensação de anonimato fornecida pela internet e o desconhecimento sobre segurança da grande massa de usuários.

A internet apresenta fragilidades que propiciam o cometimento dos cibercrimes. Isso porque a rede mundial de computadores é um espaço público e não possui um ordenamento jurídico próprio ou único. Está povoada por usuários com diferentes níveis de conhecimento sobre informática e computadores tornando alguns mais expostos mais vulneráveis. Esta reúne uma diversidade de usuários, desde analfabetos digitais até *hackers*. Assim, para quem tem mais conhecimento técnico, é extremamente fácil praticar um crime, dada a vulnerabilidade das vítimas, decorrente do desconhecimento de métodos de proteção. A rede mundial é capaz de eliminar a distância, facilitar o anonimato, diminuir os esforços e riscos pessoais do criminoso (Brito, 2013, p. 35).

Anualmente, fraudes, furtos e desvios geram bilhões de prejuízo às economias[18]. Ao passo que pornografia infantil, moedas virtuais, furtos e golpes geram lucros incalculáveis diante da cifra oculta que envolve esse tipo de criminalidade.[19] Pesquisa realizada pelo Ponemon Institute[20] indica que no mundo fraudes digitais, roubo de propriedade intelectual e danos nas redes corporativas geraram prejuízos de um (1) trilhão de reais por ano. Ainda de acordo com a referida pesquisa, o Brasil é o segundo maior país em número de crimes cibernéticos. Por outro lado, os investimentos em segurança cibernética realizados pelo referido país são pouco significantes.

A assessoria de imprensa do departamento de Defesa norte-americano estimou em 100 milhões de dólares os gastos nos últimos seis meses de 2008 para proteção de dados contidos em seus servidores. Com isso, percebe-se uma tendência de aumento nos investimentos para a defesa da informação (Wendt, 2017, p. 45).

A criminalidade cibernética é ampla e variada, vai muito além crimes como disseminação de pornografia infantil, tráfico de armas, tráfico de drogas e mais modernamente conspirações terroristas. Diante desses novos riscos, as nações foram instadas a dar uma resposta a essas condutas. Para algumas dessas condutas danosas ao tecido social já havia tipificação em diplomas legais anteriores

[18] De acordo com a *Symantec Security Response*, o crime cibernético teria gerado prejuízo de 15,9 bilhões de reais entre 2011 e 2012, o valor indicado pelo estudo seria 10 vezes maior do que o apontado pela Federação Brasileira de bancos (FEBRABAN) que apontava 1,5 bilhão de reais, 900 milhões em fraudes bancárias, incluindo cartões de débito e crédito (Jesus, 2017). A *Symantec Security Response* é uma equipe mundial de engenheiros de segurança da informação, analistas de ameaças cibernéticas e pesquisadores que desenvolvem uma variedade de conteúdos sobre as mais recentes ameaças digitais que afetam empresas e usuários finais. Os relatórios da Symantec estão disponíveis em https://www.symantec.com/pt/br/security_response/publications/threatreport.jsp

[19] Não vamos procurar estatísticas sobre os lucros gerados pelos crimes cibernéticos em face da criminalidade consistir em cifra negra impossível de ser calculada, também não havendo métodos científicos reconhecidos como confiáveis para as estimativas existentes.

[20] Disponível em https://www.ponemon.org/library/2016-cost-of-cyber-crime-study-the-risk-of-business-innovation

ao fenômeno da internet, como nos casos dos crimes patrimoniais, tráfico de armas e drogas. Para outras condutas seria preciso inovar.

Deste modo, Brasil e Portugal, em obediência ao princípio da anterioridade da Lei penal, precisaram adequar suas legislações penais para promover a adequada proteção aos bens jurídicos surgidos com o advento da internet[21]. Importante também mencionar que a produção social de riqueza com a utilização de recursos inéditos trazidos pelos avanços tecnológicos vem acompanhada de uma produção de riscos correspondentes. Os novos riscos passaram a causar conflitos até então desconhecidos pelo Direito. Embora constitua em ferramenta para o desenvolvimento econômico da sociedade, também propicia o surgimento de atritos e uma nova zona criminógena (Brito, 2013, p. 27).

A situação mundial, em particular após o 11 de setembro de 2001 e os atentados de Madri, em 11 de março de 2004, elevaram o nível de tensão e *stress*. A difusão transnacional da sensação de insegurança incentivou mudanças paradigmáticas pontuais que refletem nas práticas penais como resultado da sensação de insegurança[22]. De outro norte, a investigação dos crimes cibernéticos demanda conhecimentos e técnicas diferenciadas. A tecnologia que envolve a interconexão no ciberespaço não é estática, evolui constantemente desde a criação da internet e a todo o tempo. A internet carrega um paradoxo desde seu

[21] Conforme menciona Jesus & Milagre (2016, pp. 30-31), o Brasil adota o sistema da reserva legal, onde não há crime sem Lei anterior que o defina, especialmente quando tratamos de tecnologia da informação. A técnica para criar Leis deve ser outra isto porque o legislador deve ter cuidado para que não produzir uma legislação natimorta, que ingressa no arcabouço legislativo de modo ultrapassado. A mora legislativa no âmbito dos crimes cibernéticos produz um prejuízo a mais, concebendo normas ultrapassadas. Há que se ter o cuidado de não produzir legislação sobre técnicas. A velocidade com que a tecnologia evolui pode tornar a legislação demasiado específica, pouco eficaz e com rápida obsolescência. Nessa seara, a melhor opção reside em eleger condutas incriminadas que possam ser realizadas de forma diversas e que mereçam séries incriminadas pelo Direito Penal. Assim de pouco adiantaria criminalizar a disseminação do Cavalo de Troia, por exemplo, pois essa técnica pode ser abandonada em detrimento de outra mais nova, mais eficaz e não criminalizada.

[22] Conforme Prado (2013), a percepção cultural do risco difere do risco em si, como acontecimento antecipado compreendido de modo racional, gerando a subjetividade do risco, construída pelas tecnologias de comunicação que interconectam o mundo em um “presente comum” a todas as pessoas pela primeira vez na história.

nascimento, pois foi concebida para proteção da informação com fins militares. Entretanto, teve seu crescimento e difusão alavancado em razão da criação de *softwares* abertos e colaborativos desenvolvidos por pesquisadores de universidade, responsáveis por impregnaram a web com a cultura libertária na qual estavam inseridos. Segundo Castells (2003, p. 24), foi "na zona ambígua dos espaços ricos em recursos e relativamente livres criados pela *Advanced Research Projects Agency* (ARPA), universidades, centro de estudos inovadores e grandes centros de pesquisa que as sementes da internet foram cultivas"[23]. Essa interação resultou em uma arquitetura aberta, possibilitando seu desenvolvimento autônomo, na qual os próprios usuários são os produtores da tecnologia. As colaborações dos internautas resultaram na gama de aplicativos hoje existentes, desde o e-mail e chats, até a *deep web*[24]. Mas também resultou no desenvolvimento de tecnologias para proteção da informação e preservação do anonimato, como o tráfico criptografado de dados e ocultação do endereço IP.

Os Estados seguem buscando um maior controle do que se passa na internet. Mesmo nos Estados Unidos, berço da liberdade de expressão, algumas tentativas foram feitas para um maior controle da rede mundial, especialmente em razão do tráfego de pornografia infantil. Entretanto, a justiça dos Estados Unidos entendeu que essas tentativas colidiam com a primeira emenda e não poderiam ser

[23] De acordo com Castells "as origens da Internet podem ser encontradas na Arpanet, uma rede de computadores montada *pela Advanced Research Projects Agency* (ARPA) em setembro de 1969. A ARPA foi formada em 1958 pelo Departamento de Defesa dos Estados Unidos com a missão de mobilizar recursos de pesquisa, particularmente do mundo universitário, com o objetivo de alcançar superioridade tecnológica militar em relação à União Soviética na esteira do lançamento do primeiro Sputnik em 1957. A Arpanet não passava de um pequeno programa que surgiu de um dos departamentos da ARPA [...]. O objetivo desse departamento, tal como definido por seu primeiro diretor, Joseph Licklider, um psicólogo transformado em cientista da computação no Massachusetts Institute of Technology (MIT), era estimular a pesquisa em computação interativa. Como parte desse esforço, a montagem da Arpanet foi justificada como uma maneira de permitir aos vários centros de computadores e grupos de pesquisa que trabalhavam para a agência compartilhar on-line tempo de computação". (2003, pp. 12-13)

[24] De forma bastante sintética, a *deep web* consiste nas páginas e conteúdos restritos que não podem ser localizados por meio da utilização das ferramentas de pesquisa (buscadores) como Google e Bing, para citar as mais acessadas. Compõem a *deep web* por exemplo as intranets do governo e de grandes empresas privadas, para as quais exige-se autorização de acesos, compostas por nome de usuário, senha por exemplo.

implementadas sob pena de violação da privacidade dos cidadãos (Castells, 2003, p. 148). Em face da arquitetura aberta e colaborativa da internet, a investigação de crimes cibernéticos exige conhecimento técnicos e constante atualização. As técnicas que funcionam hoje poderão não funcionar amanhã.

Em sede de atividade repressiva de polícia judiciaria, a mais basilar das investigações inicia-se com a identificação da materialidade delitiva. Constatado o cometimento de um crime, passa-se a tentativa de identificar o autor atrás do teclado. Para tanto, a polícia terá que buscar a colaboração dos provedores de internet (*service providers*), os quais são os responsáveis por atribuir o endereço IP aos usuários que contratam seus serviços. Entretanto, as técnicas de anonimização e encriptação dificultam saber quem é o cidadão real por detrás do perfil responsável pela prática criminosa. Outra dificuldade consiste na alta probabilidade desse primeiro dado rastreado estar armazenando nos bancos de dados de uma empresa localizada além-fronteiras.

Esses elementos aliados, quais sejam: a facilidade para a prática de ilícitos, derivada da sensação de anonimato e da inabilidade dos usuários para se proteger; os prejuízos causados as empresas e pessoas físicas; as dificuldades técnicas existentes para uma investigação digital, criaram em todo o mundo um clamor pelo aumento da proteção aos bens jurídicos já existentes e aos novos bens jurídicos surgidos com a rede mundial de computadores (identidades e moedas virtuais por exemplo).

2.1 - A legislação em Portugal

Atualmente, a matéria cibernética está regulada pela Lei n.º 109/2009[25]. Conforme consta no próprio texto, a Lei em questão adaptou ao direito português a Convenção sobre o Cibercrime (Convenção de Budapeste). E trouxe para o ordenamento jurídico português a Decisão-Quadro nº 2005/222/JAI, do Conselho da Europa. A referida decisão-quadro acompanhou as linhas orientadoras promovidas pela Convenção sobre o Cibercrime, com o objetivo reforçar a cooperação entre as autoridades judiciárias e outras autoridades competentes mediante uma aproximação das suas disposições de direito penal em matéria dos ataques contra os sistemas de informação, conferindo especial atenção ao caráter transnacional e transfronteiriço da internet, evidenciando a necessidade urgente de prosseguir a harmonização das legislações penais em matéria de crimes cibernéticos (Marques, 2014, p. 7).

A Lei n.º109/2009 manteve os tipos penais introduzidos pela Lei n.º 10/91 e trouxe novos tipos penais. Entretanto, as mais expressivas inovações se referem ao processo e meios de prova considerados novidades para o ordenamento jurídico português, pois foi o primeiro diploma legal a contemplar um regime específico de obtenção da prova digital, superando a lacuna da Lei nº 109/91 de 17 de Agosto (Criminalidade Informática) que introduziu um regime processual não aplicável somente a processos relativos a crimes previstos na respectiva Lei, como também a processos relativos a crimes cometidos através de um sistema informático ou em qualquer processo criminal em que seja necessário proceder a recolha da chamada prova digital.

[25] A primeira referência sobre dados informáticos foi incluída no direito lusitano pela Constituição da República Portuguesa de 1976, a qual inseriu no artigo 35º a proteção das pessoas contra o tratamento informático de dados pessoais. As revisões constitucionais posteriores ampliaram a extensão deste artigo no que tange a acesso por terceiros de dados pessoais informatizados. Em 1991, foi promulgada a Lei 10/91 para regulamentar a matéria tratada constitucionalmente, bem como harmonizar a legislação portuguesa com a Convenção 108 do Conselho da Europa (Venâncio, Lei do Cibercrime Anotada e Comentada, 2011, p. 13)

Portanto, o espectro de aplicação das ferramentas previstas na Lei n.º109/2009 é mais amplo do que a própria Lei, seus dispositivos podem ser aplicados em investigações de quaisquer tipos penais, desde que seja necessária a recolha de prova digital. Os meios de obtenção de prova previstos nos artigos 12.º a 17.º são de aplicação geral, ou seja, podem ser utilizados em processos relativos aos crimes previstos na respectiva Lei. No entanto, o artigo 11.º restringe a aplicabilidade dos artigos 18.º e 19.º, em face do caráter bastante intrusivo destas duas diligências.

Por fim, o artigo 19.º trata das ações encobertas, determinando a admissibilidade de utilização de ações encobertas previstas na Lei nº 101/2001, nos termos aí previstos, no decurso de inquérito relativo par a um rol de crimes[26]. O artigo 19.º, n.º 1, amplia a possibilidade de recurso à ação encoberta, prevendo um conjunto de crimes que não se encontravam previstos no Regime Jurídicos sobre as Acções Encobertas[27]. Alguns doutrinadores criticam essa ampliação, que

[26] " os previstos na presente Lei: 101/2001 e os cometidos por meio de um sistema informático, quando lhes corresponda, em abstracto, pena de prisão de máximo superior a 5 anos ou, ainda que a pena seja inferior, e sendo dolosos, 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."

27 1.O âmbito de aplicação da Lei do cibercrime foi objeto de Acordo do Tribunal de Recursos conforme segue: 2015: 1. O regime processual das comunicações telefónicas previsto nos artigos 187º a 190º do Código de Processo Penal deixou de ser aplicável por extensão ás «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 deixará 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.º 109/2009, o do artigo 18º, n.º 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 as 17º

associa crimes informáticos e crimes cometidos pelo computador, e principalmente por prever uma medida de carácter muito excepcional para um leque muito amplo de crimes, sem aprofundamento normativo dos princípios da proporcionalidade e da necessidade (Marques, 2014, pp. 29-30). Segundo o artigo 1º da Lei 101/2001 "consideram-se ações encobertas aquelas que sejam desenvolvidas por funcionários de investigação criminal ou por terceiro atuando sob o controle da Política Judiciária para prevenção ou repressão dos crimes indicados nesta Lei, com ocultação da sua qualidade e identidade"[28]. O art. 2º elenca o catálogo de crimes nos quais a técnica de investigação poderá ser utilizada, aos quais se somam os crimes previstos na Lei do Cibercrime. O referido regime jurídico permite a realização da ação encoberta para **prevenção e repressão** da criminalidade, desde que demonstradas indícios mínimos da prática criminosa ou de atos preparatórios de ação criminosa futura daqueles crimes do catálogo, somados aos crimes previstos no artigo 19 da Lei do Cibercrime. Assim, a infiltração poderá ser utilizada como instrumento de prevenção da criminalidade e também para recolha de provas em uma investigação criminal posterior ao fato investigado. A Lei da infiltração não diferencia entre agente infiltrado, encoberto e à civil, deixando a impressão que todas essas formas de atuação se equivalem. Entretanto, conforme dito alhures essa diferenciação vai além de mera classificação acadêmica. O

da supramencionada Lei contêm um completo regime processual penal para os crimes que, nos termos das alíneas do n.º 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 a pesquisa e recolha, para prova, de dados já 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 ás 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» (Da Mesquita) [...]

