ESCOLA DE DIREITO
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIAS CRIMNAIS
MESTRADO EM CIÊNCIAS CRIMINAIS

CARLOS HÉLDER CARVALHO FURTADO MENDES

***MALWARE* DO ESTADO E PROCESSO PENAL:** A PROTEÇÃO DE DADOS INFORMÁTICOS FACE À INFILTRAÇÃO POR *SOFTWARE* NA INVESTIGAÇÃO CRIMINAL

Porto Alegre
2018

PÓS-GRADUAÇÃO - *STRICTO SENSU*

Pontifícia Universidade Católica
do Rio Grande do Sul

CARLOS HÉLDER CARVALHO FURTADO MENDES

***MALWARE* DO ESTADO E PROCESSO PENAL:** A PROTEÇÃO DE DADOS INFORMÁTICOS FACE À INFILTRAÇÃO POR *SOFTWARE* NA INVESTIGAÇÃO CRIMINAL

Dissertação de Mestrado apresentada à Coordenação do Programa de Pós-graduação em Ciências Criminais da Pontifícia Universidade Católica do Rio Grande do Sul (PUC-RS) como requisito parcial para obtenção do título de Mestre em Ciências Criminais

Orientador: Prof. Dr. Aury Lopes Jr.

Porto Alegre

2018

Ficha Catalográfica

M538m Mendes, Carlos Hélder Carvalho Furtado

Malware do Estado e Processo Penal : A Proteção de dados informáticos face à infiltração por software na investigação criminal / Carlos Hélder Carvalho Furtado Mendes . – 2018.

218 f.

Dissertação (Mestrado) – Programa de Pós-Graduação em Ciências Criminais, PUCRS.

Orientador: Prof. Dr. Aury Celso Lima Lopes Junior.

1. Processo Penal. 2. Meios ocultos de investigação. 3. Malware. 4. Prova Digital. 5. Vigilância online. I. Lopes Junior, Aury Celso Lima. II. Título.

Elaborada pelo Sistema de Geração Automática de Ficha Catalográfica da PUCRS
com os dados fornecidos pelo(a) autor(a).
Bibliotecária responsável: Salete Maria Sartori CRB-10/1363

CARLOS HÉLDER CARVALHO FURTADO MENDES

MALWARE DO ESTADO E PROCESSO PENAL: A PROTEÇÃO DE DADOS INFORMÁTICOS FACE À INFILTRAÇÃO POR *SOFTWARE* NA INVESTIGAÇÃO CRIMINAL

Dissertação apresentada ao Programa de Pós-Graduação em Ciências Criminais em nível Mestrado da Pontifícia Universidade Católica do Rio Grande do Sul como requisito parcial para o título de Mestre.

Aprovado em: ___/___/___

BANCA EXAMINADORA

_____

Prof. Dr. Aury Celso Lima Lopes Junior (Orientador)

_____

Prof. Dr. Alexandre Morais da Rosa

_____

Prof. Dr. Fauzi Hassan Choukr

Uma singela dedicatória àqueles que, com amor e dedicação, cuidam e torcem por mim, **por nós.** Marialda, Sérgio e Carlos Víctor.

AGRADECIMENTOS

Este momento de agradecer simboliza, ao mesmo tempo, o fechamento de um ciclo e o sentimento de gratidão por aqueles que nos acompanharam até aqui. Parece inacreditável, mas lembrar dos obstáculos existentes e desafios superados é tarefa difícil. Existiram muitos, contudo a memória nos remete apenas aos momentos de felicidade que renovaram as forças e a vontade de seguirmos firmes no percurso. Como aprendi, a gratidão representa uma dívida eterna – dívida do coração, que não prescreve e não decai – por aqueles que materializam através de gestos, olhares e abraços, sentimentos que nos impulsionam a prosseguir com nossos sonhos. A gratidão, portanto, é o reconhecimento dado àqueles que acreditaram e acreditam em nós. Já os ciclos são marcados por seu início e por seu fechamento. O fechamento deste é agora. O início se localiza há um certo distanciamento, espacial e temporal. É a memória que nos remete a este lugar e tempo distantes. Aliás, foi com Henri Bergson, em "Matéria e Memória", que entendi como era possível me transportar às minhas origens através dos cantos dos sabiás que migravam para a Pontifícia Universidade Católica do Rio Grande do Sul. Transportava-me ao ínicio, transcorrendo o distanciamento do tempo e do espaço, de tal forma que era possível relembrar os propósitos das escolhas tomadas. Esse constante retorno também foi importante para entender a função e o espaço que cada um ocupou na construção destes caminhos.

Agradeço à minha família pelo apoio incansável, por dividir angústias e saudades, pelo amor incondicional. Serei eternamente grato pela união e sintonia que temos uns com os outros. Obrigado por acreditarem e, mais que isso, obrigado por confiarem.

Agradeço ao companheirismo de Manuela Lima. Somamos nossas singularidades e hoje somos plurais, obrigado por entender e respeitar minhas perturbações mais íntimas. Quem tem a sorte de contar contigo não teme, teu amor acalma. Por isso, preciso "lhe dizer que a nossa união foi linda". Agradeço a Italo Rabelo pela parceria firmada desde o início, nestas andanças – e foram muitas – poder dividir as experiências com quem nos incentiva com sinceridade torna tudo bem mais aprazível, seguiremos juntos.

De mesmo modo agradeço aos amigos e amigas que ficaram geograficamente distantes, por todo o apoio que desafiou esta barreira imaginária e pelo carinho despendido nos momentos que necessitei saber que jamais estive só. Ficamos distanciados pelas curvas das estradas que trilhamos, mas vocês souberam ser ao mesmo tempo conforto e impulso. Agradeço então a Maíra Castro, Valter Veras, José Guimarães Mendes Neto, Ariston Apoliano, Maricy Fideles, José Muniz Neto, Amanda Marques, Amanda Thomé, Ricardo Pestana. De igual modo agradeço a Larissa Carvalho Furtado, Luana Feres, Maíra Bandeira, Luan Feres, Marcio Diego,

Fernanda Dutra, André Samenezes, Maurício Aragão Chaves e Otávio Correa. Agradeço a Júlia Bandeira e Vitória Dutra Pinto pelo amor que resiste à distância.

Agradeço imensamente a todos e todas que compõe o Programa de Pós-Graduação em Ciências Criminais da PUCRS e a Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - CAPES. Pelas lições e acolhimento agradeço a Ruth Maria Chittó Gauer, pela simpatia e respeito agradeço a Fabio Roberto D'Avila, pelos apontamentos e pela serenidade agradeço a Nereu José Giacomolli, pelas sugestões e inspiração agradeço a Ricardo Jacobsen Gloeckner. Agradeço ao abrigo ofertado na forma de abraço de Patrícia Souza de Oliveira, Marcia Brum Lopes e Uillian Vargas.

Como uma vez dito "é preciso acreditar nos sonhos e nos sonhadores" e é por isso que agradeço ao Professor Aury Lopes Junior. Nos caminhos da vida conhecemos pessoas que – verdadeiramente – nos estendem a mão, e de algum modo, são nesses momentos que as perspectivas mudam, as pessoas se transformam. Agradeço imensamente pela atenção, por ser fonte de inspiração, pelos estímulos, pela inexplicável facilidade de simplificar pensamentos complexos para transmiti-los e pela oportunidade de aprendizado. Agradeço por saber ouvir sem menosprezar. Tens meu carinho, admiração e amizade.

Agradeço a Augusto Jobim do Amaral não só pelo incentivo e pela generosidade, mas acima de tudo por transmitir coragem aos inquietos. De igual modo agradeço a Fernanda Martins pela bravura de mostrar as reais necessidades das desconstruções internas, mas também por saber acolher com ternura. Agradeço a Geraldo Prado pelo incentivo e inspiração, também por proporcionar momentos indescritíveis de aprendizado, agradeço pela humildade que lhe é peculiar. Também estendo os agradecimentos aos amigos Adriano Damasceno, Yuri Felix, Cleopas Isaías Santos, Daniel Kessler de Oliveira e Roberto Charles de Menezes Dias pelos conselhos sinceros.

Agradeço aos amigos e amigas da turma do Mestrado pelas trocas de experiências e conhecimentos. Em especial àquelas que, no frio solitário, tornaram minha vida bem mais alegre, Luiza Dutra, Daniela Dora Eilberg e Laura Gigante, as quais agradeço pela disponibilidade em ajudar, ouvir, sorrir, abraçar e ensinar. Também àqueles que nutri profunda admiração e carinho, Marcos Melo, Tiago Bunning, Theo Balducci, Fernando Vechi e Gustavo Alberine. Obrigado pela amizade verdadeira que ultrapassou fronteiras interestaduais.

Estendo os agradecimentos a Carla Justino, Manoel Alves e Gabriel Barletta pela forma gentil que me recebem. O fechamento deste ciclo marca o início de um novo, repleto de outros desafios que certamente enfrentaremos juntos. Obrigado a todos e todas.

RESUMO

A presente pesquisa tem o objetivo de investigar a possibilidade da utilização de *malware* pelo Estado como forma de infiltração em dispositivos informáticos para a captação de dados. Trata-se de um método de investigação no ambiente digital demasiadamente lesivo aos direitos fundamentais dos sujeitos, de modo que definir os limites para a execução deste método, bem como os requisitos necessários para sua decretação se mostra de suma importância. Para tanto, a partir da revisão bibliográfica, tomou-se como ponto de partida a ressalva acerca da necessidade da proteção de dados diante das complexidades decorrentes da influência da Sociedade da Informação no Processo Penal. Os efeitos desta influência são aparentes tanto na investigação criminal – que por novas tecnologias se direciona ao alcance do controle e prevenção de delitos através da vigilância –, como na aceleração do processo penal, propriamente dito, pela flexibilização de garantias processuais. Em um segundo momento, observou-se o recrudescimento de meios de investigação que se pautam em estratégias subreptícias de obtenção de provas, e no tocante às novas tecnologias, o dado informático passou a representar uma significativa fonte de prova para as resoluções de casos penais. De tal sorte que pela pesquisa documental baseada em textos legais e projetos legislativos do Brasil, constatou-se uma forte tendência legislativa à flexibilização do sigilo e das proteções a estes dados quando em contextos de investigação criminal e instrução processual penal. Contudo, de igual modo se percebeu a negligência legislativa quanto aos métodos de recolha e preservação de tais dados. Estes procedimentos notadamente constituem requisitos ao uso de novas tecnologias cuja função é a recolha do dado informático como fonte da prova penal, pois a confiabilidade e a integralidade da fonte de prova digital são certamente requisitos de admissibilidade da prova. Assim sendo, destacou-se a importância da preservação da cadeia de custódia digital. Por fim, especificamente quanto ao *malware* e a utilização deste pelo Estado na persecução penal se definiu a natureza jurídica de modo que, como instituto processual penal, identificou-se os limites ao seu uso. Quanto aos requisitos, as pesquisas jurisprudenciais e documentais se pautaram nas experiências da Itália, Estados Unidos da América e Espanha, a partir de casos penais e legislações que tratavam sobre o tema. De tal forma, após identificar o grau de lesividade do método investigativo, destacou-se direitos fundamentais diretamente afetados por tal intervenção Estatal.

Palavras-chave: Processo Penal. Meios ocultos de investigação. *Malware*. Prova digital. Vigilância Online.

RESUMEN

La presente investigación tiene el objetivo de investigar la posibilidad de la utilización de malware por el Estado como forma de infiltración en dispositivos informáticos para la captación de datos. Se trata de un método de investigación en el entorno digital demasiado perjudicial para los derechos fundamentales de los sujetos, de modo que definir los límites para la aplicación de este método, así como los requisitos necesarios para su decretación, es de suma importancia. Para ello, a partir de la revisión bibliográfica, se tomó como punto de partida la salvedad acerca de la necesidad de la protección de datos ante las complejidades derivadas de la influencia de la Sociedad de la Información en el Proceso Penal. Los efectos de esta influencia son aparentes tanto en la investigación criminal -que por nuevas tecnologías se dirige al alcance del control y prevención de delitos por la vigilancia-, como en la aceleración del proceso penal, propiamente, por la flexibilización de garantías procesales. En un segundo momento, se observó el recrudecimiento de medios de investigación que se basan en estrategias subreptiuales de obtención de pruebas, y en cuanto a las nuevas tecnologías, el dato informático pasó a representar una significativa fuente de prueba para las resoluciones de casos penales. De tal suerte que por la investigación documental basada en textos legales y proyectos legislativos de Brasil, se constató una fuerte tendencia legislativa a la flexibilización del sigilo y de las protecciones a estos datos cuando en contextos de investigación criminal e instrucción procesal penal. Sin embargo, de igual modo se percibió la negligencia legislativa en cuanto a los métodos de recogida y preservación de dichos datos. Estos procedimientos, evidentemente, constituyen requisitos para el uso de nuevas tecnologías cuya función es la recogida del dato informático como fuente de la prueba penal, pues la confiabilidad y la totalidad de la fuente de prueba digital son ciertamente requisitos de admisibilidad de la prueba. Así, se destacó la importancia de la preservación de la cadena de custodia digital. Por último, específicamente en cuanto al malware y la utilización de éste por el Estado en la persecución penal se definió la naturaleza jurídica de modo que, como instituto procesal penal, se identificaron los límites a su uso. En cuanto a los requisitos, la investigación jurisprudencial y documental se basó en las experiencias de Italia, Estados Unidos de América y España, a partir de casos penales y legislaciones que trataban sobre el tema. De tal forma, tras identificar el grado de lesividad del método investigativo, se destacaron derechos fundamentales directamente afectados por dicha intervención estatal.

Palabras clave: Proceso Penal. Medios ocultos de investigación. Malware. Prueba digital. Vigilancia online.

LISTA DE ABREVIAÇÕES

Art.	Artigo
Atual.	Atualizada
BOE	*Boletín Oficial del Estado*
CADH	Convenção Americana de Direitos Humanos
CEDH	Convenção Europeia de Direitos do Homem
CF	Constituição Federal do Brasil
CPP	Código de Processo Penal brasileiro
CPU	*Central Process Unit*
DEMF	*Digital Evidence Management Framework*
EUA	Estados Unidos da América
FBI	*Federal Bureau of Investigation*
GPS	*Global Positioning System*
HC	*Habeas Corpus*
Internet	*International network*
IP	*Internet Protocol address*
KLS	*Key Logger System*
LECrim	*Ley de Enjuiciamiento Criminal*
MAC	*Media Access Control*
Min	Ministro
MG	Minas Gerais
PLS	Projeto Lei Senado
Rel.	Relator
RHC	Recurso em *habeas corpus*
STF	Supremo Trinunal Federal
STJ	Superior Tribunal de Justiça
TEDH	Tribunal Europeu de Direitos Humanos
TI	Tecnologia da Informação
TJ	Tribunal de Justiça
TSA	*Time Stamps Authority*
URL	*Uniform Resource Locator*

"A sociedade da transparência não padece apenas com a falta de verdade, mas também com a falta de aparência. Nem a verdade nem a aparência são transparentes. Só o vazio é totalmente transparente. Para exorcizar esse vazio coloca-se em circulação uma grande massa de informações. A massa de informações e de imagens é um enchimento onde ainda se faz sentir o vazio. Mais informações e mais comunicação não clarificam o mundo. A transparência tampouco torna clarividente. A massa de informações não gera verdade. Quanto mais se liberam informações tanto mais intransparente torna-se o mundo. A hiperinformação e a hipercomunicação não trazem luz à escuridão".

Byung-Chul Han, Sociedade da transparência

SUMÁRIO

1 INTRODUÇÃO

Após a elaboração da presente pesquisa o que se pretende como objetivo principal, certamente, é convidar o leitor para a reflexão sobre um tema que está longe de ser esgotado. Ao contrário disto. Renova-se constantemente em passos acelerados possibilitando que novos problemas surjam para serem enfrentados. Tal como é a atual atualização do tema, o texto já desde o seu nascedouro é ameaçado pela obsolecência.

Ainda assim, a pesquisa se justifica pela contemporaneidade das discussões, principalmente por retratar uma realidade já vivida em contextos estrangeiros e que apresenta embates cujas soluções tomadas, por vezes, resvelam na afetação demasiada de direitos fundamentais e garantias processuais. Ademais, chamar atenção para o descompasso legislativo entre os ditames do devido processo penal e as tendenciosas leis que se referem a proteção de dados no Brasil, é certamente possibilitar uma análise crítica quanto aos iminentes prejuízos direcionados à esfera da intimidade e privacidade dos cidadãos.

Trata-se da proteção de dados informáticos face ao surgimento de novas tecnologias que possibilitam o incremento de investigações criminais, nomeadamente os métodos ocultos de investigação no ambiente digital. Diante das diversas espécies de métodos de investigação, optou-se em discorrer apenas quanto à utilização de *softwares* maliciosos como novos instrumentos utilizados pelo Estado na persecução penal.

A investida estatal se embasa nas potencialidades trazidas pelas tecnologias de comunicação e informação, de modo que como gestor de ameaças[1], a partir da óptica neoliberal, o Estado insere o processo penal na lógica securitária. A interceptação do fluxo de dados e a monitorização informacional são estratégias de atuação que trazem o utilitarismo e o imediatismo ao processo penal securitarista. Nesta senda, a tentativa é controlar ou reduzir os riscos do cometimento de ilicitudes, ou melhor, impor medidas mais eficientes que sirvam à guerra contra a criminalidade.

Identifica-se diante deste cenário a necessidade de se (r)estabelecer limites e mecanismos de controles do poder punitivo diante do uso pelo Estado de técnicas e tecnologias que se inserem na investigação criminal pela influência direta da Sociedade da Informação. Logo a pergunta problema que guiou todo o desenvolvimento do presente estudo pode ser formulada da seguinte maneira: Quais os requisitos necessários para a utilização de *softwares*

[1] AMARAL, Augusto Jobim do. **A governabilidade em tempos securitários.** In: AMARAL, Augusto Jobim do; ROSA, Alexandre Morais da. Cultura da punição e ostentação do horror. 2ª ed. rev. e ampl. Florianópolis: Empório do Direito, 2015. p, 37.

maliciosos na recolha de dados informáticos para fins investigativos e quais os limites para a execução desta nova metodologia de infiltração?

Em termos gerais, a hipótese levantada incialmente apontava que tanto os limites demarcados quanto os requisitos impostos para a utilização do *malware*, como meio de obtenção de prova no ordenamento jurídico brasileiro, estavam estabelecidos no fundamento existencial do processo penal e da investigação criminal como mecanismos de proteção dos direitos fundamentais do cidadão face ao poder punitivo. Em termos específicos a mesma hipótese apontava para observações quanto ao método investigativo tecnológico propriamente empregado, suas peculiaridades, as funcionalidades investigativas derivadas, a demonstração de confiabilidade e integralidade de seus resultados e, por fim, o grau de incidência no núcleo essencial de determinados direitos fundamentais. De modo que somente a partir da análise de cada um destes itens se tornou possível responder ao problema central.

A pesquisa realizada se insere na linha de Sistemas Jurídicos-Penais Contemporâneos e possui estrutura que se divide em três capítulos.

O primeiro capítulo destaca a influência que a Sociedade da Informação e Comunicação exerce no Direito Processual Penal, sob dois eixos principais. Primeiro, a relação desta Sociedade da Informação – resultante de uma quarta revolução industrial – e a investigação preliminar. Segundo, a incidência da Sociedade da Informação no processo penal propriamente dito, e as modificações que o impõe.

Inicia-se com as reflexões propostas por estudiosos da sociedade da informação como fenômeno que modifica os paradigmas sociais ao tornar possível o uso massivo de novas tecnologias de informação e comunicação. Tecnologias estas que são notadamente "psicotecnologias" a serviço do ser humano na ampliação de suas capacidades e circunstâncias. Ao mesmo tempo em que o indivíduo se serve das tecnologias, se dispõe à exploração exercida pelo uso da tecnologia. Neste contexto o ser humano é personificado por seus dados, produzidos voluntaria ou involuntariamente, mas que são disponibilizados pela exposição decorrente da sociedade da transparência[2].

A exploração através dos dados pessoais obedece à lógica do controle pelo "panóptipo digital", de modo que é esta a influência direta da Sociedade da Informação sobre a Investigação Criminal. Pelo acesso constante e massivo a dados dos indivíduos, tendenciosamente se impõe o controle pela vigilância, de tal sorte que a "*vigilância online*",

[2] HAN, Byung-Chul. **Sociedade da transparência.** Petrópolis: Rio de Janeiro, Vozes, 2017.

como se verá, atende aos expedientes das investigações prospectivas que buscam suspeitos "não suspeitos".

No que se refere ao processo penal, a influência percebida pela força impositiva da Sociedade da Informação, como veículo de difusão do neoliberalismo, é de dupla ordem. A primeira se relaciona às posturas que a nova racionalidade neoliberal impõe aos sujeitos processuais, de modo que o mote principal de atuação destes sujeitos é o alcance das metas de produtividade, que acabam por desconfigurar (a um só tempo) a posição do réu ou investigado como sujeito de direito para o transformar em produto a ser consumido pelo mercado populista punitivo; e o próprio processo penal, que se acelera para alcançar a eficiência em detrimento da sua efetividade. Se acelera sem sair do lugar, transformando-se em um processo penal obsceno sem utilidade constitucional. A identificação deste cenário é fundamental para entender algumas das mudanças ocorridas no sistema de justiça criminal, no tocante à dogmática processual.

No segundo capítulo, o que se propôs foi uma análise crítica da incidência tecnológica em um contexto de investigação criminal preliminar e de influência das tecnologias na produção penal probatória. Primeiramente foi necessário resgatar o fundamento existencial da investigação criminal para o estabelecer como a premissa basilar inicialmente tomada. Tal premissa foi fundamental para que fosse possível discorrer desde os preceitos básicos da categoria dos métodos ocultos de investigação até a observação de um fenômeno que corresponde ao seu significativo recrudescimento.

Destacou-se o envolvimento, possível pelas tecnologias, de técnicas de controle e investigação de delitos a partir da obtenção de dados. O dado informático referente ao sujeito alvo da investigação é o objetivo das intervenções estatais. A proteção da intimidade e da privacidade materializadas em dados pessoais deve ser tutelada pela legislação, a ressalva neste sentido foi feita para que se apontasse a tendência à legalidade excepcional, ou melhor, uma exceção legalizada que comporta abstrações perigosas a tais direitos individuais vinculados à livre personalidade.

Como exemplo ilustrativo, utilizou-se a *Ley de Enjuiciamiento Criminal* da Espanha com o objetivo de demonstrar a possível normatização de diretrizes legislativas às autoridades investigativas e judiciais quanto à utilização de tecnologias digitais na investigação. O objetivo da exemplificação é expor uma contraposição legislativa tendente no ordenamento jurídico brasileiro, caracterizada pela ausência de limites impostos ao Estado quanto a obtenção de dados informáticos frente a contextos de investigação e instrução processual penal.

Quanto à influência da tecnologia na produção probatória, ainda no segundo capítulo, (re)definiu-se categorias vinculadas à terminologia "prova" no processo penal. Por mais que se trate de um tema já demais trabalhado, neste ponto a (re)definição de categorias parece importante para que não se confunda o tratamento jurídico ofertado aos resultados da execução de *meios de obtenção de prova* e da execução de *medidas cautelares probatórias*. De tal forma, reconhece-se a necessidade de um tratamento adequado ao que posteriormente se denominou de *fonte de prova digital*, desde a sua aquisição à sua preservação para que se torne admissível no processo penal.

A partir das discussões levantadas acima foi possível destacar, no terceiro capítulo, a natureza jurídica do *malware* operado pelo Estado como um método oculto de obtenção de prova, sem descartar efetivamente a possível natureza jurídica híbrida que por ventura possa vir a existir em decorrência dos avanços da técnica de comprovação da fiabilidade e integralidade das *fontes de prova digital* recolhidas por acesso remoto.

Em outro momento, utilizou-se da legislação e jurisprudência da Itália, dos Estados Unidos da América e da Espanha para ilustrar as funcionalidades desempenhadas pelo *malware* a serviço das investigações informáticas ocultas. Buscou-se utilizar ao menos um julgado principal que correspondesse a cada espécie de investigação desempenhada pela infiltração de *malware* do Estado em dispositivos informáticos visados.

A escolha por tais países se deu pela avançada discussão sobre o tema na realidade de cada um. Na jurisprudência italiana há diversos casos emblemáticos que o Estado se utilizou de *softwares* a serviço da investigação criminal. Entender como os Tribunais italianos avaliam a utilização destes métodos, os limites e o controle exercido diante de possíveis abusos, pode direcionar a formação de entendimentos a serem adotados no Brasil.

De igual modo é a utilidade dos casos ocorridos nos EUA. Para fins da pesquisa, a ilustração do método investigativo a partir da experiência norte-americanas parece fundamental. Soma-se à escolha dos Estados Unidos da América como exemplificação, por se tratar de um dos países que mais investe em serviços de vigilância ou dispositivos de "segurança nacional". Quanto à Espanha, a relevância para também ser abordada de modo ilustrativo é justamente as disposições legislativas da *LECrim* que dispõe em rol uma série de situações de investigação informática, dentre as quais a expressa possibilidade da utilização de *software* para o registro e o sequestro de dados.

Feito isso, passou-se à análise da incidência da (nova) metodologia de infiltração do Estado face a direitos fundamentais. O recorte abordou quatro direitos fundamentais diretamente afetados com a intervenção estatal mediante o uso do *malware*, quais sejam a

proteção da intimidade, a proteção da autodeterminação informativa, a proteção do sigilo das comunicações e, por fim, a integridade e confiabilidade dos sistemas informáticos.

2 SOCIEDADE DA INFORMAÇÃO, INVESTIGAÇÃO CRIMINAL E PROCESSO PENAL[3]

O livro "O inumano" de Jean François Lyotard é composto por um conjunto de palestras feitas pelo autor para explicar o fenômeno da expansão da racionalidade em uma sociedade dita pós moderna e como este fenômeno transforma paulatinamente o ser humano no "inumano"[4]. Inicia-se o presente texto citando a referida obra, pois é nesta que Lyotard, em crítica ao pensamento filosófico, irá colocar em pauta o seguinte questionamento: É possível pensarmos sem corpo?

O curioso é que à época em que o texto fora escrito jamais se poderia imaginar que os avanços tecno-científicos pudessem ocorrer com tamanha velocidade. A resposta para o questionamento proposto pelo autor é negativa. De fato, e levando em consideração os argumentos de Lyotard, ainda não se pode pensar (reflexivamente) sem o corpo e a mente. Tanto porque, um é condição de existência e limitação do outro, corpo e mente.

Todavia, é inegável a conclusão de que – com o advento das tecnologias – o ser humano expandiu sua capacidade de armazenar informações, ampliar sua memória. Aliás, "as novas tecnologias, baseadas na eletrônica e na informática devem ser, sempre sob um mesmo aspecto, consideradas como extensões materiais da nossa capacidade de memorizar"[5]. Como define Kerckhove, são "psicotecnologias" aquelas que emulam, estendem ou amplificam o poder da mente humana. Não apenas prolongam as propriedades de envio e recepção da consciência, mas as modificam ao penetrarem na consciência de seus usuários/utilizadores. São/Foram responsáveis por acrescentarem o tato, como sentido, aos demais sentidos humanos, visão, audição e irá revestir totalmente o sistema nervoso humano, a partir da realidade virtual[6].

Hoje é impossível imaginar as complexas relações sociais sem o auxílio dessas novas tecnologias. Ao passo que somente se percebe o grau de avanço tecnológico, quando presenciada sua crise, quando da sua falta ainda que momentânea.

Grande parte da população mundial utiliza diariamente novas tecnologias digitais, sejam estas os *smartphones*, câmeras, computadores ou etc. Vive-se no tempo das tecnologias da informação e comunicação, sua velocidade estabelece o ritmo dinâmico de todas as relações

---

[3] Não se desconhece que no presente capítulo são utilizados pensamentos de autores com matrizes filosóficas diferentes, contudo o diálogo entre estes se mostrou demasiadamente necessário para que fosse alcançado o objetivo pretendido.
[4] LYOTARD, Jean François. **O Inumano, considerações sobre o tempo**. 2ª Ed: Editorial Estampa, 1997.
[5] LYOTARD, Jean François. **O Inumano, considerações sobre o tempo**. Op. cit. p, 52.
[6] KERCKHOVE, Derrick de. **A pele da cultura: uma investigação sobre a nova realidade electrónica.** São Paulo: Relógio D'Água Editores, 1997, p. 34.

sociais. A comunicação, a partir da difusão da internet, adquire a capacidade de enviar inúmeras mensagens para muitos destinatários em tempo real.

Adquiriu-se a capacidade de armazenar memória de maneira *on-line* através de nuvens cibernéticas. Operações bancárias são feitas diariamente via rede mundial de computadores. Rotas de destinos são traçadas para facilitar o deslocamento. Todos estão conectados e consequentemente mais facilidades são alcançadas.

Ao mesmo tempo em que as novas tecnologias de informação e comunicação inserem o ser humano na sociedade da informação, alarga-se a sensação de medo e perigo já amplamente difundidas, como assevera Beck[7]. Não basta fortalecer exércitos e proteger fronteiras, o perigo e o medo, advindos do risco, utilizam-se do "ciberespaço".

Nesse interim, a lógica securitária passa a ter protagonismo nas ações de governamentalidade – conjunto de procedimentos e táticas que permitem uma forma complexa e específica de poder, que tem por alvo a população, por instrumentos técnicos essenciais os dispositivos de segurança[8] –, na qual conter informações é fundamental para dirimir os riscos. Dirá Lyotard[9], com o auxílio de Leibniz, que a busca incessante por formulação de complexidades não possui outro objetivo que não o do aperfeiçoamento da mônade, ao passo que "quanto mais complexa for uma mônade, mais numerosos serão os dados que memoriza". Atualmente, esses dados são contidos em diversos mecanismos tecnológicos, a expansão da memória se dá em *bits*, seja em dispositivos físicos ou virtuais (*on-line*).

Ter acesso a tais dados é possivelmente "antecipar o futuro", pois esse é o poder da informação, neutralizar acontecimentos para que se possa reduzir os riscos[10]. A guerra contra a criminalidade a partir da Sociedade de informação obedece a lógica *fleet in being*, como destaca Virilio[11]. O embate é travado a partir do abandono do princípio de atacar o inimigo tão logo que ele é percebido, a estratégia adotada passa a ser o movimento dos corpos invisíveis. Nas

---

[7] BECK, Ulrich. **Sociedade do risco: rumo a uma outra modernidade.** São Paulo: Ed. 34, 2010.

[8] FOUCAULT, Michel. **Microfísica do poder.** 19ª ed. Rio de Janeiro: Edições Graal, 1979. A Governamentalidade, Curso do Collége de France, 1 de fevereiro, 1978. p, 291 - 292. Neste mesmo sentido, Dardot e Laval referem-se que o termo "governamentalidade" significa as múltiplas formas da atividade pela qual os homens – que podem ou não pertencer a um governo – buscam conduzir a conduta de outros homens, ou seja, governa-los. Este governo visa obter um autogoverno do indivíduo. Deste modo, explica os autores que governar é conduzir a conduta dos homens, desde que se especifique que essa conduta é tanto aquela que se tem para consigo mesmo quanto aquela que se tem para com os outros e que se exige e requer-se a liberdade como condição de possibilidade. "Governar não é governar contra a liberdade ou a despeito da liberdade, mas governar pela liberdade, isto é, agir ativamente no espaço de liberdade dado aos indivíduos para que estes venham a conformar-se por si mesmos a certas normas". (DARDOT, Pierre; LAVAL, Christian. **A nova razão do mundo: ensaio sobre a sociedade neoliberal.** 1 ed. São Paulo: Boi tempo, 2016. p, 18 – 19.