[28] Lei 101/2001 disponível em https://www.parlamento.pt/ActividadeParlamentar/Paginas/DetalheDiplomaAprovado.aspx?BID=4102

regime jurídico tratado pela Lei n.º 101/2001 tem afinidade lógica com a atuação do agente infiltrado, de modo que a disciplina jurídica desenhada pela referida Lei não se adequa a atuação policial na forma de agente à civil ou do agente encoberto.

2.2 - A legislação no Brasil

Embora a internet tenha chegado ao Brasil na década de 80, somente em 2012 foi editada a primeira Lei específica sobre cibercrimes[29]. Até então, a tutela dos bens jurídicos violados era feita com base nos diplomas legais tradicionais, entre eles o Código Penal Brasileiro, o Estatuto da Criança e do Adolescente (Lei n.º 8069/90), Lei dos crimes de software ou Lei Antipirataria (Lei n.º 9.609/98) e a Lei de Segurança Nacional (Lei n.º 7.170/83). A Lei n.º 12.737, de 30 de novembro de 2012, alterou o Código Penal para tornar típicas as condutas de "invasão de dispositivo informático", "interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública" e "falsificação de cartão de credito ou debito"[30]. Contudo, mesmo após a aprovação

[29] A Lei em questão, Lei 12737, disponível em http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/Lei/l12737.htm, dispôs sobre a tipificação criminal dos delitos informáticos, introduzindo os artigos 154-A, 154-B, e alterando os artigos 266 e 298, todos do Código Penal. O art. 154-A do Código Penal trouxe para o ordenamento jurídico o crime novo de "invasão de dispositivo informático", consistente na conduta de "invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita" O bem jurídico tutelado como sendo a liberdade individual, a privacidade e a intimidade das pessoas como um todo (Silveira, 2015).

[30] A Lei em questão passou a ser conhecida como Lei Carolina Dieckmann. A nomenclatura, embora não conste no texto da lei, consta no site da Câmara dos Deputados, como explicação da Ementa da Lei aprovada (Wendt, 2017, p.50). A divulgação de fotos íntimas da atriz Carolina Dickmann após invasão não autorizada de dispositivos informáticos teve intensa divulgação nas mídias tradicionais e digitais. A ausência de tipificação penal para o fato até então, em face da dificuldade no tramite dos diversos projetos de criminalização em curso no Congresso Nacional, gerou comoção social que resultou em um trâmite legislativo bastante célere e aprovação da Lei em questão. Conforme recorda Wendt (2017, p. 61): "O ponto crucial por assim dizer, da atividade midiática veio aos telespectadores e leitores na segunda-feira – 14/05/2012 – com a divulgação, em cadeia nacional, da entrevista dada por Carolina Dieckmann ao programa de notícias Jornal Nacional. A chamada da notícia chama a atenção pelo termo apelativo na fala da atriz vítima e da mídia: 'sensação de faca no peito'. " Embora a percepção social tenha sido de rapidez, a Lei em comento foi o resultado do apensamento de diversos projetos de Lei, sendo o principal deles o PL 84/99 apresentado pelo

da Lei n.º 12.737/2012, a sensação de lacuna legislativa permaneceu. Persistiam os reclamos de grupos da sociedade civil pela criação de normas estruturantes e garantidoras dos direitos dos usuários, delineava-se o que viria a ser o futuro "marco civil da internet" (Wendt, 2017, p. 53). Em face disso, se intensificaram os debates para a aprovação do projeto de Lei.

Cerca de um ano após a publicação da Lei 12737/2012, foram reveladas as denúncias de espionagem cibernética feita pelo ex-funcionário da Agência Nacional de Segurança dos Estados Unidos, Eduard Snowden, em desfavor do Governo desse país e tendo como vítimas outros governos, inclusive o do Brasil31. Esse fato se converteu em pressão para a aprovação pelo Congresso Nacional do Marco Civil da Internet. [32] Após longa tramitação no Congresso Nacional, foi publicada a Lei n.º 12.965/2014, conhecida no Brasil como "Marco Civil da Internet". O referido diploma legal reflete em seus inúmeros dispositivos princípiológicos e garantistas, as preocupações da sociedade brasileira com o contexto mundial de monitoramento ou espionagem cibernética[33].

Senador Eduardo Azeredo. O projeto de Lei Azeredo recebeu a alcunha de AI5 Digital, em referência as normas expedidas pela Ditadura Militar brasileira, por ter como foco a criminalização de condutas e responsabilização dos servidores e não a definição de direitos e garantias aos usuários da internet (Wendt, 2017, pp. 51-53).

[31] Para saber mais sobre os fatos acesse a reportagem "Edward Snowden e a espionagem da NSA", disponível em https://www.terra.com.br/noticias/mundo/estados-unidos/edward-snowden-e-a-espionagem-da-nsa,6289f082fe3df310VgnVCM3000009acceb0aRCRD.html

[32] Conforme Tomasevicius Filho (2016, p. 272): De qualquer forma, essa proposta de disciplina de princípios, garantias, direitos e deveres dos usuários da internet no Brasil foi concebida em 2009 em parceria do Ministério da Justiça com a Escola de Direito do Rio de Janeiro, da Fundação Getúlio Vargas (FGV Direito Rio, 2014), o que resultou na apresentação de um projeto de Lei ao Congresso Nacional, registrado sob o n.º2.126/2011, convertido na Lei n.º12.965, de 23 de abril de 2014. Sua apresentação em 2011 evidencia ser iniciativa bem anterior aos escândalos de privacidade divulgados em 2013. Inclusive diversos projetos de Lei foram apresentados desde o ano 2000, os quais tramitaram em apenso a este (Câmara dos Deputados, 2014). O texto foi submetido a consultas públicas em diversas cidades brasileiras, bem como se franqueou a possibilidade de oferecimento de sugestões pela própria internet. A partir dessa iniciativa, o relator do projeto, deputado Alessandro Molon (então PT-RJ), ofereceu substitutivo que incorporava as principais sugestões oferecidas e que foram incorporadas no texto final. Na Câmara dos Deputados, o Projeto de Lei foi intensamente discutido por ter-se requerido urgência em sua análise.

[33] Entretanto, o diploma legal não foi muito bem recebido pelos juristas. Entre as críticas, está a ausência de conteúdo normativo dos dispositivos, a preocupação em estabelecer garantias aos usuários e estabelecer a internet como um território democrático, gerando repetição de garantias já

Havia preocupação de sobre retomada da censura no país, motivo pelo qual foi inserido o texto no art.2º, caput, afirmando que “a disciplina do uso da internet no Brasil tem como fundamento o respeito à liberdade de expressão, e o art.19 declara-se que "com o intuito de assegurar a liberdade de expressão e impedir a censura [...]". Os textos aprovados não existiam no projeto original. Em face disso, repetiu-se o que consta no art.3º, I, que dispõe como princípio do uso da internet a "garantia da liberdade de expressão, comunicação e manifestação do pensamento, nos termos da Constituição Federal". (Tomasevicius Filho, 2016, pp. 269 – 285). [34]

No que tange a infiltração policial propriamente dita a primeira tentativa de implementá-la no ordenamento jurídico Brasileiro foi a previsão inserida no bojo da Lei n.º 9.034/1995, primeira resposta brasileira ao fenômeno do crime organizado. Entre os mecanismos eleitos para o enfrentamento aos grupos criminosos organizados a citada Lei trazia a previsão de infiltração. A Lei em questão foi aprovada pelo Congresso Nacional e seguiu para sanção presidencial. Entretanto, o dispositivo em que a medida estava prevista foi vetado pelo Presidente da República ao argumento de que a versão final do projeto de Lei em tela se distanciava do texto discutido na Comissão de Constituição e Justiça, o qual estabelecia a necessidade de autorização judicial para a realização da infiltração policial. A segunda razão para o veto foi a conferência de autorização para que o agente infiltrado cometesse o crime previsto no art. 288 do Código Penal (quadrilha ou bando) com previsão expressa da exclusão de antijuridicidade da conduta.

asseguradas, como o direito à privacidade e a inviolabilidade das comunicações, as quais estão previstas no art. 5, incisos X e XII da Constituição Federal (Tomasevicius Filho, 2016, pp. 269 – 285)

[34] Foi conferida atenção especial ao direito à privacidade, tanto do ponto de vista do direito ao isolamento quanto da proibição de que terceiros acessem as informações acerca desse usuário. As previsões do artigo 7º, incisos I, II, III, VII e VIII elencam os direitos dos usuários de internet: inviolabilidade da intimidade e da vida privada, a preservação do sigilo das comunicações privadas pela rede, transmitidas ou armazenadas; o não fornecimento de dados pessoais coletados pela internet a terceiros sem prévio consentimento do usuário, o dever de informar os usuários acerca da coleta de dados sobre si, quando houver justificativa para tal fato.

Segundo a mensagem de veto, tal previsão afrontaria a sistemática do código penal (Carlos & Reis, 2014, p. 2).[35]

Em 11 de abril de 2001 foi aprovada a Lei 10.217, que alterou os artigos 1º e 2º da Lei 9.034/1995. A previsão de infiltração como meio de prova e procedimento investigatório a ser utilizado em crimes praticados por quadrilha ou bando, ou por organizações criminosas de qualquer tipo, estabelecendo que, em qualquer fase da persecução penal, poderiam ser admitidos, como procedimentos de investigação e formação de prova, a ação controlada, a interceptação ambiental e a infiltração de agentes de polícia ou de inteligência, mediante autorização judicial obtida em procedimento sigiloso. Contudo, não foi estabelecido o procedimento a ser seguido para a realização da infiltração ou o tratamento jurídico aos atos ilícitos porventura praticados durante a infiltração[36]. A inexistência de parâmetros mínimos para a realização da infiltração policial, aliada a insegurança jurídica sobre o conceito de organização criminosa, tornaram inviável a utilização da infiltração policial.

A Lei n.º 11.343/2006, ao tratar do tema das drogas, trouxe a previsão de utilização da infiltração como instrumento investigativo ou meio de prova. Entretanto, persistiam os problemas dos diplomas legais anteriores, não houve detalhamento dos procedimentos necessários à produção da prova através da infiltração. Depois de intensos debates no Congresso Nacional, foi aprovada a Lei n.º 12850/2013. A Lei em questão, cuja vigência persiste até o presente momento, define organizações criminosas e traz um rol de procedimentos a disposição do estado para investigação dos crimes cometidos por organizações criminosas, bem como a aplicação de seus ditames nos processos sobre crimes transnacionais

[35] A Lei 9034 de 1995, primeira Lei sobre o crime organizado promulgada no Brasil, não contou com a possibilidade de infiltração como um dos mecanismos a serem utilizados na investigação dos crimes cometidos pelas organizações criminosas. Gerou muitas críticas doutrinarias a seu respeito. Por motivos não muito claros o mencionado diploma legal não trouxe uma definição sobre o que consistiria em “organização criminosa”. Desse modo, até o advento da Lei 12850, coube à doutrina e aos tribunais buscar uma definição para o preenchimento da lacuna legislativa

[36] Nesse período, o conceito de organização criminosa aplicado no direito Brasileiro era o trazido pela Convenção de Palermo

previstos em tratados e aqueles praticados por organizações terroristas. Traz mais detalhes sobre o procedimento, conferindo tratamento aos atos praticados pelo policial infiltrado. De modo que pode ser considerada uma lei com mais densidade normativa. Como a Lei em tela trata de organizações criminosas, a técnica investigativa poderá ser usada quando os crimes em investigação estiverem sendo praticado em "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". No §2º do art. 1º, a Lei n.º 12.850/2013 está prevista a possibilidade de aplicação de seus dispositivos às infrações previstas em tratados e às organizações terroristas. Como corolário, as técnicas de investigação trazidas no bojo do referido diploma legal, dentre elas a infiltração, possuem um âmbito de aplicação que desborda as ações praticadas pelas organizações criminosas.

No caso das infrações penais previstas em tratado, que possuam o viés da transnacionalidade, importante referir que a República Federativa do Brasil é signatária de diversos tratados em matéria penal[37]. Entre eles destacam-se a Convenção das Nações Unidas contra o Crime Organizado Transnacional, mais conhecida como Protocolo de Palermo, a Convenção contra o Tráfico Ilícito de Entorpecentes e de Substâncias Psicotrópicas, a Convenção sobre os Direitos da Criança, Convenção Internacional sobre Eliminação de todas as formas de Discriminação Racial, a Convenção contra a tortura e outros Tratamentos ou Penas cruéis, desumanas ou degradantes, a Convenção das Nações Unidas contra corrupção, dentre outras. Nesses casos, as técnicas de investigação previstas na Lei 12850/2013 podem ser utilizadas, desde que o crime em investigação esteja

[37] Para verificar todos os tratados ratificados pelo Brasil basta consultar o site do Ministério das Relações Exteriores (http://dai-mre.serpro.gov.br).

previsto em tratado e possuam a característica da transnacionalidade, a qual na maior parte das vezes é conferida pela atuação no ciberespaço[38].

Igualmente, existe previsão de aplicação dos ditames da Lei antes referida com relação às organizações terroristas[39].

A Lei n.º 13.441 publicada em 8 de maio de 2017 alterou o Estatuto da Criança e do Adolescente (Lei 8.069/1990) para incluir a Seção V-A, destinada a tratar da infiltração de agentes de polícia na internet, com o fim de investigar os crimes relacionados à exploração sexual de crianças e adolescentes por meio da internet, previstos nos artigos 240, 241, 241-A, 241-B, 241-C e 241-D da Lei n.º 8069, e nos artigos 154-A 217-A, 218, 218-A e 218-B do Código Penal[40]. A exemplo do disposto na Lei n.º 12850/2013, ficou estabelecida a necessidade de decisão

[38] A jurisprudência do Superior Tribunal de Justiça tem entendido que os crimes praticados pela internet podem ser considerados transacionais em face do *modus operandi* do grupo criminosos em investigação. Nesse sentido o entendimento do STJ ao analisar a competência da justiça criminal para o julgamento de grupo que disseminava pornografia infantil na internet. RECURSO ORDINÁRIO EM HABEAS CORPUS. PRODUÇÃO E FOTOGRAFIA DE CENA PORNOGRÁFICA ENVOLVENDO CRIANÇA, DIVULGAÇÃO DE IMAGENS OU FOTOGRAFIAS COM CONTEÚDO PORNOGRÁFICO INFANTIL E ARMAZENAMENTO DE ARQUIVOS CONTENDO CENAS OU IMAGENS PORNOGRÁFICAS OU DE SEXO EXPLÍCITO ENVOLVENDO CRIANÇAS OU ADOLESCENTES. UTILIZAÇÃO DE FÓRUNS NA INTERNET E SITE EM REDE OCULTA NA INTERNET. TRANSNACIONALIDADE DO DELITO. COMPETÊNCIA DA JUSTIÇA FEDERAL.
1. De acordo com o artigo 109, inciso V, da Constituição Federal, compete aos Juízes Federais processar e julgar "os crimes previstos em tratado ou convenção internacional, quando, iniciada a execução no País, o resultado tenha ou devesse ter ocorrido no estrangeiro, ou reciprocamente".
2. No caso dos autos, o crime em tese praticado pelo recorrente consta daqueles cujo combate o Brasil se comprometeu perante a comunidade internacional, ao aderir à Convenção sobre os Direitos da Criança e do Adolescente, promulgada no ordenamento jurídico pátrio pelo Decreto 99.710/1990. 3. Para que a competência da Justiça Federal seja firmada, não basta que o Brasil seja signatário da referida Convenção, sendo imprescindível a comprovação da internacionalidade da conduta atribuída ao acusado. Precedente. 4. Na hipótese em apreço, a forma como o recorrente disponibilizaria, transmitiria, publicaria e divulgaria arquivos contendo pornografia ou cenas de sexo explícito envolvendo crianças ou adolescentes permitirá o seu acesso por pessoas em qualquer local do mundo, bastando que também participassem dos mesmos fóruns que ele, ou que também acessassem sites na rede oculta chamada *deep web*, circunstância que revela a transnacionalidade da conduta narrada na exordial acusatória e justifica a competência da Justiça Federal para processar e julgar o feito. [*Omissis*] 2. Recurso desprovido.

[39] A Lei é fruto de projeto elaborado pela Comissão Parlamentar de Inquérito (CPI) sobre Pedofilia, ou CPI da Pedofilia, que atuou até o ano de 2010. A referida CPI foi promotora de importantes alterações e adequação dos tipos penais referentes aos crimes relacionados à pornografia infantil na internet.

[40] Lei 13441/2017 está disponível no site do Planalto (http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/Lei/L13441.htm)

judicial fundamentada e circunstanciada para a implementação da medida. Ainda em consonância com a Lei em vigor, estabelece como requisito a comprovação da necessidade da medida, dispondo que não será admitida quando a prova puder ser obtida por outros meios. Como requisitos, a lei estabelece que devem ser informados os nomes ou apelidos das pessoas investigadas, bem como os dados de conexão ou cadastrais que permitam a sua identificação. O art. 190-C trata da proporcionalidade dos atos praticados, alertando que o agente policial infiltrado que deixar de observar a estrita finalidade da investigação responderá pelos excessos praticados. A menção ao princípio da proporcionalidade não é muito comum na legislação brasileira. Mesmo a Constituição não faz referência a tal princípio. Entretanto, a jurisprudência da suprema corte reconhece e aplica a proporcionalidade.

2.3 - Será a infiltração digital uma decorrência do Direito Penal do Inimigo?

Os riscos nascidos com o uso da internet fizeram surgir pressões sobre o direito penal no sentido de sua expansão, visando criminalizar novas condutas danosas ao tecido social. De acordo com Venâncio (2011, p. 14) a Internet é instrumento de atividade econômica, cultural e social, tendo papel essencial no desenvolvimento social, entretanto também opera como instrumento potencializador e facilitador da prática de atos ilícitos (contra as pessoas, o património ou a própria estrutura organizada da sociedade). Em face disso, a informática passou também a ser o centro de muitos receios, tornando-se alvo das atenções legislativas da União Europeia e de diversos Estados ocidentais.

A cultura do medo diante das ameaças surgidas com o incremento do uso da internet, entre elas o ciberterrorismo, a pornografia infantil, as invasões e furtos a sistemas, passam a legitimar uma mudança de paradigma de um direito penal e processual penal garantista para o paradigma de um direito penal do inimigo. O delinquente assume a condição de uma não-pessoa, um câncer a ser extirpado,

que não pode nem deve ser tratado como um cidadão. A definição do criminoso cibernético como inimigo justificaria o uso de todos os meios disponíveis para neutralizar o "perigo", criando um direito penal hipertrofiado (Valente, 2010a, pp. 16-17).

Entretanto, o princípio do estado democrático de direito impõe, um equilíbrio ao direito penal moderno para o alcance de suas finalidades pois a ação penal vai incidir em um ser humano que como tal deve ser tratado (Valente, 2010a, p. 14). Importante referir que o surgimento do Direito Penal do Inimigo é bem anterior ao advento da internet. Já foi utilizado para justificar as atrocidades nazistas referente ao extermínio dos não arianos e é revisitada, de tempos em tempos, a cada nova crise do Direito Penal. [41]

Após a Segunda Guerra Mundial, o direito penal humanista firmou-se como o paradigma a ser seguido, especialmente em face dos ditames da Declaração Universal dos Direitos do Homem (DUDH), limitadores de abusos do detentor do *jus puniendi.* Essa primazia foi novamente posta em causa após os ataques de 11 de setembro de 2001 ocorridos na cidade de Nova Iorque. De outro norte, o fenômeno da internet criou bens jurídicos que efetivamente estavam carentes da proteção penal. Nesse ponto, a tipificação dos crimes informáticos está em linha de convergência com a definição de bens jurídicos defendida por Litz (*apud* Silva, 2004, p. 297), segundo a qual "a norma jurídica incriminadora encontra o bem jurídico e não o cria". Desse modo, havendo efetiva interação entre indivíduos dessa tal era digital, haverá também aquelas compreendidas no parâmetro de repercussões negativas a bem jurídico de relevante valor.

É relativamente consensual a ideia de que os bens jurídicos socialmente importantes não devem estar desprotegidos, especialmente se a justificativa for o fato de uma conduta ter sido realizada em um ambiente diverso daquele originalmente imaginado pelo legislador no tempo e espaço de criação das leis

[41] Conforme leciona Silva (2004, p. 283), a crise do direito penal é reflexo da tensão da sociedade em transformação. Em tempos de mudanças mais aceleradas, as crises se tornam mais visíveis.

(Sousa, 2015, p. 65). Sendo assim, a nova criminalidade não há que ser encarada pela perspectiva do surgimento de um inimigo (hacker ou o pedófilo *on line*), mas sim, em face da existência de bens jurídicos relevantes, violados a tal ponto que passam a merecer a tutela penal. Corolário dessa violação, os autores do crime poderão ter seus direitos fundamentais restringidos através do processo penal de índole garantista. As restrições, entretanto, devem ter como balizas os princípios processuais penais que limitam o jus puniendi. A infiltração digital, portanto, não consistiria, por essa ótica, em exacerbação dos poderes de polícia fulcrada no desejo de exterminar o inimigo. Mas na adequação de uma técnica de investigação em face de uma nova realidade tecnológica. Entretanto, os conceitos da "sociedade de risco"[42], incrementadas pelo surgimento dos crimes cibernéticos, os quais impõe mais dificuldades técnicas à investigação criminal, não podem justificar a mudança de paradigma do direito penal, de um direito penal garantista, do ser humano, para o direito penal do autor ou do inimigo (Valente, 2010a, p.54). [43]

[42] Em 1986, o filosofo alemão Ulrich Beck ele lançou o livro *Risikogesellschaft: Auf dem Weg in eine andere Moderne.* No Brasil, recebeu o título Sociedade de risco: rumo a uma outra modernidade. Ao lado do sociólogo inglês Anthony Giddens, Beck desenvolveu a noção de sociedade de risco, na qual defende a ideia de que a modernidade passa por um momento de ruptura histórica, que resultará em sua reconfiguração. A sociedade industrial clássica, caracterizada pela produção e a distribuição de riquezas, se transforma em uma chamada sociedade (industrial) de risco, na qual a produção dos riscos domina a lógica da produção de bens. Os novos riscos seriam mais democráticos e globalizados, tornando a repartição mais equalizada. Sendo assim, ninguém, nem pobres nem ricos, estariam totalmente imunes às ameaças produzidas e agravadas pelo progresso (Macedo, 2015, p.1). O conceito de sociedade de risco tem sido bastante mencionado por juristas para justificar a necessidade de alterações na lei penal.

[43] Na legislação brasileira acerca dos crimes cibernéticos, um exemplo da excessiva expansão do direito penal, de acordo com Sousa (2015, pp. 94-95) consiste no tipo penal insculpido no art. 241C do Estatuto da Criança e do Adolescente Brasileiro, que criminaliza a simulação quanto a participação de criança ou adolescente em material que contenha pornografia infantil. A conduta descrita na norma penal incriminadora atenta contra a honra e a dignidade da criança ou adolescente, bem jurídico já protegido pelo Código Penal. O tipo penal é de perigo abstrato uma vez que não prevê resultado naturalístico para a ação. Para o referido estudioso a inclusão da norma penal não teve por escopo a defesa do bem jurídico violado, mas sim a criminalização na máxima potência do autor desse tipo de crime, o pedófilo, eleito como inimigo não-humano. Para Silva (2004, p. 290) crimes de perigo abstrato contrariam a tradição de proteção a efetiva lesão a bens jurídico contribuem para dificultar a compreensão das proibições pelos cidadãos comuns, destinatários da norma, corroendo a função de limitadora do *jus puniendi* exercida pelo princípio da legalidade.

A sociedade não pode colocar sobre os ombros do direito penal a responsabilidade por extirpar todos os riscos, sendo um equívoco imaginá-lo como "panaceia primária para a proteção de bens imateriais" (Brito, 2013, p. 28).

3 - OS LIMITES IMPOSTOS AO ESTADO PELOS PRINCÍPIOS ESTRUTURANTES SUPRACONSTITUCIONAIS

A técnica de recolha de provas através da infiltração não é isenta de críticas. As vozes contrárias afirmam a recolha de provas por meio da atuação do agente infiltrado configura gravíssima contradição, que deslegitima o Estado como titular do *jus puniendi* em face da violação ao princípio da superioridade ética. Para desempenhar o seu papel de repressor das condutas ilícitas, o Estado concede aos seus agentes a faculdade de cometer os mesmos atos que repudia. Em face disso, perderia a legitimidade para a persecução criminal pois, na ânsia de fazer cumprir as regras, ele mesmo as viola.

Os métodos ocultos de investigação, apesar da grande danosidade social, passaram a ser considerados insubstituíveis na perseguição e repressão de uma nova fenomenologia criminal denominada criminalidade organizada, transnacional, transacional, consensual, imunes à devassa dos meios tradicionais e "abertos" de investigação. Entretanto, a aplicação dos métodos ocultos de investigação entra em rota de colisão com um amplo leque de direitos fundamentais extremamente caros ao processo penal, quais sejam: privacidade/intimidade, sigilo das comunicações, direito à imagem, sigilo profissional, inviolabilidade do domicílio, confidencialidade e integridade dos sistemas técnico-informacionais, entre outros (Andrade, 2009a, pp. 105-106). Para alguns doutrinadores, a infiltração policial está inserido no âmbito dos métodos proibidos de prova, por consistir em um meio

enganoso e desleal que põe em causa a dignidade e a legitimidade do processo penal[44] (Andrade, 2013, p. 229).

Importante nesse passo referir que o art. 126 do Código de Processo Penal Português[45], ao elencar os métodos proibidos de prova, estabelece literalmente que é proibida a **utilização de meios enganosos**. Logo, sendo o engano quanto a condição de policial do agente infiltrado a essência do conceito de infiltração, de plano, a técnica poderia inquinar de nulidade todas as provas recolhidas, pois seria meio proibido de prova, subespécie meios enganosos (Andrade, 2013, p. 229).

O processo criminal tem como desafio conciliar dois princípios ético-jurídicos fundamentais: o princípio da reafirmação, defesa e reintegração da comunidade ético-jurídica e o princípio do respeito e garantia da liberdade e dignidade dos cidadãos, direitos irredutíveis da pessoa humana. (Ramalho, 2017, p. 228).

Visando cotejar a técnica da infiltração com os princípios que regem o processo penal do ser humano e preservar a função do processo penal como "processo penal dos inocentes" (Valente, 2010a), serão analisados alguns desses

[44] Andrade (2013, p. 232) é um severo crítico a utilização de todas as formas de homem de confiança por considerar um meio enganoso de prova, logo configuraria método proibição de prova, conforme a constituição portuguesa e código de Processo Penal Português, entretanto o ilustre processualista acaba por capitular e admitir a utilização ao admitir que a generalidade dos autores e da jurisprudência continuam a encarar o "*polizeispitzel*" como expediente indispensável duma resposta eficaz as manifestações mais ameaçadoras da criminalidade". Manuel da Costa Andrade apresenta como solução a adoção restritiva do recurso ao "homem de confiança", excluindo em absoluto dessa atuação a provocação ao crime, especialmente em face da existência de previsão legal para a utilização desse meio de prova.

[45] Artigo 126.º - Métodos proibidos de prova:
1 - São nulas, não podendo ser utilizadas, as provas obtidas mediante tortura, coação ou, em geral, ofensa da integridade física ou moral das pessoas.
2 - São ofensivas da integridade física ou moral das pessoas as provas obtidas, mesmo que com consentimento delas, mediante:
a) Perturbação da liberdade de vontade ou de decisão através de maus tratos, ofensas corporais, administração de meios de qualquer natureza, hipnose ou utilização de meios cruéis ou enganosos;
b) Perturbação, por qualquer meio, da capacidade de memória ou de avaliação;
c) Utilização da força, fora dos casos e dos limites permitidos pela Lei;
d) Ameaça com medida legalmente inadmissível e, bem assim, com denegação ou condicionamento da obtenção de benefício legalmente previsto;
e) Promessa de vantagem legalmente inadmissível.
3 - Ressalvados os casos previstos na Lei, são igualmente nulas, não podendo ser utilizadas, as provas obtidas mediante intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações sem o consentimento do respectivo titular.

princípios, os quais devem servir como balizas para a atuação estatal no exercício do *jus puniendi*, limitando e embasando a ação de todos os atores do sistema de justiça.

No presente capítulo trataremos dos princípios supraconstitucionais estruturantes, assim entendidos aqueles mandamentos que não necessitam estarem escritos nas leis de cada país, mas que decorrem da implementação do estado democrático, quais sejam: princípio da superioridade ética do estado, princípio da lealdade, princípio da reserva de constituição e princípio da proibição da autoincriminação.

No próximo capítulo serão abordados os princípios processuais constitucionais, que estão inseridos nas constituições democráticas do Brasil e de Portugal, implícita ou explicitamente, e também na legislação infraconstitucionais, são eles o princípio da reserva legal e da reserva de catalogo, princípio da reserva de juiz, da proporcionalidade, da indispensabilidade do recurso ao meio oculto e o princípio da vinculação ao fim.

3.1 - O princípio da superioridade ética do Estado

O Processo Penal consiste em um sistema fundamentado e limitado pela dignidade da pessoa humana, com especial relevo quanto a integridade pessoal do investigado ou visado. De outra parte, o cidadão que passa a responder a um processo de índole criminal encontra-se em grande desvantagem em face do aparato estatal. Assim, necessariamente, deverá haver alguma compensação diante da desigualdade de armas entre o investigado e o Estado, consistente na definição de garantias especiais de defesa. (Ramalho, 2017, p. 209). Assim, a atuação estatal na persecução criminal encontra fundamentos e limites nas normas constitucionais e nas supraconstitucionais, especialmente nos diplomas que tratam de direitos humanos, como por exemplo a Declaração Universal dos Direitos do

Homem, entre outras. Ao admitir a existência de limites aos meios de prova, o legislador voluntariamente está impondo limites ao princípio da verdade material e consagrando a regra da superioridade ética do Estado ao proibir que a verdade seja alcançada a qualquer custo. (Jesus, 2015, p. 124).

Ao considerar o investigado ou arguido em sua condição de ser humano, parte no processo penal e detentor de direitos, os servidores do estado encarregados da persecução criminal estarão incumbidos de afirmar a superioridade ética do estado, a qual se manifestará na produção legislativa lícitas e permitidas e na interpretação das normas penais e processuais. Em face do princípio da superioridade ética a infiltração policial por vezes tem sido considerada indigna de um estado democrático de direito que deseja a promoção do bem geral. A atuação de servidores do Estado em meio a criminosos e muitas vezes agindo como criminosos, entraria em conflito com os fundamentos do estado democrático de direito[46], maculando a sua superioridade como ente que deve dizer, interpretar e aplicar o direito.