[9] LYOTARD, Jean François. **O inumano.** Op cit. p, 72.

[10] LYOTARD, Jean François. **O inumano.** Op cit. p, 72.

[11] VIRILIO, Paul. **Velocidade e política.** São Paulo: Estação Liberdade, 1996. p, 50.

palavras do autor, a *fleet in being* consagra uma nova ideia dromocrática, na qual a distância cede espaço à posse do tempo.

Sob a óptica securitária se causa detrimento demasiado à privacidade e à intimidade dos cidadãos, direitos estes tão caros a um Estado que se pretende Democrático de Direito. No Brasil, a proteção à privacidade é garantida constitucionalmente (Art. 5, X, CF), todavia há que se perceber que a proteção de dados na nova era das tecnologias de informação e comunicação demanda maior proteção do que a exigida para proteger a simples intimidade. A privacidade como direito fundamental está sob constante ameaça, principalmente a partir da "era do terror", pois veio a ser considerada como um obstáculo à segurança, sendo golpeada constantemente por legislações abusivas e emergenciais[12].

Diante deste panorama, Rodotá avalia que a partir da caracterização da organização social vigente, cada vez mais baseada no poder de informação – sendo este um novo e verdadeiro "recurso de base" – surge o problema da legitimação deste poder. Esclarece que o processo de legitimação se dá por meio do somatório da inexistência de possibilidade do Estado e da indústria recuarem no aprimoramento de novas técnicas informativas, mais amplas e sofisticadas, e a promessa de alcançar a garantia efetiva de direitos individuais tradicionais[13].

Porém, ainda segundo o autor, o fornecimento de dados e informações não se justifica tão somente para alcançar em contrapartida alguns benefícios sociais. Estas informações tornarão possível o exercício de qualquer tipo de controle sobre o cidadão, ademais, permitem novas práticas de poder ou o fortalecimento de poderes já existentes[14].

Para o Direito Processual Penal esta é uma matéria muito cara, principalmente por ser o processo, instrumento de garantias face aos abusos do controle penal. Todavia, de acordo com Chirino Sanchez, nos últimos anos se tem flexibilizado as garantias processuais e se pode perceber uma crescente quantidade de mudanças referentes à redução de possibilidade de controle do cidadão dos dados que podem ser obtidos e processados pelas autoridades da investigação criminal[15].

Tem-se discutido diferentes projetos legislativos que adotam meios informáticos e eletrônicos para a obtenção e tratamento de dados informáticos e pessoais no processo penal.

---

[12] RODOTÁ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje.** Rio de Janeiro: Renovar, 2008. p, 14.
[13] RODOTÁ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje.** Op. cit. p, 35 – 37.
[14] RODOTÁ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje.** Op. cit. p, 35 – 37.
[15] CHIRINO SANCHEZ, Alfredo. *Las tecnologias de la informacion y el processo penal: análisis de uns crisis anunciada.* ***Revista de ciências penales de Costa Rica*****.** Rep. Fed. de Alemania 6 (1982): 275. p, 46.

Há incidência direta no direito da autodeterminação informativa, principalmente para que se aceite, como meios de prova, esses dados obtidos.

Os usos de novos meios de investigação no processo penal, segundo Chirino Sanchez, nos leva a uma necessária reflexão sobre o papel do Estado de Direito no moderno processo penal, que busca alcançar a "verdade" por meio de ferramentas cada vez mais sofisticadas. Pauta-se essa política criminal em um discurso populista que fomenta uma grande crise de garantias no processo penal[16].

Se é certo que a dinâmica processual se assemelha ao estado de guerra na medida em que se adentra na lógica da incerteza[17], tal como a guerra tenderá à velocidade, buscar-se-á imobilizar o inimigo sob o viés da surpresa repentina. Se o próprio "material de guerra" desaparece na aceleração das performances dos meios de comunicação da destruição[18], assim o será no Processo Penal.

Como Weissberg afirma – ao relembrar as lições de Virilio – o momento estratégico se desloca do campo de batalha para uma anterior programação militar-econômica de sistemas automáticos, que assumem o papel e ao mesmo tempo, desqualificam, as capacidades humanas de decisão. Aumentam o caráter estratégico do domínio da comunicação, que se funda a partir do princípio da reatividade, quase instantânea[19].

No processo penal desaparecerão os meios de investigação tradicionais na aceleração das performances dos meios de comunicação e informação que possibilitarem maior velocidade na obtenção de provas que – pelo alto grau de violação a privacidade e intimidade – serão capazes de impossibilitar contestações.

O detrimento de garantias fundamentais do Processo Penal o afasta de seu caráter de Direito Constitucional aplicado e, consequentemente, aproxima-o de um processo penal simbólico, útil para tranquilizar o clamor público no combate à criminalidade.

Essa guerra, que como qualquer outra não possui fundamento jurídico, mas político[20], afasta do Processo Penal da compatibilidade com qualquer fundamento jurídico, pois este passa a atender (ou pretender) propósitos de erradicação da criminalidade.

---

[16] CHIRINO SANCHEZ, Alfredo. *Las tecnologias de la informacion y el processo penal: análisis de uns crisis anunciada.* Op. cit. p, 46.
[17] LOPES JR, Aury. **Fundamentos do processo penal: introdução crítica.** 2ª ed. São Paulo; Saraiva, 2016. p, 199.
[18] VIRILIO, Paul. **Velocidade e política.** Op. cit. p, 126.
[19] WEISSBERG, Jean-Louis. **Paradoxos da teleinformática.** *In:* PARENTE, André (Org). Tramas da rede: novas dimensões filosóficas, estéticas e políticas da comunicação. Porto Alegre: Sulina, 2013. p, 129 – 130.
[20] GLOECKNER, Ricardo Jacobsen e AMARAL, Augusto Jobim do. **Criminologia e(m) crítica**. Curitiba: Editora Champagnat – PUC-PR; Porto Alegre, RS: Edipucrs, 2013. p, 357.

As intervenções estatais na esfera privada dos cidadãos diante de uma persecução criminal deve ser somente admissível no explícito limite imposto pela lei que obedeça a ordem constitucional. Ademais, estas ingerências não são permitidas em circunstâncias gerais, sendo tão somente admitidas em específicas situações e condições que permitam o equilíbrio processual entre o interesses na persecução penal e o direito ao âmbito privado da personalidade[21].

De acordo com Roxin, permitir ao Estado utilizar das chamadas operações de vigilância eletrônica intensiva (como por exemplo o uso de equipamentos eletrônicos de vigilância dentro da residência de um suspeito e usar o monitoramento das conversas privadas deste para provar sua culpabilidade), seria uma drástica restrição da regra básica da autoincriminação. Para além, ao mesmo tempo, muitos aspectos da proteção do âmbito privado também seriam perdidos, visto que de todos os lugares, a residência de uma pessoa é o mais importante para a expressão de seu livre desenvolvimento à personalidade[22].

Mutatis mutandis, entende-se que assim também o será quanto aos dados e informações pessoais que os cidadãos armazenam em mídias digitais, sejam estas físicas ou virtuais. Aliás, como argumentado acima, o que se tem – a partir das mídias – é uma expansão da memória humana, de modo que esses tipos de atuações de vigilância não se compatibilizam com as bases constitucionais.

Neste sentido e ao se levar em consideração todo o exposto acima, o que se tem em total evidência é a exposição do nó górdio entre o Direito Processual Penal e os reflexos oriundos da sociedade de informação, seus avanços tecnológicos na informação e na comunicação. Embora aparentemente distantes, se misturam à medida em que toda essa reviravolta, ou como dito por muitos uma revolução tecnológica, afeta substancialmente diversos setores e aspectos sociais e jurídicos. Principalmente no tocante ao surgimento de modernas tecnologias de controle e de investigação de delitos. Neste ponto é que reatar o nó górdio, a partir de Latour[23], no sentido de "atravessar o corte que separa os conhecimentos exatos e o exercício de poder" se faz necessário.

---

[21] ROXIN, Claus. ***Pasado, presente y futuro del derecho procesal penal.*** 1ªed. 1ªreimp. Santa Fé: Rubinzal Culzoni, 2009. p, 102.
[22] ROXIN, Claus. ***Pasado, presente y futuro del derecho procesal penal.*** Op. cit. p, 108.
[23] LATOUR, Bruno. **Jamais fomos modernos: ensaios de antropologia simétrica.** Rio de Janeiro: Ed. 34. 1994. p, 8 – 11.

2.1 Sociedade da Informação: Tecnologia, Velocidade e Tempo

Quando Manuel Castells se questionou acerca da revolução cuja sociedade no final do Séc. XX perpassara, traçou paradoxalmente a diferença entre a mudança da história da vida (suave, lenta e firme), composta por uma série de situações estáveis, para aquela que observou: momento de grande rapidez, final do século XX, marcado pela transformação da "cultura material" por mecanismos tecnológicos[24].

A partir das últimas décadas do Séc. XX com os avanços tecnológicos, possibilitados pelas tecnologias da informação, o mundo – na visão do autor – se tornou digital. Tamanha e fundamental é a grandeza destas transformações que Castells assemelha a revolução da tecnologia da informação à Revolução Industrial do Séc. XVIII. Isso porque, toda a estrutura padronizada em bases materiais da economia, sociedade e cultura é rompida, ou descontinuada. A revolução vivida se refere às tecnologias da informação, processamento e comunicação, tal qual a Revolução Industrial se deu por meio da substituição das antigas para as novas fontes de energia.

A importância da *Internet* pode ser equiparada à rede elétrica ou ao motor elétrico na Era Industrial devido à sua capacidade de distribuir informação por todo o "domínio da atividade humana"[25]. Todavia, "o que caracteriza a revolução tecnológica não é a centralidade de conhecimentos e informação, mas a aplicação desses conhecimentos e dessa informação para a geração de conhecimentos e de dispositivos de processamento/comunicação da informação, em um ciclo de realimentação cumulativo entre a inovação e seu uso"[26].

O denominado ciberespaço – na definição de Levy[27] – nada mais é que um novo meio de comunicação decorrente da interconexão mundial dos computadores, não se tratando meramente de uma infra-estrutura material de comunicação digital, mas o universo de informações nela abrigado, os seres que estão inseridos e que alimentam este universo. Nesta senda, a *Internet*, portanto, é um cérebro incansável que não para de produzir, de analisar e combinar informações[28].

---

[24] CASTELLS, Manuel. **A Sociedade em rede.** Vol. 1. 8ª ed. rev. e ampl. Tradução: Roneide Venâncio Majer. Editora: Paz e Terra. São Paulo, 2005. p, 67.
[25] CASTELLS, Manuel. **A galáxia da internet: reflexões sobre a internet, os negócios e a sociedade.** Rio de Janeiro: Jorge Zahar Ed., 2003. p, 7.
[26] CASTELLS, Manuel. **A Sociedade em rede.** Op. cit. p, 68 – 69.
[27] LEVY, Pierre. **Cibercultura**. São Paulo: Ed. 34. 1999. p, 17.
[28] KERCKHOVE, Derrick de. **A pele da cultura: uma investigação sobre a nova realidade electrónica.** Op. cit. p. 90.

Neste aspecto a *Internet* assemelha-se a uma complexidade rizomática, não há padrão de conexão entre seus pontos ou nós. Afirma Kastrup[29] que como rizoma, a *internet* "articula elementos heterogêneos como saberes e coisas, inteligências e interesses, onde as matérias trabalham fora do controle dos métodos". Para compreender uma complexidade rizomática, faz-se necessário retomarmos o pensamento de Deleuze e Guattari[30] quanto aos princípios ou características aproximativas de tal conceito.

Destaca-se de imediato os princípios de conexão e de heterogeneidade em que qualquer ponto de um rizoma pode ser conectado a qualquer outro, não possuindo um centro faz conexões sem obedecer padrões já estabelecidos. Em seguida, há o princípio da multiplicidade. Afirmam Deleuze e Guattari que multiplicidade é a inexistência de uma unidade, o não pertencimento a um sujeito ou objeto, mas tão somente determinações, grandezas, e dimensões. É composto por singularidades que estabelecem conexões entre si, agenciamentos, relações recíprocas, formando as linhas do rizoma e explicando as suas transformações sem atrela-las a qualquer instância exterior[31]. Nas palavras de Deleuze e Guattari[32], as multiplicidades se definem pela desterritorialização, pela linha abstrata ou linha de fuga, na qual mudam sua natureza ao se conectarem às outras.

O quarto princípio é o chamado "ruptura a-significante", que por sua vez, define um rizoma como uma complexidade não demasiadamente prejudicada por cortes, como os que atravessam as estruturas. Um rizoma pode ser rompido, em qualquer lugar, e retomará sua organização ou criação de novas formas, por meio de outras linhas ou conexões em constante devir. Por fim, o quinto e sexto princípios, denominados respectivamente de "princípio da cartografia" e da "decalcomania" denotam o rizoma como um sistema de modelo não estrutural. O rizoma é estranho a qualquer ideia de eixo baseado em uma estruturação, como unidade pivotante, sob a qual se organizam estados sucessivos.

Para Kastrup[33], definir rizoma como um conceito é afirmá-lo como sistema aberto, na medida em que repudia a causalidade linear e transforma a noção de tempo, além de afirmar que há "um outro domínio" que não se limita à forma.

---

[29] KASTRUP, Virgínia. **A rede: uma figura empírica da ontologia do presente.** *In:* PARENTE, André (Org). Tramas da rede: novas dimensões filosóficas, estéticas e políticas da comunicação. Porto Alegre: Sulina, 2013. p, 85.
[30] DELEUZE, Gilles e GUATTARI, Félix. **Mil platôs – capitalismo e esquizofrenia, vol. 1**. Rio de Janeiro: Ed. 34, 1995. p, 15 e ss.
[31] KASTRUP, Virgínia. **A rede: uma figura empírica da ontologia do presente.** Op. cit. p, 81.
[32] DELEUZE, Gilles e GUATTARI, Félix. **Mil platôs – capitalismo e esquizofrenia, vol. 1**. Op. cit. p, 20.
[33] KASTRUP, Virgínia. **A rede: uma figura empírica da ontologia do presente.** Op. cit. p, 83.

Toda essa interação entre a *internet* e o ser, ou o(s) ser(es) conectado(s) entre si e na *internet*, modifica fundamentalmente a forma como o indivíduo se enxerga e se relaciona com tudo em sua volta, seja com outros indivíduos ou com máquinas. Em outras palavras, é a *Internet* "a base tecnológica para a forma organizacional da Era da informação"[34], uma possibilidade de interconexão de todos a tudo e vice versa.

Por todas essas modificações substanciais inseridas na dinâmica da vida, é que Schwab[35] afirma que essa dita revolução, não se trata tão somente de uma continuidade da terceira revolução industrial, e sim de uma outra e distinta revolução. É que algumas características lhe são peculiares. Quanto à sua velocidade, Schwab afirma ser contrário às revoluções industriais anteriores, visto que se dá em ritmo exponencial e não linear. Ademais, sua amplitude e profundidade resulta da combinação de várias tecnologias, modificando, ou melhor, criando novos paradigmas até então desconhecidos, tanto no que se refere à economia, quanto aos negócios, à sociedade e aos indivíduos. Além disso, observa-se um impacto sistêmico no qual se percebe a transformação de sistemas inteiros, seja em empresas, indústrias e em toda sociedade[36]. Afinal de contas, como afirma Castells[37], o "paradigma da tecnologia da informação" é que esta não evolui para reduzir-se em uma complexidade de um sistema fechado e finito, mas a caminho de uma abertura como uma rede de acessos múltiplos.

Em "A pele da Cultura", Derrick de Kerckhove[38] relata os obstáculos cuja computação enfrentaria para que fosse possível o advento de uma Realidade dita Virtual (RV). Alguns obstáculos já foram superados pelos desenvolvimentos tecnológicos, o que em passos rápidos se possibilitará, como disse Marshall Mcluhan, iniciar "uma dinâmica pela qual todas as tecnologias anteriores que eram meras extensões das mãos e dos pés e dos dentes, mecanismos de controle do corpo – todas as extensões do nosso corpo tais como as cidades – serão traduzidos em sistemas de informação", ou seja, transformar *hardware* em *software*, sair do poder físico à força do pensamento, na intenção de comandar através do pensamento simulações psicológicas externas[39].

Kerckhove se refere à possibilidade, a partir das novas tecnologias, do indivíduo não apenas interagir com o real, mas ter todos os sentimentos reais, proporcionados pelos

---

[34] CASTELLS, Manuel. **A galáxia da internet.** Op. cit. p, 7.
[35] SCHWAB, Klaus. **A quarta revolução industrial.** São Paulo: Edipro, 2016. p, 13.
[36] SCHWAB, Klaus. **A quarta revolução industrial.** Op. cit. p, 13.
[37] CASTELLS, Manuel. **A Sociedade em rede.** Op. cit. p, 113.
[38] KERCKHOVE, Derrick de. **A pele da cultura: uma investigação sobre a nova realidade electrónica.** Op. cit., p. 72 – 73.
[39] KERCKHOVE, Derrick de. **A pele da cultura: uma investigação sobre a nova realidade electrónica.** Op. cit., p, 74.

sentidos humanos, por aquilo que se mostra virtual. Integrar, como diz o autor, é tato[40], e por meio das tecnologias avançadas, a realidade virtual será sentida, tocada e ouvida através dos sentidos reais.

A virtualização do corpo[41] ou a possibilidade de todos esses dispositivos virtualizarem os sentidos faz com que o indivíduo experimente uma integração dinâmica de diversas modalidades perceptivas. Conforme Levy, por vezes, é como possibilitar reviver – a partir de equipamentos tecnológicos como fotografia, televisão, câmeras e etc. – a experiência sensorial completa de outra pessoa.

Virtualizar os sentidos (ou o corpo) é a capacidade dessas tecnologias de se apropriarem ou possibilitarem a experiência da Virtualidade atrelada a determinado sentido. Levy[42] exemplifica de maneira simples, ao afirmar que uma ferramenta é bem mais que uma extensão do corpo, é uma virtualização da ação, e para isso se utiliza da figura do martelo e da roda. Conforme o autor, "o martelo pode dar a ilusão de um prolongamento do braço; a roda, em troca, evidentemente não é um prolongamento da perna, mas sim a virtualização do andar". Nesta senda é que Deleuze[43] afirma que todo objeto atual se rodeia de uma névoa de imagens virtuais, tão pouco separáveis do objeto atual quanto o próprio objeto atual é separável das imagens virtuais.

Para além do campo da percepção, outra função emergente a partir da virtualização dos corpos é a sua própria projeção. Neste ponto, a virtualização, por se tratar de "desterritorialização", possibilita o indivíduo à ubiquidade. Ao corpo se permite estar aqui ou em qualquer outro lugar ao mesmo tempo.

---

[40] Neste ponto, é preciso esclarecer que a extensão a ser possibilitada ao tato, como sugere o autor, refere-se ao contato corpóreo diante de uma realidade, ainda não alcançada em completude, chamada virtual (RV). Todavia, é importante ressaltar já nesta altura do texto, que as dimensões do tato são diversas, não se reduzindo apenas ao contato corporal. É possível, com o auxílio de Byung-Chul Han, em **No Enxame: reflexões sobre o digital** (2016, p. 33 – 35) perceber que a dimensão do tátil, como forma não verbal de comunicação, não se resume ao contato corporal, mas a uma pluralidade de dimensões e níveis da percepção humana. Neste ponto, discorre o autor que o meio digital elimina da comunicação o seu caráter corporal e táctil, isso porque pelo meio digital o encontro real desaparece, evita-se cada vez mais o contato direto com as pessoas reais, ao ponto da comunicação pelo seu meio digital se torne desprovida de corpo e de rosto. A comunicação digital, continua Byung-Chul Han, é pobre em termos de olhares, pelas câmeras acopladas em qualquer nova tecnologia de comunicação, por mais que permita a aproximação que desafia a distância espacial, jamais irá permitir o contato visual olho no olho, a tela digital não tem olhos, é transparente. Desta forma, por mais que se tente o olhar o outro nos olhos, será impossível pela assimetria do olhar. Sempre ter-se-á a impressão de que o interlocutor "olha ligeiramente para baixo, uma vez que a câmera se encontra instalada na parte de cima do computador (ou de qualquer outra tecnologia que permita chamadas visuais). Ou seja, um interlocutor olha diretamente para a câmera, ao passo que o outro, olha para a tela, jamais olhos nos olhos.

[41] LEVY, Pierre. **O que é virtual?** São Paulo: Ed. 34, 1996. p, 27 – 33.

[42] LEVY, Pierre. **O que é virtual?** Op. cit. p, 75.

[43] DELEUZE, Gilles. **O atual e o virtual**. *In:* ALLIEZ, Éric. **Deleuze filosofia virtual.** São Paulo: Ed; 34, 1996. p, 49 – 50.

Falar em tempo é, antes de tudo, perceber que esse conceito – antes absoluto – sofreu diversas mudanças. Como aduz Gauer[44], com Einstein, e sua teoria da relatividade[45], se introduziu a noção de simultaneidade tendo como reflexo o desaparecimento da noção de tempo absoluto. Notadamente, a relatividade também implicou em alterações na noção de tempo histórico em decorrência de questionamentos acerca do tempo, espaço e outras categorias da ciência moderna.

À medida em que novos meios de interação são proporcionados, novos espaços e tempos surgem. Na explicação de Levy[46], não se poderá mais considerar uma extensão ou cronologia uniforme, senão uma variabilidade de espacialidade e duração que decorre da ligação entre subjetividade, significação e pertinência. Quer-se dizer que a percepção de tempo e espaço varia de acordo com o observador referencial. O "aqui" e "agora" deixam de ser conceitos permanentes e passam também à relatividade.

As mudanças de perspectivas do tempo real identificadas por Virilio[47] se relacionam diretamente com a interação dos fenômenos óticos e da eletrônica. A perspectiva do tempo real deixa de ser geométrica e passa a ser eletrônica, relacionada com a emissão e a recepção instantânea dos sinais de áudio e vídeo. Desta forma, a ausência do horizonte de uma tela diminui a distância entre pessoas e/ou objetos, e por sua vez, a unidade do tempo predomina sobre a do lugar. Dirá Virilio que o ponto de fuga da focalização dos raios luminosos vão cedendo espaço para a fuga de todos os *pixels*.

Ademais, o volume de informações em velocidade instantânea rompe qualquer ponto que sustenta "o passado" como passado, o passado torna-se secundário, uma vez que o dado imediato passa ser o instante e a sua duração também torna-se secundária[48].

Kerckhove traça a diferença entre o humano de massa e o humano de velocidade, em que este rodeado por aceleração constante, jamais pode deixar de acelerar, é tanto receptor como emissor de informações. O homem de velocidade somente o é devido ao acesso instantâneo que têm às coisas e à informação. Já o humano de massa é representado pela figura da passividade, rodeado por redes de difusão, preso no mundo feito pelas indústrias da

---

[44] GAUER, Ruth M. Chittó. **Falar em tempo, viver o tempo!** *In*: GAUER, Ruth (coord.); SILVA, Mozart Linhares da (org). Tempo/História. Porto Alegre: EDIPUCRS, 1998. p, 17 – 18.

[45] HAWKING, Stephen. **O universo numa casca de noz.** 1 ed. Rio de Janeiro: Intrínseca, 2016. p, 116 – 117. "O conceito de tempo absoluto foi derrubado pela teoria da relatividade restrita, segundo a qual o tempo não era mais uma grandeza independente em si mesma, mas apenas uma direção num *continuum* quadridimensional chamado espaço-tempo. Na relatividade restrita, observadores diferentes viajando a velocidades diferentes se deslocam através do espaço-tempo por trajetórias diferentes. Cada observador tem sua própria medição do tempo ao longo da trajetória que está seguindo, e observadores diferentes medirão intervalos de tempo diferentes entre os eventos".

[46] LEVY, Pierre. **O que é virtual?** Op. cit. p, 21 – 22.

[47] VIRILIO, Paul. **O espaço crítico**. Rio de Janeiro: Ed. 34, 1993. p, 101.

[48] GAUER, Ruth. M. Chittó. **Falar o tempo, viver o tempo!** Op. cit. p, 21.

consciência (*mass media*)[49]. São as novas tecnologias que possibilitam ultrapassar o obstáculo criado por essa cultura (tradicional) da apreensão[50]. Isso porque, pela técnica, o homem otimiza sua performance.

A esse pensamento adere Han[51] ao afirmar que a temporalidade do meio digital é o presente imediato. Isso, nas palavras do autor, é permitido pela própria topologia da rede, que transforma os indivíduos receptores e consumidores de informação em um papel de extensão, ou seja, emissores e produtores ativos de informações. Eliminam-se os filtros, liquidam as mediações das comunicações. Essa é a principal diferença entre os *media* digitais dos *media* de massa.

É essa mesma velocidade e aceleração que transforma o cotidiano em um eterno culto ao tempo presente. Lipovetsky[52] denomina este fenômeno como o "presentismo" de segunda geração[53], que a partir dos anos 80, com a revolução informática e a globalização neoliberal comprimiu-se o espaço-tempo e se ressaltou a lógica da brevidade.

Assevera o autor que a mídia eletrônica e informática ao passo que possibilita a troca incessante de informações em "tempo real", acaba por contribuir para a culminância de uma sensação de imediatismo, ou ainda, desperta o desejo pelo imediato e desvaloriza toda forma que contemple o transcorrer necessário do tempo, a essa altura, considerado lento.

A análise referente à transformação do tempo através da cultura da "virtualidade real" em nossa sociedade faz com que Castells identifique duas formas singulares que essa transformação se apresenta: simultânea e intemporal[54].

A informação, temporalmente instantânea, está em todo o globo. É possível acompanhar as notícias mais atuais sobre qualquer acontecimento global sem necessariamente presenciá-lo. Nas palavras do autor, com o avanço da era da comunicação, tornou-se possível "fazer" história, (simultaneamente) testemunhando a própria história. Na prática, o tempo real para as novas tecnologias é um tempo sem relação com o "tempo histórico". Antes, todo acontecimento histórico e todo o curso da própria história tinha um "tempo local", como afirma

---

[49] KERCKOVE, Derrick de. **A pele da cultura.** Op. cit. p, 186.
[50] LYOTARD, Jean François. **O inumano.** Op. cit. p, 70.
[51] HAN, Byung-Chul. **No Enxame: reflexões sobre o digital.** Lisboa: RelógioD'Água, 2016. p, 27 – 30.
[52] LIPOVETSKY, Gilles. **Os tempos hipermodernos.** São Paulo: Editora Barcarolla, 2004. p, 62.
[53] A consagração do presente surge a partir da revolução do cotidiano. Segundo Lipovetsky este novo arranjo do tempo social possui em seu cerne a passagem do capitalismo de produção para uma economia de consumo e de comunicação de massa e a substituição de uma "sociedade rigorística-disciplinar" por uma "sociedade-moda" (re)estrututrada pelas técnicas do efêmero, da renovação e da sedução permanente. Essa cultuação ao presente, segundo o autor, precedeu em décadas a queda do Muro de Berlim, o universo do ciberespaço e o liberalismo globalizado, nas palavras de Lipovetsky "iniciou muito antes que se houvessem enfraquecido as razçoes para ter esperança num futuro melhor". (Id. p, 55 – 60).
[54] CASTELLS, Manuel. **A Sociedade em rede.** Op. cit. p, 553.

Virilio[55], ou melhor, um lugar no tempo local (na América, França, Itália), todavia, a capacidade de interação e de interatividade instantânea possibilitam colocar a história em tempo único, um tempo universal.

São reflexos do não distanciamento entre o receptor e a fonte de emissão que se cria em tempo real, de acordo com Baudrillard[56], a "indemonstrabilidade", a virtualidade do acontecimento que retira deste a sua dimensão histórica e o subtrai a memória.

Quanto a *intemporalidade* da informação, refere-se à possibilidade de acesso ao seu conteúdo sem necessariamente identificar o contexto específico em que foi produzido. A *intemporalidade* cria uma colagem temporal disponível ao "espectador/interagente" sem sequência lógica/histórica definida. Como Gauer sugere, essa *intemporalidade* diferencia-se diametralmente da periodização da história, tão evidenciada na modernidade, na qual se ratifica a contagem do tempo a partir de um ponto inicial. A ilusão do início e do fim causou o desencontro do tempo e do homem, o tempo que atualmente não é mais "a promessa do devir", e nas palavras da autora, somente a velocidade do presente-vivo é que baliza o encontro deste tempo[57].

Castells salienta que a ordem dos eventos significativos perde o seu ritmo cronológico estando apenas condicionada ao interesse momentâneo que será utilizada. Por esse motivo, denomina este fenômeno de *cultura do eterno e do efêmero*[58]. Primeiro por permitir o alcance de toda sequência entre passado e futuro das expressões culturais. Segundo, pois cada sequência histórica específica depende do contexto e do objetivo da construção cultural solicitada. A *intemporalidade* do tempo "ocorre quando as características de um dado contexto, ou seja, o paradigma informacional e a sociedade em rede, causam confusão sistêmica na ordem sequencial dos fenômenos sucedidos naquele contexto", sendo que esta confusão pode tanto desvelar uma compreensão de fenômenos visando a instantaneidade ou a introdução de descontinuidade aleatória da sequência[59].

Esse alcance instantâneo provoca uma vertigem temporal como explica Virilio[60]. A partir da inovação da ótica ondulatória da radiação eletromagnética das partículas que veiculam

---

[55] VIRILIO, Paul. ***El cibermundo, la política de lo peor*.** Entrevista con Philippe Petit. *Traducion* Mónica Poole. Teorema, Madrid: Ediciones Catedra S.A, 1997. p, 15.
[56] BAUDRILLARD, Jean. **Tela total: mito-ironias do virtual e da imagem.** 4 ed. Porto Alegre: Editora Sulinas. 2005. p, 129.
[57] GAUER, Ruth M. Chittó. **Falar o tempo, viver o tempo!** Op. cit. p, 30.
[58] CASTELLS, Manuel. **A Sociedade em rede.** Op. cit. p, 554.
[59] Castells se utiliza do conceito de tempo proposto por Leibniz para prosseguir com seu raciocínio, em que o tempo é a ordem de sucessão das coisas, de forma que sem as coisas não existiria tempo. CASTELLS, Manuel. **A Sociedade em rede.** Op. cit. p, 556.
[60] VIRILIO, Paul. **O espaço crítico.** Op. cit. p, 102 – 114.

a visão e audição, surge um outro tipo de transparência que se soma à transparência natural da atmosfera terrestre. Denominada de transparência das aparências, ou trans-aparência.

Esta nova transparência completa a transparência direta do espaço à medida em que como transparência indireta do tempo da velocidade das ondas eletromagnéticas, transmitem nossas imagens e vozes. A iluminação para esta "nova" transparência é uma iluminação indireta, não decorrente de um astro solar, mas uma luz de tecnologia que desdobra a personalidade do tempo real.

Por sua vez, é a velocidade das ondas eletromagnéticas que faz com que haja um esquecimento da exterioridade espacial do mundo e também da exterioridade temporal (*now-future*) beneficiando o único instante do "presente" da realidade proporcionada pela telecomunicação instantânea. Nesta senda, toda a superfície de dimensões variadas somente terá existência objetiva através (na e pela) interface de uma observação indireta, ou seja, possibilitada não pela iluminação direta do Sol, mas sim pelo campo rádio-elétrico ou de fibra ótica[61].