O nº 1 do RJAE em Portugal estabelece a não punibilidade da conduta do agente encoberto no que tange a atos preparatórios eventualmente realizados no decurso de uma ação de infiltração. Não se trata, entretanto, de autorização para o cometimento de crimes, apenas a autorização para que o infiltrado simule a intenção de cometer o crime, motivo pelo qual não poderia ser punido em face da ausência do elemento subjetivo do injusto. Entretanto, se as condutas perpetradas não forem proporcionais aos fins da infiltração, poderá haver punição e inclusive a classificação do policial como agente provocador, tornando inadmissível toda a

[46] O fundamento do Estado Brasileiro, segundo a Constituição Federal são: a soberania, a cidadania, a dignidade da pessoa humana, os valores sociais do trabalho e da livre iniciativa, o pluralismo político. Entre os objetivos fundamentais desse estado estão a construir uma sociedade livre, justa e solidária; garantir o desenvolvimento nacional; erradicar a pobreza e a marginalização e reduzir as desigualdades sociais e regionais e promover o bem de todos, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação.

prova obtida, em face do regime da proibição de provas (Valente, 2017b, pp. 600-601).

No Brasil, a Lei 12850/2013 silencia a respeito dessa temática, donde seria legitimo inferir que a *mens legis* consistiu em vedar a prática de atos ilícitos pelo agente infiltrado. Inobstante, as cortes brasileiras têm firmado entendimento que o agente infiltrado não responde por associação criminosa, pois entendimento em contrário inviabilizaria a realização da infiltração. Já a Lei 13441/2017, dispõe de que não configura crime a atividade do policial que oculta a sua identidade para, por meio da internet, colher indícios de autoria e materialidade dos crimes do catálogo.

O princípio da superioridade ética do Estado se decompõe em outros princípios: princípio da lealdade ou boa-fé, princípio da legalidade, da constitucionalidade, da igualdade e imparcialidade, da autonomia e no princípio da prossecução do interesse público. (Valente, 2013, p. 393). Em face do recorte desse trabalho, abordaremos os princípios da lealdade, reserva de constituição, reserva de lei, além de outros princípios relacionados ao tema dos limites aos métodos ocultos de investigação que serão aprofundados no capítulo 4.

3.2 - Princípio da Lealdade ou boa-fé

O princípio em questão opera como legitimador de todas as funções do estado, sendo necessário para a manutenção da confiança que os cidadãos depositam nas referidas ações. Em Portugal, o referido princípio está consagrado constitucionalmente no n.º 8 do art. 32 da CRP que estabelece a nulidade das provas obtidas mediante tortura, coação, ofensa da integridade física ou moral da pessoa, abusiva intromissão na vida privada, no domicílio, na correspondência ou

nas telecomunicações, bem como no art. 266º, nº 2, in fine, da Constituição da República Portuguesa, no qual é literalmente referido[47].

Com relação à ação policial, o princípio em questão opera para criar um clima de confiança e previsibilidade no seio da administração pública, onerando os funcionários da administração pública a atuar de acordo com os valores básicos do ordenamento, adotando condutas não contraditórias, atendendo as expectativas dos cidadãos, investigados ou não, de que os atos praticados pelos servidores do sistema de justiça serão aqueles previstos nas normas e limitados pelos princípios gerais do direito. Assim, o investigado ou arguido deve ser encarado como um ser humano membro ativo da comunidade e também responsável pela construção de uma sociedade mais livre, mais justa e solidária e não apenas como objeto (alvo) das investigações policiais, com desprezo à dignidade que lhe é inerente (Valente, 2013, p. 393).

O princípio da lealdade é algo inerente à própria estrutura do processo penal, pois tem o condão de imprimir *a priori* uma atitude de respeito à dignidade da pessoa humana, podendo ser considerada como fundamento da proibição de prova (Silva, 2010, p. 234).

A atuação dos órgãos que compõe o sistema de justiça deve estar atrelada profundamente ao respeito à dignidade da pessoa humana. Nas palavras Valente (2017b, p.286), o incitamento à pratica de crime, que venha a confirma suposta aptidão do visado para o crime, “é um meio de obtenção de prova próprio dos processos de estrutura inquisitória em que a verdade material era o fim essencial do processo”. O princípio da lealdade impede a polícia de recorrer a meios enganosos, ardilosos, “que induzem o arguido à prática de factos que não praticaria se não fosse ardilosamente interpelado, provocado e incitado” (Valente, 2017b p. 288). Assim, a atuação dos órgãos do sistema de justiça no cumprimento de sua função constitucional, qual seja: defesa da legalidade democrática, garantia da

[47] Texto da Constituição da República Portuguesa está disponível em http://www.parlamento.pt/Legislacao/Paginas/ConstituicaoRepublicaPortuguesa.aspx

segurança interna e dos direitos dos cidadãos, está adstrita aos princípios éticos, deontológicos e morais que são a essência de bens jurídicos de tutelados pelo estado (Valente, 2014, pp. 285-288). Será leal o procedimento que respeitar as proibições de prova elencadas na constituição e nas Leis processuais, tendo-se em mente que o princípio da lealdade, que imanta as ações da polícia, proíbe que se faça uso de meios e métodos de atuação e de investigação proibidos. A ação do agente infiltrado deve ser de tal modo cuidadosa a ponto de jamais interferir na formação da vontade do investigado. Conforme já dito alhures, não pode o infiltrado atuar como provocador da prática dos ilícitos. A provocação consistiria em estratagema verdadeiramente indigno para o Estado, violador do princípio da lealdade. Assim, a utilização da infiltração terá de ser empregada de modo tal que preserve a confiança do cidadão nas ações estatais.

3.3 - Princípio da Reserva de Constituição

Conforme visto anteriormente, a infiltração digital pode ser definida como um meio oculto de investigação, donde se infere que consiste em meio de prova mais gravoso do que os meios abertos, uma vez que para sua realização direitos fundamentais serão restringidos, especialmente a privacidade e o direito ao sigilo das comunicações.

As constituições do Brasil e de Portugal estabeleceram garantias sobre os referidos direitos fundamentais e em seus próprios textos dispuseram acerca da redução ou não dessas garantias. No caso do Brasil, o regime jurídico da intervenção nas comunicações é disciplinado n o art. 5º, inc. XII, da Constituição da República.[48] Da leitura do dispositivo, infere-se que a Constituição Federal

[48] Art. 5º, inciso XII da CFB: é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;

permitiu apenas a “violação” do sigilo das comunicações telefônicas, não tendo permitido, em qualquer hipótese, a quebra do sigilo de dados e correspondência. Entretanto, o legislador brasileiro, ao regulamentar o referido dispositivo por meio da Lei 9296/1996, incluiu a possibilidade de quebra de sigilo telemático ao lado da quebra de sigilo telefônico. Posteriormente, a Lei 12.965/14, denominada Marco Civil da Internet no Brasil, convalidou a possibilidade de afastamento do sigilo de dados telemáticos, desde que determinado por ordem judicial. A vedação constitucional tem sido ignorada diante dos argumentos de que em face de uma nova criminalidade organizada e transnacional, com acesso a ferramentas tecnologias para sua atuação, também a repressão penal deve utilizar meios sofisticados de observação e captura de informações para poder fazer frente aos novos fenômenos e suas consequências danosas (Prado, 2013, pp. 10-11). As decisões das cortes brasileiras têm sido no sentido de igualar a interceptação de dados à interceptação telefônica, ao argumento de que não podem existir direitos absolutos. Por essa exegese a Constituição estaria submetida aos parâmetros de interpretação do direito ordinário (Prado, 2013, p. 12).

Em Portugal, a CRP dispõe sobre a inviolabilidade da correspondência e dos outros meios de comunicação privada no art. 34, estabelecendo proibição de ingerência das autoridades públicas na correspondência, nas telecomunicações e nos demais meios de comunicação, salvos os casos previstos na lei em matéria de processo criminal. A exegese deve ser feita em conjunto com o art. 18, o qual determina que a restrição a direitos, liberdades e garantias nos casos expressamente previstos na Constituição, devem estar limitadas ao necessário para salvaguardar outros direitos ou interesses constitucionalmente protegidos, além de possuírem carácter geral e abstrato, sem efeito retroativo ou diminuição à extensão e o alcance do conteúdo essencial dos preceitos constitucionais.

De acordo com Valente (2015b, p. 117), não se pode admitir uma expansão incontrolada de meios ocultos de investigação criminal tipificados em lei – princípio da legalidade formal, sem uma interpretação conforme a constituição quanto à

admissibilidade de meios de elevada restritividade de bens jurídicos pessoais ou direitos fundamentais pessoais, entre eles o sigilo das comunicações. Assim, o catálogo dos tipos penais sujeitos aos meios ocultos de investigação e os próprios meios ocultos devem estar submetidos ao princípio da reserva de constituição.

3.4 - O princípio da proibição da autoincriminação ou nemo *tenetur se detegere*

Outro questionamento frequentemente vinculado à infiltração, relaciona-se a vedação à autoincriminação, também conhecida através do brocardo latino *nemo tenetur se detegere* ou *nemo tenetur se ipso acusare*. A assimilação do referido princípio pelos estados democráticos de direito foi e continua sendo de extrema importância para a abolição da tortura e de outros métodos degradantes utilizados para a obtenção da prova. Constituem exemplos de aplicação do *nemo tenetur* o direito ao silêncio (no interrogatório policial ou judicial), o direito de não participar de acareações, reconhecimentos, reconstituições, não fornecer padrões gráficos ou de voz para perícia, etc. Não se pode compelir o acusado a praticar tais atos e tampouco extrair consequências negativas da sua recusa. Desse princípio decorre a obrigação para o estado acusador de produzir as provas necessárias à condenação (Giacomolli, 2015, p. 211).

Conforme Andrade (2013, p. 121) “o arguido não pode ser fraudulentamente induzido ou coagido a contribuir a sua condenação*, s.c*, a carrear ou oferecer meios de prova contra a sua defesa”. Não existe para o investigado o dever de colaborar com a descoberta da verdade. No direito português o princípio que veda a autoincriminação está refletido na norma constitucional que prescreve a nulidade de todas as provas obtidas mediante tortura, coação, ofensa da integridade física ou moral da pessoa, bem como inserido no processo penal como total e absoluto

direito ao silêncio, previsto no art. 61º, n.º1, alínea c., do CPP. Além disso, a Lei impõe as autoridades o dever de esclarecimento acerca do direito ao silêncio e suas consequências. No direito Brasileiro, a Constituição Federal consagra o direito ao silêncio a teor do disposto no art. 5.º, LXIII, e a proibição da tortura e tratamento desumano ou degradante no art. 5º, inciso III. Entretanto, no âmbito da infiltração, real ou digital, os visados contribuem, sem saber, para a constituição da prova; e o fazem desconhecendo a condição do infiltrado, a quem consideram membro da organização criminosa e por isso "digno" de confiança. Para Andrade (2009a, p. 107) os meios ocultos sacrificam o direito a recusar testemunho ou depoimento (artigos 134º e 135º), o direito ao silêncio, permitindo, portanto, a "obtenção fraudulenta de confissões inconscientes e, como tais, não livres. De fato, não se pode negar que a admissão da infiltração como método de obtenção de prova representa uma mitigação do *nemo tenetur.* Em razão disso, a infiltração há de ser admitida em caráter de excepcionalidade, em casos em que os bens jurídicos em risco sejam sobremaneira caros à sociedade para justificar uma atuação excepcionalmente severa. Mesmo assim, a adoção de alguns cuidados é imprescindível. O principal deles consiste em não interferir na formação da vontade dos investigados, de modo a ficar cristalinamente demostrado que, presente ou ausente o agente infiltrado, o resultado obtido seria o mesmo, ou seja, a formação da vontade do autor do delito e o *iter criminis* por ele percorrido seria idêntico.

3.5 - Princípio da proporcionalidade *Lato Sensu*

O princípio da razoabilidade ou proporcionalidade *lato sensu* opera como limite a qualquer atividade do estado, seja do poder legislativo, do poder judiciário ou do poder executivo. Trata-se de um **dever** de proporcionalidade que sobrepaira a atuação dos poderes públicos, uma ferramenta hermenêutica que deve estar sempre presente no processo decisório (Feldens, 2005, p. 160).

No que tange às origens, a referência normativa mais remota sobre a aplicação da proporcionalidade consta na Magna Carta de 1215. Contudo desenvolveu-se de modo mais intenso durante o iluminismo, a ser mencionado por Montesquieu e Beccaria em seus ensaios. Este último tratou explicitamente da proporção entre os delitos e as penas. Mais tarde, em 1789, a proporcionalidade seria inserida na Declaração de Direitos do Homem e do Cidadão (Feldens, 2005, p. 157).

Embora esteja presente “desde sempre” nos estados democráticos de direito, ainda há intenso debate sobre a natureza normativa do princípio da proporcionalidade, se sua natureza seria de princípio, regra ou postulado normativo aplicativo (metanorma). Ficamos com aqueles que consideram a proporcionalidade como um princípio imanente à clausula do Estado Democrático de Direito, assim caracterizado (como princípio) para que tenha envergadura suficiente para determinar sua observância e aplicação (Feldens, 2005, p. 159).

Esse princípio se aplica nas situações em que exista uma relação de causalidade entre dois elementos distintos, um meio e um fim. De acordo com esse princípio, as atividades dos órgãos do sistema de justiça, especialmente das polícias, devem se limitar ao extremamente necessário, restringindo o mínimo possível os direitos, garantias e liberdades fundamentais dos investigados. O princípio funciona como um freio para o arbítrio ou abuso na aplicação das medidas de polícia, devendo ser utilizado pelo juiz criminal ao analisar a representação do Ministério Público e da Polícia Judiciária.

O princípio da proporcionalidade tem como seu principal campo de atuação o âmbito dos direitos fundamentais, enquanto critério valorativo constitucional determinante das restrições que podem ser impostas na esfera individual dos cidadãos para o alcance das finalidades do Estado. O referido princípio impõe a proteção do indivíduo contra intervenções estatais desnecessárias ou excessivas, que causem danos maiores do que o estritamente indispensável para a proteção dos interesses públicos.

O princípio da proporcionalidade, impõe que as restrições às liberdades garantida constitucionalmente devem ser **adequadas, necessárias e proporcionais** à proteção de um bem jurídico que seja, pelo menos, de igual valor, vez que, partindo do pressuposto de que liberdade é a regra, sua restrição, portanto, deve constituir exceção. Esses parâmetros, necessidade, adequação e proporcionalidade em sentido estrito, constituem um critério trifásico para a aplicação do princípio da proporcionalidade *Lato* S*ensu*. Havendo proporção, é possível equilibrar as exigências do indivíduo e da sociedade, estabelecendo um balanceamento entre os direitos fundamentais.

Os meios de investigação e de produção de prova devem ser adequados aos fins a que se destinam. Deve haver um nexo de pertinência fundamentada entre o problema gerador da controvérsia e os meios (ações ou omissões que minimamente interfiram na liberdade individual) utilizados para se atingir o resultado desejado. Segundo Fernandes (2012, p. 57), “a adequação, a ser verificada empiricamente, deve ser analisada de maneira objetiva, como adequação qualitativa ou quantitativa, e de forma subjetiva, ligada a idoneidade em face do sujeito passivo”. A medida deve ser apta a alcançar o fim pretendido (adequação qualitativa), a sua duração ou intensidade deve ser condizente com a sua finalidade (adequação quantitativa), por fim “a medida deve ser dirigida a um indivíduo sobre o qual incidam as circunstâncias exigíveis para ser atuada (adequação subjetiva) ”. A necessidade diz respeito à preservação do direito fundamental restringido em face da medida restritiva ou a outro em igual ou superior patamar de importância. Ou seja, impende ser procurado o meio menos nocivo capaz de produzir o fim propugnado pela norma em questão.

O subprincípio da necessidade impõe a realização de uma ponderação pelos órgãos do sistema de justiça, diante de valores altamente relevantes, de garantias constitucionalmente asseguradas, há que se realizar uma acomodação desses valores, sem retirar-lhes o manto de proteção, mas afastando-o em prol da aplicação da garantia de outros valores. Entre os meios idôneos, considerados em

abstrato, deve ser escolhido aquele que, em concreto, se revele necessário, exigível ou indispensável, para atingir o fim visado (Ramalho, 2017, p. 259).

Por fim, de acordo com princípio da proporcionalidade em sentido estrito os ganhos devem superar as perdas. Os resultados da intervenção estatal devem se situar em uma justa e proporcionada medida, impedindo-se a adoção de medidas legais restritivas desproporcionais, excessivas em relação aos fins obtidos. Se analisa a efetiva proporcionalidade entre a medida tomada e o objetivo perquirido. Ao contrário, haveria sacrifício exagerado de outros bens jurídicos não menos relevantes à sociedade. Conforme Andrade (2009a, p. 116), o regime dos meios ocultos "terá de obedecer a um princípio de proporcionalidade em sentido estrito". Deverão ser sopesados em uma balança "o universo dos direitos e dos sujeitos atingidos, a eminência e dignidade dos bens jurídicos a salvaguardar bem como a idoneidade da medida para o conseguir". O postulado da proporcionalidade está presente na CRP, especialmente no art. 18, n.º 2 e 3, que tratam sobre os limites as restrições à direitos, liberdades e garantias e no art. 272, n.º 2, que disciplina a utilização das medidas de polícia. A Lei 101/2001 que trata das ações encobertas em Portugal dispõe que as ações encobertas devem ser **adequadas** aos fins de prevenção e repressão criminais identificados em concreto, nomeadamente a descoberta de material probatório, e **proporcionais** quer àquelas finalidades quer à gravidade do crime em investigação. Dessa forma, o legislador português impôs a aplicação do princípio da proporcionalidade explicitamente para o deferimento das ações encobertas. No que tange ao Brasil, o Supremo Tribunal Constitucional em algumas ocasiões aplicou o princípio da proporcionalidade e tem feito a correlação desse princípio com as normas referentes ao devido processo legal, insculpido no artigo 5º, LIV da Constituição Federal (Feldens, 2005, pp. 171-176).

4 - OS LIMITES IMPOSTOS AO ESTADO PELOS PRINCÍPIOS PROCESSUAIS CONSTITUCIONAIS

4.1 - Princípio da Reserva Legal

O princípio da reserva legal afigura-se, antes de tudo, como um princípio político, cunhado no século XVIII, no seio da doutrina de divisão dos poderes, visando submeter à lei o exercício dos poderes do Estado. Estabelece o artigo 125º do Código de Processo Penal Português que são admissíveis as provas que não forem proibidas por Lei. A interpretação literal desse artigo permitiria concluir que os meios de obtenção de prova não se encontram limitados ao um rol taxativo ou catálogo legal, sendo todos eles permitidos desde que não se encontrem no rol exemplificativo dos meios proibidos de prova, previstos no artigo 126 do mesmo diploma legal (Silva, 2004, p. 288). Entretanto, os meios atípicos ou inominados não incluem atividades que possam reduzir direitos fundamentais constitucional ou legalmente assegurados. O art. 18º, n.º 2, da CRP estabelece a lei só pode restringir os direitos, liberdades e garantias "nos casos expressamente previstos na Constituição", devendo as restrições se limitarem ao necessário para salvaguardar outros direitos ou interesses constitucionalmente protegidos. Assim, qualquer medida investigativa que importe na restrição, redução ou danos a direitos fundamentais somente poderá ser executada se prevista em Lei.

No Brasil, de forma similar à Portugal, são admitidos todos os meios de prova, vigendo o princípio da atipicidade da prova, fulcrado no princípio do livre convencimento do Juiz (Rubin, 2010)[49]. A liberdade de produção das provas

[49] De acordo com o art. 155 do Código de Processo Penal, "O juiz formará sua convicção pela livre apreciação da prova produzida em contraditório judicial, não podendo fundamentar sua decisão exclusivamente nos elementos informativos colhidos na investigação, ressalvadas as provas cautelares, não repetíveis e antecipadas". O art. 157, do mesmo diploma, por sua vez, dispõe que "são inadmissíveis, devendo ser desentranhadas do processo, as provas ilícitas, assim entendidas as obtidas em violação a normas constitucionais ou legais. (Redação dada pela Lei nº 11.690, de

encontra limites nas vedações às provas ilícitas, previstas na Constituição Federal e no Código de Processo Penal. Entretanto, de modo bastante similar à Portugal, no que tange aos métodos ocultos de produção de prova, diversos doutrinadores consideram que vige o princípio da reserva legal, o qual decorre do devido processo legal o do princípio da legalidade insculpidos no art. 5º da Constituição Federal[50]. Os métodos ocultos de investigação criminal, em virtude da sua natureza tendencialmente invasiva e insidiosa são, por excelência, campo fértil em matéria de ingerências e restrições a direitos fundamentais, pelo que, submetidos à "intransponível exigência de reserva de Lei" (Ramalho, 2017, p. 244). Havendo margens de dúvida, lacunas na lei que estabelece a possibilidade de utilização da infiltração, a exegese deverá ser necessariamente *pro libertate* (Andrade, 2009b, p. 541).

Ademais, a lei que autorizar a utilização dos meios ocultos deverá ter densidade normativa suficiente para estabelecer todos os limites para a atividade policial, devendo identificar tanto o bem jurídico e o direito fundamental lesado ou posto em perigo, bem como os limites da intromissão, visando reduzir a s margens para discricionariedade (Jesus, 2015, p. 234). De modo que não bastará ao legislador autorizar o uso da infiltração digital. Deverá estabelecer as hipóteses de aplicação, os requisitos, os limites, e as consequências da atividade.

4.2 - Reserva de catálogo

O princípio da reserva de catálogo consiste em um desdobramento do princípio da reserva legal. Conforme dito acima, no que concerne aos métodos

2008), e no § 1º que "são também inadmissíveis as provas derivadas das ilícitas, salvo quando não evidenciado o nexo de causalidade entre umas e outras, ou quando as derivadas puderem ser obtidas por uma fonte independente das primeiras. (Incluído pela Lei nº 11.690, de 2008)". Disponível em http://www.planalto.gov.br/ccivil_03/decreto-Lei/Del3689.htm

[50] Reza o artigo 5º da Constituição Federal: Art. 5º (*omissis*)[...] LVI - são inadmissíveis, no processo, as provas obtidas por meios ilícitos;

ocultos de investigação, a autorização deve estar adstrita à reserva de lei; mas não qualquer lei, uma lei com densidade normativa suficiente para impor os limites e servir de baliza aos atores do sistema de justiça para a realização das finalidades do processo penal, conforme o estado democrático de direito, visto que estamos no âmbito de técnicas especiais de investigação redutoras de direitos fundamentais. O legislador opta, portanto, por admitir a medida para um catálogo taxativo de crimes (*numerus clausus*), ou seja, sem possibilidade de ampliação para outros delitos.

Tanto o RJAE e a Lei do Crime cibernético autorizam a realização da infiltração para um catálogo de crimes. No Brasil, a Lei 12.850/2013, ao tratar das infiltrações em campo (ou reais), não definiu um rol de crimes que permitiriam a utilização da técnica, mas autorizou o uso dos meios de produção de prova nela previstos nas investigações que tratam de crimes cometidos por organizações criminosas, conduta tipificada como crime no bojo do referido normativo, crimes previstos em tratados cuja forma de execução seja transnacional e terrorismo. Embora não haja um rol especifico de crimes, o crime deverá ser praticado por organizações criminosas, o que impõe um limite à realização da infiltração policial. Embora o rol de possibilidade seja bastante amplo, praticamente todos os tipos penais podem ser cometidos por organizações criminosas, o modo do cometimento do crime, para justificar a utilização da infiltração, deve ser a “associação de 4 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”.

De outra parte, existe ainda a possibilidade de utilização da infiltração para investigar crimes transnacionais, desde que previstos em tratados, e o terrorismo. No âmbito dos crimes transnacionais previstos em tratados, destacam-se os crimes cometidos pela internet, que, em face do alcance da rede mundial, não respeitam limites territoriais geográficos. Entretanto, embora um crime cibernético possa estar

previsto em tratado, como no caso dos crimes contra a dignidade sexual das crianças, adequando-se ao disposto na Lei 12850/2013, a melhor técnica de investigação consistiria na infiltração digital.

A lei que trata da infiltração digital, conforme visto acima, não tratou a amplitude da utilização da mesma forma, mas sim explicitou todos os crimes em que a infiltração digital poderá ser realizada na forma de catálogo fechado de crimes. Desse modo, os regimes jurídicos brasileiros que tratam da infiltração, diferentemente dos regimes jurídicos de Portugal, que se somam um ao outro, adotarem técnicas legislativas diferentes acerca do catálogo de crimes.

4.3 - Princípio da Reserva de Juiz ou Reserva Jurisdicional

No Direito Português, o princípio da reserva de juiz está contido no artigo 32º, n.º4 da CRP, ao referir que a instrução é da competência de um juiz, o qual pode, nos termos da Lei, delegar noutras entidades a prática dos atos instrutórios que se não prendam diretamente com os direitos fundamentais. A garantia imposta pela reserva de jurisdição consiste, por certo, em limitação à atividade probatória em face da danosidade que carregam em seu âmago, sendo razoável a exigência da reserva absoluta de jurisdição. Ao juiz caberá a tutela preventiva dos direitos fundamentais reduzidos com a medida da infiltração. Sendo a medida do tipo secreta, obviamente não será oportunizado ao arguido exercer a própria defesa, motivo pelo qual, o Juiz, atuando como terceiro sem interesse na lide e com independência, exercerá o papel de Juiz das garantias (Andrade, 2009a, p. 118). Além disso, deverá decidir fundamentadamente acerca de todos os pressupostos legais para a implementação da medida. A fundamentação nesse contexto, além de prevenção de medidas arbitrárias, permitirá o questionamento quanto à legalidade da medida, em grau de recurso (Andrade, 2009b, p. 548).

Desse preceito se infere que a decisão final acerca de meios de obtenção de prova que promovam restrição a direitos fundamentais não podem escapar da alçada do juiz. Os métodos ocultos de produção de prova, danosos que são aos direitos fundamentais, obviamente, estão adstritos a essa imposição constitucional. A legislação brasileira está em consonância com o princípio da reserva de juiz, ao submeter à apreciação do requerimento de infiltração real ou digital, à decisão judicial. Em Portugal, entretanto, mesmo o inquérito sendo concebido como processo[51], a Lei criou a possibilidade de autorização da infiltração pelo Ministério Público. inobstante, Guedes Valente (2017b, p. 596) considera que a autoridade judiciária competente para autorizar a utilização do agente infiltrado somente pode ser o Juiz de Instrução Criminal, pois "a operação de infiltração gera restrição do direito à reserva de intimidade da vida privada e familiar, direito fundamental pessoal, que merece a tutela jurisdicional *ab initio ad finem* do processo crime". Conclui o doutrinador, afirmando que o nº.3 do art. 3º do RJAE está ferido de inconstitucionalidade material por violação do n.º 4 do art. 32º da CRP.

4.4 - Princípio da subsidiariedade

O princípio da subsidiariedade está intimamente relacionado com a ideia de excepcionalidade. Os meios ocultos de investigação e, entre eles a utilização da infiltração digital, promovem severas restrições a direitos fundamentais de modo que sua utilização não pode ser banalizada. O princípio da subsidiariedade na aplicação dos métodos ocultos de investigação criminal determina que sejam cogitadas e avaliadas primeiramente a utilização das técnicas abertas de investigação, não sigilosas, abstratamente aplicáveis ao caso concreto. Essa avaliação deverá constituir a fundamentação do pedido de autorização judicial que visa implementar a infiltração digital.

[51] De acordo com Silva (2008, p. 74) "com o Código de 1987 toda a investigação penal passou a ter natureza exclusivamente processual; não há investigação criminal fora do processo".

No Brasil, no que tange à infiltração real, não virtual, a observância ao princípio da subsidiariedade está consagrada na Lei 12.850/2013 que autoriza a utilização da infiltração como meio de produção de prova, conforme disposto no art. 12, §1º do referido diploma legal. Do texto legal se infere que não se pode conceber a atuação do agente infiltrado somente para facilitar a descoberta da verdade. A demonstração de que os demais meios de prova (abertos) já foram tentados e falharam deve ser relatada ao juiz da investigação para que verifique no caso concreto e autorize a realização da infiltração.

A Lei 101/2001, RJAE, ao qual está submetida a infiltração digital em Portugal, não trata diretamente da subsidiariedade, trazendo apenas a previsão quanto à adequação da medida aos fins de prevenção e repressão da criminalidade. A referida lei não seguiu a mesma sistemática presente no regime das escutas telefônicas que em seu art. 187º dispõe que a medida só poderá ser autorizada havendo razões para crer que a diligência é **indispensável** para a descoberta da verdade ou que a prova seria, de outra forma, **impossível** ou **muito difícil** de obter, por despacho fundamentado do juiz de instrução e mediante requerimento do Ministério Público, quanto a crimes: Sendo a escuta telefônica método oculto que restringe a privacidade, do mesmo modo que a infiltração digital, não poderia haver diferenciação substancial nos requisitos de admissão das medidas. Para a mesma espécie de medida, as mesmas exigências deveriam estar legalmente previstas. Assim, embora a lei 101/2001, não trate explicitamente da subsidiariedade dessa medida, deverá ela ser demonstrada e explicitadas nas das razões de decidir do juiz criminal que avaliar a aplicação da medida. Alguns doutrinadores também colocam na avaliação do caráter subsidiário do meio de investigação a impossibilidade de cumulação com outros métodos ocultos (Ramalho, 2017, p. 262).

4.5 - Princípio de indispensabilidade do recurso ao meio oculto de prova para a descoberta da verdade e para a obtenção da prova

O Processual Penal não procura a verdade a todo o preço. O “preço a pagar para a descoberta da verdade é variável em função da preponderância geral ou casuística de certos interesses em relação a outros”. O preço será o sacrifício que o Estado está disposto a fazer em matéria de direitos fundamentais e processuais para a prossecução penal dos delinquentes. Recorrendo a um arsenal de meios de investigação criminal progressivamente mais agressivos dos direitos dos cidadãos em função da gravidade e danosidade social do crime em causa ou da absoluta indispensabilidade do meio de prova em face das circunstâncias (Ramalho, 2017, pp. 209-210).

O sistema processual penal configura um instrumento para a efetivação das garantias do direito processual do ser humano, que deve respeitar e preservar os direitos fundamentais constitucional e legalmente assegurados. De outra parte, o reestabelecimento da paz pública também é um dos desígnios do processo penal. Nesse sentido, a lição de David Ramalho (2017, p. 210) ao destacar que “não é possível conceber-se um sistema processual penal eficaz sem qualquer ingerência nos direitos fundamentais dos cidadãos”. A tutela adequada dos direitos, liberdades e garantias do cidadão deverá ser coadunada com os fins de pacificação social pretendidos pelo Processo Penal.

A Lei 12850/2013, Regime jurídico das organizações criminosas no Brasil, dispõe que a infiltração somente será autorizada quando em seu requerimento for demonstrada a necessidade da medida. A Lei 13441/2017, que autoriza a infiltração digital, para crimes contra a dignidade da criança e adolescente, dispõe no § 3º do art. 190-A que a infiltração de agentes de polícia na internet não será admitida se a prova puder ser obtida por outros meios.