O desenvolvimento de tecnologias de informação e comunicação produzem uma imperceptível "contração" espacial do mundo. Nesta atual conjuntura, para o "*voyeur*-viajante" ultra rápido - como dirá Virilio[62] - a perspectiva da aceleração ou vertigem do tempo real é causada pela inércia. Essa velocidade transforma o meio eletrônico naquilo que ele denomina de último vácuo, ou seja, um vácuo que não existe a partir da dependência do intervalo entre lugares ou coisas, mas sim por meio da interface de uma transmissão instantânea.

Quanto ao referido “esquecimento da exterioridade espacial”, da mesma forma Weissberg[63] ao trazer à baila a temática sobre a “presença à distância”, lembra que a transmissão da presença opera por meio do suporte semiótico avançado e que a transmissão dos sinais da presença equivale à duplicação da presença, negando por isso mesmo a operação de transporte. Tal fato, sugere que a localização geográfica, a territorialização, tenderia a se tornar arcaica em virtude da crescente eficácia das teletecnologias. Logo, um dos primeiros efeitos percebidos – segundo o autor – foi o crescimento deduzido do transporte da presença que se traduziu em uma desterritorialização, ou até como uma negação do território.

Entretanto, o contraponto destacado por Weissberg[64] é de que por uma observação mais flexível surge a hipótese de que a importância da localização, de modo algum, se diluiu.

---

[61] VIRILIO, Paul. **A inércia polar.** Tradução de Ana Luísa Faria. Lisboa: Publicações Dom Quixote, 1993. p, 17.
[62] VIRILIO, Paul. **O espaço crítico.** Op. cit. p, 102 – 114.
[63] WEISSBERG, Jean-Louis. **Paradoxos da teleinformática.** Op. cit. p, 114 – 115.
[64] WEISSBERG, Jean-Louis. **Paradoxos da teleinformática.** Op. cit. p, 115.

Ao contrário, as redes aumentaram-na. Destaca que as comunidades territorialmente próximas tiveram seus vínculos afetados pela internet, na medida em que encontraram na rede um meio de reforçar seus laços, de aumentar a intensidade e a frequência de seus encontros reais. Salienta o autor que "através de uma localização no espaço informacional, reforça-se, pois, frequentemente, e paradoxalmente, a importância da localização geográfica.

Tal hipótese é evidenciada de modo a se perceber o incremento de sistemas de informações geográficas. Segundo Weissberg, "estes sistemas, atrelados à captadores de tráfego, ou a dispositivos de localização de veículos por satélites geoestacionais (G.P.S) permitem organizar e visualizar a evolução temporal de uma situação"[65]. São informações "geoestratégicas". Conclui, portanto, que o território foi (re)colonizado pelo universo informacional, tendo como principal sintoma disto o crescimento dos sistemas de informação geográfica como indício de uma força que compele para a espacialização da informação. Toda informação a partir disto com ligação territorial, e consequentemente um manifesto poder de tratamento informático.

As tecnologias móveis seriam assim consubstanciadas de "ubiquidade" e "onipresença". A primeira no sentido de compartilhamento simultâneo de vários lugares, em uma continuidade temporal desde o vínculo comunicacional até uma plurilocalização instantânea. A segunda, ainda conforme Weissberg[66], por permitir o indivíduo se libertar da localização única, multiplicando as localizações possíveis.

A constatação de que é possível alcançar alguém em todo lugar e em qualquer momento, traça o paradoxo destacado pelo autor, de que embora se pense que haja apenas um esquecimento ou abandono do território, há em verdade uma ligação com este.

Os paradoxos destacados são reflexos do próprio sistema aberto, rizomático, que é a *internet*. Os seus efeitos não são excludentes, mas paradoxalmente abrangentes, ao mesmo tempo em que possibilita a presença (proximidade), possibilita a ausência (afastamento), ou a presença pela distância, a tele-presença, a ubiquidade e a onipresença.

---

[65] WEISSBERG, Jean-Louis. **Paradoxos da teleinformática.** Op. cit. p, 118.
[66] WEISSBERG, Jean-Louis. **Paradoxos da teleinformática.** Op. cit. p, 121.

2.2 Acesso e tratamento de dados: Vigilância e(m) tempo securitário, outro possível traumatismo do nascimento

Antes de avançar sobre o tema é preciso revisitar alguns ensinamentos de Foucault para a construção da ideia central deste tópico que é a vigilância em tempos securitários. Portanto, fundamental é uma breve síntese daquilo que o autor vai denominar de biopoder.

O direito de vida e morte, antes absoluto nas mãos do soberano, tornou-se condicionado às hipóteses de ameaça à sua soberania, seja para a defesa do Estado – impondo a seus súditos que tomem parte de sua defesa –, seja para a sua sobrevivência – quando um de seus súditos se levanta contra o Estado e infringe suas leis[67].

Tendo condições de exigir, portanto, seu direito de matar, dirá Foucault que o direito formulado como "de vida e morte" se perpassa ao direito de causar a morte ou de deixar viver. Nestes termos, o poder era exercido a partir do privilégio sobretudo de apreensão das coisas, do tempo, dos corpos e da vida.

Paulatinamente, outras formas de exercício deste direito de morte, além da apreensão ou confisco, surgem e se expandem para o controle, a vigilância e para a organização de forças, ao passo que o direito "se apoiará nas exigências de um poder que gere a vida, que a proteja, a mantenha e a desenvolva[68]. O poder de morte, portanto, se apresentará – nas palavras de Foucault – "como complemento de um poder que se exerce positivamente, sobre a vida, que empreende sua gestão, sua majoração, sua multiplicação, o exercício, sobre ela, de controles precisos e regulações de conjunto".

Mata-se ou causa-se a morte para manter as populações vivas. Nesta altura, uma aparente contradição perante o direito de morte surge. O poder que faz gerir a vida e multiplica-la, acaba por determinar a morte. Entretanto, é nesse ponto que Foucault se atenta para destacar que, o exercício do direito de morte – para não se mostrar contraditório – irá invocar e se utilizar da monstruosidade daquele que morre.

Ou seja, aqueles que são mortos, os são legitimamente, na substituição do direito de "causar a morte ou deixar viver" pelo poder de "causar a vida ou devolver à morte"[69]. O poder, nessa trajetória de passar a ser cada vez menos o "direito de fazer morrer" para se tornar cada vez mais "o direito de intervir para fazer viver", interfere diretamente na própria maneira

---

[67] FOUCAULT, Michel. **História da sexualidade I: A vontade do saber.** 4ª ed. Rio de Janeiro/São Paulo: Paz e Terra, 2017. p, 145.
[68] FOUCAULT, Michel. **História da sexualidade I: A vontade do saber.** Op. cit. p, 147.
[69] FOUCAULT, Michel. **História da sexualidade I: A vontade do saber.** Op. cit. p, 148.

de viver, ou nas palavras de Foucault, no "como" da vida: "aumentar a vida, controlar seus acidentes, suas eventualidades, suas deficiências, daí por diante"[70].

O poder sobre a vida se desenvolve a partir do Séc. XVII pela forma do controle ou adestramento do corpo. Ademais, surge a preocupação pelas políticas de saúde e natalidade, a partir do Séc. XVIII. É a era daquilo que Foucault vai denominar de biopoder.

O biopoder, na definição de Hardt e Negri[71], seria então a forma pela qual o poder rege e regulamenta a vida social no seu interior, seguindo-a, interpretando-a, assimilando-a e reformulando-a. Inevitavelmente, para a perpetuação da biopolítica se faz necessário o deslocamento (não a substituição) de uma sociedade disciplinar para uma sociedade do controle. Logo, pretendendo-se domínio efetivo, o biopoder tornar-se-á função integrante que todo indivíduo adota e reativa por espontânea vontade[72].

O corpo é disciplinado, vigiado e isolado nesta Sociedade disciplinar e a arquitetura Benthaniana do panóptico, ao mesmo tempo em que permite maior transparência ao vigia, induz seu habitante a um estado de consciente e permanente visibilidade. Para além, não basta ter a possibilidade de vigiar o habitante, mas mais eficiente e essencial, nesta estrutura, é mantê-lo em constante consciência desta vigília. Nas palavras de Foucault, uma sujeição real nasce mecanicamente de uma relação fictícia, que assegura ao funcionamento automático de poder, a partir da permanente visibilidade. O poder não tem necessidade de ser exercitado efetivamente, não sendo necessário o recurso da força para obrigar comportamentos desejados[73].

Nada obstante, na Sociedade da informação, o panóptico digital, sem margem para dúvidas, simboliza o fator da eficiência por excelência. "Aperspectivístico", na observação de Han[74], totalmente desprovido de ótica perspectivística, se difere daquele proposto por Bentham e, assim, o faz desaparecer. Já não se configura pela supervisão onipotente de um olhar central. Entretanto, se possibilita iluminar e se tornar transparente por qualquer um, todos os que possam vir a ser alvos.

O isolamento utilizado nas instituições pertencentes às Sociedades disciplinares não é, neste contexto, empregado. Os habitantes do panóptico digital não são observados por meio de um vigia, todos se imaginam inteiramente livres[75], ligados em uma rede com intensa

---

[70] FOUCAULT, Michel. **Em defesa da sociedade: curso no Collège de France (1975-1976).** São Paulo: Martins Pontes, 1999. p, 295.
[71] HARDT, Michael e NEGRI, Antonio. **A produção biopolítica.** *In:* PARENTE, André (Org). **Tramas da rede: novas dimensões filosóficas, estéticas e políticas da comunicação.** Porto Alegre: Sulinas, 2013. p, 162.
[72] HARDT, Michael e NEGRI, Antonio. **A produção biopolítica.** Op. cit. p, 162.
[73] FOUCAULT, Michel. **Vigiar e punir: nascimento da prisão.** Petrópolis: Vozes, 1987. p, 166.
[74] HAN, Byung-Chul. **A sociedade da transparência.** Petrópolis, RJ: Vozes, 2017. p, 106.
[75] HAN, Byung-Chul. **A sociedade da transparência.** Op. cit. p. 108.

comunicabilidade entre si. Esse último aspecto aparente é que garante a transparência e, consequente, controle: a hipercomunicação.

Espectadores e emissores ativos se expõem e assim, alimentam e mantem a rede panóptica. Não há uma coação para tal comportamento, ao contrário, a desnudação é espontânea. Uma necessidade gerada por si. Todos tem acesso a todos, em constante exposição[76].

Enfoque este descrito por Foucault quando trata de dispositivos de segurança. Como destaca Amaral[77], a disciplina funciona no isolamento do espaço, circunscreve o local vigiado para que o poder atue plenamente, mas os dispositivos securitários são tendencialmente expansivos. A segurança é o princípio de cálculo do liberalismo na fabricação da liberdade. Esta, como salienta Amaral, não sendo a liberdade que se opõe ao exercício de poder, ou contraria aos abusos de governo, mas sim uma liberdade que se converte em elemento indispensável e inafastável às políticas correlatas aos dispositivos de segurança[78].

Aliás, tais dispositivos são caracterizados por serem em um primeiro momento, aqueles que inserem um fenômeno[79] numa série de acontecimentos prováveis. Em seguida, por identificarem os custos necessários para as reações de poder frente ao fenômeno, para então, em um terceiro momento, estabelecer medidas impostas nos limites do aceitável[80].

Neste contexto de segurança, evidente que serão utilizados também mecanismos disciplinares. Afinal de contas, a vigilância serve à segurança, em que pese haja diferenças entre mecanismos de segurança e dispositivos disciplinares[81].

---

[76] Neste mesmo sentido, Byung-Chul Han afirma ser pornográfica esta sociedade da transparência pela imposição do afastamento do oculto e pela coação em expor tudo à comunicação e à visibilidade. "Para a sociedade da transparência de hoje a exposição pornográfica e o controle panóptico se interpenetram e complementam. O exibicionismo e o voyeurismo alimentam a rede de comunicação como um panóptico eletrônico". HAN, Byung-Chul. **Topologia da violência.** Petrópolis, Rio de Janeiro: Vozes, 2017. p, 210 – 211.

[77] AMARAL, Augusto Jobim do. **Governamentalidade em tempos securitários.** *In:* ROSA, Alexandre Morais da; AMARAL, Augusto Jobim do. **Cultura da punição: a ostentação do horror.** 2ª ed. Florianópolis: Empório do Direito, 2015. p, 35.

[78] AMARAL, Augusto Jobim do. **Governamentalidade em tempos securitários.** Op. cit. p, 36.

[79] Fenômeno para Foucault como aquilo que se quer evitar.

[80] FOUCAULT, Michel. **Segurança, território e população: curso dado no Collége de France (1977-1978).** São Paulo: Martins Fontes, 2008. p, 9.

[81] Michel Foucault vai estabelecer diferenças iniciais acerca dos dispositivos disciplinares e mecanismos de segurança, identificando nesta toada que a disciplina é essencialmente centrípeta, na medida em que isola um espaço, determina seu enfoque ou um seguimento. "A disciplina concentra, centra, encerra. O primeiro gesto da disciplina é, de fato, circunscrever um espaço no qual seu poder e os mecanismos do seu poder funcionarão plenamente e sem limites". Enquanto que os mecanismos de segurança são antagônicos, pois tedem perpetuamente a ampliar, serão portanto centrífugos. Uma segunda diferença entre os dois é que a disciplina, por excelência, pretende regular ou melhor, regulamenta tudo. A menor infração ao método disciplinar deve ser corrigida com o máximo de rigor e cuidado possível. Todavia, em se tratando de mecanismos de segurança, não há rigor excessivo para o proibir o fazer, este cede lugar ao "deixar fazer", um nível de liberdade indispensável é assegurado. Uma terceira diferença destacada por Foucault é a divisão feita pelos dispositivos de disciplina na construção ou – melhor – estabelecimento de atos permitidos e proibidos e "no interior destes dois campos vão especificar,

Dirá Foucault[82] que o *corpus* disciplinar é ativado por mecanismos de segurança, afinal "técnicas de vigilância, vigilância dos indivíduos", ou qualquer técnica que faça parte do conjunto disciplinar se produz sob mecanismos de segurança, e como tais, consideram acontecimentos como fenômenos naturais sem atribuir a estes juízos valorativos entre bom e mal. O funcionamento dos dispositivos de segurança voltam-se a evitar que estes fenômenos ocorram, conectam-se à própria realidade para gradativamente compensar, frear, limitar e em último grau, anular o fenômeno.

Ainda sob a análise foucaultiana, este fenômeno sofrerá uma divisão fundamental em dois níveis, um em relação à ação econômica-política do governo – este nível voltado à população –, outro em relação à multiplicidade de indivíduos[83]. Nesta perspectiva, é a população que se apresenta como objetivo final, sendo a multiplicidade dos indivíduos um instrumento para obter algo no nível da ação econômica de indivíduos.

Ou seja, a população vai se apresentar sob dois aspectos, como objeto e como sujeito. O primeiro aspecto sob o qual se identifica a população como aquilo a que se dirigem os mecanismos de segurança para obter certos efeitos desejados. Todavia, o segundo aspecto, identifica a população sendo a titular do comportamento desejado específico. "Comportamentos que fazem que cada um dos indivíduos funcione como membro, como elemento dessa coisa que se quer administrar da melhor maneira possível, a saber, a população".

Em outras palavras, voltando-se ao tema central, o habitante se expõe e se permite vigiar. Logo, cada indivíduo como membro, se expõe e vigia outro, ininterruptamente para melhor administrar a população. Os elementos da realidade atuarão uns em relação aos outros, como uma técnica política, ligada profundamente ao princípio geral do liberalismo[84]. Esta liberdade que segundo Foucault é ao "mesmo tempo ideológica e técnica de governo, deve ser compreendida no interior das mutações e transformações das tecnologias de poder, ou seja, de

---

determinar exatamente o que é proibido, o que é permitido, ou melhor, o que é obrigatório. [...] uma boa disciplina é o que lhes diz a cada instante o que vocês devem fazer". Conclui, Foucault que em contrapartida o mecanismo de segurança se apresentará de modo a não adotar nem determinações impeditivas e muito menos obrigatórias, mas sim "distanciar-se suficientemente para poder apreender o ponto em que as coisas vão se produzir, sejam elas desejáveis ou não". FOUCAULT, Michel. **Segurança, território e população: curso dado no Collége de France (1977-1978).** Op. cit. p, 58 – 64.

[82] FOUCAULT, Michel. **Segurança, território e população: curso dado no Collége de France (1977-1978).** Op. cit. p, 11 – 50.

[83] Este segundo nível, dirá Foucault, só terá pertinência à medida em que possibilita o que se pretende obter no primeiro nível (este sim, de fato pertinente), consequentemente após ser administrado, mantido e incentivado devidamente. FOUCAULT, Michel. **Segurança, território e população: curso dado no Collége de France (1977-1978).** Op. cit. p, 55.

[84] Liberalismo como esclarece Foucault, na medida em que deixa as pessoas fazerem, as coisas passarem, de maneira que a realidade se desenvolva por seus princípios. FOUCAULT, Michel. **Segurança, território e população: curso dado no Collége de France (1977-1978).** Op. cit. p, 62 – 64.

maneira mais precisa e particular, a liberdade nada mais é que o correlativo da implantação dos dispositivos de segurança". Os dispositivos securitários, que somente funcionam em perfeito estado quando lhe é dado a liberdade, transformam as pessoas em escravas de sua própria liberdade. Esta, como possibilidade de deslocamento, de movimento, como processo de circulação.

Deste modo, não há que se falar em uma autêntica sociedade livre. Nem mesmo quando o Estado tem sua essência calcada em ditames democráticos e liberais. Na visão de Whitaker[85], nenhum governo tem se furtado à utilização de dispositivos de vigilância e controle, portanto, constitui-se de elementos autoritários e antiliberais a serviço da (in)segurança nacional. Os governos se utilizam de recursos de inteligência para estabelecer uma vigilância político-policial nacional. A política de segurança se concentra mais nos riscos a serem identificados e evitados, que em atos criminosos efetivamente.

Toda a lógica de governamentalidade – nesta órbita – se escolta no binômio liberdade e segurança. O governo por sua vez é o gestor dos perigos e tais implicações se pautam fundamentalmente no estímulo liberal do "viver perigosamente", o que em consequência elege os cálculos dos riscos no centro das preocupações[86].

A sociedade do controle funciona por um controle contínuo e comunicação instantânea, cuja máquina a operar são as cibernéticas e os computadores[87]. São máquinas que Deleuze denomina de máquinas de terceira espécie, cujo perigo é a interferência, o ativo, a pirataria e a introdução de vírus.

Deleuze atenta-se à passagem da sociedade disciplinar para o controle[88], tendo como principal e notável mudança a passagem da utilização de moedas marcadas em ouro, com padrões, para o controle de transações flutuantes. Passa-se da assinatura e do número de identificação – presentes nas sociedades disciplinares – para uma senha (ou cifra) que marca o acesso à informação, ou sua rejeição.

Neste último ponto, afirma o autor que não é demais imaginar (ou constatar) os novos mecanismos de controle que surgem a cada instante, cuja função é o fluxo de informações

---

[85] WHITAKER, Reg. ***El fin de la privacidad.*** Buenos Aires: Paidós, 1999. p, 32 – 44. "*Por más repulsivo que sea el rostro de la represión totalitaria, no deberíamos ser ciegos a ciertas prácticas similares en las democracias liberales occidentales – ellas mismas Estados de inseguridad – aunque no hayan alcanzado nunca algo parecido a lo ocurrido en las pesadillas del Estado policial nazi o comunista*".

[86] AMARAL, Augusto Jobim. **Governamentalidade em tempos securitários.** Op. cit. p, 37.

[87] DELEUZE, Gilles. **Conversações, 1972 - 1990.** São Paulo: Ed. 34, 1992. p, 216 – 225.

[88] DELEUZE, Gilles. **Conversações, 1972 - 1990.** Op. cit. p, 222. "A velha toupeira monetária é o animal dos meios de confinamento, mas a serpente o é das sociedades de controle. Passamos de um animal a outro, da toupeira à serpente, no regime em que vivemos, mas também na nossa maneira de viver e nas relações com outrem".

de cada indivíduo para bancos de dados (a exemplo a posição de um elemento em espaço aberto, animal numa reserva, homem numa empresa).

Ademais, é lícito ressaltar que as tecnologias de controle da *rede* são compostas por tecnologias de identificação, vigilância e de investigação. Pela definição de Castells[89], as tecnologias de identificação (senhas, *cookies* e procedimentos de autenticação) são aquelas que registram e identificam todos os movimentos *on-line*, desde a verificação da origem e característica do usuário por meio de assinaturas digitais, até a autenticidade gerada por servidores que identificam o usuário. Possibilita-se por meio dessas tecnologias a elaboração de protocolos de segurança na *Internet*.

Tecnologias de vigilância são diferentes, embora muitas vezes se baseiam em identificação para localizar o usuário individual. Interceptam mensagens, instalam marcadores que permitem o rastreamento de fluxos de comunicação, monitoram a atividade de máquinas initerruptamente. Castells destaca que a partir de tais tecnologias é possível, pelo uso de persuasão ou coerção, obter a identidade do réu potencial pelo provedor de serviços da internet[90].

Com as novas tecnologias de vigilância, "a noite passa a ter mil olhos"[91]. Tal afirmação tem como ponto de partida e sustentação, a facilidade direta no acesso a tecnologias de vídeo. Um olho eletrônico que trouxe consigo duas inovações. A primeira, segundo Whitaker[92], quantitativa na medida em que o alcance destes olhos eletrônicos é mais penetrante e onipresente. A segunda, de caráter qualitativo, refere-se ao fato de que a tecnologia de reconhecimento facial e consequente digitalização da informação conectadas a uma base de dados, oferece um deslocamento dos propósitos de segurança, para a implementação de uma tecnologia de identificação e localização de indivíduos.

Os indivíduos são localizáveis por seus dispositivos digitais, são observados e vigiados por todas os olhos eletrônicos espalhados pelo globo – câmeras públicas ou privadas

---

[89] CASTELLS, Manuel. **A galáxia da internet: reflexões sobre a internet, os negócios e a sociedade.** Op. cit. p, 141.
[90] CASTELLS, Manuel. **A galáxia da internet: reflexões sobre a internet, os negócios e a sociedade.** Op. cit. p, 142.
[91] WHITAKER, Reg. ***El fin de la privacidad*.** Op. cit. p, 101.
[92] WHITAKER, Reg. ***El fin de la privacidad*.** Op. cit. p, 103. "*Pero la tecnologia de la vigilancia videográfica está en un proceso de innovaciones que aumentan sus hasta ahora limitadas consecuencias. El primer tipo de innovaciones es cuantitativo:el alcance de estos ojos eletrónicos es mucho más penetrante y omnipresente. El segundo es cualitativo: la tecnología del reconocimiento facil y la digitalización de la información, conectada a una base de datos central, ofrecen la perspectiva de un desplazamiento: desde los propósitos defensivos o de seguridad pasiva, en los que se ha empleado básicamente hasta ahora tal tecnología, hasta una nueva era de identificación activa y de localización de indivíduos*".

– e também escutados por ouvidos eletrônicos. Os avanços das tecnologias de áudio também são constatados e as informações produzidas também passam pelo processo de digitalização.

Por sua vez, seguindo o ensinamento de Castells[93], tecnologias de investigação se referem à construção de bancos de dados provenientes das atividades de vigilância e do armazenamento de informações. Dados coletados são informações utilizáveis, combináveis e processáveis de acordo com o objetivo e o poder legal.

Paulatinamente os ambientes de confinamento característicos das sociedades disciplinares vão cedendo lugar aos espaços de livre fluxo ou deslocamento, cuja limitação não mais se dá por grades ou barreiras, mas pelo controle através de permissões ou rejeições de acesso, cuja evolução alcançou novos limites aos quais não se tem delimitação superficial, mas provavelmente interfacial. As grandes distâncias de tempo não são mais problemas frente às *interfachadas* dos monitores ou telas de controle[94].

A superexposição determina as demarcações conceituais do que seria "próximo" ou "distante". Na sociedade da exposição[95] há uma coação pela exposição sob o pretexto da visibilidade, o ser visto adquire valor. Não o mesmo sabor de ser visto, mas um valor próprio, de uso ou de troca, como essência unicamente de chamar a atenção para si.

Consequentemente, exposição pela e para a própria exposição é neste sentido, exploração. Segundo Han[96], o imperativo da transparência faz tudo ter o dever de se tornar visível e coloca sob suspeita tudo o que não se submete à visibilidade.

A transparência é violenta, uma coação levada a cabo pelo excesso de positividade da hipercomunicação, hiperinformação e hipervisibilidade. Coação tal incompatível com a natureza humana, pois transforma o humano – através da violência da transparência – em elemento funcional de determinado sistema. Ser humano é por excelência ter na sua constituição certa medida de inacessibilidade e impermeabilidade que naturalmente é eliminada pela hipervisibilidade[97]. A luz em excesso, segundo Han, não ilumina, mas elimina. Faz desaparecer totalmente a alteridade, a essência individual, e brotar – pela transparência – a condenação pela

---

[93] CASTELLS, Manuel. **A galáxia da internet: reflexões sobre a internet, os negócios e a sociedade.** Op. cit. p, 142.
[94] VIRILIO, Paul. **O espaço crítico.** Op. cit. p, 9.
[95] HAN, Byung-Chul. **Sociedade da transparência.** Op. cit. p, 28 – 31. Byung-Chul Han sintetiza esta reflexão ao afirmar nesta sociedade da exposição, cada sujeito é seu objeto-propaganda, tudo se mensura em seu valor expositivo. Exposição pela produtividade. A hipervisibilidade serve ao capital, mas não se pode deixar de perceber que a mesma hipervisibilidade serve à própria segurança, ou aos dispositivos de segurança em uma sociedade de controle.
[96] HAN, Byung-Chul. **Sociedade da transparência.** Op. cit. p, p, 35.
[97] HAN, Byung-Chul. **Topologia da violência.** Petrópolis: Rio de Janeiro, Vozes, 2017. p, 201 – 212.

luz do igual, a mediocridade da eliminação de si. É uma luz que nivela diferentes, a eliminação da alteridade impõe a *ditadura do igual*[98].

O advento das tecnologias de informação e comunicação, e das máquinas da informática, traz consigo riscos. Não se pode ignorar que o alto grau de exposição presente na sociedade de informação (que se permite e se impõe) demonstram seu traumatismo intrínseco.

Como explica Virilio[99], toda nova invenção tem em seu nascimento uma demonstração, o traumatismo do nascimento é um acontecimento voluntário, um acidente original. Não atinge tão somente o sujeito, a criança, mas também igualmente o objeto, o instrumento que é criado. Não que esteja intrinsicamente relacionado a uma catástrofe ou um traumatismo tradicionalmente conhecido, mas quanto ao risco à liberdade digital, observa-se por Beck[100], que a catástrofe real seria o controle hegemônico invisível numa escala global.

Dirá Virilio[101] que não se pensou em criar o naufrágio quando da criação do navio, muito menos a invenção do acidente ferroviário, quando da criação do trem. A face oculta das invenções representam os "traumatismos do nascimento" que se impõem contra a nossa vontade, logo fica a cargo de nós, tentar descobrir qual o acidente original desta nova invenção, que em comento se trata das novas tecnologias de informação, comunicação (e porque não dizer vigilância, segurança e investigação).

Toda informação é digitalizável e neste formato disponibilizado ou armazenado em grandes bases de dados. Para Whitaker[102] a digitalização é uma espécie de alquimia que se sustenta na chave de uma linguagem universal – códigos binários – e permite a transformação de objetos físicos em comunicação por meio de *bits* de informação.

Pela magnitude da invenção e ao se levar em conta a amplitude de seu alcance, não se descarta o surgimento de diversos acidentes originais. A vigilância incansável das pessoas e a modulação de suas mentes (a essa altura alcançáveis) podem ser apenas mais um.

---

[98] HAN, Byung-Chul. **Topologia da violência.** Op. cit. p, 201 – 212. Nesse mesmo sentido dirá Paul Virilio que as novas tecnologias da informação são tecnologias que reduzem a humanidade a uma uniformidade (VIRILIO, Paul. ***El cibermundo, la politica de lo peor*.** Op. cit. p, 14).

[99] VIRILIO, Paul. **O espaço crítico.** Op. cit. p, 105.

[100] BECK, Ulrich. **A metamorfose do mundo: novos conceitos para uma nova realidade.** 1ª ed. Rio de Janeiro: Zahar, 2018. p, 185 – 187. Beck afirma que o risco digital pertence a uma categoria de ameaça invisível, pois não é sentido por quem é ameaçado, não se assemelha a uma inundação, a uma catástrofe nuclear, a perdas financeiras, mas sim à perda de principais conquistas da civilização moderna que são a liberdade e autonomia pessoais, privacidade e as instituições básicas da democracia, do direito, todas baseadas no Estado-nação. Não é uma ameaça sentida, pois quanto mais próximo está a catástrofe, menos visível ela se apresenta, quanto mais completo e total é o controle global da informação, mais ele desaparece da consciência das pessoas.

[101] VIRILIO, Paul. **O espaço crítico.** Op. cit. p, 105.

[102] WHITAKER, Reg. ***El fin de la privacidade.*** Op. cit. p, 69.

Um dos efeitos perversos da conexão digital – diretamente ligado à facilidade de acesso a informação – é fazer se perder a confiança como valor social[103]. A possibilidade da aquisição de informações lesa gravemente a construção da confiança que se constrói a partir do oculto, neste ponto a confiança cede lugar ao controle. Assim a sociedade da transparência se estrutura no alicerce da sociedade da vigilância. Todas as atividades são registradas, de modo que a *internet* se ocupa em reproduzir de maneira exata a vida em formato digital. Trata-se da protocolização geral da vida[104].

Mais além disso, os dados disponibilizados em rede ou em dispositivos físicos digitais – direta e indiretamente – são a fragmentação da personalidade do usuário, o que permite dizer que a completude desses dados é o reflexo da própria personalidade. O acesso à completude dos dados é por via reflexa e indireta acesso à mente do ser.

Segundo Rodotá[105], por mais perigoso que possa parecer, "somos nossos dados". A representação social do indivíduo se firma nas mais diversas informações armazenadas em bancos de dados. Neste sentido é que a partir das novas tecnologias de comunicação e informação, a dimensão trazida pelo virtual, somada ao real, permite uma mudança acerca da concepção sobre "a pessoa" e o seu "corpo".

Uma "entidade desencarnada"[106] se forma e por isso a máxima necessidade de se proteger o "corpo eletrônico". Esclarece Rodotá[107] que as informações que constituem o indivíduo e sua identidade são tratadas eletronicamente em dimensões mundiais por bancos de dados que tem a capacidade de localizar todos os rastros ou registros deixados na rede, nesta conjuntura condiciona a existência do indivíduo a algo muito além do mero corpo físico. Um indivíduo planetário, a distribuição dos "corpos" pelo globo por meio dos dados.