Em Portugal, o Regime Jurídico das Escutas Telefônicas exige a indispensabilidade da utilização do meio oculto para a produção da prova. A palavra

necessidade, utilizada pelo legislador, precisa ser entendida como **indispensabilidade**. Assim, é imprescindível demonstrar ao Juiz que este é o único caminho para a obtenção da prova, pois todos os demais já falharam ou, diante das particularidades do caso em concreto, certamente falhariam.

No que tange aos crimes informáticos, as possibilidades de investigação através de meios abertos são extremamente restritas. Embora possam ser colhidos elementos em sites e redes sociais públicas, as atividades ilícitas de maior gravidade normalmente são realizadas em espaços privados, não disponíveis ao público, em que a segurança e o anonimato são garantidos, como a *deep web* por exemplo. As dificuldades de investigação dos cibercrimes são consequências de todas as características dos referidos delitos (transnacionalidade, atemporalidade, deslocalização, diversidade de ordens jurídicas afetadas pelo crime, permanência, automatismo e repetição, anonimato, alta tecnicidade, disseminação e potenciação dos danos), as quais, ao mesmo tempo em que facilitam a comissão do crime, trazem dificuldades para a persecução penal. Além dos procedimentos técnicos necessários a identificar o local da conexão, os investigadores poderão se deparar com programas de anonimização, codificação e antirrastro, bem como com a falta de controle e identificação dos usuários nas empresas e principalmente em locais públicos como cibercafés, universidades ou bibliotecas (Dias, 2012, pp. 74-75). Nesses casos, o uso o uso de infiltração digital poderá ser considerado como indispensável pois o acesso a esses verdadeiros **locais de crime** não será conferido à Polícia pelos criminosos. Conforme Valente (2017b, p. 567), o agente infiltrado “Somente, e repetimos, somente, deverá ser usado quando todos os outros meios de obtenção da prova não forem suficientemente capazes e eficazes para a descoberta da verdade e obtenção da prova”. O presente princípio difere do princípio da subsidiariedade, pois a indispensabilidade deverá ser constatada de plano, naqueles casos em que os meios abertos e não invasivos de investigação não contribuirão para a descoberta da verdade material. Ao passo que a subsidiariedade, dependerá de uma análise casuística na qual os demais meios de prova disponíveis foram testados e falharam. Entretanto, em ambos os casos, a

finalidade do processo, ou seja, a proteção aos bens jurídicos violados, deve superar as restrições a intimidade e privacidade a que serão submetidos os visados.

4.6 - Princípio da vinculação ao fim

O princípio da vinculação ao fim determina que a realização da investigação deverá direcionar-se a descoberta dos elementos probatórios referentes aos fatos criminosos ou indícios de fatos criminosos informados ao juiz criminal para obtenção da autorização do meio oculto de investigação.

A razão de pedir ou causa de pedir contida na representação pela autorização da infiltração criaria uma espécie de trilha a ser percorrida pelo investigador, direcionando-o pelo caminho em que podem ser recolhidos os elementos probatórios dos crimes cujos indícios foram apontados no requerimento analisado pelo juiz. Isso porque a infiltração digital, como método oculto de investigação, deve atender a requisitos de proporcionalidade, excepcionalidade, subsidiariedade e indispensabilidade do meio, entre outros. A submissão a todos esses requisitos somente poderá ser examinada com a exposição de dados fáticos concretos a partir dos quais será feita a análise do pedido e a fundamentação da autorização. O fim pretendido ao se iniciar uma investigação deverá perseguido até o término da investigação. Assim, a mudança de objeto ou de sujeitos investigados, *a priori*, contraria o princípio da vinculação ao fim, resultando na impossibilidade de valoração de elementos referentes a outros fatos e finalidades.

Inobstante, não é incomum que no decurso de uma investigação criminal que se utiliza de meios ocultos de investigação, extremamente invasivos, sejam descobertas informações referentes a fatos que não se relacionam com o objeto da investigação, como fatos afetos à intimidade dos visados ou de terceiros que com esses se relacionam. Nesse ponto, importante referir a questão dos conhecimentos

fortuitos ou “encontros fortuitos de prova”, para diferenciá-los dos “conhecimentos da investigação”. A doutrina conceitua os “conhecimentos da investigação” como os fatos casualmente descobertos no decurso de uma investigação, mas que possuam um liame com a própria investigação. Outros fatos, em que não se verifique esse liame, ou conexão probatória, são denominados “conhecimentos fortuitos”.

Importante referir que estamos no âmbito da valoração da prova, uma vez que já houve a autorização para a produção da prova que está sendo colhida pela infiltração digital e pressupõe-se que todas as normas para a produção da prova estão sendo cumpridas. A verificação sobre quais são os conhecimentos da investigação e quais são os conhecimentos fortuitos deverá ser feita no plano concreto, visto que é bastante difícil uma classificação capaz de abranger todos os fatos com potencial para serem descobertos em uma investigação bastante intrusiva como é o caso dos métodos ocultos e especialmente das infiltrações digitais, nas quais o agente infiltrado poderá ter acesso a uma vasta quantidade de informação, tendo-se em consideração a capacidade de armazenamento dos dispositivos informáticos e do armazenamento em nuvem por exemplo. Os conhecimentos de investigação que configurem atos ilícitos passam a ser considerados objetos da investigação desde que exista uma conexão processual entre eles. Entretanto, a valoração de provas de outros crimes, diversos dos inicialmente apontados, pode consistir em desvirtuamento da finalidade da investigação, uma vez que poderá ultrapassar os limites em que se fundamentou a medida, violando o princípio da vinculação ao fim (Valente, 2008, p. 118).

Outros doutrinadores defendem que a autorização de um método oculto de investigação abrange o delito que a motiva e igualmente os eventos ocorridos no entorno na mesma “unidade de investigação em sentido processual” (Rodrigues, 2012, p. 120).[52] A mesma solução não serve para os conhecimentos fortuitos de

[52] No que tange a possibilidade de valoração dos conhecimentos da investigação, existem diversos entendimentos na doutrina e na Jurisprudência.

outros ilícitos. No âmbito da infiltração digital, técnica adstrita ao princípio do catálogo, a primeira verificação que deverá ser feita consiste em saber se o crime que foi descoberto é um dos crimes previstos no catálogo. Do contrário, estar-se-ia utilizando a infiltração digital para a investigação de crime menos graves, para os quais esse nível de intrusão não está legalmente previsto, o que configuraria uma burla à previsão legislativa limitadora do uso da técnica de infiltração digital e, portanto, uma mácula formal em torno da prova descoberta (Valente, 2010b, p. 608).

Para Valente (2010b, p. 67), quanto os conhecimentos fortuitos; não vigora uma proibição absoluta de valoração. O autor conclui que os conhecimentos fortuitos podem ser valorados desde que se destinem à prova de um dos crimes do catálogo; se mostrem indispensáveis e necessários a esse esclarecimento e que, face um juízo de "hipotética repetição de intromissão" (estado de necessidade investigatório) se verifique uma probabilidade qualificada de que se recorreria à interceptação e gravação das comunicações por se mostrar de "grande interesse para a descoberta da verdade ou para a prova" e, por fim, que os conhecimentos sejam comunicados imediatamente ao juiz que autorizou ou ordenou a diligência processual.

A possibilidade de valorar uma prova referente a crimes que não estão no catálogo e não são conexos aos crimes investigados poderia possibilitar o desvirtuamento da ferramenta que, embora prevista em lei com alta densidade normativa, poderia ser utilizada para a investigação de crimes menos graves, configurando abuso de autoridade e permitindo-se o alargamento da lista de crimes de um regime jurídico propositadamente fechado (Rodrigues, 2012, p. 120).

5 - A ADMISSIBILIDADE DA INFILTRAÇÃO DIGITAL COMO MEIO DE PRODUÇÃO DE PROVA VÁLIDO

Conforme referimos anteriormente, a infiltração digital configura um método oculto de investigação, ou técnica especial de investigação a qual tem recorrido as polícias para fazer frente à criminalidade cibernética. A necessidade de utilização dessa técnica de investigação deriva das alterações sociais impulsionada pelo crescimento da internet; os novos bens jurídicos surgidos com o advento da rede mundial e os velhos bens jurídicos submetidos a novas ameaças forçaram a inclusão dos crimes cibernéticos na política criminal dos governos ocidentais e orientais.

As novas tecnologias desafiam os juristas e rever os conceitos jurídicos existentes, especialmente a jurisdição baseada em critérios geopolíticos; os fluxos de comunicação não encontram barreiras nos limites geográficos territoriais e os autores dos crimes encontram-se em locais diferentes dos locais onde seus atos produzem efeitos. O ambiente transfronteiriço e imaterial da internet conecta diferentes sistemas legais. De acordo com Brandão, no Blog Jurisdição e Governança na Internet, “ a internet revela-se um problema para as regras de conexão tradicionais porque elas são baseadas, sobretudo, na territorialidade (Jurisdição e Governança na Internet, 2017).

Em princípio, os Estados regulavam somente o que acontecia fisicamente em seu território, limitando o exercício de sua jurisdição a um determinado espaço geográfico. Entretanto, a internet passou a permitir a extrapolação desse território físico, possibilitando o estabelecimento de relações transnacionais sem o conhecimento do Estado, propiciando contato e conflitos entre diferentes territórios, ordenamentos jurídicos e culturas. Nesse contexto, faltam critérios de definição de jurisdição estatal para casos que têm como pano de fundo o ciberespaço e, por isso, se conectam, de diferentes formas, a mais de uma jurisdição estatal. (Jurisdição e Governança na Internet, 2017).

Do ponto de vista clássico, geopolítico, a aplicação da Lei penal somente seria feita no caso de o crime romper o tecido social da própria nação. Entretanto, em se tratando de crimes cibernéticos, não vigora a mesma lógica. Vejamos um exemplo hipotético: cidadão “X” que está fisicamente no país “A”, contrata um serviço de internet de um país “B”, infecta máquinas localizadas no pais “C”, consegue dados bancários de cidadãos do país “D”, adquire moeda virtual e as trocas de forma diluída por bens e serviços de valores irrisórios de diversos outros países. Qual a jurisdição competente para infligir uma punição ao cidadão “X”? Por outra ótica, menos tecnicista, a qual estado soberano interessaria punir o cidadão “X”? De outro norte, sendo o ciberespaço algo diverso dos territórios nacionais, qual seria a legislação aplicável?

Para os que advogam a internet como uma jurisdição autônoma, a regulação das condutas deveria se dar em face de normas próprias desse ambiente, fazendo sentido a definição da rede como um espaço autopoiético. Segundo Alexandre Libório Pereira “à semelhança do big-bang, a internet formou-se se caoticamente”, prossegue afirmando que “a internet seria um verdadeiro “woodstock electrónico”, no qual tudo seria livremente partilhável. Os eventuais problemas seriam resolvidos segundo a máxima Clarckiana “a resposta para a máquina está na máquina”, tendo em conta a segurança oferecida pelas tecnologias criptográficas. Segundo essa visão, a internet seria regulada pelos códigos informáticos e não pela Lei dos Estados (Pereira, 2017, p. 2).

Entretanto, essa tese tem angariado pouco espaço na construção dos diplomas legais. É assente na doutrina, que uma adequada regulamentação da internet exigiria a redefinição dos conceitos de soberania. Para Manuel Castells o caráter global da internet foçou os governos a tentarem agir de maneira conjunta, criando um novo espaço, global de vigilância, mesmo correndo o risco de redução de soberania, em face da necessidade de construir padrões comuns de regulação, uma vez que “compartilhar a soberania era o preço a pagar para conservar coletivamente algum grau de controle político” (Castells, 2003, p. 155).

Essas pressões resultaram na elaboração de instrumentos jurídicos de âmbito internacional. Nesse sentido, a Convenção do Cibercrime, também conhecida como a Convenção de Budapeste[53], representa um esforço da comunidade europeia para fazer frente aos crimes cibernéticos, criando novas tipologias, instrumentos para a investigação e mecanismos para tornar mais eficiente a cooperação jurídica internacional. Isso porque a maior parte dos crimes envolve atores de diferentes países e continentes (Venâncio, 2011, p. 158).

A pressa dos estados em ter algum controle sobre a internet deu origem a legislações de natureza material, que tipificaram os novos crimes, bem como à criação e alteração de normas substantivas, de caráter procedimental, autorizando a utilização de técnicas especiais de investigação ou métodos ocultos de recolha de provas no âmbito dos crimes digitais, entre eles a infiltração digital. Isso porque a nova onda de criminalidade trouxe um componente a mais: a necessidade de conhecimento tecnológico, assimilado de maneira rápida por parte dos novos usuários, pressionando os estados a envidarem esforços para que esses mesmos conhecimentos e habilidades fossem incorporados pelas agências de investigação, em um anseio de busca de responsabilidades em um lugar idealizado para subsistir como território sem lei.

[53] A convenção previu medidas processuais consideradas imprescindíveis para uma investigação de crimes cibernéticos, são elas: preservação de dados armazenados, preservação e divulgação parcial de dados de tráfego; ordem de produção; investigação e apreensão de dados informatizados; recolha de dados de tráfego em tempo real; interceptação de dados de conteúdo. Ao tratar das normas processuais o relatório justificativo da convenção ressalta que não basta a adequação dos tipos penais, é de suma importância a criação de novos poderes processuais para a investigação dos crimes cibernéticos. Ressalta ainda como um dos principais desafios a identificação do infrator e do impacto da infração em face da fugacidade das informações virtuais. Embora tenha um caráter bastante inovador, a Convenção não tratou da infiltração digital. Portugal subscreveu a Convenção sobre o Cibercrime em 2001. Entretanto, somente em 2009 procedeu à ratificação do documento por meio da Resolução da Assembleia da República nº 88/2009 e pelo Decreto do Presidente da República nº 92/2009, ambos publicados a 15 de setembro (data da publicação da Lei nº 109/2009, de 15 de Setembro). O Brasil não foi convidado até a data da redação da presente tese a assinar a Convenção do Cibercrime, estando impedido, portanto, de fazê-lo, pois, os países que não compõe a União Europeia somete podem assinar o documento se forem convidados a tanto. O texto da convenção está disponível em http://www.cijic.org/wp-content/uploads/2015/10/ETS_185_Portugese.pdf. Para mais informações sobre a Convenção de Budapeste Lei do Cibercrime Anotada e Comentada, de Pedro Dias Venâncio.

Embora Brasil e Portugal possuam diplomas legais específicos sobre a infiltração digital, existem lacunas que geram problemas de várias ordens, especialmente quanto às hipóteses e limites de utilização da infiltração digital. Primeiramente, o legislador não tratou de definir e delimitar de forma suficientemente densa a figura da infiltração cibernética.

Fazendo-se um paralelo com o conceito de agente infiltrado real (*off line*) para o qual existem inúmeras definições, chegou-se ao conceito de infiltração digital como sendo uma técnica especial de investigação desenvolvida por uma equipe de policiais especificamente designada para a tarefa que, em face de indícios da prática de crimes cibernéticos – próprios ou impróprios, obtém uma autorização judicial e estabelece uma relação de confiança com um usuário da internet ainda não qualificado, mediante ocultação da condição de policial e criação de uma identidade fictícia, visando com isso, obter a qualificação do investigado e provas dos crimes praticados.

Diferentemente da infiltração de aspecto real, em campo, a infiltração digital poderá ser realizada com a criação de um perfil que fará as vezes do agente infiltrado. Esse perfil, construído cuidadosamente e com auto grau de verossimilhança, poderá ficar à disposição da equipe de policias para sua utilização de forma simultânea pelos membros da equipe.

Outra diferença bastante marcante consiste na redução do risco para os policiais infiltrados; a infiltração digital não exigirá necessariamente o encontro do policial infiltrado com os investigados. Ao passo que a infiltração de campo se inicia com o encontro pessoal, encerrando um alto grau de risco para a vida do agente infiltrado.

Estando no âmbito dos métodos ocultos, a infiltração digital deverá ser “formatada” a partir de requisitos limitadores da atividade probatória, pois a prova será produzida a partir da restrição (violação para alguns) de direitos fundamentais. Esses requisitos mínimos de admissibilidade devem ser extraídos, tanto pelo legislador quanto pelo juiz criminal, dos princípios supraconstitucionais

estruturantes (princípio da superioridade ética do estado, princípio da lealdade, princípio da reserva de constituição, princípio da proibição de autoincriminação, princípio da proporcionalidade) e dos princípios processuais penais constitucionais (princípio da reserva legal, princípio da reserva de catálogo, princípio da reserva de juiz, princípio da subsidiariedade, princípio da indispensabilidade do meio oculto de prova, princípio da vinculação ao fim), os quais foram detalhados nos capítulos anteriores, de modo a fornecer a base jurídica para a admissibilidade da infiltração digital como meio de prova lícito e legítimo.

A aplicação do princípio da superioridade ética do estado exige que os servidores públicos não pratiquem atos que os igualem aos criminosos, mas que atuem conforme os fundamentos do estado democrático de direitos, e promovam os seus objetivos, cumprindo as normas legais quanto as proibições de prova. Assim, a atuação de funcionários do sistema de justiça ao lado de criminosos e com a utilização do engodo para obtenção de elementos de prova entre em choque com esses primados.

Por essa ótica a única, a infiltração digital deverá ser moderada pelo princípio da proporcionalidade: os bens jurídicos em risco devem ser de tal grandeza que o desconforto causado pela utilização de ardis típicos daqueles que quebram as regras sociais poderá ser minimizado. A partir do caso concreto, das evidencias pré-existentes, será necessário aplicar o critério trifásico, verificando se a medida é adequada, necessária e proporcional.

A infiltração digital será adequada se for apta a alcançar o fim pretendido. Deve ser adequada objetivamente, devendo ficar claramente demostrado que o crime que se pretende investigar está vinculado ao espaço cibernético e somente uma infiltração digital poderá demonstrá-lo (adequação qualitativa) e vigorar durante período de tempo razoável e definido (adequação quantitativa). E deve ser adequada subjetivamente, os indícios apontam para o indivíduo ou perfil que se pretende investigar. Embora alguns diplomas legais autorizem, não se verificaria adequado, por exemplo, submeter uma vítima a esse tipo de investigação,

devassando-lhe a intimidade. Nesse caso, o dano com a utilização da medida poderá ser maior do que o dano causado pelo crime. A infiltração digital deverá ser considerada necessária, ou seja, indispensável para atingir o fim visado, como por exemplo atividades que ocorrem em ambientes altamente restritos com utilização de criptografia e imposição de condições para ingresso no referido ambiente pelos administradores do site.

Haverá proporcionalidade em sentido estrito se os direitos restringidos sopesados perante os bens jurídicos em risco justifiquem a medida. Tome-se por exemplo a prática de algum crime de bagatela, um adminículo penal, como o desvio de poucos reais da conta bancária pertencente ao Tesouro Nacional. Pelo critério da proporcionalidade não será viável restringir a privacidade em face de tão módico prejuízo. Em contrapartida, o esforço dos estados para barrar a disseminação de pornografia infantil e proteger a dignidade sexual de crianças e adolescentes, sabidamente vulneráveis a predadores sexuais que atuam *on line*, tem peso suficiente quando comparado aos direitos fundamentais restringidos pela infiltração digital, especialmente privacidade.

Na mesma linha, a infiltração digital choca-se com o princípio da lealdade, primado da proibição de prova, em face do qual garante-se os cidadãos que o estado-investigação não se utilizará de meios indignos e enganosos para comodamente recolher a prova de local privilegiado e sem esforços. Assim, a infiltração digital jamais poderá resultar em provocação ao crime, a posição dos policias infiltrados deverá ser de tal modo cuidadosa que não interfira na formação da vontade, afastando-se terminantemente a provocação.

O princípio da reserva de constituição determina que a restrição a direitos constitucionalmente protegidos somente pode ser admitida nos casos em que a própria carta magna autorize. Em contrapartida a infiltração digital é medida que restringe fortemente o direito ao sigilo das comunicações, além de restringir o direito à privacidade. Portanto, é preciso verificar se esse método de produção de prova pode ser considerado admitido em âmbito constitucional.

Sempre bom referir que ao tempo em que foram promulgadas tanto a Constituição de Portugal quanto a Constituição do Brasil, a internet ainda era algo bastante incipiente, de modo que a utilização em massa para as comunicações bem com a possibilidade de um monitoramento dessas comunicações por meio da internet, não estavam ao alcance da previsibilidade do legislador constituinte.

A redação da Constituição Portuguesa é mais consentânea como a interpretação quanto à restrição do sigilo das comunicações pela internet, ao dispor que “é proibida toda a ingerência das autoridades públicas na correspondência, nas telecomunicações e nos demais meios de comunicação, salvos os casos previstos na lei em matéria de processo criminal. Entretanto, a Constituição Brasileira somente permite o levantamento do sigilo das “telecomunicações”, uma vez que o art. 5º, inciso XII determina que "é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal. Uma interpretação literal vedaria a criação de leis que permitissem a realização da infiltração digital, por violar o dispositivo constitucional em sua literalidade. Sobre isso a Corte Constitucional tem decidido que deve ser aplicada uma interpretação não tão restritiva em homenagem ao princípio da proporcionalidade (Prado, 2013).

A aplicação integral dos princípios aqui referidos promoveria o reenquadramento da infiltração digital, lançando-a para o âmbito dos métodos proibidos de prova. Entretanto, as cortes constitucionais do Brasil e de Portugal preferem se socorrer do princípio da proporcionalidade para promover uma adequação da infiltração digital aos fins do estado democrático de direito, optando por considerá-la legítima em casos em que os bens jurídicos violados justifiquem a mitigação dos princípios antes referidos, somados ao atendimento dos primados da reserva legal, reserva de juiz, subsidiariedade e indispensabilidade do meio de prova.

A infiltração digital deverá ser prevista em prévia e densa lei processual. A exigência de lei para a infiltração digital, em face das particularidades que a distinguem da infiltração real, obedece ao princípio da reserva de lei específica, pois, em se tratando de restrição a direitos fundamentais constitucionalmente protegidos, a existência de diploma legal denso e detalhado reforça o sistema de garantias, por meio do balizamento legal dos limites da ação policial, visando a preservação do núcleo mínimo da dignidade da pessoa humana (Ramalho, 2017, p. 251).

A base legal deve ser suficiente para prever o conteúdo e extensão da medida restritiva de direitos fundamentais, prescrever o respectivo regime, incluindo os seus pressupostos materiais, formais, orgânicos e procedimentais. Exige-se um grau de densificação absoluto em matérias como a definição do catálogo de crimes, da competência para a sua determinação, o prazo máximo da medida, o grau de suspeita necessário, ao carácter subsidiário da medida. No mais, a liberdade de conformação do aplicador deve ser permanentemente pautada por critérios de proporcionalidade (Ramalho, 2017, p. 250).

No que tange ao catálogo de crimes, a Lei do Cibercrime de Portugal prevê a possibilidade da infiltração digital para os crimes nela relacionados, seguindo a metodologia utilizada no RJAE que também prevê um rol de infrações passíveis de serem apuradas pela infiltração policial.

No Brasil, a infiltração digital poderá ser realizada nas investigações de um rol taxativo de crimes relacionados na Lei 13.441/2017. A Lei 12850/2013, no entanto, não definiu um catálogo de crimes, dispondo que os meios de obtenção de provas por elas previsto, entre eles a infiltração policial, são aplicáveis as investigações de crimes cometidos por organizações criminosas, infrações penais previstas em tratado ou convenção internacional quando, iniciada a execução no País, o resultado tenha ou devesse ter ocorrido no estrangeiro, ou reciprocamente e às organizações terroristas, entendidas como aquelas voltadas para a prática dos atos de terrorismo legalmente definidos.

Critérios diversos permitem interpretações variadas pelos juízes criminais, dando mais espaço ao subjetivismo, de modo que consiste em falha quanto a densidade normativa que se exigiria para normas restritivas a direitos fundamentais. Imaginemos, por exemplo, um crime cibernético, como o previsto no art. 266, §1º, do Código Penal Brasileiro consistente na interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública. Caso praticado por organização criminosa, ensejaria uma infiltração policial em espaço cibernético com base nos ditames da Lei 12850/2013? Seria possível autorizar a infiltração digital para os crimes previstos na Lei n.º 12850/2013, que trata da infiltração de agentes para investigar crimes cometidos por organizações criminosas, crime de terrorismo, ou ainda aqueles previstos em tratados internacionais ratificados pelo Brasil? Por esse raciocínio, o catálogo de crimes previsto na lei que trata da infiltração digital no Brasil poderia não alcançar as finalidades restritivas em tese idealizadas pelo legislador.

Outra questão deveras importante no âmbito da infiltração digital se refere a responsabilidade pela prática de atos ilícitos durante a infiltração digital. O nº 1 do RJAE em Portugal estabelece a não punibilidade da conduta do agente encoberto no que tange a atos preparatórios eventualmente realizados no decurso de uma ação de infiltração. Não se trata, entretanto, de autorização para o cometimento de crimes, apenas a autorização para que o infiltrado simule a intenção de cometer o crime, motivo pelo qual não poderia ser punido em face da ausência do elemento subjetivo do injusto. Entretanto, se as condutas perpetradas não forem proporcionais aos fins da infiltração, poderá haver punição e inclusive a classificação do policial como agente provocador, tornando inadmissível toda a prova obtida, em face do regime da proibição de provas (Valente, 2017, pp. 600-601).

No Brasil, a Lei n.º 12.850/2013 silencia a respeito dessa temática, donde seria legítimo inferir que a mens legis consistiu em vedar a prática de atos ilícitos pelo agente infiltrado, mesmo atos preparatórios. Inobstante, as cortes brasileiras

têm firmado entendimento que o agente infiltrado não responde por associação criminosa, pois entendimento em contrário inviabilizaria a realização da infiltração.

A Lei 13441/2017, dispõe que não configura crime a atividade do policial que oculta a sua identidade para, por meio da internet, colher indícios de autoria e materialidade dos crimes do catálogo. Entretanto, esse dispositivo, embora topologicamente localizado no âmbito da regulamentação da infiltração cibernética, trata, em verdade, das atividades do agente encoberto e não do agente infiltrado. A recolha de informações ou de elementos de prova e, ocasionalmente, a verificação da ocorrência do crime (flagrante delito) de forma proativa por policiais ainda que no âmbito da internet não configura a infiltração digital, pois não será escopo da atuação do agente encoberto ingressar ou fazer parte da organização criminosa. Estará atuando como observador das condutas praticadas em alguns ambientes virtuais abertos ou públicos, como redes sociais ou fóruns, sem interagir com os autores dos crimes.

O agente infiltrado, por sua vez, tem por missão primeira conquistar a confiança dos membros do grupo, para então com eles conviver, eventualmente partilhando da intimidade dos investigados, tudo com o objetivo de amealhar informações relevantes. Ademais, a atuação de policiais em operações encobertas, ou seja, sem que se identifiquem como policiais, consiste em atividade rotineira das polícias que prescinde de autorização judicial uma vez que não restringe direitos constitucionalmente assegurados, como, por exemplo, a intimidade, o sigilo das comunicações ou a inviolabilidade do domicílio. A nosso ver, a atividade consiste em simples medida de polícia, que integra o poder geral de investigação fulcrado no Código de Processo Penal. A descriminalização da conduta referente as ações encobertas, não resolve o problema da responsabilidade penal do agente infiltrado, quando atua em conjunto com membros da Orcrim durante a ação de infiltração.

Assim, conclui-se que o Brasil não tratou diretamente sobre a prática de atos ilícitos, ou atos preparatórios, apenas referiu a punição por desvio de finalidade. Existe uma lacuna legislativa que deverá necessariamente ser enfrentada pelo juiz

que autorizar a medida. E então surgiria a possibilidade, inclusive, de autorização para o cometimento de crimes, diversos da associação criminosa o qual é requisito para a atuação do agente infiltrado.

Por fim, no que tange ao procedimento a ser seguido durante a infiltração para permitir a recolha da prova, dois problemas precisam ser enfrentados. Em primeiro lugar necessário estabelecer a forma como se dará o registro das atividades do agente infiltrado, uma vez que todas as atividades serão realizadas no espaço virtual, ambiente que permite o registro dessas atividades, de modo que não podemos nos contentar com um simples relatório, seguido de um depoimento testemunhal quando se está utilizando uma técnica altamente avançada, que permite a reprodução fidedigna dos acontecimentos, sem subjetivismos inerentes ao depoimento de testemunhas, por mais bem intencionadas que sejam.

Embora a matéria seja eminentemente técnica, pois se refere à utilização de softwares que funcionaram como suportes para as ações da infiltração, não se pode negar que produzirá efeitos jurídicos, na medida em que um adequado registro possibilitará o exercício do contraditório diferido, uma vez que a medida pertence aos métodos ocultos de investigação.

Retornando a anteriormente mencionada necessidade de densidade normativa, as normas do Brasil e de Portugal não satisfazem nesse ponto. A insuficiência de dispositivos sobre os procedimentos a serem utilizados para a preservação das evidências e monitoração das atividades do agente infiltrado é extremamente grave, pois poderá resultar na impossibilidade do visado produzir sua defesa uma vez que não será possível refutar os elementos trazidos ao processo como resultados da infiltração. Sendo assim, a ausência de regramento permite a quebra da cadeia de custódia da prova penal. A cadeia de custódia consiste em um processo usado para manter e documentar a história cronológica da evidência, tendo por resultado a documentação formal do processo. Através da demonstração da cadeia de custodia imprime-se fiabilidade ao elemento probatório (Prado, 2014, pp. 82-86).

Para que a prova possa ser submetida a escrutínio que demonstre que ela foi registrada da exata forma como é apresentada ao juiz, é necessária a utilização de ferramentas, mecanismos ou programas que sejam passiveis de auditoria e periciamento a ser requerido pelo visado caso entenda pertinente a sua defesa.

A observância dos primados aqui referidos consistem em requisitos para a qualificação da infiltração digital como método de obtenção de prova legítimo e lícito.

6 - CONCLUSÃO

A presente dissertação foi produzida para analisar a técncia da infiltração digital a partir de diversas indagações sobre a utilização da técnica como método de recolha de prova. Visando responder a esses questinamentos, buscamos estabeler as diferenças entre a infiltração digital e a infiltração policial clássica, construindo para tanto uma definição autônoma. Foi analisado o pano de fundo que resultou na tipificação dos crimes cibernéticos e as pressões políticas e sociais geradas sobre o processo penal para fazer frente à criminalidade digital.

A partir da definição do conceito da infiltração digital e da constatação de que esse tipo de procedimento é deveras invasivo e restringe fortememnte o direito à privaciadade e ao sigilo das comunicações, foram analisados quais são os limites para que o estado processe o visado com base nos elementos colhidos durante a infiltração digital. Essa análise foi feita a partir dos princípios que regem o processo penal. O estudo permitiu inferir que a técnica é pobremente regulada nos normativos, as leis contém lacunas que abrem um espectro decisório deveras amplo ao juiz da instrução criminal, inadequado na seara dos métodos ocultos de investigação, os quais são deferidos sob o manto do sigilo, *inaudita altera pars*.