Han[108] atenta para a substituição – a essa altura – do biopoder por aquilo que irá chamar de *psicopoder*[109]. A limitação do biopoder se dá na barreira que encontra em penetrar

---

[103] HAN, Byung-Chul. **No Enxame: reflexões sobre o digital.** Op. cit. p, 84.
[104] HAN, Byung-Chul. **No Enxame: reflexões sobre o digital.** Op. cit. p, 84.
[105] RODOTA, Stefano. ***Cual derecho para el nuevo mundo?*** Revista de Derecho Privado, núm. 9, julio-diciembre, 2005, pp. 5-20. Universidad Externado de Colombia, Bogotá, Colombia. p, 19
[106] RODOTA, Stefano. ***El derecho a tener derechos.*** Editorial Trotta, 2014. p, 293.
[107] RODOTA, Stefano. ***El derecho a tener derechos.*** Editorial Trotta, 2014. p, 293.
[108] HAN, Byung-Chul. **No Enxame: reflexões sobre o digital.** Op. cit. p, 90.
[109] Não se pode afirmar que essa substituição se dá por completo. Precisa se atentar para as peculiaridades de cada realidade social, ou ainda as peculiaridades deste *poder* aplicado sob as diversas classes sociais. Evidentemente que há um acoplamento do *Biopoder* e do *Psicopoder* para o controle mais amplo. Um voltado para o controle do corpo, como afirmado acima, outro ao controle da *psique*. Neste sentido também discorre Casara, em sociedades com menos desigualdade social, se aposta em recursos do *psicopoder* em detrimento do poder penal, vez que este auto-controle pelo *psicopoder* revela-se mais efetivo e menos traumático do que a disciplina de um poder externo sobre o corpo. Nas palavras de Casara, "ao lado do recurso ao psicopoder, o uso do poder penal e a lógica da sociedade disciplinar continuam necessários à realização do projeto neoliberal". (CASARA, Rubens. **Estado pós-democrático: neo-obscurantismo.** 2 ed. Rio de Janeiro: Civilização Brasileira, 2017. p, 47 – 57).

ou intervir na psique da população. Deste modo os pensamentos não são acessíveis. A psicopolítica portanto, permite que a partir da vigilância digital se alcance os pensamentos a fim de controla-los. Para este modelo de controle, aqui está a importância da existência de bases de dados com capacidades inimagináveis de armazenamento, tais como o *big data*.

Em síntese, é dizer que os dados falam por si e a informação contida despreza a negatividade de maiores reflexões. "A questão do *porquê* torna-se inútil perante a evidência do *é*"[110]. Han alerta para a possibilidade de extrair esquemas de comportamento das massas a partir dos dados disponíveis em rede, um início da psicopolítica digital em que se torna aparente padrões de comportamentos, que embora inconscientes cada um tem o seu próprio. A informação presente nos dados são padrões submetidos ao controle e à vigilância que se volta à previsão de (re)ações futuras[111].

O fim da privacidade destacado por Castells[112] simboliza a transformação da intimidade e privacidade em moeda de troca para acessibilidade na *rede*. Desta forma a concessão dos dados pessoais às forças da *rede*, ou a renúncia de um direito à proteção da privacidade dos dados pessoais é imposta sob condição para usar a *Internet.*

A realidade da vigilância cibernética é concreta. O autor conta que o *FBI* se utiliza de programas como o "*Carnivore*" – em cooperação com provedores de serviços de *internet* – para registrar *e-mails*, e posteriormente coletar informações a partir da busca por palavras-chave. O investimento neste setor tem sido elevado e recorrente, principalmente quanto à implementação de financiamentos em programas de vigilância. O *Digital Storm*, por exemplo, é atualmente uma modalidade de gravação da comunicação telefônica combinada com programas de computador que extrai palavras-chave de mensagens alvo.

Whitaker destaca o risco que as vítimas da ingerência estatal sofrem quanto à facilidade que estas possui de terem sua liberdade restringida (ou serem mortas por se tratarem de inimigos do Estado). Tanto no primeiro caso, como no segundo, salienta o autor que as pessoas se transformam em *cases*, arquivos, "perfis abstratos de si mesmos mais ou menos caricaturizados" que se destacam por terem atrelados a si determinados atributos ou atribuições tidas – aparentemente – suspeitas. O exemplo é claro: Um indivíduo X se relacionou uma vez com outro indivíduo Y, que por sua vez tem relações com uma reconhecida organização

---

[110] HAN, Byung-Chul. **No Enxame: reflexões sobre o digital.** Op. cit. p, 90.
[111] HAN, Byung-Chul. **No Enxame: reflexões sobre o digital.** Op. cit. p, 91 – 92. Neste mesmo sentido HAN, Byung-Chul. **Psicopolítica: neoliberalismo e novas técnicas de poder.** Antropos. Lisboa: Relógio D'água Editores. 2015. p, 31. Sobre o *Big Data*, Han afirma ser possível a construção de um psicograma individual e coletivo, e até mesmo, um psicograma do inconsciente, "deste modo, seria possível iluminar e explorar a psique até o nível do inconsciente".
[112] CASTELLS, Manuel. **A galáxia da *Internet.*** Op. cit. p, 145.

criminosa; Imagine-se que outro indivíduo Z, também relacionado àquela organização, mantenha uma conexão com X; A atitude de X deverá ser reinterpretada como um membro da mesma organização criminosa[113].

Neste sentido, Whitaker afirma que quando os arquivos substituem a pessoa real no mundo real, as palavras e os atos que em circunstâncias normais pareceriam inocentes adquirem as mais sinistras conotações. Um cenário que se impõe consequências reais para pessoas reais baseadas na presunção das informações colhidas em arquivos ou dados[114].

É uma espécie da chamada "análise das formas de vida"[115] – técnica utilizada para auxiliar na localização, vigilância e aniquilamento de alvos em conflitos militares – que consiste na detecção de comportamentos, padrões de informações que a partir do uso de probabilidades por tecnologias automatizadas prospectam trajetórias, ações ou comportamentos futuros. Deste modo é possível se antecipar as intervenções de bloqueio.

Nas palavras utilizadas por Chamayou, "o futuro se apoia pelo conhecimento do passado", ou seja, os arquivos *das vidas* formam uma base de informações – disponíveis em bases de dados – sob pretexto de identificar atividades de risco e, assim, antecipar intervenções de segurança[116].

---

[113] WHITAKER, Reg. ***El fin de la privacidad.*** Op. cit. p, 37.
[114] WHITAKER, Reg. ***El fin de la privacidad.*** Op. cit. p, 37.
[115] CHAMAYOU, Grégore. **Teoria do drone.** São Paulo: Cosac Naify. Coleção Exit. 2015. p, 46 – 62. Sob esta perspectiva, Chamayou trata da estratégia de guerra à distância protagonizada pela utilização de *Drones.* Afirma o autor que a onisciência, neste aspecto, corresponde à onipotência, pois todas as informações (o olho que tudo vê) utilizadas permitem descobrir quem é o alvo inimigo, qual a sua importância em uma rede, onde vive, quem são seus familiares e amigos. O poder informativo é o poder de guerra, poder de destruição. A informação alimenta a estratégia de *vigiar e aniquilar*. Aquilo que o autor chama de "revolução do olhar". Chamayou colaciona princípios utilizados à esta inovação, tais princípios adequáveis ao tema central deste trabalho. Todavia é preciso ressaltar que existem peculiaridades em uma situação de guerra não comparadas (em seu conjunto) com a realidade processual penal e que metodologias de combate ou de estratégia de vigilância em combate, de igual modo não são comparáveis (em sua totalidade) às metodologias de investigação preliminar. Contudo, discorrer-se-á sobre tais princípios em rodapé para facilitar a compreensão do que se argumenta. O primeiro princípio denominasse *princípio do olhar persistente ou de vigília permanente* que consiste em disponibilizar um dispositivo patrulha em vigília geoespacial constante do olhar institucional. Em sequência se tem o *princípio de totalização das perspectivas ou de vista sinóptica* que se traduz em uma noção de vigilância de ampla extensão de campo, uma espécie de onividência dos dispositivos utilizados. Como terceiro princípio, destaca-se o *arquivamento total ou filme de todas as vidas*, que se desdobra em utilizar dispositivos para a gravação e arquivamento. Uma linha histórica de acontecimentos passados e presentes em que há a possibilidade de escolher-se trechos mais interessantes, rever, adiantar ou voltar cenas ou informações. Um *Dejà vu* digital em que a vida se torna altamente pesquisável. Em um quarto princípio se identifica a capacidade de *fusão de dados* coletados, seja via vídeo, imagem, localizadores de *GPS* e áudio. O quinto princípio é denominado de *esquematização das formas de vida* que se apresenta como sendo esta capacidade de visualizar dados provenientes de diversas fontes. "O objetivo é poder seguir vários indivíduos através de diferentes redes sociais a fim de estabelecer um padrão ou um 'esquema de vida'". Por fim, o sexto princípio, por sua vez, é o de *detecção das anomalias e de antecipação preventiva*. Este visa identificar por meio de todas as atividades, os acontecimentos pertinentes e detectar anomias ou irregularidades, na medida em que qualquer comportamento que altere as atividades habituais se destaque como possível ameaça. O "esquema da vida" serve para destacar os desvios de padrões eleitos, distinguir atividades de riscos, antecipar os riscos (o futuro) e reduzi-los ou elimina-los.
[116] CHAMAYOU, Grégore. **Teoria do drone.** Op. cit. p, 58.

É possível identificar ações cotidianas dos alvos, os locais em que transitam diariamente e com quem se relacionam. As tecnologias de informação, portanto, possuem dois aspectos antagônicos, aumentam a capacidade e o poder (comodidade), ao mesmo tempo em que acarreta ao usuário mais vulnerabilidade e manipulação. Os dados pessoais disponibilizados em rede, jamais esquecidos ou descartados, tornam a pessoa mais transparente e nas palavras de Han[117], sendo transparência a total iluminação, quem está totalmente exposto à iluminação está "inapelavelmente entregue à exploração".

Neste cenário, o Direito – na lógica da segurança e vigilância – se entrega à exploração ou melhor usurpação de si. Rodotá[118] denuncia o niilismo jurídico no qual é registrada a impotência do Direito em face das demais potências que dominam o mundo. Rebaixam-no a instrumento que se limita em aceitar a lógica da tecnologia. Afirma ainda que as políticas de ações militares ou policiais percebem o Direito como incompatível ou inaceitável aos seus propósitos.

Salienta o autor que nos últimos tempos houve (e ainda há) uma forte tendência em se inverter a dimensão do Direito, caracterizada pela garantia à autonomia decisiva das pessoas face a interesses personalíssimos (modo de entender a vida, as relações sociais e o vínculo consigo mesmo), por sua utilização como elemento essencial de uma disciplina plena e autoritária da vida[119].

As soberanias estatais quanto ao controle da informação vão cedendo espaço à cooperação governamental de países frente às ameaças veiculadas pela *internet*. Cria-se um novo espaço global da vigilância. Os Estados perdem soberania ao compartilharem poderes e concordarem com padrões comuns de regulação[120].

A estratégia principal é tentar neutralizar, através de dispositivos, o poder da criptografia-cidadã, ou seja, restringir ou proibir o poder da tecnologia criptográfica nas mãos dos cidadãos. *Softwares* de segurança pessoal são proibidos e, somados a isso, são impostas obrigações aos provedores de serviços da *Internet* a utilização de técnicas de localização e rastreamento de usuários. Ampliam-se, nesta mesma órbita, os poderes do Estado em interceptar a comunicação ou o tráfego de dados dos cidadãos.

---

[117] HAN, Byung-Chul. **Topologia da Violência.** Op. cit. p, 211 – 212.
[118] RODOTÁ, Stefano. ***Cual derecho para el nuevo mundo?*** Op. cit. p, 6.
[119] RODOTÁ, Stefano. ***Cual derecho para el nuevo mundo?*** Op. cit. p, 8. "*En los últimos tiempos la opinión pública multiplicó sus peticiones de intervención jurídica tendientes a regularmomentos de la vida que deberían dejarse a la decisión autónoma de los interesados, a su personalíssimo modo de entender la vida, las relaciones sociales y el vínculo consigo mismo*".
[120] CASTELLS, Manuel. **A galáxia da internet.** Op. cit. p, 146.

O trinômio que sustenta essa estratégia de redução à privacidade se configura por meio do controle, vigilância e punição. A "esquizofrenia do eu"[121] se desenvolve pela permanente exposição e monitoramento da vida. Ao mesmo tempo em que o temor se origina pela liberdade de comportamento e o respectivo monitoramento, somado à falta de consequência decorrente do comportamento exposto[122], também surge – inexoravelmente – pela padronização do comportamento dos indivíduos.

Por isso é que Rodotá[123] articula uma argumentação para propor proteção mais eficaz aos dados informáticos disponíveis em bases de alta capacidade de armazenamento[124]. A *internet* segundo o autor é uma gigantesca mina de dados pessoais na qual se tem prevalecido a lógica neoliberal que favorece o desenvolvimento de uma sociedade da vigilância e classificação. Constatar a necessidade de normas constitucionais para o ciberespaço é fundamental para retomar o Direito como instrumento regulador e limitador dos abusos decorrentes do acesso e tratamento incerto de dados pessoais.

2.3 A eficiente e obscena urgência processual penal (?): o domínio da nova racionalidade

A sociedade de informação é um dos pilares que sustentam e intensificam a expansão daquilo denominado por Dardot e Laval de norma neoliberal. Tem-se que a globalização da tecnologia funciona como veículo privilegiado, utilizado para esta difusão em nível mundial, que impôs a todos uma submissão ao chamado princípio de *accountability*, ou seja, submeter-se à necessidade de prestar contas e ser avaliado em função dos resultados que obtiver[125].

Deste modo, a este espaço será dedicado lugar para se abordar mais uma das diversas "sombras" projetadas pelo neoliberalismo sobre o campo do Direito[126], precisamente

---

[121] Nas palavras de Castells, "a esquizofrenia do eu" trata-se de viver em plena exposição de sua vida, dividida entre o que somos *off-line* e a imagem que temos de nós *on-line*.
[122] CASTELLS, Manuel. **A galáxia da internet.** Op. cit. p, 148 – 149.
[123] RODOTÁ, Stefano. ***Cual derecho para el nuevo mundo?*** Op. cit. p, 19 – 20.
[124] No mesmo sentido, BECK, Ulrich. **Risco Digital.** Op. cit. p, 190 – 193, dirá que como efeito emancipatório deste risco digital globalizado é a produção de expectativa do humanismo digital, pelo qual corrobora-se "a exigência de que o direito à proteção de dados e à liberdade digital seja um direito humano, que deve prevalecer como qualquer outro direito humano".
[125] DARDOT, Pierre; LAVAL, Christian. **A nova razão do mundo: ensaio sobre a sociedade neoliberal.** Op. cit. p, 199 – 201.
[126] MARQUES NETO, Agostinho Ramalho. **Neoliberalismo e gozo.** Conferência proferida sob o título *A Banalização da Lei: com que Direito Podemos Contar Hoje?*, por ocasião do Congresso Brasileiro de Direito e Psicanálise, sob o tema "A Lei em Tempos Sombrios", promovido pela Escola Lacaniana de Psicanálise de Vitória e pela Faculdade de Vitória. Vitória (ES), 29 de maio de 2008.

do Direito Processual Penal. Desta forma, mesmo que – nas palavras de Coutinho[127] – esse discurso de matriz economicista seja enfadonho, trata-se de matéria cuja relevância tem se mostrado umbilical às novas reformas legislativas no campo do Direito Processual Penal, principalmente quanto à aceleração que combina novas tecnologias de investigação mais eficientes com a aquisição de fontes probatórias sem o respeito a garantias mínimas inerentes ao próprio Direito Processual Penal.

Pois bem, quando Dardot e Laval discorrem sobre uma nova racionalidade mundial, denominada razão neoliberal, tratam da influência do neoliberalismo que como sistema normativo ampliou-se pelo mundo e estendeu a lógica do capital a todas as relações sociais e esferas da vida. Racionalidade pois tende a estruturar e organizar as condutas de todos, governantes e governados, na medida em que possui como característica principal a generalização da concorrência como norma de conduta e da "empresa" como modelo de subjetivação[128].

Um conjunto de novas práticas, discursos e dispositivos que visam a instauração dessa nova condição política compõem a estratégia neoliberal. De acordo com os autores o caráter estratégico da concorrência como nova norma mundial decorre diretamente da relação de apoio entre as políticas neoliberais e as transformações do capitalismo. Isso provém de uma luta ideológica crítica contra o Estado de bem-estar, pautada diretamente nas ações de certos governos, cominadas – em grande parte – por técnicas e dispositivos de disciplina (com função de obrigar os indivíduos a governar a si mesmos sob a pressão da competição), cuja ampliação em codificações institucionais instauraram uma racionalidade geral norteadora da conduta humana[129]. Ou seja, a instauração da nova norma de racionalidade mundial da concorrência se deu, "pela conexão de um projeto político a uma dinâmica endógena, a um só tempo tecnológica, comercial e produtiva"[130].

A dominação do Estado pela lógica do Mercado (ou a reestruturação neoliberal do Estado) se dá – definitivamente – pela desmoralização do "Estado de bem-estar" pautada na argumentação neoliberal da eficácia e do custo. Transforma-se o indivíduo no único

---

[127] COUTINHO, Jacinto Nelson de Miranda. **Efetividade do Processo Penal e Golpe de Cena: um problema às reformas processuais no Brasil.** *In*: SILVEIRA, Marco Aurélio Nunes da; DE PAULA, Leonardo Costa (org). Observações sobre os sistemas processuais penais: escritos do Prof. Jacinto Nelson de Miranda Coutinho Vol. 1. Curitiba: Observatório da mentalidade inquisitória, 2018. p, 324.

[128] DARDOT, Pierre; LAVAL, Christian. **A nova razão do mundo: ensaio sobre a sociedade neoliberal.** Op. cit. p, 7 – 17. O sujeito empresário de si.

[129] DARDOT, Pierre; LAVAL, Christian. **A nova razão do mundo: ensaio sobre a sociedade neoliberal.** Op. cit. p, 193.

[130] DARDOT, Pierre; LAVAL, Christian. **A nova razão do mundo: ensaio sobre a sociedade neoliberal.** Op. cit. p, 194.

responsável pela demonstração constante do seu valor e consequente merecimento de condições existenciais. A exigência imposta não se trata da "retirada" do Estado, mas a imposição pelo Estado, de normas de concorrência e exigências de eficácia e produtividade.

A lei não serve mais para limitar a competição, mas sim é usurpada de seu lugar de controle pela própria competição. "A competição no lugar da lei" se soma a outros dois pilares de matriz neoliberal, a desigualdade e a eficiência para incrementar uma lógica social que cria vencedores e perdedores[131].

Toda essa estratégia funciona para subverter os fundamentos modernos da democracia, na medida em que a circunscreve nas regras de eficácia das empresas privadas. Ou seja, além de aumentar a eficácia e reduzir os custos da ação pública, desconhece direitos sociais (e porque não dizer fundamentais) ligados ao *status* de cidadão. Ademais, essa reestruturação da ação pública se pauta na concepção de que os funcionários públicos (e aqui neste estudo os atores judiciários) "são agentes econômicos que respondem apenas à lógica do interesse pessoal" como atores egoístas e racionais. Além de buscarem alcançar metas estabelecidas por políticas de incentivo, buscarão maximizar os resultados da ação pública mediante o mínimo possível de gastos públicos[132].

A ação eficiente transforma um Juiz em um servidor público formato *Eichmann* que influenciado pela melhor alocação de riquezas em sociedade, aliada ao método custo-benefício para as relações humanas, se submete aos princípios da economia, subvertendo-se, ou melhor, abstendo-se da posição de garante[133]. Reserva-se ao papel neoliberal estratégico com o objetivo de equilibrar o mercado, um servidor exemplar e cumpridor de suas obrigações que não reflete sobre as consequências de suas ações, apenas segue o fluxo orientado por determinações superiores[134], ou seja com "competência técnica e indiferença ética"[135].

---

[131] MARQUES NETO, Agostinho Ramalho. **Neoliberalismo e gozo.** Op. cit. p, 3. Agostinho Ramalho dirá que os três pilares de sustentação do neoliberalismo são a desigualdade, a competição e a eficiência, de modo a romper e ao mesmo tempo dar continuidade ao liberalismo (clássico). Para o autor, o pilar da desigualdade consiste em uma dissimetria situacional entre aqueles sujeitos que competem entre si no mercado econômico. A competição neste aspecto é hipervalorizada, sendo caracterizada como o próprio motor da economia de mercado nesta perspectiva. Por fim, a eficiência corresponde ao pilar que se refere à aptidão técnica do agente capacitado, cuja principal característica é o exercício de suas funções de maneira acrítica, exerce seu papel sem o questionar ou avaliar sua prática e as consequências desta.

[132] DARDOT, Pierre; LAVAL, Christian. **A nova razão do mundo: ensaio sobre a sociedade neoliberal.** Op. cit. p, 274 - 290.

[133] ROSA, Alexandre Morais da e MARCELLINO JR, Julio Cesar. **O processo eficiente na lógica econômica [recurso eletrônico]: desenvolvimento, aceleração e direitos fundamentais.** Itajaí: UNIVALI; FAPESC, 2012. p, 24.

[134] ROSA, Alexandre Morais da e MARCELLINO JR, Julio Cesar. **O processo eficiente na lógica econômica [recurso eletrônico]: desenvolvimento, aceleração e direitos fundamentais.** Op. cit. p, 26.

[135] MARQUES NETO, Agostinho Ramalho. **Neoliberalismo e gozo.** Op. cit. p, 3.

Reduzir os custos e maximizar os resultados, em matéria processual, é reduzir o tempo na resolução do caso penal. Nestes termos, explica Coutinho[136] que eficiência quando alinhada ao tempo (ainda mais este demasiadamente acelerado) trata-se de exclusão, ou seja, a supressão de direitos fundamentais e garantias processuais. Flexibilizar garantias fundamentais faz parte da grande onda que afoga o Direito Processual Penal no mar agitado/acelerado do imaginário punitivo.

Esquece-se que o Direito Processual Penal exerce seu tempo para fomentar a prudência de quem julga[137]. Lopes Jr.[138], neste sentido, segue ao afirmar que a urgência conduz a uma inversão do eixo lógico do processo, antecipa-se os efeitos graves e dolorosos que seriam percebidos somente à posteriori, e desta forma, gera-se – pela urgência/eficiência – um grave atentado contra a liberdade individual. Em concordância, entende-se que esse atentado se estende à personalidade, privacidade, intimidade e dignidade. Ou seja, o descarte de qualquer indivíduo e tudo o que o compõe como tal, a dissolução, desconstitucionalização e a desregulamentação de direitos demasiadamente caros, bem como o enfraquecimento da função garantidora do próprio Direito[139].

Se "o intervencionismo neoliberal" cria situações concorrenciais que privilegiam os mais "aptos" e os fortes e adapta os indivíduos à competição[140], por evidente que serve ao descarte daqueles indivíduos que não se adaptam ou não se mostram como fortes à concorrência. Com efeito, pode-se dizer que o intervencionismo neoliberal no Processo Penal, promove um direito pós-processual, na medida em que o Processo Penal não mais se mostrará como garantia e limitação de poder, mas como mero instrumento a promover a exclusão daqueles que não servem ao Mercado, instrumento de punição aos descartáveis ou ferramenta de "gestão dos indesejáveis"[141].

Mais além, este intervencionismo possui ao menos dois campos de incidência, ambos com auxílio na "desmoralização do indivíduo". O primeiro referente ao sujeito passivo da ingerência estatal penal, pela qual o transforma em detentor da carga processual probatória,

---

[136] COUTINHO, Jacinto Nelson de Miranda. **Efetividade do Processo Penal e Golpe de Cena: um problema às reformas processuais no Brasil.** Op. cit. p, 326.
[137] LOPES JR. Aury. **(Des)Velando o Risco e o Tempo no Processo Penal.** Op. cit. p. 167 – 168.
[138] LOPES JR. Aury. **(Des)Velando o Risco e o Tempo no Processo Penal.** Op. cit. p. 170.
[139] MARQUES NETO, Agostinho Ramalho. **Neoliberalismo e gozo.** Op. cit. p, 6. "Se o Direito não pode garantir o que se consumou sob o império da lei atual, não pode, a rigor, garantir mais nada!".
[140] DARDOT, Pierre; LAVAL, Christian. **A nova razão do mundo: ensaio sobre a sociedade neoliberal.** Op. cit. p, 288.
[141] CASARA, Rubens. **Estado pós-democrático: neo-obscurantismo.** Op. cit. p, 17.

posto que a essa altura não mais é inocente, sendo portanto presumidamente (ainda) não culpado (mas, culpável)[142].

O segundo campo de incidência se dá no Juiz penal, que também possuirá a carga de demonstrar sua utilidade face ao seu custo. Despreza-se a função (re)cognitiva/reflexiva do julgador em apreço à função de gerenciamento[143], o gestor de processos, que se apresenta pela aplicação de técnicas que solucionam questões e procuram sistematicamente a eficiência[144]. O Julgador (produtor) busca atingir a meta (institucionalizada) e, ao mesmo tempo, se auto expõe por meio de dispositivos de transparência para o alcance de seus consumidores. Esse comportamento é chamado por Dardot e Laval, com o auxílio de Bentham e teóricos da Escola da *Public Choice* como James Buchanam e Gordon Tullock, de "a nova gestão pública"[145]. Ou seja, "trata-se de criar incentivos positivos [ex. metas de bonificação] e negativos [ex. representações aos conselhos das classes], similares aos do mercado, para guiar o interesse do funcionário"[146].

Ora, é de se saber que o Processo Penal não se ocupa do combate à criminalidade. Toda a preocupação em proteger interesses da coletividade contra a violência[147] que derrama

---

[142] Trazer ao debate a reflexão de Casara sobre este tocante parece fundamental, principalmente pela relevância e atualidade da temática. Discorre o autor que o valor da liberdade e consequentemente sua determinação como princípio constitucional sofre coação direta pela lógica gerencial/concorrencial presente em um Estado Pós-democrático. A presunção de inocência, vista pela lupa da pós democracia, por via reflexa, é encarada como uma negatividade a ser afastada. Conforme o autor, a dignidade da liberdade trazida por Kant, desaparece. O presumir-se inocente deve, portanto, ser compreendido e resgatado em nome da necessidade de conter o poder penal. CASARA, Rubens. **Estado pós-democrático: neo-obscurantismo.** Op. cit. p, 149 – 156.

[143] Evidentemente, a partir da "intervenção neoliberal" que prioriza a análise custo-benefício, passa-se a enxergar o julgador como um agente econômico da administração da justiça, adquirindo assim uma responsabilidade pela resolução mais célere e menos custosa do processo.

[144] DARDOT, Pierre; LAVAL, Christian. **A nova razão do mundo: ensaio sobre a sociedade neoliberal.** Op. cit. p, 290.

[145] DARDOT, Pierre; LAVAL, Christian. **A nova razão do mundo: ensaio sobre a sociedade neoliberal.** Op. cit. p, 292 – 302. "Bentham tenta racionalizar a ação pública para aumentar sua eficácia, utilizando mecanismos de controle e incentivo estritos e refinados, cujo objetivo é orientar o comportamento dos indivíduos num sentido favorável ao interesse geral, ou ao menos diminuir a divergência entre o interesse de cada agente e o que é coletivamente esperado dele em termos de sérvios úteis. [...] A originalidade de Bentham deve-se ao fato de que ele não se contenta em apelar para o mercado a fim de lutar contra os desperdícios burocráticos. Ele deseja descobrir meios substitutos de controle dos agentes públicos que tenham a mesma eficácia do mercado sobre os indivíduos que participam dele. O objetivo é eliminar todos os abusos, as incompetências, as vexações, as delongas, as opressões e as fraudes que os administrados sofrem nas mãos dos políticos e funcionários públicos espontaneamente corrompidos por seu "*sinistre interest*", contrário ao interesse do maior número de indivíduos". Sobre a Escola da *Public Choice* e a nova gestão pública, discorrem Dardot e Laval que: "o funcionário público é um homem igual aos outros, um indivíduo calculador, racional e egoísta, que procura maximizar seu interesse pessoal em detrimento do interesse geral. [...] O Estado não maximiza o interesse geral, os agentes públicos é que buscam na maior parte do tempo seus interesses particulares à custa de um desperdício social considerável. [...] Se a empresa privada procura maximizar o lucro, a repartição pública procura maximizar o orçamento".

[146] DARDOT, Pierre; LAVAL, Christian. **A nova razão do mundo: ensaio sobre a sociedade neoliberal.** Op. cit. p, 299.

[147] Violência aqui no sentido limitado e rasteiro concebido na Modernidade à tão somente noção de violência ligada a aspectos criminais. BIZZOTO, Alexandre. **A mão invisível do medo e o pensamento criminal libertário.** 1ª ed. Florianópolis: Empório do Direito. 2015. p, 101.

sobre a sociedade o sentimento do medo não deve ser objeto a ser protegido pelo Processo Penal. Contudo, se existe um clamor em favor de punições maiores e mais céleres, fatalmente pela nova gestão pública – "que consiste em fazer com que os agentes públicos não ajam mais por simples conformidade com as regras burocráticas, mas procurem maximizar os resultados e respeitar as expectativas dos clientes"[148] – haverá tendencialmente o desrespeito às formalidades processuais de viés constitucional (a essa altura tidas como regras burocráticas) por expedientes inquisitivos, autoritários e ("mais") eficientes. Aliás, é exatamente isso que se espera, muito mais a obtenção de resultados do que o respeito aos procedimentos funcionais e às regras jurídicas[149].

No âmbito do Direito Processual Penal, este atendendo a preceitos de celeridade, dirige-se às expectativas. Nessa conjuntura, o dispositivo probatório que possui mecanismo duplo, uma maquinaria processual *de convicções* e outra *das expectativas*, deixa-se entorpecer. Explica Cunha Martins[150] que o campo jurídico penal recebe uma tensão advinda das expectativas sociais, expectativas estas que já surgem com parcela de *preenchimento*. A expectativa, que inspira-se no campo da experiência acaba determinando o *expectável*[151], ou seja, a expectativa antecipa um determinado *preenchimento*, cujo sentimento corresponde à satisfação de um desejo. A discussão fundamental, como reflexão trazida por Cunha Martins é que justamente quando o *preenchimento*, e indiretamente a expectativa, se subtrair de um enquadramento moral restando assim um espaço *vazio* disponível, este será preenchido por um produto pronto a ser consumido. A expectativa (punitiva) surge como matriz fundadora do produto (condenação).

Noutros termos, pelo princípio da *accountability*, "a eficácia deve aumentar em razão da pressão constante e objetivada que pesará sobre os agentes públicos, em todos os

---

[148] DARDOT, Pierre; LAVAL, Christian. **A nova razão do mundo: ensaio sobre a sociedade neoliberal.** Op. cit. p, 302. Nesse sentido, discorre Casara (**Estado Pós-democrático.** Op. cit. p, 171 – 177) em "Um tribunal que julgava para agradar a opinião pública", que a população alemã que apoiava o estado nazista clamava por repressão mais severa face aos delitos. O apoio da opinião pública à relativização/desconsideração de direitos e garantias individuais em benefício de um "interesse do povo" condizente à "lei e ordem" e à "disciplina e moral", era alicerce para alterações legislativas em matéria penal que visavam o combate ao crime. O legislativo aplaudia as propostas de Hitler e o Judiciário do mesmo modo não representou obstáculo ao projeto nazista.

[149] DARDOT, Pierre; LAVAL, Christian. **A nova razão do mundo: ensaio sobre a sociedade neoliberal.** Op. cit. p, 314 – 315. A nova gestão pública como tecnologia de controle "tende a moldar a própria atividade e visa a produzir transformações subjetivas nos 'avaliados' para que se adequem a seus "compromissos contratuais" com as instâncias superiores. Trata-se de reduzir a autonomia adquirida por alguns grupos profissionais, como médicos, juízes e professores, considerados dispendiosos, permissivos ou pouco produtivos, impondo-lhes critérios de resultados constituídos por uma tecnoestrutura especializada proliferante. Idealmente, cada indivíduo deve ser seu próprio supervisor, mantendo atualizadas a contabilidade de seus resultados e a adequação às metas que lhe foram atribuídas. Um dos objetivos disso é fazer o indivíduo interiorizar as normas de desempenho e às vezes, mais do que isso, fazer com que *o avaliado seja o produtor das normas que servirão para julgá-lo*".

[150] CUNHA MARTINS, Rui. **O ponto cego do direito.** 3 ed. São Paulo: Atlas, 2013. p, 40 – 41.

[151] CUNHA MARTINS, Rui. **O ponto cego do direito.** Op. cit. p, 42.

níveis, de tal modo que acabem artificialmente na mesma situação do assalariado do setor privado, que está sujeito às exigências dos clientes[152] e às de seus superiores"[153].

A exigência pelo máximo de desempenho está diretamente ligada ao ritmo desenfreado da dinâmica (hiper) acelerada desta sociedade neoliberal, fetichizada por números e pela fabricação de resultados. Na esfera penal constata-se a busca por dois diferentes resultados. O primeiro no campo da repressão de condutas típicas com a resolução mais célere possível do caso penal. O segundo, no campo da previsão de condutas, sob a qual não se pode desprezar a influência direta da nova racionalidade mundial no âmbito legislativo (penal e processual penal).

Não por acaso, tanto leis penais como leis processuais buscam tipificar condutas abertas, sem definições de bens jurídicos penalmente tuteláveis e com procedimentos dispostos em normas processuais compostas por termos abstratos (ex. ordem pública).

Ost[154] avalia que o Estado ao levar em consideração o medo[155] que toma centro nas preocupações coletivas e o risco inerente à sociedade, transmuda a natureza e a escala deste risco que passa ser considerado inassegurável. Uma ameaça absoluta, na qual a única estratégia de combate se dá, absolutamente, pela prevenção.

Porém, prevenir-se de algo desconhecido ou invisível se mostra tarefa hercúlea. Impõe-se o saber antecipado, a busca do saber como princípio da prevenção, para se precaver diante da gravidade do risco. Neste mesmo sentido, Hassemer[156] afirma que essa exigência tem sido satisfeita por reformas penais (materiais e processuais) na luta preventiva contra o delito, na qual se busca eliminar os mais sensíveis limites e garantias constitucionais do Direito (Processual) Penal.

---

[152] Ressalta-se, por oportuno, que a clientela deste Direito (processual) Penal eficiente são os expectadores da sentença penal. Desde sempre se tem a ideia de que a "clientela" penal é composta por pessoas sob as quais o sistema penal, tradicionalmente, incide. Contudo, a partir desta lógica da influência neoliberal da produção, do desempenho e do resultado, acredita-se que estas pessoas são realocadas para a categoria de produto, juntamente com as sentenças que as condenam, as incriminam e as encarceram. A "clientela" consome este encarceramento, e o sistema de justiça criminal eficiente produz o encarceramento a ser consumido.

[153] DARDOT, Pierre; LAVAL, Christian. **A nova razão do mundo: ensaio sobre a sociedade neoliberal.** Op. cit. p, 302.

[154] OST, François. **O tempo do direito.** Bauru, SP: Edusc, 2005. p, 323.

[155] O medo é também produto vendido pela sensação constante de risco a partir da qual se promove a dinâmica da eficiência. A política criminal passa a atender aqueles setores que para a opinião pública (clientela do sistema de justiça criminal) se encontram mais ameaçados. Para Bizzotto (**A mão invisível do medo.** Op. cit. p, 98) atualmente se pode falar em uma cultura do medo, na qual o comportamento humano – a existência humana – tem se definido por meio do próprio medo. Reproduz-se com base na estabelecida cultura do medo, táticas de manipulação deste e sua consequente disseminação. Estratégias que, em se tratando de processo penal, acabam por disseminar a sensação de insegurança, de impunidade, de violência, para que se possa favorecer interesses políticos, sociais ou econômicos, como por exemplo para promover mudanças legislativas mais repressivas.

[156] HASSEMER, Winfried. ***El destino de los derechos del ciudadano en un derecho penal eficaz.*** *Estudios Penales y Criminológicos, vol. XV (1992). Cursos e Congresos nº 71 Servizo de Publicacións da Universidade de Santiago de Compostela.* ISBN 84-7191-866-8, pp. 182-198.p, 189.

Adota-se bens jurídicos universais que se descrevem de maneira vaga, a fim de que se justifique qualquer intervenção penal[157]. A técnica legislativa da eficiência é a construção de tipos penais que protejam abstrações jurídicas, crimes de perigo, que segundo Hassemer[158] – em sua maioria são crimes de perigo abstrato – se basta na suficiente demonstração do ato que o legislador descreveu como perigoso.

A nova gestão neoliberal carrega, sob seus três "ee" (eficácia, economia, eficiência)[159] a perversidade que impõe um conflito de valores entre a "cultura gerencial" e os valores da atividade profissional desempenhada, que consequentemente faz desaparecer as categorias de dever e da consciência profissional. Ou seja, atender aos anseios da população (consumidora de sentenças penais) acarreta a subtração da função contra majoritária do julgador penal.

Decisões contra os anseios da maioria em um Estado democrático de Direito simboliza o poder-dever do Judiciário enquanto mantenedor dos direitos fundamentais de todos. Contudo, como trazido à baila por Casara[160], no contexto pós-democrático, o "dever" desaparece e passa-se ao "poder" o único verbo modal.

Distorções que já são perceptíveis no Sistema de Justiça são potencializadas na pós-democracia, de modo que torna-se sintomático o incentivo da produtividade sem compromisso com o valor "justiça". Na visão de Casara, o ativismo judicial ultrapassa todas as barreiras da legitimidade e faz da atuação do Poder Judiciário, na tentativa de satisfazer demandas e atender às expectativas, um recurso pragmático que diminui a ação política tradicional[161].

Se o sistema neoliberal colocou o mundo na *era pós-democrática*[162], ou em termos mais claros, "a destruição da democracia e o auxílio da exclusão social"[163], esse mesmo sistema também inaugura a era do efêmero caracterizada pelo império da volatilidade do tempo.

O tempo necessário para cumprimento da atividade reflexiva e (re)cognitiva, se esvai pela produtividade na gestão jurisdicional neoliberal. Dirá Ost[164], que o tempo saiu do seu eixo. Não é mais o tempo da lógica duradoura, da expectativa. Do longo prazo passa-se ao curto prazo, e deste ao imediatismo.

---

[157] HASSEMER, Winfried. ***El destino de los derechos del ciudadano en un derecho penal eficaz.*** Op. cit. p, 190.
[158] HASSEMER, Winfried. ***El destino de los derechos del ciudadano en un derecho penal eficaz.*** Op. cit. p, 191.
[159] DARDOT, Pierre; LAVAL, Christian. **A nova razão do mundo: ensaio sobre a sociedade neoliberal.** Op. cit. p, 316 – 320.
[160] CASARA, Rubens. **Estado Pós-democrático.** Op. cit. p, 132.
[161] CASARA, Rubens. **Estado Pós-democrático.** Op. cit. p, p, 127.
[162] DARDOT, Pierre; LAVAL, Christian. **A nova razão do mundo: ensaio sobre a sociedade neoliberal.** Op. cit. p, 8.
[163] COUTINHO, Jacinto Nelson de Miranda. **Efetividade do Processo Penal e Golpe de Cena: um problema às reformas processuais no Brasil.** Op. cit. p, 327.
[164] OST, François. **O tempo do direito.** Op. cit. p, 327.

A urgência, uma ação imediata, dedica-se ao combate a estes riscos. Ost[165] relembra que a situação crítica que demanda urgência é caso excepcional em princípio, e nesta até mesmo a violação dos procedimentos ordinários é válida. Esta urgência, ou melhor, Estado de urgência, possui a capacidade – danosa – de produzir um efeito de generalização, ou seja, não há espaço para a espera quando busca-se alcançar o objetivo imediato, imediatamente. "A urgência nutre a cultura da impaciência que transforma qualquer prazo em prorrogação insuportável e qualquer transição, por um bloqueio institucional, criticável"[166].

Se essa dinâmica social afeta tudo ao seu redor, não seria diferente que em uma hiper-aceleração constante, o direito – e no presente estudo o processo penal – não sofresse com seus efeitos. Como discorre Lopes Jr.[167], o processo penal não fica imune aos riscos e o fator "aceleração" os potencializam. Não se pode sacrificar a necessária maturação do ato de julgar, esta aceleração "atropela" direitos e garantias do acusado. O processo penal somente se sustenta como uma garantia contra julgamentos imediatos e precipitados[168].

Neste contexto, uma consequência lógica da aceleração é a eliminação de todos os rituais e cerimônias. Conforme esclarece Han[169], esta aceleração é demasiadamente obscena, assim como todos os movimentos da "Sociedade da Aceleração", tais como a hiperatividade, a hiperprodução e a hipercomunicação. Obsceno, portanto, com o auxílio de Sartre, é esse puro movimento que se acelera por causa de si mesmo, mas que não se move realmente e sequer leva algo adiante.

Han afirma ser somente possível acelerar um processo que é aditivo, jamais aquele caracterizado pela narratividade. A exemplo se toma a aceleração possível de um processador, vez que puramente aditivo. Todavia, jamais seria possível a aceleração de rituais ou cerimônias, característicos pela sua construção de acontecimentos narrativos que, por sua vez, fogem da aceleração. Assim é certamente no Processo Penal, tendo em vista a sua própria ritualidade obedecente ao seu curso temporal e ritmo específico. A desritualização processual é a consumação da obscenidade eficientista, ou poderia ser dito: uma profana[170] produtividade processual.

---

[165] OST, François. **O tempo do direito.** Op. cit. p, 331.
[166] OST, François. **O tempo do direito.** Op. cit. p, 334 – 335.
[167] LOPES JR. Aury. **(Des)Velando o Risco e o Tempo no Processo Penal.** *In:* GAUER, Ruth M. Chittó (Org). **A qualidade do tempo: para além das aparências históricas.** Rio de Janeiro: Editora Lumen Juris, 2004. p. 139 - 177.
[168] LOPES JR. Aury. **(Des)Velando o Risco e o Tempo no Processo Penal.** Op. cit. p, 167.
[169] HAN, Byung-Chul. **A sociedade da transparência.** Op. cit. p, 69 – 71. Neste mesmo sentido, Han em Topologia da Violência (Op. cit. p, 209.) afirma que obsceno é característica fundamental de um mundo em que tudo é expressado em forma de preço, projeta-se pelo (e para) algum lucro.
[170] HAN, Byung-Chul. ***El agonia del Eros.*** Herder Editorial, S. L. 2014. p, 25 – 28.

Agamben[171] explica que o profano é aquilo que – já não mais sagrado – retorna ao livre uso dos homens, profanar portanto, significa restituir a coisa – antes sagrada – ao livre uso, um abrir de possibilidade de novos meios de uso (ou reuso) totalmente incongruente com o sagrado. Este uso libera um comportamento que se esvai de seu sentido e da relação imposta com uma finalidade, abrindo-se e dispondo-se para um novo uso.

O processo penal profano liberta-se de sua vinculação à atividade de garantia, sua vinculação à limitação do poder punitivo. Apesar disso, o Estado apresenta os mesmos comportamentos (atos processuais) que definem o Processo Penal, todavia descabidos de sua função precípua. Pelas lições de Agamben, a atividade resultante torna-se dessa forma um puro meio, uma prática que, embora conserve a sua natureza de meio, não mantem relação fiel à sua finalidade. Subtraiu-se de seu objetivo. Portanto, o processo penal profano transforma-se em meio sem fim, qual seja este último, o limite ao poder punitivo.

Neste sentido, completa Han[172] que a profanação se realiza como desritualização. Os espaços e ações rituais desaparecem numa velocidade cada vez maior, tornando o mundo mais obsceno. Isto não significa dizer que o Processo Penal não pode ser reformulado a fim de que se alcance uma resolução do caso penal com maior rapidez. O que se afirma é, justamente, oposto.

A celeridade processual não pode estar relacionada à supressão de direitos e/ou garantias fundamentais, estas não são passíveis de supressão pela lógica eficientista. A reformulação do Processo Penal, como processo aditivo, se dá inteiramente pela reformulação de todo o sistema processual. Um sistema que ao mesmo tempo contemple a dinâmica necessária para a efetividade do próprio sistema, bem como o respeito às garantias individuais.

O processo penal como evento narrativo é "procissão" e, consequentemente, é isso que o diferencia de qualquer outro movimento acelerado subtraído de narratividade. Portanto, como tal, não faz sentido a mera aceleração processual. Seu *procedere*[173] tem tempo singular. Logo, a entrega do Direito Processual Penal às promessas fajutas da redução da complexidade propagadas pela adoção de tecnologias de informação ou comunicação, como salienta Cunha Martins[174], insere – a partir do desejo pelo resultado imediato – a *maquinaria processual das expectativas* e o sistema jurídico na órbita do mercado e do consumo. Este direito, nas palavras

---

[171] AGAMBEN, Giorgio. **Profanações.** São Paulo: Boi tempo, 2007. p, 65 – 79.
[172] HAN, Byung-Chul. ***El agonia del Eros*.** Op. cit. p, 27 – 28. "*La profanación de Agamben incluso da aliento a la actual desritualización del mundo y a la ola pornográfica que lo está invadiendo, en cuanto hace sospechos los espacios rituales como formas coactivas de separacion*".
[173] HAN, Byung-Chul. **A sociedade da transparência.** Op. cit.p, 72.
[174] CUNHA MARTINS, Rui. **O ponto cego do direito.** Op. cit. p, 47 – 53.

do autor, é um "direito preocupado em responder a expectativas que o pressionam desde um exterior cada vez menos demarcado".

A velocidade condutora da sociedade (dromológica – Virilio) intensifica a destemporalização do tempo processual e promove a consequente deformação estrutural do processo penal. Este expediente reflete diretamente na orientação para o aproveitamento máximo de atos jurídicos descabidos de obediência formal, cuja premissa movente é a busca pela incorporação da velocidade ao sistema jurídico e a constante perseguição por eficiência[175].

Privilegiar a antecipação do tempo – "o momento, numa sucessão de eternos instantes" –, sendo tempo uma construção histórica e, portanto, constituído de narratividade, é eliminar por completo a possibilidade de reconstrução/reflexão. Aquilo que Gloeckner[176] irá denominar de "nadificação do tempo" do direito processual penal.

Coloca-se a evidência sobreposta ao formalismo, nos dizeres de Coutinho[177], o direito passa a ser acusado de burocrático, considerado um obstáculo e nesta senda a eficiência toma de assalto o lugar da efetividade. O formalismo, a forma, é o *procedere* no sentido do ritual construído a partir da narrativa, único caminho que possibilita a "conclusão". O imediato da produtividade em aceleração processual se traduz no excesso de positividade[178], no efêmero da ausência de reflexão, sem narrativa e sem semântica.

O resultado (o produto) é aquilo que merece protagonismo. Aliás, em nome deste processo penal para resultados (leia-se condenações) é que se invoca a velocidade e eficiência. O viés econômico no qual se pauta o processo penal eficiente, em que os fins justificam os meios, enxerga as formas processuais[179] somente como justificadas quando não demonstrarem óbices ao exercício do poder punitivo[180]. Tal como ensina Casara[181] o eficientismo é um modo de racionalizar o processo penal para transformá-lo em procedimento mais célere e menos custoso.

---

[175] GLOECKNER, Ricardo Jacobsen. **Risco e processo penal: uma análise a partir dos direitos fundamentais do acusado.** Editora: JusPodivm. 2015, p, 80 – ss.
[176] GLOECKNER, Ricardo Jacobsen. **Risco e processo penal: uma análise a partir dos direitos fundamentais do acusado.** Op. cit. p, 80 – ss.
[177] COUTINHO, Jacinto Nelson de Miranda. **Efetividade do Processo Penal e Golpe de Cena: um problema às reformas processuais.** Op. cit. p, 326.
[178] HAN, Byung-Chul. **A sociedade da transparência.** Op. cit. p, 73.
[179] Formas como garantia e limite de poder. LOPES JR., Aury. **Direito processual penal.** 11. ed. São Paulo: Saraiva. p, 154.
[180] CASARA, Rubens R. R. **Processo penal do espetáculo: ensaios sobre o poder penal, a dogmática e o autoritarismo na sociedade brasileira.** 1ª ed. Florianópolis: Empório do Direito, 2015. p, 138.
[181] CASARA, Rubens R. R. **Processo penal do espetáculo: ensaios sobre o poder penal, a dogmática e o autoritarismo na sociedade brasileira.** Op. cit. p, 140.

Transformar o Direito Processual Penal em meio sem fim é redimensiona-lo. Serve para excluir de seu âmbito o aspecto de Direito, ou melhor, conforme Marques Neto[182] redimensiona-lo à sua infância, na perspectiva de que sendo "infância" palavra cujas raízes etimológicas querem dizer "que não fala", ou "sem voz", significaria então se tratar da retirada da voz ou o esvaziamento do Direito Processual Penal. Desta forma, reduzi-lo a um procedimento meramente simbólico de punição.

Sobre os fins e os meios, necessita-se um esclarecimento. O "fim" como objetivo do devido processo penal, reflete a sua essência como garantia efetiva ao limite da intervenção estatal. Seu "meio" é sua forma procedimental, um obstáculo a ser ultrapassado pelo Estado para o exercício da acusação e posterior eventual punição. Não é demais reafirmar que efetividade e eficiência não se confundem. Um processo penal efetivo é somente aquele que obedece aos ditames constitucionais e convencionais. Não haverá devido processo penal quando não respeitados direitos fundamentais.

No processo penal, como forma que se inscreve no tempo, há sempre um começo, meio e fim[183], ou seja um tempo processual, uma linha contínua construída a partir da linguagem. Este tempo do ritual, é um tempo particular não controlado pelo homem e impossível deste o dispor[184]. Quando Garapon traz tal afirmativa, demonstra que, de fato, o tempo do processo não é um tempo ordinário, mas uma ruptura com o escoamento linear do tempo cotidiano. E é essa ruptura com a linearidade que permite à sociedade, pelo tempo do processo, regenerar a ordem social e jurídica[185].

Por Garapon, regenerar a ordem é "repetir a gênese da ordem", somente possível – através do ritual processual – por meio do regresso ao caos, perpassando a confrontação de pormenores fáticos ínfimos, e se encerrando com o retorno da paz. Pelo ritual judiciário cria-se uma ordem a partir da desordem do crime.

No pós-processo penal eficiente busca-se concluir casos penais, sem a preocupação do reestabelecimento da ordem. Ao contrário, a desordem do crime é convalidada pela desordem judicial, na medida em que pelo cálculo de custos e metas, se atropela o tempo e a forma do ritual. Esquece-se, todavia, que "conclusão" não se vincula tão somente ao resultado alcançado, mas sim ao percurso traçado. O caminho reflexivo desagua em conclusão. Portanto,

---

[182] MARQUES NETO, Agostinho Ramalho. **Neoliberalismo: o declínio do Direito.** In: RUBIO, David Sanchez; FLORES, Joaquin Herrera; CARVALHO, Salo de. Direitos humanos e globalização: fundamentos e possibilidades desde a teoria crítica. 2. Ed. Porto Alegre: EDIPUCRS, 2010. p, 111.
[183] GARAPON, Antoine. **Bem julgar: ensaio sobre o ritual judiciário.** Coleção: direito e direitos do homem. Instituto Piaget: Lisboa, 1997. p, 61.
[184] GARAPON, Antoine. **Bem julgar: ensaio sobre o ritual judiciário.** Op. cit. p, 61.
[185] GARAPON, Antoine. **Bem julgar: ensaio sobre o ritual judiciário.** Op. cit. p, 53 – 54.

o concluir impreterivelmente carrega consigo o refletir – este último construído pela narratividade. Ou seja, no atropelo das formas e do tempo impede-se que o crime seja revivido por meio das palavras[186] no seio do ritual que preza pela narrativa da linguagem.

O ritual judiciário restitui a um povo os seus valores, o seu passado e o seu Direito. E relembra a todos o objetivo de alcançar a harmonia[187]. Para retomar o pensamento de Ost[188], fica claro que a ordem social não será edificada quando se baseia em processos mais repressivos. Ao contrário, não parece se sustentar que uma sociedade possa ser duradoura quando lastreada por uma política pautada na "defesa social". Intervenções de urgência que na intenção de produzir resultados mais céleres acabam por mitigar direitos fundamentais.

O novo risco (endógeno) perceptível no Processo Penal se dá sob as vestes das técnicas de aceleração procedimental e da urgência. Dá-se forma a uma nova insegurança jurídica à qual se deve opor uma segurança jurídica compatível com a clara definição de garantias de proteção do indivíduo[189].

Toda essa inobservância a preceitos constitucionais do processo penal acarreta – como assevera Gloeckner[190] – na transformação da eficiência num conceito jurídico-valorativo que permite a desformalização material do processo penal. Essa desformalização compõe um conjunto de elementos que, pautados no eficientismo, assombram o futuro do processo penal.

A partir desta ordem de eficiência retornam (ou talvez nunca se tenha afastado) ao processo penal conceitos que satisfazem a mediocridade do arbítrio, enquanto que "introduzem a abertura necessária para se estabelecer limites à dicotomia jurídico/não jurídico"[191], tais como perigo, risco, necessidade, ou até mesmo busca da verdade a qualquer custo.

---

[186] Dirá Garapon em reflexão que "a elaboração simbólica do processo é hoje alvo de ataques. Acusa-se a justiça de ser demasiado lenta e há quem pense ter encontrado o antídoto para essa morosidade com o tratamento dos processos "em tempo real". Os julgamentos são cada vez menos seguros de si. A necessidade de concluir um debate é cada vez mais negligenciada pela justiça actual e, nomeadamente, pela justiça de gabinete. [...] Quem diz justiça flexível e pouco formalista, diz uma justiça solicitada com mais frequência, cujas decisões têm, em consequência disso mesmo, um caráter cada vez menos definitivo. Na época atual, assiste-se à multiplicação das decisões urgentes, preparatórias e conservatórias ou, ao invés, das medidas de execução e de aplicação. Crescem igualmente as instâncias modificativas, cujo objetivo passa por uma melhor adequação da justiça à realidade, mas que a fazem perder grande parte da sua substância no debate judiciário. Não há certa virtude em pôr definitivamente fim a uma querela, a um litígio ou a uma infracção? Um tal gosto pelo provisório não acabará por fazer com que impere uma incerteza permanente e contrária à segurança, quando esta é uma das virtudes principais do direito? A justiça não deve esquecer-se de que, aquilo que a sociedade espera de si, é que ponha cobro a uma situação ou a um acto, remetendo-os definitivamente para a categoria do passado". GARAPON, Antoine. **Bem julgar: ensaio sobre o ritual judiciário.** Op. cit. p, 66 – 69.

[187] GARAPON, Antoine. **Bem julgar: ensaio sobre o ritual judiciário.** Op. cit. p, 72.

[188] OST, François. **O tempo do direito.** Op. cit. p, 358.

[189] LOPES JR. Aury. **(Des)Velando o Risco e o Tempo no Processo Penal.** Op. cit. p. 171.

[190] GLOECKNER, Ricardo Jacobsen. **Nulidades no processo penal: introdução principiológica à teoria do ato processual irregular.** 2ª ed., Editora Juspodivm. 2015, p. 507.

[191] GLOECKNER, Ricardo Jacobsen. **Risco e processo penal.** Op. cit. p, 89.

Cumpre ressaltar que a verdade real para o processo penal é um mito construído pelo substancialismo inquisitório. Lopes Jr. esclarece que a busca pela verdade real, ou ao menos a mais material e consistente, surge no processo penal quando este não guardava limites, quando eram permitidos abusos nas atividades de busca, admitindo-se inclusive a tortura [192].

Este "mito" está diretamente ligado à "estrutura do sistema inquisitorial, com o interesse público (cláusula geral que serviu de argumento para as maiores atrocidades), com sistemas políticos autoritários, com a busca de uma verdade a qualquer custo; e com a figura do juiz ator (inquisidor)"[193].

Em nome dessa tal verdade aceita-se o inaceitável, as mais absurdas violações a direitos e garantias são permitidas para que se produza o resultado (em se tratando do processo penal do eficientismo, eliminar a criminalidade). A eficiência necrosa os laços de proteção do indivíduo diante do poder estatal, transforma-se em uma concepção funcionalista do processo penal[194].

O Direito Penal eficaz, para Hassemer, utiliza-se de dois critérios dogmáticos principais, a funcionalidade da administração da justiça penal e o critério metódico da ponderação de bens. Quanto ao primeiro, trata-se de uma inversão sistemática autêntica, vez que consagra injustificadamente a funcionalidade da administração da justiça penal como um princípio normativo básico, que mancha o contraste entre segurança jurídica e justiça, investigação da verdade e proteção dos direitos do imputado, eficácia e formalização[195].

Quanto ao segundo, o critério da ponderação entre bens – nos casos de necessidade –, a ponderação de interesses legitima a intervenção em direitos e princípios que são a base de nossa cultura jurídica. Conclui Hassemer que, tal "critério dogmático" funciona como instrumento contundente para o aumento da "eficácia" do Direito Penal[196].

Diante deste cenário, em que o processamento penal segue por um percorrer eficientista e que rompe – consequentemente – com as barreiras que o caracterizam como limitação do poder punitivo, a pergunta que surge é: Pode ser chamado de Direito Processual Penal este procedimento subtraído de suas bases fundantes?

---

[192] LOPES JR., Aury. **O problema da "verdade" no processo penal.** *In:* GRINOVER, Ada Pellegrini, *et all.* Verdade e prova no processo penal: Estudos em homenagem ao professor Michele Taruffo. Coordenador Flávio Cardoso Pereira. 1 ed. Brasília, DF: Gazeta Jurídica,2016. p, 67.
[193] LOPES JR., Aury. **O problema da "verdade" no processo penal.** Op. cit. p, 68.
[194] GLOECKNER, Ricardo Jacobsen. **Nulidades no processo penal: introdução principiológica à teoria do ato processual irregular.** Op. cit. p, 509.
[195] HASSEMER, Winfried. ***El destino de los derechos del ciudadano en un derecho penal eficaz.*** Op. cit. p, 194.
[196] HASSEMER, Winfried. ***El destino de los derechos del ciudadano en un derecho penal eficaz.*** Op. cit. p, 195.

O pós-processo penal, galgado pela nova razão do mundo, é protagonizado por agentes públicos (juiz e legislador neoliberais) que internalizam os dispositivos de eficácia, ou seja, os processos de normatização e técnicas disciplinares. Sob eles incide o mesmo domínio do psicopoder, uma educação da mente, uma modelagem ao novo ideal institucionalizado de produtividade. Como dito acima, uma gestão de mentes e consequente criação da nova subjetividade[197].

Como explica Han[198], "a coação por transparência, hoje, não é um imperativo explicitamente moral ou biopolítico, mas sobretudo um imperativo econômico; quem se ilumina completamente se expõe e se oferece à exploração". O sujeito se transforma em agente público *accountable*, é exigido e exige-se sempre mais produtividade, mais desempenho e mais gozo[199]. Funciona como uma espécie de engrenagem para a perpetuação do sistema que se retro alimenta, enquanto estes sujeitos intensificam a busca pelos resultados de desempenho exigidos pelos clientes. Se expõem para a vigilância, assim como se autovigiam para demonstrar sua utilidade e valor (produtividade), em constante cálculo custo-benefício.

Os reflexos da busca por mais eficiência são explicitados por Dardot e Laval, a partir de dois questionamentos que servem como convite à reflexão: "Quando o desempenho é o único critério de uma política, que importância tem o respeito à consciência e à liberdade de pensamento e expressão? Que importância tem o respeito às formas legais e aos procedimentos democráticos?"[200].

Sendo a nova racionalidade pautada em um viés estritamente gerencial, promove seus próprios critérios de validação dessincronizados dos princípios morais e jurídicos da democracia liberal. As normas são travestidas de instrumentos exclusivamente úteis para a realização dos objetivos econômicos[201].

---

[197] DARDOT, Pierre; LAVAL, Christian. **A nova razão do mundo.** Op. cit. p, 324 – 325.
[198] HAN, Byung-Chul. **Sociedade da transparência.** Op. cit. p, 113.
[199] DARDOT, Pierre; LAVAL, Christian. **A nova razão do mundo.** Op. cit. p, 350 – 374. Os autores explicitam a face sombria do governo do sujeito neoliberal: "a vigilância cada vez mais densa do espaço público e privado, a rastreabilidade cada vez mais minuciosa e mesquinha da atividade dos indivíduos, a ação cada vez mais pregnante dos sistemas conjuntos de informação e publicidade e, talvez sobretudo, as formas cada vez mais insidiosas de autocontrole dos próprios sujeitos".
[200] DARDOT, Pierre; LAVAL, Christian. **A nova razão do mundo.** Op. cit. p, 382.
[201] DARDOT, Pierre; LAVAL, Christian. **A nova razão do mundo.** Op. cit. p, 382.

3 DA INVESTIGAÇÃO À PROVA PENAL E NOVAS TECNOLOGIAS

"Assim como é inevitável para um adequado cumprimento dos fins políticos-criminais do processo organizar a persecução penal sob um paradigma diferente, é impensável que ela cumpra suas finalidades sem o apoio de um sistema [efetivo] e moderno de investigações dos delitos"[202]. O pensamento expressado por Binder simboliza uma verdadeira preocupação quanto as mudanças atuais referentes à investigação criminal.

Ao passo que se pretende modernizar a persecução penal, desde a investigação preliminar até o processo penal judicial, reflete-se acerca dos efeitos que modernas tecnologias agregam tanto às engrenagens do sistema de justiça criminal quanto ao indivíduo investigado nele inserido. Equilibrar estes dois pontos de tensão não é tarefa simples, contudo enfrenta-la parece inevitável.

O texto que segue tem essa pretensão. Inicia-se do fundamento existencial de uma investigação criminal para que sejam (r)estabelecidas premissas inafastáveis. Não se poderia pensar um sistema de investigação moderno e efetivo – a partir do que salienta Binder –, sem lições iniciais do que é a investigação criminal como procedimento formal que garante ao indivíduo ser um sujeito de direitos.

O resgate se tornou obrigatório, do mesmo modo que a partir dele – e como sugere Binder – não se pode desvencilhar a efetividade do sistema de investigação da efetividade do processo penal. Não por outro motivo que a proposta desembocou no pensar sobre as tecnologias e sua influência na atividade probatória.

A sistemática das provas penais em influência tecnológica, se não balizada pelas premissas iniciais, tende a violar o núcleo essencial de direitos fundamentais. Sobre isso, reflete-se quanto aos conceitos e aos procedimentos que atendam, em maior grau, a uma leitura constitucionalmente orientada do Direito Processual Penal.