As lacunas constatadas vão desde a falta de definição legal do que é a infitlração digital, passam pela não definição do procedimento técnico a ser empregado, até a falta de definições sobre os atos praticados pelos policias infiltrados. Todos os problemas mencionados ao longo do presente trabalho, derivados de uma legislação assodada e perfunctória, podem resultar na autorização para uma atuação ilegítima das polícias, afrontosa à superioridade ética do estado. Inobstante, o entendimento que soergue-se das decisões das cortes constitucionais, no Brasil e Portugal, é no sentido de chancelar a infiltração digital como meio de prova válido.

Ao concluir esse estudo, entretanto, consideramos que a infitlração digital poderá ser legitimada em determinados casos, feitos os devidos ajustes conforme

ressaltado ao longo dos nossos apontamentos. O principal requisito para a legitimação da infitlração consistirá em partir-se de indícios veementes da prática do crime (materialidade) e da devida individualização dos sujeitos investigados, ainda que essa individualização seja materializada em um perfil, nickname ou email. Com isso, estaremos afastando a possibilidade de uma infiltração preventiva que mais se aproximaria de atos de espionagem ao inverter o princípio da inocência para uma presunção de culpabilidade, niilificando a garantia de sigilo das comunicações e da privacidade de todos que utilizam o ciberespaço.

E porque precisamos “salvar” a infiltração digital, resgatando-a da nódoa moral na qual está imersa? Porque o o espaço “virtual” tem a capacidade de produzir danos a bens jurídicos extremamente caros a nossa sociedade, como a dignidade sexual de crianças e adolescentes, os quais, diante das peculiaridades desse espaço, como a utilização de criptografia e de técnicas de anonimização, poderiam restar impunes, negando à sociedade o reestabelecimento da paz social da qual o Estado é o guardião-mor.

7 – BIBLIOGRAFIA

Andrade, M. D. (2009a). *Bruscamente no Verão Passado: Observações Críticas sobre uma Lei que Podia e Devia ter Sido Diferente*. Coimbra: Coimbra Editora.

Andrade, M. D. (2009b). Métodos Ocultos de Investigação. In: M. Ferreira Monte, M. C. Calheiros, F. C. Monteiro & F. N. Loureiro, *Que Futuro para o Direito Processual Penal?* (pp. 525-550). Coimbra: Coimbra Editora.

Andrade, M. D. (2013). *Sobre as proibições de prova em processo penal*. Coimbra: Coimbra Editora.

Anselmo, M. A. (2016). *Colaboração Premiada: O novo paradigma do Processo Penal Brasileiro*. Rio de Janeiro: Mallet.

Blog Jurisdição e Governança na Internet (2017, agosto 14). *Jurisdição e governança da internet [Blog].* Acedido em http://irisbh.com.br: http://irisbh.com.br/jurisdicao-e-governanca-da-internet/

Brasil. (1983). *Lei nº 7.170 de 14 de dezembro de 1983.* Define os crimes contra a Segurança Nacional, a Ordem Política e Social, estabelece seu processo e julgamento, e dá outras providências. Acedido em 27 de outubro de 2017, em https://www.planalto.gov.br/ccivil_03/leis/l7170.htm

Brasil. (1990). *Lei nº 8.069 de 13 de julho de 1990.* Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Acedido em 27 de outubro de 2017, em http://www.planalto.gov.br/ccivil_03/leis/L8069.htm

Brasil. (1996). *Lei nº 9.296 de 24 de julho de 1996.* Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal. Acedido em 27 de outubro de 2017, em http://www.planalto.gov.br/ccivil_03/leis/L9296.htm

Brasil. (1998). *Lei nº 9.609 de 19 de fevereiro de 1998.* Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências. Acedido em 27 de outubro de 2017, em http://www.planalto.gov.br/ccivil_03/leis/L9609.htm

Brasil. (1999). *Lei nº 9.883 de 07 de dezembro de 1999.* Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência - ABIN, e dá outras providências. Acedido em 27 de outubro de 2017, em http://www.planalto.gov.br/ccivil_03/leis/L9883.htm

Brasil. (2001). *Lei nº 10.217 de 11 de abril de 2001.* Altera os arts. 1o e 2o da Lei no 9.034, de 3 de maio de 1995, que dispõe sobre a utilização de meios operacionais para a prevenção e repressão de ações praticadas por organizações criminosas. Acedido em 27 de outubro de 2017, em http://www.planalto.gov.br/ccivil_03/leis/LEIS_2001/L10217.htm

Brasil. (2006). *Lei nº 11.343 de 23 de agosto de 2006.* Institui o Sistema Nacional de Políticas Públicas sobre Drogas - Sisnad; prescreve medidas para prevenção do uso indevido, atenção e reinserção social de usuários e dependentes de drogas;

estabelece normas para repressão à produção não autorizada e ao tráfico ilícito de drogas; define crimes e dá outras providências. Acedido em 27 de outubro de 2017, em http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11343.htm

Brasil. (2012). *Lei nº 12.737 de 30 de novembro de 2012.* Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Acedido em 27 de outubro de 2017, em http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm

Brasil. (2013). *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; altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 (Código Penal); revoga a Lei no 9.034, de 3 de maio de 1995; e dá outras providências. Acedido em 27 de outubro de 2017, em http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm

Brasil. (2014). *Lei nº 12.965 de 23 de abril de 2014.* Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Acedido em 27 de outubro de 2017, em http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

Brasil. (2017). *Lei nº 13.441 de 08 de maio de 2017.* Altera a Lei nº 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente), para prever a infiltração de agentes de polícia na internet com o fim de investigar crimes contra a dignidade sexual de criança e de adolescente. Acedido em 27 de outubro de 2017, em http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/L13441.htm

Brito, A. (2013). *Direito Penal Informático*. São Paulo: Saraiva.

Carlos, A. & Reis, F. (2014). *Aspectos Jurídico-Operacionais do Agente Infiltrado*. Rio de Janeiro: Freitas Bastos Editora.

Castells, M. (2003). *A Galáxia da Internet - Reflexões sobre Internet, Negócios e Sociedade*. Rio de Janeiro: Jorge Zahar Edito Ltda.

Colli, M. (2010). *Cibercrimes - Limites e Perspectivas à Investigação Policial de Crimes Cibernéticos*. Curitiba: Juruá Editora.

Dias, V. M. (2012). A Problemática da Investigação do Cibercrime. *Data Venia - Revista Jurídica Digital, 01*, 63-88. Acedido em 23 de agosto de 2017, em http://www.datavenia.pt/ficheiros/edicao01/datavenia01_p063-088.pdf

Faria, L. & Monteiro, T. (2012). A Identidade Adquirida nas Redes Sociais Através do Conceito de Persona. In: *Exposição da Pesquisa Experimental em Comunicação, Intercom – Sociedade Brasileira de Estudos Interdisciplinares da Comunicação, Fortaleza, 1-11*. Acedido em 26 de outubro de 2017, em http://www.intercom.org.br/papers/regionais/nordeste2012/resumos/R32-1497-1.pdf

Feldens, L. (2005). *A Constituição Penal. A dupla face da proporcionalidade no controle de normas penais*. Porto Alegre: Livraria do Advogado.

Fernandes, A. S. (2012). *Processo Penal Constitucional*. São Paulo: Revista dos Tribunais.

Giacomolli, N. J. (2015). *O Devido Processo Penal*. São Paulo: Atlas.

Gontijo, C. A. C. (2016, Novembro 02). 1ª das 10 medidas: Reminiscências do Manual da Inquisição. *Jota.info Coluna do iddd*. Acedido em 28 de Setembro de 2017, disponível em Jota: https://jota.info/colunas/coluna-do-iddd/coluna-iddd-medida-1-contra-corrupcao-reminiscencias-manual-da-inquisicao-02112016

Jesus, D. D. & Milagre, J. A. (2016). *Manual de Crimes Informáticos*. São Paulo: Saraiva.

Jesus, F. M. (2015). *Os Meios de Obtenção de Prova em Processo Penal*. Coimbra: Almedina.

Macedo, R. F. (2015). Sociedade de risco: rumo a uma outra modernidade. *Jusbrasil*, 1-7. Acedido em 04 de outubro de 2017, em https://ferreiramacedo.jusbrasil.com.br/artigos/160037557/sociedade-de-risco-rumo-a-uma-outra-modernidade

Marques, M. J. X-B. (2014). *Os Meios de Obtenção de Prova na Lei do Cibercrime e o seu confronto com o Código de Processo Penal.* Dissertação de Mestrado, Universidade Católica Portuguesa, Lisboa, Portugal. Acedido em 22 de agosto de 2017, em http://repositorio.ucp.pt/bitstream/10400.14/17887/1/Dissertacao%20de%20Mestrado%20final%20-%20JoanaXaraBrasilMarques%20-%20Final.pdf

Oneto, I. (2015). *O Agente Infiltrado. Contributo para a Compreensão do Regime Jurídico das Acções Encobertas*. Coimbra: Coimbra Editora.

Pereira, A. D. L. (2001). A Jurisdição na Internet Segundo o Regulamento 44/2001 (E as Alternativas Extrajudiciais e Tecnológicas). *Boletim da Faculdade de Direito, LXXVII*, 633-687. Acedido em 14 de agosto de 2017, em Estudo Geral: https://estudogeral.sib.uc.pt/bitstream/10316/28775/1/A%20JURISDI%C3%87%C3%83O%20NA%20INTERNET.pdf

Pereira, F. C. (2007). A investigação criminal realizada por agentes infiltrados. *Revista Jurídica do Ministério Público do Estado do Mato Grosso, 2* (2), 173-186.

/

Pereira, F. C. (2008). Meios extraordinários de investigação criminal: infiltrações policiais e entregas vigiadas (controladas). *Revista do Ministério Público do Estado de Goiás*, 13-54.

Pereira, F. C. (2017, Maio 19). Agente Infiltrado Virtual: Primeiras Impressões da Lei 13.441/2017. *Escola Superior de Direito Público*. Acedido em 09 de setembro de 2017, em http://esdp.net.br/agente-infiltrado-virtual-primeiras-impressoes-da-lei-13-4412017/

Pereira, S. (2013). A Recolha da Prova por Agente Infiltrado. In: T. P. Beleza, & F. d. Pinto, Prova Criminal e o Direito de Defesa, *Estudos sobre Teoria da Prova e Garantia de Defesa em Processo Penal* (137-159). Coimbra: Almedina.

Portugal. (1991). *Lei nº 10 de 12 de abril de 1991.* Lei da Protecção de Dados Pessoais face à Informática Acedido em 27 de outubro de 2017, em https://www.cnpd.pt/bin/legis/nacional/lei_1091.htm

Portugal. (2001). *Lei nº 101 de 25 de agosto de 2001.* Regime jurídico das acções encobertas para fins de prevenção e investigação criminal. Acedido em 27 de outubro de 2017, em http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=89&tabela=leis

Portugal. (2009). *Lei nº 109 de 15 de setembro de 2009.* Lei do Cibercrime. Acedido em 27 de outubro de 2017, em http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1137&tabela=leis

Prado, G. (2013). A produção da prova penal e as novas tecnologias: o caso brasileiro. Acedido em 05 de outubro de 2017, em *Empório do Direito*: http://emporiododireito.com.br/leitura/a-producao-da-prova-penal-e-as-novas-tecnologias-o-caso-brasileiro

Prado, G. (2014). *Prova penal e sistema de controles epistémicos. A quebra da cadeia de custódia das provas obtidas por meios ocultos*. São Paulo: Marcial Pons.

Ramalho, D. S. (2017). *Métodos Ocultos de Investigação em Ambiente Digital*. Coimbra: Almedina.

Rodrigues, C. L. (2012). Da valoração dos conhecimentos fortuitos obtidos durante a realização de uma escuta telefónica. *Verbo Jurídico*, 1-244. Acedido em 14 de outubro de 2017, em

http://www.verbojuridico.net/ficheiros/doutrina/penal/claudiorodrigues_conhecimentosfortuitos.pdf

Rubin, F. (2010). Provas atípicas. *Revista Jus Navigandi*, 1-6. Acedido em 26 de setembro de 2017, em https://jus.com.br/artigos/17838

Silva, G. M. (2004). O Direito Penal em Crise de Mudança. In: I. G. Martins, & D. L. Camos, *O Direito Contemporâneo em Portugal e no Brasil* (283-309). São Paulo: Saraiva.

Silva, G. M. (2008). Notas Soltas sobre as alterações de 2007 ao Código de Processo Penal Português. In: L. C. Carvalho, G. M. Silva, G. Prado, & N. Brandão, *Processo Penal do Brasil e de Portugal* (71-93). Lisboa: Almedina.

Silva, G. M. (2010). *Curso de Processo Penal* (5ª ed., Vol. II). Loures: Verbo.

Silveira, A. B. (2015). Os crimes cibernéticos e a Lei nº 12.737/2012. *Conteúdo Jurídico*, 1-5. Acedido em 30 de agosto de 2017, em http://www.conteudojuridico.com.br/artigo,os-crimes-ciberneticos-e-a-lei-no-127372012,52253.html

Sousa, M. (2015). *Crime Organizado e Infiltração Policial - Parâmetros para a Validação da Prova Colhida no Combae às Organizações Criminosas*. São Paulo: Atlas.

Sousa, S. S. (2015). *Investigação Criminal Cibernética. Por uma Política Criminal de Proteção à Criança e ao Adolescente na Internet*. Porto Alegre: Nuria Fabris Editora.

Sydow, S. T. (2015). *Crimes Informáticos e suas Vítimas* (2ª ed.). São Paulo: Saraiva.

Tomasevicius Filho, E. (2016). Marco Civil da Internet: uma lei sem conteúdo normativo. *Estudos Avançados, 30* (86), 269 – 285. Acedido em 26/10/2017, de Scielo. doi:http://dx.doi.org/10.1590/S0103-40142016.00100017

Valente, M. M. (2008). *Escutas telefónicas – da excepcionalidade à vulgaridade* (2ª ed.). Coimbra, Portugal: Almedina.

Valente, M. M. (2010a*). Direito Penal do Inimigo e o Terrorista. O "Progresso ao Retrocesso"* (1ª ed.). Coimbra: Almedina.

Valente, M. M. (2010b). *Processo Penal – Tomo I*. Coimbra: Almedina.

Valente, M. M. (2013). *Do Ministério Público e Da Polícia, Prevenção Criminal e Acção Penal como Execução de uma Política Criminal do Ser Humanos*. Lisboa, Portugal: Universidade Católica.

Valente, M. M. (2015a). Meios ocultos de investigação. Contributo mínimo para uma investigação maior. *Boletim IBCCRRIM*, 2-3.

Valente, M. M. (2015b). Processo Penal, Segurança e Liberdade: uma provocação. *Revista Brasileira de Direito Processual Penal, 1* (1), 105-120. Acedido em 26 de outubro de 2017, em http://dx.doi.org/10.22197/rbdpp.v1i1.6

Valente, M. M. (2017a). Editorial dossiê "Investigação preliminar, meios ocultos e novas tecnologias". *Revista Brasileira de Direito Processual Penal, 3* (2), 473-482. Acedido em 26 de outubro de 2017, em https://doi.org/10.22197/rbdpp.v3i2.82

Valente, M. M. (2017b). *Teoria Geral do Direito Policial* (5ª ed.). Coimbra: Almedina.

Venâncio, P. D. (2011). *Lei do Cibercrime Anotada e Comentada*. Coimbra: Coimbra Editora.

Wendt, E. (2017). *Internet e Direito Penal - Risco e Cultura do Medo*. Porto Alegre: Livraria do Advogado.

Wendt, E. & Jorge, H. N. (2013). *Crimes Cibernéticos: Ameaças a Procedimentos e Investigação.* 2ª Edição, S. M. Oliveira, Ed: Rio de Janeiro, RJ.