---

[202] BINDER, Alberto. **Fundamentos para a reforma da justiça penal.** (Org.) GOSTINSKI, Aline; PRADO, Geraldo; GONZALEZ POSTIGO, Leonel. 1 ed. Florianópolis, SC: Empório do Direito, 2017. p, 200. O autor utiliza a expressão "sistema [eficiente]", contudo se compreende que Alberto Binder está ressaltando a preocupação de se ter um sistema de investigação pautado na efetividade, de modo que se busque ao mesmo tempo a resolução de casos penais com maior aperfeiçoamento técnico das polícias, sem burocratização de alguns sistemas de instituições e uma cooperação entre polícias e Ministério Público, mas que se garanta direitos fundamentais e garantias ao sujeito passivo. Não é por acaso que Binder manifesta "não [ser] possível construir um sistema de investigação moderno e eficiente alheio às exigências, demandas, controles e resultados do processo penal, pois é quem recebe, dá validade e processa os resultados de uma investigação".

3.1 Investigação Criminal: O fundamento existencial ainda existe? A necessidade de um breve resgate

Para conceituar o objeto de estudo, utilizar-se-á a definição de Lopes Jr. e Gloeckner[203] quanto a investigação preliminar como um "conjunto de atividades realizadas concatenadamente por órgãos do Estado, a partir de uma notícia-crime ou atividade de ofício, com caráter prévio e de natureza preparatória em relação ao processo penal, que pretende averiguar a autoria e as circunstâncias de um fato aparentemente delitivo, com o fim de justificar o exercício da ação penal ou o arquivamento (não processo)".

Ao passo que se destina à elucidação do fato delitivo na colheita de elementos que irão embasar a acusação penal, quais sejam a materialidade do ilícito e os indícios suficientes de autoria, constitui-se como filtro necessário às acusações infundadas, temerárias e destituídas de razoabilidade[204]. Ou seja, como aduz Giacomolli[205] possui um face dupla cuja função precípua é de, ao mesmo tempo, viabilizar a acusação penal e impedir o exercício desta.

Sobre tais funções, Gomez Colomer[206] no mesmo sentido irá frisar que serve para preparar *el juicio oral*, fundamentando a acusação e a defesa quanto à atribuição de determinado fato criminal a uma pessoa concreta. Ademais, afirma que a realização do *juicio oral* contra alguém, imputando-lhe um fato determinado, somente deve existir quando superada a fase preliminar, tendo-se obtido como resultado a existência de indícios que permitam chegar à conclusão – ainda que provisória – de que é conveniente o prosseguimento a uma fase judicial. Isto por se levar em consideração todos os infortúnios que é supor, ou atribuir a alguém o fardo de suportar um processamento criminal. Deste modo, o processo penal somente irá se justificar se antes for possível supor a existência de indícios suficientes do cometimento do ilícito.

Neste aspecto, "sua essência ativa é confirmatória da hipótese da existência de uma infração criminal e certificatória de quem foi o autor desta", contudo, em igual patamar de importância se tem a perspectiva negativa da fase preliminar, a já mencionada filtragem de acusações infundadas[207]. Na visão de Saad[208] são funções denominadas de preparatória e

---

[203] LOPES JR. Aury, GLOECKNER, Ricardo Jacobsen. **Investigação preliminar no processo penal.** 6 ed. rev., atual e ampl. São Paulo: Saraiva, 2014. p, 90.
[204] GIACOMOLLI, Nereu José. **A fase preliminar do processo penal: crises, misérias e novas metodologias investigatórias.** Rio de Janeiro: Editora *Lumen Juris*, 2011. p, 50 – 51.
[205] GIACOMOLLI, Nereu José. **A fase preliminar do processo penal.** Op. cit. p, 50 – 51.
[206] GOMEZ COLOMER, Juan-Luis. *In:* MONTERO AROCA, Juan *et* all. ***Derecho Jurisdiccional: III Proceso Penal.*** 10ª Edición. Valencia: Tirant lo Bllanch. 2001. p, 118.
[207] GIACOMOLLI, Nereu José. **A fase preliminar do processo penal.** Op. cit. p, 51.
[208] SAAD, Marta. **Exercício do direito de defesa no inquérito policial.** *In:* Boletim do IBCCRIM, nº 166, setembro de 2006.

preservadora, sendo a primeira por possibilitar – ainda – o acautelamento de eventuais fontes de prova, que poderiam desaparecer no decurso temporal.

Portanto, tem-se como um obstáculo a ser superado de modo que o fundamento existencial da investigação preliminar também é o patente interesse da eficácia de direitos fundamentais[209]. Enxergar a investigação preliminar sob esta óptica é para Choukr[210] um "despertar de uma consciência" que se origina pela invasão estatal ao *status dignitatis* do investigado, na qual inevitavelmente se insere desde esta fase o dever de observar garantias fundamentais constitucionalmente exigidas. Está umbilicalmente ligada ao Direito Processual Penal, que por sua vez é instrumento de garantia dos direitos e liberdades individuais contra abusividades e arbitrariedades estatais.

Como esclarece Lopes Jr e Gloeckner, a investigação preliminar se sustenta por três pilares básicos, quais sejam a *busca do fato oculto, uma função simbólica da investigação* e o *impedimento de acusações infundadas*[211]. O primeiro pilar também pode ser enxergado como um primeiro degrau a ser superado pelo Estado na persecução penal. Como se trata da *busca pelo fato oculto*, a investigação preliminar irá inaugurar o percurso gradual para a descoberta deste fato por completo e materialização de seu agente.

Por sua vez, tem-se como *função simbólica* um desestímulo às novas práticas delitivas desempenhado pela atuação oficial dos órgãos de controle penal. Principalmente por exercerem uma contribuição para sanar o mal-estar social ocasionado pelo fato ilícito.

Por fim, como *filtro processual* que busca evitar acusações infundadas, na visão dos autores[212] aglutina as duas outras funções, pois na medida em que uma acusação possui fundamento para se estruturar, significa que um "fato oculto" foi esclarecido, e por consequência a sociedade é assegurada pela contenção de abusos e a promessa de reparos aos danos provocados pelo ilícito.

Segundo Sampaio[213] se trata de apurar a infração para impedir que o provável inocente seja alvo de um processo penal. Apurar no sentido de "tornar pura" o suficiente para

---

[209] LOPES JR. Aury, GLOECKNER, Ricardo Jacobsen. **Investigação preliminar no processo penal.** Op. cit. p, 99.
[210] CHOUKR, Fauzi Hassan. **Garantias constitucionais na investigação criminal.** 3ª ed. Revista, ampliada e atualizada. Rio de Janeiro: Editora Lumen Juris, 2006. p, 4.
[211] LOPES JR. Aury, GLOECKNER, Ricardo Jacobsen. **Investigação preliminar no processo penal.** Op. cit. p, 100.
[212] LOPES JR. Aury, GLOECKNER, Ricardo Jacobsen. **Investigação preliminar no processo penal.** Op. cit. p, 108.
[213] SAMPAIO, André Rocha. **A onipresença processual dos atos de investigação como sintoma biopolítico.** Tese (Doutorado em Ciências Criminais) Faculdade de Direito, Pontifícia Universidade Católica do Rio Grande do Sul. 2015. p, 87.

que, a partir do que fora colhido (resultado da purificação das informações), se possa invocar a intervenção do Poder Judiciário (inerte) e processar alguém criminalmente.

Entretanto, não é preciso muito esforço para perceber que as investigações criminais no Brasil não cumprem, em sua grande maioria, as funções que possuem (possuíam). Azevedo e Vasconcellos mostram que diante da precariedade dos meios, os procedimentos realizados no inquérito policial não são seguidos, e este descumprimento da legalidade tem ocorrência justificada pela resposta rápida, ou eficiente, às demandas. Uma "ilegalidade prática" que retoma diretrizes autoritárias, uma lógica justificada pela eficiência, uma "ilegalidade eficiente"[214].

Nos dizeres de Giacomolli[215], o completo abandono da fase preliminar processual, seja a realidade prática ou teórica, atinge diretamente toda a persecução criminal. A conclusão da investigação servirá de base para acusações, processos criminais e decisões finais consequentemente eivadas de vícios e erros[216] frutos da fase preliminar. Isto porque, mesmo sendo uma fase pré-processual, costumeiramente, é dominante também na fase judicial[217] por dois motivos, o primeiro por acabar se configurando como um primeiro juízo do Estado acerca de um evento criminoso[218], e o segundo pelo reflexo de um sistema misto processual que há muito se critica[219].

---

[214] AZEVEDO, Rodrigo Ghiringhelli de; VASCONCELLOS, Fernanda Bestetti de. **O Inquérito Policial em questão – Situação atual e a percepção dos delegados de polícia sobre as fragilidades do modelo brasileiro de investigação criminal.** Revista Sociedade e Estado. Volume 6 Número 1. Jan/Abr. 2011, p, 60.

[215] GIACOMOLLI, Nereu José. **A fase preliminar do processo penal.** Op. cit. p, 20.

[216] AZEVEDO, Rodrigo Ghiringhelli de; VASCONCELLOS, Fernanda Bestetti de. **O Inquérito Policial em questão – Situação atual e a percepção dos delegados de polícia sobre as fragilidades do modelo brasileiro de investigação criminal.** Op. cit. p, 61. "O que ocorre na gestão prática do inquérito policial são desvios da lei geridos institucionalmente, através de acordos e pactos informais que envolvem a polícia, o Ministério Público e até o Judiciário, e que são mantidos em nome da racionalidade do sistema".

[217] SAMPAIO, André Rocha. **A onipresença processual dos atos de investigação como sintoma biopolítico.** Op. cit. p, 72 – 100. Sampaio nesta obra ilustra por meio de pesquisa qualitativa como se fazem presentes, ou como são transportados para o processo judicial, os autos do inquérito policial. Justificam decisões condenatórias baseadas ainda que "não exclusivamente", mas de forma preponderante nos depoimentos, confissões ou reconhecimentos colhidos em fase de investigação, sem o crivo do contraditório. Ademais, atesta o autor por meio de decisões judiciais de 1ª, 2ª e 3ª instância, que embora as informações trazidas pela investigação policial se mostrem contrárias às provas colhidas em fase judicial, aquelas tem maior relevo e destaque nas decisões que insistem em reduzir a importância do contraditório judicial como garantia constitucionalmente imposta.

[218] SAMPAIO, André Rocha. **Profanando o dispositivo "inquérito policial" e seu ritual de produção de verdades**. Revista Brasileira de Ciências Criminais. Vol 134/2017. p. 351 – 383. Ago/2017. p, 2. "O inquérito policial escrito, como é o brasileiro, funciona como uma espécie de "memória oficial"; compreendido em seu conjunto, trata-se de espécie de arquivo que reúne todo o discurso (oficial) policial (a ser) utilizado ou não em um contingente processo penal. Assim, compreendido como arquivo, não podemos olvidar de seu poder de enunciação, ao mesmo tempo constituído e constitutivo de identidade da polícia judiciária".

[219] Especialmente CORDERO, Franco. ***Procedimiento Penal Tomo I.*** Editorial Temis S.A: Santa Fe de Bogotá, Colombia. 2000. p, 57.

Quanto ao abandono – ou ao menos o tratamento acrítico – teórico da matéria, Sampaio[220] expõe alguns equívocos da doutrina brasileira clássica que ao definir a investigação preliminar, faz uma inapropriada aglutinação desta à instrução e julgamento típica de uma estrutura inquisitorial, neo inquisitorial, não democrática. (Des)Forma o papel do sujeito passivo em mero objeto da investigação e neste espaço o transforma em *fonte* de prova cuja compressão de direitos fundamentais é a máxima levada a cabo para uma investigação "satisfatória", na qual sucumbe a presunção de inocência para se dar espaço a um preenchimento de expectativas da investigação[221]. Razão assiste Sampaio quando afirma que por mais que sejam distintas as fases – investigação e instrução processual – é ingênuo acreditar em uma descontinuidade, ou a impossibilidade da contaminação processual pelo inquérito policial.

Tanto é verdade que o Código de Processo Penal brasileiro, em seu dispositivo 155[222], possibilita ao juiz formar sua convicção pela livre apreciação da prova produzida em contraditório judicial, limitando-o timidamente a fundamentar sua decisão não exclusivamente nos elementos informativos colhidos na investigação. No artigo, faz-se a ressalva para a fundamentação da decisão que leve em consideração as provas cautelares, não repetíveis e antecipadas[223].

Do disposto é possível retirar algumas noções que servem para o início de uma reflexão. Contudo, preliminarmente é preciso dizer que é fundamental se levar em consideração que os autos do inquérito policial seguem apensados aos autos do processo, e neste prisma formando um só *corpus*, inquérito e processo se imiscuem tanto pela facilidade de manuseio de ambos em um só tempo, quanto pela penetração de informações daquele via anexos de petições direcionadas a este.

Portanto, se há uma narrativa fática oficial do que foi o ilícito apurado – posto que passado histórico – que constitui o conhecimento a partir da linguagem[224] e sendo o conhecimento possível, somente possível quando dotado da parcialidade e não do todo, é a linguagem (por óbvio subjetiva daquele que fala) que forma o conhecimento penetrado no

---

[220] SAMPAIO, André Rocha. **Profanando o dispositivo "inquérito policial" e seu ritual de produção de verdades.** Op. cit. p, 3.

[221] Como visto acima, por Rui Cunha Martins, toda expectativa traz consigo uma antecipação de resultados.

[222] BRASIL, Código de Processo Penal. Artigo 155 – 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.

[223] Definições que serão abordadas a seguir, em prova penal.

[224] COUTINHO, Jacinto Nelson de Mira/nda. **Por que sustentar a democracia do sistema processual penal brasileiro?** *In: In*: SILVEIRA, Marco Aurélio Nunes da; DE PAULA, Leonardo Costa (org). Observações sobre os sistemas processuais penais: escritos do Prof. Jacinto Nelson de Miranda Coutinho Vol. 1. Curitiba: Observatório da mentalidade inquisitória, 2018. p, 106.

processo. Um conhecimento que, não bastasse seu aspecto inquisitorial, como se vê é formado na "ilegalidade eficiente".

Ademais, como já pontuou Casara[225] o livre convencimento trazido pela expressão "livre apreciação da prova" não passa de um mito que serve ao arbítrio e ao dispositivo inquisitório, na medida em que imuniza a decisão penal quando esta, não raras as vezes, se baseia exclusivamente no conhecimento trazido pela narrativa da investigação preliminar.

Cordero também é enfático ao dizer que do livre convencimento decorrem casuísmos dos mais "interessantes", justamente pelo fato do dispositivo inquisitorial se remodelar. Nesta órbita, o livre convencimento irá funcionar como um "trunfo" nas mãos do juiz que se considera onisciente. Ocasionalmente, a força de uma produção probatória ilícita, que direciona a racionalidade do julgador para uma condenação, pode ser convalidada pelo "livre convencimento". Salienta o autor, que o "livre convencimento" chega a ser a fórmula de um conhecimento em perfeita harmonia com o estilo inquisitório, e tal constatação decorre da frequente utilização das informações policiais como fundamentação para decisões[226].

Tomar como centro de análise o Artigo 155, do Código de Processo Penal brasileiro, serve para outros apontamentos. Pode-se constatar que o próprio legislador processual atribui a característica de "elementos informativos" aos conhecimentos colhidos na investigação, tornando nítido que a produção probatória processual decorre do contraditório judicial. Ainda, o legislador faz distinção acerca das provas ditas cautelares, não repetíveis e antecipadas. Analisar-se-á, ainda que de maneira breve, parte a parte relacionando-as com a investigação preliminar.

Quanto aos "elementos informativos", e para entender o que de fato são, primeiramente é preciso estabelecer a diferença entre atos de investigação e atos de prova. Para tanto, esclarece Gimeno Sendra[227] que a investigação preliminar comporta os chamados *actos de aportación de hechos*, pelos quais seria possibilitado o ingresso dos fatos no processo. São gêneros dos quais atos instrutórios ou de investigação e atos de prova são espécies. Os primeiros, conforme dispõe o autor, são diligências sumárias destinadas à fase preliminar (*fase instructora*) para apurar a existência de um fato punível, sua tipicidade e autoria[228].

---

[225] CASARA, Rubens R. R. **Mitologia processual penal.** São Paulo: Saraiva, 2015. p, 183.
[226] CORDERO, Franco. ***Procedimiento penal* Tomo II.** Editorial Temis S. A. Sanfa Fé de Bogotá – Colombia, 2000, p, 34 – 36.
[227]GIMENO SENDRA, Vicente; MORENO CATENA, Victor; CORTÉS DOMÍNGEZ, Valentín. ***Derecho Procesal Penal*.** 3ª Edición 1999. Editorial COLEX, 1999. p, 368.
[228]GIMENO SENDRA, Vicente; MORENO CATENA, Victor; CORTÉS DOMÍNGEZ, Valentín. ***Derecho Procesal Penal***. Op. cit. p, 368.

Pela limitação cognitiva os atos de investigação se referem ao estabelecimento de uma hipótese a ser confirmada ou não após o transcorrer do processo judicial. Atendem a uma fase pré-processual para a formação de um juízo de probabilidade que fundamenta a formação da *opinio delicti* do acusador. Não estão destinados à sentença, mas ao recebimento da ação penal, ou seja, demonstram a existência de indícios suficientes de autoria e materialidade delitiva. Portanto, tem como destinatário o titular da ação penal, atingindo somente o julgador[229] quando fundamentar decisões interlocutórias ou medidas cautelares, jamais em tomadas de decisões definitivas que exigem um juízo de "certeza"[230]. Gimeno Sendra afirma que os atos de investigação não se convertem por si só em atos probatórios, somente servem para facilitar às partes na fundamentação fática de suas respectivas hipóteses, não cabendo àquele que irá sentenciar estender seu conhecimento sobre os atos de investigação na declaração dos fatos provados na sentença[231].

Deste modo, há de se convir que a terminologia empregada pelo legislador quanto aos "elementos informativos" se refere aos informativos não contemplados pelo contraditório judicial, ou ainda, como descreve Soares[232], *indícios*. Como tais, estes dados objetivos colhidos sem o rigor proporcionado pelo exercício do contraditório não podem servir para embasar uma sentença penal condenatória.

Atos de prova, por sua vez, são voltados à atuação das partes processuais, dirigidos a obter a convicção do juiz ou tribunal sobre os fatos, ou seja, o acolhimento de uma das hipóteses levantadas pelas partes na tomada da decisão ou escolha judicial. Sendo a finalidade da prova formar a convicção do julgador sobre a existência ou não do fato punível[233], por evidente que é este o destinatário dos atos de prova. Com efeito, o ato de prova[234] exige o contraditório judicial.

---

[229]Não se desconhece às razoáveis críticas estabelecidas a partir da quebra da imparcialidade pelo contato do julgador (que tomará decisão definitiva) com a instrução preliminar, ou tomada de medidas em fase de investigação. Sob este ponto, pela limitação do espaço, não abordar-se-á o tema do "juiz de garantias" ou "juiz da instrução", mas se reconhece a sua suma importância para o estabelecimento de um processo penal democrático.

[230]LOPES JR. Aury, GLOECKNER, Ricardo Jacobsen. **Investigação preliminar no processo penal.** Op. cit. p, 205.

[231]GIMENO SENDRA, Vicente; MORENO CATENA, Victor; CORTÉS DOMÍNGEZ, Valentín. ***Derecho Procesal Penal.*** Op. cit. p, 371.

[232] SOARES, Gustavo Torres. **Investigação criminal e inovações técnicas e tecnológicas.** Belo Horizonte: Editora D'Plácido, 2017. p, 50.

[233] GIMENO SENDRA, Vicente; MORENO CATENA, Victor; CORTÉS DOMÍNGEZ, Valentín. ***Derecho Procesal Penal.*** Op.cit. p, 628.

[234] Abordar-se-á, com mais precisão, os sentidos dados ao vocábulo "prova" para o Direito Processual Penal no sub capítulo seguinte destinado ao tratamento da prova penal.

Não por acaso, Carnelutti[235] assevera que a "certeza", como drama do processo, é um ato de escolha tomado a partir das questões "Escolher entre o que?" e "Escolher por quê?". Por óbvio, para que haja "escolha" não basta uma única hipótese, e é por isso que a tomada de decisão é um drama do processo (necessário para ser democrático) vivido pelo julgador. A tomada de decisão definitiva somente poderá ocorrer a partir do exercício de acusação e defesa em contraditório, ou seja, teses alternativas, estabelecidas no processo penal, disponíveis à escolha jurisdicional.

O drama do processo é o drama do julgador, pois a este incumbe uma escolha. A dúvida, por seu turno, ao mesmo tempo em que impede a tomada de decisão, é contraproducente a um sistema de matriz inquisitória (Código de Processo Penal brasileiro de 1941), pois impõe a absolvição (*in dubio pro reo*). Dadas tais premissas, constata-se – a partir de Carnelutti[236] – que a resolução legislativa ao drama do processo é determinar um agir para o julgador, "a lei libera o juiz do peso da escolha, escolhendo em seu lugar".

Logo, a intromissão do inquérito policial no processo penal (fase judicial)~~,~~ carrega os resultados da investigação como hipótese ao processo. A um só tempo reduz o contraditório a um espetáculo teatral~~,~~ e autoriza o juiz à escolha fugaz pelos resultados colhidos em fase pré-processual, evidentemente sem a obediência a "um padrão rígido e pré-determinado de provas, ditadas a partir de um conjunto de regras"[237].

Para reduzir os riscos da contaminação decorrente da investigação criminal em relação ao processo judicial, é possível se pensar no descarte dos atos de investigação depois de cumprida sua função (endoprocedimental). Principalmente por que prova validamente produzida somente é possível a partir do exercício em "contraditório judicial". Ou seja, a produção da prova penal não ocorre a partir de *uno actu*, mas por uma atividade complexa na qual convergem as partes e o juiz que instruirá o processo[238]. É essencialmente praticada no "curso da fase processual, com plena observância da publicidade, oralidade, imediação, contraditório e ampla defesa"[239].

---

[235]CARNELUTTI, Francesco. **Verdade, dúvida e certeza.** *Rivista di diritto processuale, Padova: Cedam,* 1965, vol. XX, p, 4 – 9. Tradução do Prof. Dr. Eduardo Cambi, publicada na Folha Acadêmica, n. 116, a. LIX, p. 5, 1997. p, 2.

[236] CARNELUTTI, Francesco. **Verdade, dúvida e certeza.** Op. cit. p, 3.

[237] GLOECKNER, Ricardo Jacobsen. **Autoritarismo e processo penal: uma genealogia das ideias autoritárias no processo penal brasileiro.** Vol. 1, 1ª ed. Florianópolis: Tirant lo blanch, 2018. p, 423.

[238] CORDERO, Franco. ***Tre studi sulle prove penali.*** Milano: Dott. A. Giuffrè Editore, 1963. p, 197.

[239] LOPES JR. Aury, GLOECKNER, Ricardo Jacobsen. **Investigação preliminar no processo penal.** Op. cit. p, 207. Neste prisma, Fauzi Hassan Choukr afirma que a legalidade, o contraditório, a ampla defesa, e todas as garantias constitucionais sevem para a promoção dignidade humana. Não são fins em si mesmo, mas instrumentos pelos quais se alcança a tutela integral desta dignidade. Ou seja, garantias (CHOUKR, Fauzi Hassan. **Garantias constitucionais na investigação criminal.** Op. cit. p, 7).

Evidentemente, a eliminação dos autos de investigação não seria completa. O objetivo é reduzir os danos impostos ao processo através da contaminação do juiz. Portanto, excetuar-se-ia a exclusão das provas técnicas irrepetíveis e a produzida no respectivo incidente probatório[240].

Ademais, é de fundamental importância não colocar o contraditório judicial como requisito único para a validação da produção probatória, os atos de prova que restringem demasiadamente direitos fundamentais devem ser cumpridos com especial rigor a requisitos, procedimentos de recolha e garantias[241]. Quando não preenchidos os requisitos ou desrespeitadas as garantias exigidas para o cumprimento do ato de prova, Gimeno Sendra atesta que o conhecimento decorrente do ato ilícito vulnerador de um direito fundamental deve ser reduzido à categoria de mero ato de investigação, "como tal, inidóneo para poder fundamentar uma sentença de condenação se degenera em um ato de prova de valoração proibida pelo tribunal sentenciador"[242].

O raciocínio é interessante, todavia, como demostrado acima, a estrutura do Sistema Processual Penal brasileiro não protege de maneira efetiva direitos fundamentais expostos às violações investigatórias. A propositura de Lopes Jr. e Gloeckner[243] em excluir os atos de investigação do processo vem a calhar, não é que servirá para eliminar todos os riscos ou prejuízos ao polo passivo da ingerência estatal, mas razão os assistem quanto à redução destes danos. Principalmente pelo fato de que com a exclusão física do inquérito policial dos autos do processo, evitar-se-ia "indesejáveis confusões de fontes cognoscitivas atendíveis, contribuindo assim, para orientar sobre o alcance e a finalidade da prática probatória realizada no debate"[244] e a partir dele (contraditório).

Ademais, métodos investigativos essencialmente invasivos colhem informações e as transformam, ainda que com base na lei processual, em materiais probatórios. Elimina-se pela própria essência do ato a possibilidade deste vir a ser considerado um ato de prova, não

---

[240] LOPES JR. Aury, GLOECKNER, Ricardo Jacobsen. **Investigação preliminar no processo penal.** Op. cit. p, 209.

[241] GIMENO SENDRA, Vicente; MORENO CATENA, Victor; CORTÉS DOMÍNGEZ, Valentín. ***Derecho Procesal Penal.*** Op.cit. p, 633.

[242] GIMENO SENDRA, Vicente; MORENO CATENA, Victor; CORTÉS DOMÍNGEZ, Valentín. ***Derecho Procesal Penal.*** Op.cit. p, 633.

[243] LOPES JR. Aury, GLOECKNER, Ricardo Jacobsen. **Investigação preliminar no processo penal.** Op. cit. p, 330.

[244] Os autores partem do raciocínio decorrente das legislações espanhola e italiana. Nesta última, assevera Lopes Jr. e Gloeckner que, o objetivo é a absoluta *originalità* do processo penal, de modo que na fase pré-processual não é atribuído o poder de aquisição da prova, sendo somente útil para a determinação do fato e da autoria para justificar a ação penal. LOPES JR. Aury, GLOECKNER, Ricardo Jacobsen. **Investigação preliminar no processo penal.** Op. cit. p, 330.

por outra razão, mas pelo fato de que a própria essência do ato praticado elimina a possibilidade de exercício do contraditório. Excluir a possibilidade do contraditório às partes é eliminar a legítima produção probatória. Neste ponto, estar-se a falar de métodos invasivos cuja intencionalidade fulcral é o recolhimento de comportamentos ou declarações não voluntárias que atestem ou confirmem a imputação penal a ser apurada em detrimento do princípio *nemo tenetur se detegere*.

Não é forçoso concluir que métodos investigativos que coletam declarações ou comportamentos involuntários e auto incriminadores além de violarem o núcleo essencial de um direito fundamental (exemplo: dignidade e privacidade), impedem o exercício concreto do contraditório como garantia e como requisito à produção probatória. Quer-se dizer: eliminam a capacidade do direito de defesa e neste tocante, como ressalta Prado[245], a possibilidade de refutação pela defesa constitui elemento indispensável à validade jurídica de um processo penal que se fundamenta na verificação do fato para, somente após, punir o acusado.

Não é que inexista um momento a se contraditar os fatos ou declarações colhidas, mas o que é impossibilitado ou impossível por essência é o próprio "desdizer" o que foi dito, ou "desfazer" o que foi feito, tendo em vista que as informações colhidas por tais métodos darão origem a interpretações – posto que inseridos no processo a partir da narrativa de quem acusa –, conclusões ou constatações impossíveis de serem desfeitas. É a impossibilidade de reação, que sendo um dos polos da garantia do contraditório (informação e reação)[246], impossibilita a própria prática deste. Serão nestas interpretações ou conclusões – ressalta-se, feitas pelo julgador – decorrentes das informações/declarações colhidas que se pautará um suposto e prejudicado contraditório. Um contraditório precário, ineficaz pela impossibilidade de, a partir de si, ter-se a pretendida originalidade cognitiva judicial. Nas palavras de Gloeckner[247] um "contrator da verdade" presumidamente encontrada na fase preliminar, à espera de uma formal ratificação em juízo.

Deste modo, pelo impedimento ao efetivo contraditório proporcionado pelo método investigativo utilizado, ou melhor, pela declaração auto incriminadora involuntariamente coletada, tem-se como consequência a transformação do processo penal em mera formalidade[248]. A imposição da exclusão do material recolhido resulta da tentativa de se extirpar as matrizes inquisitoriais e autoritárias de processo penal fincado em um sistema probatório

---

[245] PRADO, Geraldo. **Prova penal e sistema de controles epistêmicos.** 1 ed. São Paulo: Marcial Pons, 2014. p, 41.
[246] LOPES JR. Aury. **Direito processual penal.** 11. ed. São Paulo: Saraiva, 2014. p, 570.
[247] GLOECKNER, Ricardo Jacobsen. **Autoritarismo e processo penal.** Op. cit. p, 423.
[248] PRADO, Geraldo. **Prova penal e sistema de controles epistêmicos.** Op. cit. p, 73 – 74.

voltado a atingir a confissão do réu. Como afirma Cordero[249] quando o processo penal se move a partir de tal corolário, da ânsia pelo saber que refuta qualquer limite imposto com objetivo de atingir uma "decisão justa", acaba-se por se permitir a tortura.

Neste sentido é que o autor reforça a necessidade de se revisitar a ancestralidade do instituto da instrução probatória em que se afastou os fundamentos irracionais e os instrumentos de investigação não civilizados, reconhecendo ao imputado o papel de sujeito do processo. Deste modo a investigação preliminar[250] irá ter menos caráter inquisitório a depender da relativização legalmente imposta às operações sigilosas e à concessão do contraditório. Não que se desconsidere os efeitos prejudiciais proporcionados por um contraditório sem limite ou por uma investigação sem o devido e necessário sigilo, mas se a produção probatória é desempenhada somente com a atuação de uma das partes (acusatória), condiciona-se o julgador a agir na sentença como mero ator de cumprimento ao protocolo procedimental e não ao agir na escolha entre as hipóteses alternativas e provas levantadas em contraditório pela acusação e defesa.

3.1.1 Métodos Ocultos de Investigação: Dos preceitos básicos ao recrudescimento e(m) crítica

Como visto, as novas tecnologias de informação e de comunicação tem afetado fundamentalmente a vida dos indivíduos. Agudizam não apenas as relações destes com os outros, mas os fazem desenvolver uma subjetividade controladora de si, que se alastra por todos os campos. Do privado ao público, do indivíduo ao Estado.

Permitem a implementação de um sistema de controle correspondente à fusão de dois outros sistemas cujas características se pautam em um controle social-disciplinar e também estatal disciplinar. O primeiro, presente em comunidades fortemente moralizantes e ideologizadas que se submetem a ações rígidas de conformismos operacionalizadas na forma de autocensura, assim como aos "olhos" coletivos, policiamentos morais, panoptismo social difuso, perseguições sociais, demonizações públicas e ostracismos. O segundo, por sua vez,

---

[249] CORDERO, Franco. ***Tre studi sulle prove penale.*** Op. cit. p, 201. "*quando si muove da up'ansia di sapere, che rifiuta ogni limite, pur di trovare il bandolo della decisione giusta, si finisce con la tortura*".

[250] CORDERO, Franco. ***Tre studi sulle prove penale.*** Op. cit. p, 201 – 202. "*Che poi il Vorprozess assuma meno carattere inquisitorio, quanto alle modalità secondo cui sono formate le prove, dipende dalla misura in cui la legge sottrae le relative operazioni al segreto e consente il contraddittorio sotto questo aspetto, si è già visto come ad un'istruzione di fatto inquisitoria, condotta dal publico ministero, si contrappongano le maggiori garanzia riconosciute alla difesa nel rito formale. D'altro lato, non ci si può dissimulare che il contraddittorio praticato senza limiti, oltre a frustrare uno degli scopi pratici ai quali serve l'istruzione, svuoterebbe di contenuto il dibatimento. Se l'intervento attivo dei testimoni è avvenuta "coram partibus" e con l'intervento attivo di queste ultime, a qual fine reiterate l'assunzione della prova? Al giudice non rimarrebbe che decidere secondo i protocolli*".

destaca-se por ser mais moderno que o anterior, considerado um futuro caracterizado pelo desenvolvimento das funções preventivas de segurança pública mediante técnicas de vigilância total, tais quais a espionagem de indivíduos por polícias secretas, sistemas informáticos de armazenamento e controle audiovisual[251].

Ferrajoli discorre sobre estes sistemas como dois potenciais iminentes resultantes da penetração da "crise" ao Direito Penal. Para o autor, é o sistema de controle estatal-disciplinar o mais alarmante, pois possui a capacidade insidiosa de conviver com as democracias modernas. Atende aos anseios de emergência do Direito (Processual) Penal em crise, pois de modo mais discreto, "com microfones, câmeras nos locais de trabalho e lazer, interceptações telefônicas e todo o conjunto de técnicas informáticas e telemáticas de controle a distância" desempenham funções não apenas de prevenção dos delitos mas também do governo político da sociedade[252].

Trata-se de medidas cuja função precípua é o estabelecimento de uma prevenção policial, ou um estado de polícia, em que se intervém *ex ante*, pela simples menção ao perigo ou ao risco de futuros delitos, indeterminados e previstos em normas indetermináveis[253].

Contudo, a violência contra a subjetividade do ser também é destaque do Sistema de controle social-disciplinar, vez que pela interiorização da repressão e o temor à reprovação social informal, elimina a garantia da liberdade moral ou subjetiva. O Direito (Processual) Penal não é compatível com este sistema de controle, posto que não serve à eliminação de paixões e desejos de cada um, de suas singularidades, por meio de uma homogeneização da consciência coletiva. Ao contrário, garante-se – ainda com Ferrajoli – o respeito à pessoa, a formação da sua personalidade afastada de coações e censuras morais.

Ademais, o Estado amplia seus recursos para a repressão penal, viola não somente a legalidade penal, como comprime direitos fundamentais, tais quais a privacidade e o tão

---

[251] FERRAJOLI, Luigi. ***Derecho y Razon: teoría del garantismo penal*.** Editorial Trotta: Madrid. 1995. p, 338. Ferrajoli em crítica ao abolicionismo penal, elenca quatro modelos de sistemas de controle (*social-salvaje; estatal-salvaje; social-disciplinario; estatal disciplinario*) que traz como hipóteses alternativas ao Direito penal. Mecanismos de controle que podem ser espontâneos ou institucionais, mas segundo o autor, nenhum será capaz de conter a prepotência e o arbítrio. Para a análise aqui proposta, destacam-se apenas os dois mencionados.

[252] FERRAJOLI, Luigi. ***Derecho y Razon: teoría del garantismo penal*.** Op. cit. p, 339. "*El ultimo de estos sistemas es el más alarmante, por su capacidad de convivir insidiosamente incluso con las modernas democracias. Es desde luego posible eliminar o reducir al máximo los delitos mediante una limitación preventiva de la libertad de todos: con los tanques en las calles y con policías a la espalda de los ciudadanos, pero también -más moderna y discretamente -con micrófonos, cámaras de televisión en viviendas y lugares de trabajo, interceptaciones telefónicas y todo el conjunto de técnicas informáticas y telemáticas de control a distancia que hacen posible un Panopticon social mucho más capilar y penetrante que el carcelario que concibió Bentham e idóneo para desempeñar funciones no sólo de prevención de los delitos sino también de gobierno político de la sociedad*".

[253] FERRAJOLI, Luigi. ***Derecho y Razon: teoría del garantismo penal*.** Op. cit. p, 339.

renegado *nemo tenetur*, por meio de sua produção normativa[254]. O contexto do qual se trata é definido por De Giorgi[255] como algo muito além do estado de polícia. Trata-se de um estado de guerra, que a partir da representação do inimigo público, normaliza diversas violações – a tortura, é utilizada como exemplo pelo autor – que destoam a própria democracia. É a partir da análise da retórica da guerra e o processo de formação do inimigo, que De Giorgi irá perceber uma clara semelhança entre a construção simbólica e linguística entre o inimigo que se pretende combater em uma guerra bélica e aquele que se combate na guerra à criminalidade.

Contra o terrorismo, por exemplo, salienta Roxin[256] que diversas foram as modificações legislativas que ocorreram no Direito Processual Penal alemão do pós guerra, cuja tentativa não era uma reforma sistemática, mas sim a adequação das leis para assegurar a execução de um processo penal mais eficaz face ao terror[257]. Tais modificações possibilitavam a exclusão do direito de defesa daqueles considerados terroristas, restringiam via controle judicial a comunicação escrita entre o indiciado/acusado e seu defensor, bem como obstruíram a comunicação (oral e escrita) daqueles tidos por terroristas ou acusados de terrorismo.

É esta normalização da guerra que possibilita admitir estratégias tidas como "necessárias" ao enfrentamento do inimigo emergente. Medidas tidas como indispensáveis mesmo que, como De Giorgi[258] relata, possuam efeitos colaterais. Aliás, segundo o autor, a

---

[254] PRADO, Geraldo. **Prova penal e sistema de controles epistêmicos.** Op. cit. p, 59.

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

[256] ROXIN, Claus. ***Pasado, presente y futuro del Derecho Procesal Penal.*** Op. cit. p, 147.

[257] No mesmo sentido, referindo-se ao Sistema processual penal Italiano quanto às investigações criminais que tem como objeto fatos ou atentados ligados a grupo terroristas, Alessandra Testaguzza ressalta que houve uma "esquizofrenia interceptativa" após atentados mundiais, desde 2001 – com o 11 de setembro – até atentados ocorridos em 2015 – com o atentado à sede do Jornal Francês Charlie Hebdo – que culminaram na ampliação de investimentos financeiros no setor de comunicação investigativa ou o aprimoramento de técnicas de TI. Segundo a autora no triênio entre 2015 e 2017 o Centro de Responsabilidade do Departamento de Justiça cresceu em 15,14%, o que significa um investimento de 134.137.589,00 Euros em aparelhagem e sistematização de interceptação em comunicações telefônicas. A preocupação primordial quando o assunto refere-se à "esquizofrenia interceptativa" é o risco que volta-se às garantias constitucionais como a privacidade de milhões de cidadãos (TESTAGUZZA, Alessandra. ***Schizofrenia itálica (prevenzione dei fenomeni terroristici e hipertrofia intercettiva).*** L'opinione. *Archivio Penale, 2015.* N.3. p, 3. Acesso em jun 2018. Disponível em: http://www.archiviopenale.it/File/DownloadArticolo?codice=59e97fba-e5eb-4b35-8fad-c8115d4d03bd&idarticolo=9304.

[258] DI GIORGI, Alessandro; PRADO, Geraldo. **Mesa 3: O processo penal das formações sociais do capitalismo pós-industrial e globalizado e o retorno à prevalência da confissão – da subsistiência da tortura aos novos meios invasivos de busca de prova e à pena negociada.** Op. cit. p, 150. Alessandro De Giorgi discorre a partir da constatação de que a eleição de um inimigo pela normalização da guerra é a eleição do *outro* como inimigo. Não se enxerga a si como o possível *outro*, ou melhor, não enxerga-se o *outro* dentro de si. A perspectiva trazida pelo autor, decorre dos eventos pós 11 de setembro de 2001, bem como a guerra contra as drogas dos anos 80 e 90, a política de "tolerância zero", criminalização de imigrantes, criminalização dos guetos e do povo afro. O outro (inimigo público) é indispensável para a política de guerra contra a criminalidade. O outro "para funcionar como instrumento de coesão social, deve apresentar algumas características, [...], alguém que se aproveita da nossa 'civilização', fazendo dela um uso perverso para volta-la contra nós". O inimigo nunca morre, pois a guerra precisa

definição deste efeito colateral é justamente tudo aquilo que se "deve" aceitar em nome de uma guerra legitimada pela emergência ou exceção.

Greco[259] salienta que esta exceção expressa uma regra, sob a qual impera o regime de permanente aplicabilidade na ocorrência de casos excepcionais. As exceções trazem regras implícitas, *regras de decadência*, que atuam para mutilar e mutacionar a essência humana, traduzida por Greco como dignidade. Aceitar as regras de decadência é sinônimo de incorporar um tratamento legalmente desrespeitoso a direitos e garantias fundamentais em investigações cujos alvos são aqueles tidos como inimigos[260]. A decadência da dignidade, por sua vez, traz consigo uma *regra de custos*, na medida em que caso este respeito à dignidade ultrapasse limites impostos pelos interesses dos demais indivíduos, a violação à dignidade estaria permitida[261].

A exclusão do *Ser* faz parte da normalização da inclusão do *Outro* ao aparato criminal. O *outro*, conforme Giacomolli, é o indesejável, entidade perigosa, inimigo a ser combatido[262], que se renova em multifaces, mas permanece como uma antiga e conhecida ameaça.

---

durar infinitamente. Um inimigo capaz de fazer com que se justifique um regime de "repressão preventiva" e de "prevenção repressiva". O inimigo é recriado constantemente, mas sempre com a visão do outro como desumano. Assim, pergunta o autor: "Como se espantar com as torturas fotografadas no Iraque, se, para a opinião pública das democracias ocidentais, virou normal centenas e centenas de migrantes morrerem nos mares da Europa, na tentativa de alcançar uma existência diversa daquela a que o mundo ocidental os condenou em seus países? Como se espantar que os soldados da maior democracia do mundo submetam a torturas os prisioneiros iraquianos, se os juízes desta mesma democracia podem condenar à morte presos afetados por graves enfermidades mentais? Como se espantar que os soldados americanos torturem os presos iraquianos, se os policiais da mesma democracia podem seviciar um afro-americano com um cassetete, provocando-lhe uma dilaceração intestinal irreversível e se os mesmos policiais brancos da mesma grande democracia podem, impunemente, espancar até à morte um outro afro-americano? [...]. Como se espantar que os soldados americanos torturem no Iraque, se nos Estados Unidos, a polícia pôde matar, com quarenta tiros de pistola, um afro-americano de nome Amadou Diallo, que estava simplesmente tirando da carteira um documento de identidade?"

[259] GRECO, Luis. **As regras por trás da exceção – reflexões sobre tortura nos chamados "casos de bomba-relógio".** R. Jurídica, Curitiba, n. 23, Temática n. 7, p. 229-264, 2009-2. p, 243. Evidentemente que Luís Greco se refere explicitamente aos casos de bomba-relógio, todavia não parece que as reflexões levantadas não sejam compatíveis com as situações de investigação, ou aos excepcionais métodos de investigação (colheita de informação), em que de igual modo – *mutatis mutandis* – vilipendiam em demasia direitos fundamentais.

[260] GRECO, Luis. **As regras por trás da exceção – reflexões sobre tortura nos chamados "casos de bomba-relógio".** Op. cit. p, 244. "A dignidade humana seria algo disponível, que se pode perder dependendo das decisões que anteriormente se tomem. O ser humano não seria portador de dignidade *per se*, pelo mero fato de ser humano. A dignidade seria uma qualidade externam, que se agrega aos seres humanos que a merecem, e que, por isso, também pode ser deles retirada ou sujeita a uma condição resolutiva cuja verificação transformaria o afetado num indivíduo de segunda categoria. [...] Uma vez aceita a regra de decadência, abre-se um flanco que permite legitimar a pena de morte, a castração obrigatória de delinquentes sexuais ou, inclusive, os assassinatos seletivos de terroristas conhecidos".

[261] GRECO, Luis. **As regras por trás da exceção – reflexões sobre tortura nos chamados "casos de bomba-relógio".** Op. cit. p, 245. "Não se reconheceria, assim, qualquer núcleo da personalidade absolutamente protegido contra intervenções de terceiros. O ser humano poderia, em sua totalidade, ser instrumentalizado para fins alheios, se os demais considerarem estes fins suficientemente valiosos. Uma vez admitida a regra dos custos, não há mais razões para que somente se torture o terrorista e não também, por exemplo, seus filhos, se esta for a única maneira de fazê-lo falar".

[262] GIACOMOLLI, Nereu José. **A fase preliminar do processo penal: crises, misérias e novas metodologias investigatórias.** Op. cit. p, 2.

Como tentativa de combate à criminalidade busca-se métodos mais invasivos, arbitrários e emergenciais que violam direitos fundamentais incontestavelmente pelo exercício do poder. A crise constante da ameaça emergente é o vetor que move as modificações legislativas processuais penais. Conforme salienta Andrade[263], uma crise de eficácia correspondente à lentidão e irresolubilidade dos casos penais. Ademais, uma crise de perspectiva, tendo em vista o duradouro, e talvez irreversível, paradigma que lança o Direito Processual Penal a uma ruptura com sua matriz epistemológica iluminista e sugere o retorno a um procedimento enganoso ou oculto que gira em torno da autoincriminação involuntária e violação àquilo denominado por Andrade de "área nuclear e inviolável da intimidade". Até então uma barreira irredutível que pela busca do resultado, como poder da informação, sofre corriqueiras devassas[264].

Esquece-se que a aplicação de toda e qualquer metodologia probatória/investigativa se vincula à Constituição Federal, como consequência as novas práticas investigatórias se sucedem sem qualquer aderência constitucional[265]. Paralelamente, passa-se à espetacularização do ridículo, o *pós*-processo que fomenta mais violência sem nenhum proveito eficaz à investigação, senão o meramente simbólico (pró forma) que resulta na perda de referencial da fase preliminar do processo penal, no escamoteamento da (devida) investigação que se sustenta pela resposta imediata e presenteísta, e pelo incremento do totalitarismo punitivo[266].

As soluções jurídico-positivas pairam sob o mesmo teor normativo de redução, afastamento, ou enfraquecimento de conceitos e princípios fundantes para alastrar a incidência da compressão e da compreensão limitada de certos direitos fundamentais. Em certa medida, trata-se da ampliação de respostas proativas das instâncias formais sob o aspecto da prevenção[267].

Os métodos ocultos de investigação, por sua vez, não são técnicas desconhecidas. Contudo, sob o prisma do combate à criminalidade, durante as duas décadas passadas houve uma forte ampliação e definitiva instalação no processo penal desta metodologia investigativa. O aparecimento em massa dos meios ocultos de investigação como fenômeno se deu por dois

---

[263] ANDRADE, Manuel da Costa. **Métodos Ocultos de Investigação (*plädoyer* para uma teoria geral)**. *In:* Que futuro para o direito processual penal? Simpósio em homenagem a Jorge de Figueiredo Dias, por ocasião dos 20 anos do Código de Processo Penal Português. Coimbra Editora, 2009. p, 526 – 528.
[264] ANDRADE, Manuel da Costa. **Métodos Ocultos de Investigação (*plädoyer* para uma teoria geral)**. Op. cit. p, 528 - 530.
[265] GIACOMOLLI, Nereu José. **A fase preliminar do processo penal.** Op. cit. p, 15.
[266] GIACOMOLLI, Nereu José. **A fase preliminar do processo penal.** Op. cit. p, 11.
[267] ANDRADE, Manuel da Costa. **Métodos Ocultos de Investigação (*plädoyer* para uma teoria geral)**. Op. cit. p, 527.

fatores fundamentais, conforme acentua Andrade[268]. O primeiro deles foi o triunfo da ideologia da guerra contra o terror, expansão ideológica estadunidense. O segundo foi o avanço estrutural desencadeado pelo progresso tecnológico. As novidades trazidas consigo são duas: a primeira é a institucionalização dessas medidas, sua legitimação material e formal-procedimental pela ordem jurídica; a segunda, é o efeito de generalização ou massificação destas metodologias[269], uma tendência expansionista.

Por vezes obscuros, são incognoscíveis, intrusivos e especiais, circunscritos em uma lógico-sistemática de atender a um Direito Penal de eficácia imediata e mediática[270]. Em definição, para Andrade, são a representação de uma intromissão nos processos de ação, interação e comunicação das pessoas concretamente visadas, sem que estas tenham conhecimento do fato e nem se apercebam de tais[271]. Ou seja, uma autêntica intrusão nos *tempos* e *espaços* humanos subtraídos de autodeterminação na liberdade de pensamento, decisão e ação[272].

Pela ignorância do método empregado, os indivíduos-alvos continuam a agir, em um sentido claramente auto-incriminatório ou incriminatório daqueles com os quais interagem[273]. Levam as pessoas atingidas a expor de modo inconsciente confissões não esclarecidas nem livres, que posteriormente se voltarão contra si, em um processo judicial[274]. Inexoravelmente práticas de matrizes totalitárias, sob o véu de que tais contribuem para o aniquilamento de organizações delituosas, como por exemplo cartéis de contrabando e narcotráfico[275], pornografia infantil, terrorismo, ou corrupção.

O fato é que meios ocultos de investigação mascaram o secretismo no processo penal, e a mistura de conceitos por detrás das denominações dos métodos ocultos (Agente infiltrado, Agente provocador e etc. por exemplo) retiram do Direito Processual Penal a proposta de reconhecer no indivíduo a liberdade de ser, e o faz retroceder a um procedimento dotado de uma sensação de falta de seriedade[276].

---

[268] ANDRADE, Manuel da Costa. "**Bruscamente no verão passado", a reforma do Código de Processo Penal.** Coimbra Editora, 2009. p, 105.
[269] ANDRADE, Manuel da Costa. **Métodos Ocultos de Investigação (*plädoyer* para uma teoria geral)**. Op. cit. p, 532.
[270] VALENTE, Manuel M. Guedes. **Os meios ocultos de investigação.** 21º Seminário Internacional de Ciências Criminais. São Paulo: IBCCRIM, 2015. p, 27.
[271] ANDRADE, Manuel da Costa. "**Bruscamente no verão passado"**. Op. cit. p, 105.
[272] VALENTE, Manuel M. Guedes. **Os meios ocultos de investigação.** Op. cit. p, 28.
[273] ANDRADE, Manuel da Costa. "**Bruscamente no verão passado"**. Op. cit. p, 106.
[274] ANDRADE, Manuel da Costa. "**Bruscamente no verão passado"**. Op. cit. p, 106.
[275] GIACOMOLLI, Nereu José. **A fase preliminar do processo penal.** Op. cit. p, 18.
[276] BRAUM, Stefan. ***La investigación encubierta como característica del proceso penal autoritário***. *In*: ROMEO CASABONA, Carlos Maria (org). ***La insostenible situacion del derecho penal.*** Instituto de Ciencias Criminales de Frankfurt (Ed.) Área de Derecho Penal de la Universidad Pompeu Fabra (ed. española). Granada, 2000. p, 4.

Braum afirma que a investigação encoberta é um claro exemplo do empenho pela eficiência no processo penal, que cede espaço e lugar a um modelo de processo conflitante com os princípios clássicos do Estado de Direito. Sobre tal modelo, o autor ressalta que essa metodologia tem, por um lado, uma impetuosa força de poder político, contudo transformam a legalidade, a presunção de inocência e a imediação em expressões tímidas[277].

Essa constante invasão e retaliação de direitos fundamentais retoma paulatinamente à persecução penal, princípios autoritários e abusivos que destoam proteções constitucionais e processuais, tais quais o direito a recusar testemunho e o direito ao silêncio (*nemo tenetur se ipsum acusare*)[278].

Não é possível contrapor reações à execução dos métodos ocultos, nem quando estes se executam a partir de ilegalidades e violações constitucionais. Medidas de investigação são decretadas ou prorrogadas de modo indefinido, sem respeito à fundamentação devida, sem prazo, e com intermináveis alvos. Ou ainda, quando pior, são executadas sem prévia autorização judicial, convalidadas por autorização posterior.

Tanto é assim que Montoya[279] irá destacar que a instrumentalização da técnica de investigação encoberta, na atualidade, realizada pela polícia consiste na ação guiada pelo próprio sentido de justiça e moralidade (policialesca) independentemente do procedimento material ou processual requerido pela lei. E mais, "do ponto de vista sociológico, podem ser utilizadas para a distorção da vida dos movimentos sociais, a servir como mecanismos de contenção, prolongação, alteração ou repressão".

---

[277] BRAUM, Stefan. ***La investigación encubierta como característica del proceso penal autoritário***. Op. cit. p, 12 – 13.

[278] ANDRADE, Manuel da Costa. "**Bruscamente no verão passado"**. Op. cit. p, 107.

[279] MONTOYA, Mario Daniel. ***Informantes y técnicas de investigación encubiertas: análisis Constitucional y Procesal Penal***. Buenos Aires: Ad-Hoc, 1998. p, 25 – 28. "*Em la actualidad, el uso de agentes puede ser visto como um instrumento con el cual la policía realiza una acción guiada por su propio sentido de justicia y moralidad independientemente del procedimiento sustancial o procesal requerido por la ley. En el pasado un miembro del Congreso escribió: 'si se establece el sistema de espionaje, el país será un enjambre de informantes, espías, delatores, y toda la odiosa tribu de reptiles que habitan a la luz del despótico poder. Las horas de mayores insospechables confidencias, las intimidades de la amistad o el descanso del retiro domiciliario no aportarán seguridad'. En 1893 la historia de Inglaterra puso de manifiesto: 'Nada es más repugnante para los ingleses que el espionaje, el cual forma parte del sistema de administración del despotismo continental'". […] Desde el punto de vista sociológico, en sus diversos roles, los agentes encubiertos pueden seriamente distorsionar la vida de los movimientos sociales, al servir como mecanismos de contención, prolongacíon, alteración, o represión. […] Sin embargo, fuentes policiales expresan que los policías encubiertos pueden ser debidamente entrenados a fin de que social o políticamente sean camaleones hábiles, para mezclarse naturalmene dentro del área a ser observada. Ello fue necesario dentro de cierto período de la historia americana, como por ejemplo para infiltrar a la organización de Las Panteras Negras que reunía una base compuesta de gente de bajo status social, y la Nueva Izquierda, generalmente integrada por estudiantes e intelectuales".*

Adverte Prado[280] que tais medidas podem vir caracterizadas por aquilo denominado, pelos Alemães, de "efeito hidra", em que se mantem medidas ocultas de investigação "invasivas atuando permanentemente, em aberto, em busca de fatos delituosos comprováveis mediante os "achados" das medidas investigativas anteriores, dos quais sequer havia suspeita, mas que eventualmente podem surgir pela pressão resultante da violação da intimidade e vida privada alheias". Com o auxílio de Bernd Schünemann, Prado afirma que em virtude da existência de um ambiente legalmente frágil, os meios invasivos de investigação e as medidas cautelares tendem a produzir abusos[281].

É preciso realçar, como fez Silva[282], que no combate à criminalidade – mesmo a mais prejudicial delas – importa assegurar o mais profundo respeito aos princípios e valores de Estado Democrático de Direito. Não basta, como assevera Braum, verificar a existência de infrações dos princípios para conter o processo (atualmente avançado) de desformalização, resultante da ideia de aptidão funcional da administração da justiça, a qual funciona como princípio legitimador. A aptidão funcional, nesta dimensão, acaba sendo entendida como consequência do princípio do Estado de Direito, deste modo situando-se pari passu aos princípios do modelo clássico do Estado de Direito[283]. A liberdade individual, portanto, torna-se ponderável para que quando necessário, possa vir a ser menoscabada para manter a estabilidade do Estado.

---

[280] PRADO, Geraldo. **O dever de fundamentação reforçada das decisões no âmbito das medidas cautelares.** *In:* GRINOVER, Ada Pellegrini, *et all.* Verdade e prova no processo penal: Estudos em homenagem ao professor Michele Taruffo. Coordenador Flávio Cardoso Pereira. 1 ed. Brasília, DF: Gazeta Jurídica,2016. p, 140.

[281] PRADO, Geraldo. **O dever de fundamentação reforçada das decisões no âmbito das medidas cautelares.** Op. cit. p, 140. "Coloca-se em funcionamento uma prática processual consistente em buscar declarações mesmo sobre fatos até então desconhecidos".

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

[283] BRAUM, Stefan. ***La investigación encubierta como característica del proceso penal autoritário***. Op. cit. p, 13. "*Dado el 'actual estilo del Derecho', verificar que existe la infracción de principios expuesta no parece sin embargo suficiente para contener los procesos de desformalización. El control de las comunicaciones telefónicas, la pesquisa policial mediante rastreo de datos informáticos (Rasterfahndung), la reciente introducción de juicios rápidos y la ampliación de competencias de los servicios secretos, encuentran su fundamento legitimador, al igual que el investigador encubierto, en la idea de que resultan aptas para la Administración de Justicia en términos funcionales. De este modo, la 'aptitud funcional' se ha entendido como consecuencia del principio de Estado de Derecho, situándola así en régimen de paridad junto a los principios derivados del modelo clásico de Estado de Derecho. El Estado y su instrumentario de normas pasan a ser valores aptos para el discurso. Se han hecho así compatibles con la idea de Estado de Derecho la posibilidad de oponer el poder del Estado sancionador frente a la libertad de sus ciudadanos entendida como valor ponderable, y el permitir que dicha libertad cuando sea necesario se vea menospreciada para manterner a estabilidade del Estado. El concepto de aptitud funcional de la Administración de Justicia se impone así a la vaguedad e indeterminación de la idea misma de Estado de Derecho".*

Trata-se de uma autoincriminação involuntária forçada estatalmente[284]. Esta, por Roxin, decorre da frequente invasão do âmbito privado da personalidade. Notadamente, a preocupação com a proteção provém diretamente da voluntariedade, ou vontade livre e consciente de se auto incriminar, de modo que qualquer técnica sub-reptícia ou de interrogatório que afete a vontade livre do acusado ou indiciado está proibida.

Admitir que a utilização da autoincriminação involuntária forçada pelo Estado é necessária para um efetivo controle do delito, é inaceitável. Razão assiste Roxin, uma vez que tal argumentação tende a se adequar em qualquer caso, com efeito, gerando o abandono de todo o princípio do "*nemo tenetur*". Significa, como consequência, admitir a (re)incorporação de um viés equivocado ao Processo Penal, que se funda sob a égide da "necessidade do descobrimento da verdade na investigação de atos puníveis"[285]. Uma ideia óbvia, mas com o desenvolvimento perverso, de que – conforme salienta Cordero[286] – culpado ou não, o acusado ou indiciado sabe de coisas importantes e retirar da sua mente qualquer informação que seja, infalivelmente, resolverá o caso penal.

Diante do atual panorama Andrade[287] separa os decorrentes pensamentos doutrinários opostos. Posiciona de um lado aqueles que carregam na consciência a ideia de que os meios ocultos de investigação vieram para ficar, sendo – deste modo – insubstituíveis diante da nova perspectiva criminal composta por uma criminalidade organizada e transfronteiriça. Doutro lado, os que evidenciam a danosidade social carregada por tais meios de investigação.

---

[284] ROXIN, Claus. ***Pasado, presente y futuro del Derecho Procesal Penal.*** Op. cit. p, 87 – 95. O trabalho desenvolvido por Roxin analisa o comportamento jurisprudencial acerca da autoincriminação e os limites à violação da personalidade e intimidade. Neste ponto é que para o autor, não há que se falar em relativização deste princípio quando a prova, mesmo uma prova indireta (ainda que mediante agente infiltrados), que servir para condenar advenha do vilipendio involuntário da vontade do indiciado ou acusado. "*El Derecho Penal alemán dispone de una garantía contra la autoincriminación forzada o subrepticia. A este efecto, cualquier técnica de interrogatório que afecte la voluntad libre del acusado está prohibida en virtud del §136ª de la Ordenanza Procesal Penal, la cual también afirma que cualquier violación de esta prohibición hará inadmisible la declaración. […] La jurisprudencia ha aplicado el princípio a todos los tipos de autoincriminacion involuntaria realizados en el proceso penal. […] Otro caso importante es el de un informante de policía infiltrado dentro de la celda de reclusión de una persona detenida antes del jucio. El informante obtiene la confianza del prisionero forzándolo a hablar acerca del delito y así pasar esta información a la policía. […] El detenido le había confiado al informante que él habia tenido un cómplice en la comisión del delito. […] El Tribunal Supremo Federal aceptó que esto era admisible, de tal manera que la doctrina de los frutos del árbol envenenado no resultó reconocida por la jurisprudencia. […] Yo pienso que esto es un error. Si la prueba indirecta es admitida esto puede significar "pasarse por alto el principio del nemo tenetur". Si a una persona se le hace confesar un delito debido a que ha sido inducida a un error por el Estado y si tal confesión no puede ser utilizada como prueba, mientras que la indentidad revelada del cómplice en tal confesión puede ser utilizada para condenar al acusado, la decisión en últimas yace sobre una autoincriminación causada por un método ilícito".*

[285] ROXIN, Claus. ***Pasado, presente y futuro del Derecho Procesal Penal.*** Op. cit. p, 101.

[286] CORDERO, Franco. ***Procedimiento Penal Tomo I.*** Op. cit. p, 21.

[287] ANDRADE, Manuel da Costa. "**Bruscamente no verão passado"**. Op. cit. p, 106 – 107.

Uma danosidade apontada tanto no plano *material-substantivo* como no plano *adjetivo-processual*. Quanto ao primeiro, trata-se do sacrifício de bens jurídicos ou de direitos fundamentais[288]. Já no plano *adjetivo-processual*, sacrifica o princípio *nemo tenetur*, que em linhas breves – como salienta Giacomolli – abarca o direito de não produzir ou colaborar na produção de quaisquer provas, sejam elas documentais, periciais ou outras; preserva, com efeito, "o estado de inocência, a dignidade sobre o corpo, a expectativa da privacidade, a incolumidade física e a disposição de ser deixado em paz" [289].

Andrade constata uma tendência ao recrudescimento metodológico desta tipologia investigativa, na qual o autor destaca dois eixos que agravam a danosidade social. O primeiro voltado para a compressão da autonomia pessoal do sujeito alvo dos métodos ocultos. Antes, o Estado esperava, passivamente, um comportamento auto incriminador individual. Contudo, passa-se ao comportamento ativo institucionalizado, a privatização da produção estatal da informação, sendo o contexto remodelado e redefinido pela autoridade estatal para a recolha das informações relevantes à investigação. E com a expansão tecnológica, o Estado adota uma postura de antecipação, não espera que o sujeito-alvo conceda as informações, "intromete-se e arranca outras informações ou dados" dos quais possa tirar algum proveito, (dados de localização, por exemplo). O segundo eixo de constatação pauta-se na invasão da privacidade e da violação à autodeterminação informativa[290], ou seja, uma violação à proteção jurídica dos interesses desta intimidade e privacidade[291].

Ademais, os meios ocultos deformam a dinâmica processual ao retirar, dos julgamentos, o centro gravitacional das decisões, deslocando-o para os resultados das investigações ocultas. Mais ainda, como salienta Giacomolli[292], atribuir a responsabilidade de

---

[288] ANDRADE, Manuel da Costa. "**Bruscamente no verão passado"**. Op. cit. p, 106 – 107. "Privacidade/intimidade, palavra, imagem, sigilo profissional, inviolabilidade do domicílio, segredo de Estado, sigilo das telecomunicações, confidencialidade e integridade dos sistemas técnicos-informacionais (*Vertraulichkeit und Integrität informationstechnischer Systeme*), autodeterminação informacional".

[289] GIACOMOLLI, Nereu. **O Devido Processo Penal: Abordagem conforme a Constituição Federal e o Pacto de São José da Costa Rica.** 2ª ed. rev. e ampl. São Paulo: Atlas, 2015. p, 207 – 211. "Do art. 5º, LXIII, da CF se infere que o sujeito, ao ser preso, deverá ser informado de seu direito a permanecer calado. Após a qualificação do réu e da comunicação da acusação, o interrogando deverá ser cientificado pelo magistrado de seu direito de permanecer calado e de não responder às perguntas formuladas (art. 186 do CPP), bem como de que o silêncio não importa confissão e não será interpretado em prejuízo de sua defesa (art. 186, parágrafo único, do CPP). Segundo o CPP militar**, "**ninguém está obrigado a produzir prova que o incrimine, ou ao seu cônjuge, descendente, ascendente ou irmão" (art. 296, § 2º). O silêncio não poderá ser utilizado como argumento nos debates no plenário do Tribunal do Júri, sob pena de nulidade (art. 478, II, do CPP)".

[290] ANDRADE, Manuel da Costa. **Métodos Ocultos de Investigação (*plädoyer* para uma teoria geral)**. Op. cit. p, 536 – 538.

[291] HASSEMER, Winfried; CHIRINO SANCHEZ, Alfredo. ***El derecho a la autodeterminación informativa y los retos del procesamiento automatizado de datos personales.*** Editores del Puerto, 1997. p, 32. Cabe informar que sobre o princípio da autodeterminação informativa dedicar-se-á neste trabalho um espaço próprio, pois demasiado relevante.

[292] GIACOMOLLI, Nereu. **A fase preliminar do processo penal.** Op. cit. p, 19.

alguns métodos ocultos, a exemplo o sistema de interceptação, aos órgãos políticos vinculados ao Poder Executivo, "desnatura a *ultima ratio* da *persecutio criminis*" e possibilita uma vigilância que desvirtua a finalidade da investigação criminal. Destarte, transformam o indiciado ou acusado em mero objeto do processo, não mais pertencendo à categoria de sujeito[293].

Diante de todo o exposto é que se faz imprescindível delimitar o papel dos meios de investigação dentre os quais aqueles que são executados por meios ocultos, principalmente pelas complexidades que decorrem da contemporaneidade tecnológica. Se é certa a premissa de que o sujeito passivo de um processo penal garantidor não pode se tornar *fonte* de prova exceto quando agir de maneira livre e voluntária, ou seja, somente de maneira voluntária, mediante um *meio* de prova, pode trazer ao processo elementos probatórios[294]; por evidente que qualquer declaração autoincriminatória involuntária obtida através de um meio oculto de investigação, não pode(ria) ingressar no processo penal, principalmente tendo em vista o alto grau de lesividade provocado por este em direitos fundamentais.

Se existe alguma função atrelada a esta declaração, corresponde(ria) à categoria de indícios ou "elemento informativo", que por excelência, como resultado decorrente da execução de um mero ato de investigação não possui como destinatário aquele que irá sentenciar. Portanto, tal declaração não poderá ser utilizada para fundamentar uma condenação. Em verdade, destina-se à autoridade policial ou ao titular da ação penal, e após cumprida sua função informativa (endo-procedimental) a nada mais servirá, impondo-se em respeito ao princípio *nemo tenetur* sua eliminação juntamente com os autos do inquérito policial.

Não há simplicidade neste assunto pois através das complexidades tecnológicas que incidem na investigação preliminar e no processo penal como um todo, com frequência surgem institutos processuais de natureza jurídica híbrida. Ao mesmo tempo em que se apresentam como meios (ocultos) de investigação, também se mostram como cautelares probatórias.

Por tal fato é que Lopes Jr[295] afirma que alguns institutos processuais devem resguardar-se na relação meio-fim e por consequência, a natureza jurídica do instituto esbarra na complexidade

---

[293] ANDRADE, Manuel da Costa. "**Bruscamente no verão passado"**. Op. cit. p, 107. Ponto fulcral destacado pelo autor é o agravamento decorrente da falta de conhecimento (consequente falta de contraditório) acerca da medida oculta antes e durante a sua execução, tendo em vista "as pessoas atingidas não poderem actualizar qualquer pretensão de reação e tutela, mesmo que legalmente subsistente e consignada. Elas não podem, concretamente, fazer valer a ilegalidade da medida por violação de qualquer dos pressupostos legais".

[294] GOMES FILHO, Antônio Magalhães. **Notas sobre a terminologia da prova (reflexos no processo penal brasileiro).** *In*: YARSHELL, Flavio Luiz; MORAES, Maurício Zanoide de. (Coord.). **Estudos em homenagem à professora Ada Pellegrini Grinover.** 1 ed. São Paulo: DPJ Editora, 2005. p, 309.

[295] LOPES JR. Aury. **Direito processual penal.** 11. ed. São Paulo: Saraiva, 2014. p, 737. "tudo irá depender do caso concreto, sem descartar a possibilidade de coexistência desses diferentes fins, dai porque é reducionista qualquer classificação fechada".

do próprio instituto. Ou seja, pela natureza híbrida do instituto (meio), somente se poderá definilo a partir do "fim", do objetivo ao qual se pretende. Se voltado para investigação – busca de indícios de autoria e materialidade – se utilizará das vestes de um meio de investigação; se voltado para a proteção probatória a fim de evitar uma frustração processual, na medida em que recolhe fontes e protege cautelarmente a produção da prova, será medida cautelar probatória.

3.1.2 Modernas tecnologias digitais, técnicas de controle e investigação do delito

A preocupação inicial sobre o tema que segue se relaciona ao controle e à possibilidade de invasão da privacidade e intimidade da população que surge a partir das novas tecnologias, ou seja, a violação de um núcleo fundamental que se acredita intransponível ao exercício do poder e persecução criminal. Não somente isso, constata-se uma verdadeira compressão ao princípio *nemo tenetur* sendo imposta por essa moderna persecução penal.

O embate entre as novas tecnologias que enrobustecem e aprimoram modernas tecnologias de investigação e a proibição de produzir provas contra si, traz de maneira nítida à baila uma percepção de esvaziamento e limitação do conteúdo do princípio *nemo tenetur*, de modo que o transforma na reduzida garantia de impedir coações a serem exercidas sobre imputado (corpo e mente). Para Garibaldi, uma redução conceitual que somente remonta ao histórico da renúncia ao uso de métodos violentos, mas que pela força de seu conteúdo deveria permanecer como limitador do uso de dispositivos mais sofisticados e tecnológicos[296].

Entende-se que a exposição possibilitada por novas tecnologias, principalmente digitais, não elimina o núcleo fundamental que protege o íntimo, o privado. Aliás é o oposto disto, compartilhar da privacidade faz parte da órbita volitiva do ser humano, decide-se "o que", "quando", "como" e "com quem" haverá este compartilhamento. Portanto, mostra-se imprescindível uma regulamentação devida para o uso de novas tecnologias no incremento da investigação penal que exploram a privacidade e a intimidade.

Contudo, este não é um desafio isolado, sequer o maior. Revela-se ínfimo diante da tarefa de limitar a "generalização" dos casos penais enquadrados como possíveis de serem investigados com o auxílio tecnológico digital. É preciso estabelecer um critério objetivo mínimo de "necessidade" – se é que possível –, para a utilização de algumas tecnologias que se mostram demasiadamente lesivas a direitos fundamentais.

---

[296] GARIBALDI, Gustavo E. L. ***Las modernas tecnologías de control y de investigación del delito: su incidencia en el derecho penal y los principios constitucionales.*** 1ª ed. Buenos Aires: Ad-Hoc, 2010. p, 37.

Tendo em vista que o tema sobre o combate "eficiente" à criminalidade perpassa pela vinculação do Direito Processual Penal e uma política de Estado voltados à prevenção do ilícito, há que se falar inevitavelmente no tema acerca da proteção de dados[297]. Cotidianamente, por exemplo, é propagado o interesse pelo acesso a dados e informações digitais dos cidadãos por parte dos órgãos de controle penal do Estado. Conforme Chirino Sanchez[298], dentro das redes de investigações criminais não são considerados apenas os dados pessoais dos sujeitos "suspeitos", indiciados ou acusados, mas todas as pessoas por ventura inocentes ou que não possua nenhuma ligação com o fato ilícito investigado.

A investigação criminal que pretende adotar como metodologia investigativa a operacionalização digital informática não se limita aos crimes resultantes de ações da criminalidade organizada, tampouco a crimes cometidos exclusivamente por meio do ciberespaço. Possui como objetivo o alcance de qualquer infração delitiva, principalmente por proporcionar à investigação uma maior eficiência[299] na produção probatória, seja correspondente à cibercriminalidade[300], seja a ilícitos tradicionais que necessitam da prova informática ou digital.

Sem embargos, a necessidade de obtenção da prova digital (eletrônica[301] ou científica[302]) não se vincula estritamente aos delitos informáticos. Extrapola este âmbito e se

---

[297] CHIRINO SANCHEZ, Alfredo. ***Proteccion de datos y moderno processo penal aspectos constitucionales y legales.*** *Conferencia presentada en el Seminario "Nuevo Ministério Público y Crisis de la Justicia Penal", que se celebró em la Ciudad de Buenos Aires, Argentina, auspiciado por la Procuraduría General de la Nación, los días 14 y 15 de diciembre de* 1998. p, 23.

[298] CHIRINO SANCHEZ, Alfredo. ***Proteccion de datos y moderno processo penal aspectos constitucionales y legales.*** Op. cit. p, 24.

[299] Aliás, a eficiência é sempre a palavra utilizada para justificar o emprego de métodos novos de busca e obtenção da prova penal, principalmente quando se tratam de provas penais relacionadas a dados digitais. Aqui utiliza-se esse termo, mas sem menosprezar, evidentemente, a discussão empregada no item 2.3. Ademais, mais uma vez atenta-se para a necessidade de pretender a efetividade, não eficiência, de modo que é somente aquela que ressalva a preservação de garantias fundamentais intrínsecas a qualquer persecução criminal que se pretende constitucional.

[300] FRANÇA, Leandro Ayres. **Cibercriminologias.** *In:* FRANÇA, L. A; CARLEN, Pat. **Criminologias Alternativas.** Porto alegre: Canal Ciências Criminais, 2017. p, 231. Neste contexto parece fundamental destacar a ressalva que o autor faz sobre violações no âmbito *cyber*. São três categorias específicas. "*Cybercrime* é a violação de uma norma legal (o comportamento foi explicitamente proibido pela lei, ou seja, criminalizado em determinada jurisdição local); *cyber violation*, ou *cyber deviance*, é a violação de um regramento social (há um significado social à violação, considerada indesejável ou censurável), mas não de uma norma legal. E o *neo cyber threat* é a prática de ato injusto, desenvolvido a partir da própria natureza da tecnologia, mas contra a qual não há (ainda) qualquer regra local ou universal sob a qual ela possa ser categorizada (dado um sentido). Em outras palavras: enquanto não constitui uma conduta criminosa em algumas jurisdições, uma *neo cuber threat* é geralmente tratada como um problema técnico ou uma novidade, e seu sentido não tende a gerar imediata reprovação social e a traduzir a gravidade nem a dramaticidade do termo "crime", o que pode ser alterado em decorrência de possíveis danos causados pela ameaça, por sua maior difusão e/ou pela melhor compreensão dela".

[301] ORTIZ PRADILLO, Juan Carlos. ***Informática y derechos fundamentales: hacia un derecho fundamental a la confidencialidad e integridad de los equipos informáticos.*** *In:* BAUZÁ REILLY, Marcelo; BUENO DE MATA, Federico (Coord.). *El derecho en la sociedad telemática: estúdios en homenaje a Valentín Carrascosa López*. 2012. p, 65.

[302] DOMINIONI, Oreste. ***La prova penale scientifica: gii strumenti scientifico-tecnici nuovi o controversi e di elevata specializzazione.*** Milano: Giuffrè Editore, 2005.

insere na investigação de quase qualquer tipo de ilícito[303], pois diversas informações ou arquivos armazenados em meios tecnológicos podem servir de fonte de prova do fato delituoso. Não se pode desconsiderar os diferentes graus de importância e ligação que a tecnologia informática possui seja na realização dos ilícitos, seja no armazenamento de informações relacionadas a estes[304].

Por se tratar de graus de variabilidade da incidência tecnológica no âmbito do ilícito penal, é possível se pensar na equiparação entre o grau de lesividade do método de investigação tecnológica que incide nos direitos fundamentais do investigado, e o grau de ligação entre o cometimento do ilícito investigado e o meio tecnológico. Isso porque a materialidade do delito a ser apurado pode não corresponder diretamente ou não possuir relação alguma com meios tecnológicos ou tecnologias de informação ou comunicação, seja na execução do ilícito ou no armazenamento de documentos em formato digital necessários para a atividade probatória.

Neste aspecto, por exemplo, não seria possível – porquanto que inapropriada e demasiadamente lesiva – a investigação por meios digitais ou informáticos de um homicídio ou de um roubo comum não relacionados aos meios tecnológicos. Não se poderia supor a utilização de tais mecanismos pela facilidade em determinar um suspeito ou buscar uma fonte de prova contra o indiciado ou acusado através de mecanismos que sirvam para identificar o lugar, o horário e o trajeto seguido pelo investigado na data do fato apurado.

Quer-se dizer que não existindo liame entre o ilícito investigado e o meio digital, jamais se poderá falar em uma investigação que se utiliza prioritariamente ou exclusivamente de métodos tecnológicos informáticos ou digitais, sob pena de serem demasiadamente lesivos a direitos como a privacidade, intimidade e personalidade[305].

---

[303] SALT, Marcos G. ***Tecnológia informática: un nuevo desafío para el Derecho Procesal Penal?***. XXV Congreso Nacional de Derecho Procesal Penal, Rubinzal Editores, Argentina. p, 7.

[304] Neste ponto, com o auxílio de Hollinger e Wall, ressalta França que os cibercrimes de são dispostos em gerações diferentes. A primeira geração trata de cibercrimes tradicionais nos quais os computadores são utilizados no estágio preparatório do crime, como uma ferramenta de comunicação, para obter informações preparatórias, enfim, para assistir violações tradicionais, ressalta-se que a retirada da tecnologia na execução do crime, não o evita, podendo ocorrer por outros meios que não o tecnológico. A segunda geração, também destacada pelo autor, compõe-se por crimes cometidos através da rede, porém quando extraída a internet, o comportamento infrator permanece. "As novas oportunidades de infrações desaparecem e o comportamento se realiza por outros meios, em menores número e escala". Por fim, uma terceira geração de cibercrimes, que compreende os cibercrimes próprios, produtos da oportunidade criada pela *internet* e somente podem ser perpetrados dentro do ciberespaço. Quando excluída a tecnologia da execução do ilícito, será impossível este permanecer como atividade realizada ou realizável. Salienta o autor que agentes do ilícito e vítimas não se conhecem e sequer pretendem se conhecer, todavia se relacionam em decorrência de vulnerabilidades que constam nas falhas dos sistemas informáticos operacionais (FRANÇA, Leandro Ayres. **Cibercriminologias.** Op. cit. p. 231-232).

[305] Refere-se aqui aos costumeiros exemplos de devassas em celulares de indivíduos presos em flagrante delito, ou levados às delegacias de polícia por atitudes "suspeitas". Sobre a matéria, o Superior Tribunal de Justiça no recurso em *Habeas Corpus* nº. 89.981 do Estado de Minas Gerais, de relatoria do Min. Reynaldo da Fonseca, entendeu que a devassa em aparelho celular, mesmo apenas em aplicativo *whatsapp*, embora não se tratando de hipótese abarcada pela lei n. 9.296/1996 ou protegida pela Lei n. 12.965/2014 por não se tratar de quebra de sigilo por

Há um deslocamento significativo da proteção de dados diante do conceito tradicional da privacidade e intimidade. Como destaca Chirino Sanchez[306] o direito a proteção de dados abarca um conceito muito mais amplo, sob o qual é possível se pensar outros fenômenos de interesses para o desenvolvimento do tratamento de dados e também da administração da justiça.

Esclarece o autor que surgem conceitos como "perda do contexto"; "multifuncionalidade da valoração e seleção dos dados"; "autodeterminação informativa", entre outros, resultando por certo uma necessária "reprogramação" destas proteções às novas tendências. Aliás, assevera o autor que para haver uma reprogramação de um direito à proteção de dados, deve se observar toda e qualquer medida coercitiva processual penal desde a perspectiva de uma lesão ao direito à personalidade individual. Ou seja, deve-se observar o objetivo, a formalidade e a configuração da medida processual relacionada a tal direito fundamental.

Contextos imprecisos de processamento e tratamento de dados pelos órgãos de controle penal devem ser proibidos, principalmente por não ser vislumbrado um limite ao

interceptação de comunicação telefônica, entendeu que viola a garantia da inviolabilidade das comunicações, na medida em que vilipendia os dados armazenados no celular do acusado. Nestes casos, salienta o Ministro que a autoridade policial deveria, após apreensão do telefone, ter requerido judicialmente a quebra do sigilo dos dados armazenados, haja vista garantia (requisito tido como imprescindível), igualmente constitucional, à inviolabilidade da intimidade, da vida privada, da honra, e da imagem das pessoas, prevista no art. 5º, inciso X, da Constituição Federal. Em continuidade, salienta o Ministro que a obtenção de dados telefônicos do recorrente em violação às normas constitucionais e legais impõe o desentranhamento da prova obtida dos autos processuais, por motivos de ser ilícita, conforme artigo 157, do Código de Processo Penal. (STJ, RHC nº 89.981 – MG, Relator: Min. Reynaldo Soares da Fonseca). Rosa e Lopes Jr. (*In:* Limite Penal: Vasculhar aparelho celular só é possível com autorização judicial. **Revista Consultor Jurídico.** 23 de fev. 2018. Disponível em: https://www.conjur.com.br/2018-fev-23/limite-penal-vasculhar-aparelho-celular-somente-autorizacao-judicial) convalidam o entendimento deste julgado. Entendem que "a intimidade e a privacidade armazenadas no dispositivo transcendem os limites analógicos de bens materiais, abarcando aspectos que se reconheceu tutela de direitos fundamentais". Ademais, "a extração dos dados e mensagens implica no reconhecimento da privacidade do agente que não pode, pela simples abordagem, perder-se em análise de seu histórico e arquivos por profissionais que não são, necessariamente, preparados para garantia da autenticidade e validade das provas extraídas". Concorda-se com os autores, todavia ressalta-se que não basta se ter autorização judicial (quase sempre genéricas) para tal diligência, devendo a requisição da autoridade policial ou do órgão ministerial, antes de mais nada, conter elementos suficientes que justifiquem tal medida, apresentando o nexo causal entre o suposto crime praticado pelo indiciado ou acusado, e o meio de prova que se pretende alcançar a partir da medida de acesso e tratamento de dados pretendida, para que a autorização judicial enfrente a problemática com necessária adesão constitucional. Em outras palavras, a medida de acesso e tratamento de dados em dispositivos eletrônicos somente se justifica quando funcionar como único caminho necessário, dentre outras alternativas que se mostram incapazes, para alcançar uma prova do fato ilícito praticado. Ademais, ressalva os autores (*In:* Limite Penal: Critérios de validade para vasculhar o celular – *whatsapp* – do preso. **Revista Consultor** Jurídico. 25 Mai. 2018. Disponível em: https://www.conjur.com.br/2018-mai-25/limite-penal-criterios-validade-vasculhar-celular-whatsapp-preso) que falar em autorização pessoal do indiciado ou acusado direcionada à autoridade policial, somente é possível em uma situação. Se o investigado solto, se dirige voluntariamente e na companhia do seu defensor, à autoridade policial e autoriza o acesso às mensagens. Quando preso ou detido, "inexiste condições de validar o assentimento dado o contexto fático manifestamente hostil", configurando o denominado constrangimento ambiental.

[306] CHIRINO SANCHEZ, Alfredo. ***Proteccion de datos y moderno processo penal aspectos constitucionales y legales.*** Op. cit. p, 25.

alcance do tratamento e acesso a tais dados. E nesta ocasião, para Chirino Sanchez, não é suficiente dizer que os dados que se pretende acessar são adequados para os objetivos da investigação, mas principalmente se o acesso a tais dados se percebe como necessário para tanto. Ou seja, se de fato é o único caminho possível para se atingir o que se pretende[307].

Salt, em linha semelhante, adverte que pelo desafio estabelecido a partir da mutação do conceito tradicional da intimidade e privacidade, há que se ter uma reforma legislativa para regulamentar as novas técnicas de persecução penal. Não basta uma construção conceitual a partir de decisões jurisprudenciais, tão pouco a regulamentação de modo análogo às metodologias investigativas já existentes. Uma nova regulação se faz necessária principalmente por possibilitar a diferenciação entre o "nível de proteção necessário para a intervenção do conteúdo das comunicações eletrônicas" daquele nível de proteção necessário para "a obtenção de dados de tráfego ou de ordem de armazenamento de algum dado eletrônico"[308]. Toda nova função tecnológica voltada para a colheita da prova penal merece peculiar atenção, pois são graves os efeitos decorrentes de sua utilização sem o devido procedimento formal.

Em contrapartida, tem-se que as tecnologias de informação e comunicação e seus respectivos avanços, cujos efeitos são percebidos no entorno de tudo, evoluem de modo exponencial quando comparados aos avanços legislativos necessários para sua regulamentação[309].

Fugir das dificuldades para não enfrentá-las é uma alternativa inadequada, principalmente porque devido aos desenvolvimentos tecnológicos relativos aos registros de comportamentos individuais, tendencialmente se busca a exibição direta destes comportamentos em substituição à reconstrução processual probatória devida[310]. Ou seja, a exibição comportamental delitiva – em um cenário de evidência[311] por vezes conflituoso com

---

[307] CHIRINO SANCHEZ, Alfredo. ***Proteccion de datos y moderno processo penal aspectos constitucionales y legales.*** Op. cit. p, 26.

[308] SALT, Marcos G. ***Tecnologia informática: un nuevo desafío para el Derecho Procesal Penal?***. Op. cit. p, 4. Tradução livre "*En este tema, ségun entiendo, tampoco es conveniente la aplicación analógica de las normas vigentes ni es suficiente la construcción jurisprudencial de nuestro máximo tribunal en la interpretación de la garantía en su sentido tradicional. Antes bien, es conveniente un análisis de cada un de estas nuevas herramientas tomando en consideración para la regulación de las salvaguardas necesarias su potencial de afectación del derecho a la intimidad […]. Así, por ejemplo es posible diferenciar el nivel de protección necesario para la intervención del contenido de comunicaciones electrónicas del necesario para la obtención de datos de tráfico o la orden de aseguramiento de algún dato electrónico*".

[309] No mesmo sentido ORTIZ PRADILLO, Juan Carlos. ***Informática y derechos fundamentales: hacia un derecho fundamental a la confidencialidad e integridad de los equipos informáticos.*** Op. cit.

[310] GARIBALDI, Gustavo E. L. ***Las modernas tecnologías de control y de investigación del delito: su incidencia en el derecho penal y los principios constitucionales.*** Op. cit. p, 98.

[311] Evidência aqui no sentido empregado por CUNHA MARTINS, Rui. **O ponto cego do direito.** Op. cit.

a proteção principiológica do *nemo tenetur* – em detrimento da construção probatória em contraditório processual.

Neste sentido, Garibaldi[312] ressalta que a não regulação é a pior opção, demonstra uma renúncia de toda fixação de limites e marcos aceitáveis de utilização destas novas tecnologias, o que é um erro inaceitável do Estado de Direito. Segundo o autor, o vazio legislativo tende a ser preenchido por intenções dos tribunais que se mostram infrutíferas. Conforme Salt[313], o vazio é preenchido pela obtenção ou incorporação destas "provas" penais por meio do uso análogo de normas próprias da produção probatória tradicional e que nem sempre trazem uma solução adequada à aplicação referente a estas modernas provas.

Na Espanha, os mecanismos deste matiz se denominam "medidas de investigação tecnológica" e devem ser deferidas pela autoridade judiciária de maneira minimamente detalhada, a partir da solicitação do Ministério Público ou da autoridade policial. Como destaca Vegas Torres[314], o artigo 588 *bis* "b" da *Ley Enjuiciamiento Criminal*, dispõe que a solicitação deve fazer referência à (1º) descrição do fato objeto de investigação e a identidade do investigado ou de qualquer outro afetado pela medida, sempre que essas informações sejam conhecidas; (2º) à exposição detalhada das razões que justifiquem a necessidade da medida, atendendo aos princípios da especialidade, idoneidade, excepcionalidade, necessidade e proporcionalidade (Art. 588 *bis* "a"), assim como os indícios de "criminalidade" notados durante a investigação, anteriores à solicitação da autorização das referidas medidas; (3º) aos dados de identificação do investigado ou acusado e, nesse caso, dos meios de comunicação empregados que permitem a execução da medida; (4º) à extensão da medida com especificação de seu conteúdo; (5º) à unidade da Polícia investigativa à qual competirá a ingerência investigativa; (6º) à forma de execução da medida; (7º) à duração da medida solicitada; e por fim (8º) referir-se ao sujeito incumbido da obrigação de levar a cabo a medida[315].

---

[312] GARIBALDI, Gustavo E. L. ***Las modernas tecnologías de control y de investigación del delito: su incidencia en el derecho penal y los principios constitucionales.*** Op. cit. p, 103. "*Acordar regulaciones al uso de ciertas tecnologías que inciden en la vida social requiere controvérsia y acuerdo ético-jurídico. [...] La peor actitud frente a tal estado de cosas es la renuncia a toda regulacion, y reconocer el fenómeno como ilimitable em función de su velocidad de diversificación. Legitimar simplemente certa realidade y renunciar a toda fijación de límites y marcos aceptables de utilización sería uma claudificacíon inaceptable del Estado de derecho".*

[313] SALT, Marcos G. ***Tecnológia informática: un nuevo desafío para el Derecho Procesal Penal?***. Op. cit. p, 7.

[314] VEGAS TORRES, Jaime. ***Las medidas de investigación tecnológica*** *In:* CEDEÑO HERNAN, M. (Coord.). *Nuevas tecnologías y derechos fundamentales en el proceso.* Aranzadi, 2017. p, 10.

[315] ESPANHA. ***Real decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal.*** *Ministerio de Gracia y Justicia.* <BOE> núm. 260, de 17 de septiembre de 1882. Referencia: BOE-A-1882-6036. Disponível em: https://www.boe.es/buscar/pdf/1882/BOE-A-1882-6036-consolidado.pdf. Acesso em: 25 mai. 18.

Uma vez iniciado o processo, cabe aos agentes da investigação realizarem os procedimentos em estrito cumprimento ao mandado judicial. Apresenta-se um relato limitado produzido pela autoridade policial ao Juiz competente, capaz de permitir a este a tomada de decisão que valore a "conveniência" de adotar ou não, no exercício de suas funções como diretor da investigação, de oficio[316], as medidas mencionadas.

O rol de medidas de investigação tecnológica referidas pela legislação espanhola é composto pela interceptação das comunicações telefônicas e telemáticas, a captação e gravação de comunicações orais mediante a utilização de dispositivos eletrônicos, a utilização de dispositivos técnicos de seguimento, localização e captação de imagem, o registro de dispositivos de armazenamento massivo de informação e os registros remotos sobre equipamentos informáticos.

Em que pese o cumprimento da exigência de lei, embora se possa questioná-la como suficiente para levar a cabo ingerência estatal face aos dados informáticos (no contexto Espanhol), ainda assim, a crítica feita por Ortiz Pradillo[317] soa pertinente. Segundo o autor, as violações incidentes sobre os dispositivos eletrônicos decorrem da insuficiente proteção destes dispositivos sobre a luz de uma proteção constitucional de direitos fundamentais, seja o direito à liberdade informática, ao segredo das comunicações, à inviolabilidade de domicílio, à intimidade.

Os limites investigativos dos órgãos de controle penal do Estado quanto ao exame de telefones móveis não podem ser estendidos aos demais equipamentos informáticos e dispositivos eletrônicos. Mesmo que os atuais *smartphones* possuam ao mesmo tempo funções tradicionais de telefonia móvel e os mais modernos dispositivos informáticos, o autor[318] não vislumbra a possibilidade do preenchimento dos requisitos para o desdobramento de investigações policiais que incidem sob dados armazenados em dispositivos informáticos.

Como requisitos trazidos por Ortiz Pradillo[319] tem-se a necessária existência de uma suficiente e específica previsão legal, a constituição de tais práticas investigativas como intervenções leves na intimidade das pessoas, a existência de razões de urgência e necessidade

---

[316] A atuação de ofício pelo julgador é matéria de suma importância para o processo penal, principalmente quando fundado em bases do sistema acusatório, neste ponto, ressalva-se e concorda-se com as críticas feitas à tal oficialidade, bem como sua violação a preceitos de imparcialidade e ao desenvolvimento de "quadros mentais paranoicos" pelo julgador.

[317] ORTIZ PRADILLO, Juan Carlos. ***Informática y derechos fundamentales: hacia un derecho fundamental a la confidencialidad e integridad de los equipos informáticos.*** Op. cit. p, 73.

[318] ORTIZ PRADILLO, Juan Carlos. ***Informática y derechos fundamentales: hacia un derecho fundamental a la confidencialidad e integridad de los equipos informáticos.*** Op. cit. p, 74.

[319] ORTIZ PRADILLO, Juan Carlos. ***Informática y derechos fundamentales: hacia un derecho fundamental a la confidencialidad e integridad de los equipos informáticos.*** Op. cit. p, 74.

para a atuação policial nesta direção, bem como a realização da diligência sob o respeito ao princípio da proporcionalidade. Justifica-se pela argumentação de três aspectos. Em primeiro lugar, por não ser possível a equiparação entre tradicionais meios de comunicação ou equipamentos de armazenamento (cartas, papéis, agendas ou mochilas) que uma pessoa carrega consigo, com os atuais dispositivos eletrônicos portáteis que potencializam a quantidade e a diversidade de informações[320].

Não sem razão, argumenta o autor que por vezes as pessoas sentem que uma intervenção estatal sob seu domicílio físico pode ser menos lesiva a sua intimidade quando comparada às violações em computadores pessoais. Nos dispositivos digitais podem constar informações mais íntimas, confidenciais e reveladoras – guardadas em *bits* – da personalidade do usuário.

Em segundo, a preocupação do autor se volta para a integridade e confiabilidade dos documentos ou arquivos extraídos dos dispositivos. O manejo imprudente dos agentes investigadores podem alterar determinados dados e com isso acarretar inutilidade ao potencial material probatório[321]. Sinaliza o autor pela preferência da coleta do material e a garantia da integridade das provas para posterior perícia.

Por fim, em terceiro lugar, argumenta Ortiz Pradillo quanto ao risco que é legitimar atuações policiais a partir da alusão genérica a motivos de urgência e necessidade, tendo em vista a uma possível interpretação fraudulenta da legalidade. Ou seja, a urgência reclamada deve ser fundada a partir de situações com mais detalhes e exatidão, tais como o perigo à vida, a liberdade ou a integridade física das pessoas, ou ainda em se tratando de flagrante delito[322]. Ou seja, o critério de necessidade mais objetivo.

---

[320] Id. p, 77. "*Resultaría desproporcionado amparar tal registro bajo el clássico 'cacheo' o en la ocupación de objetos que se deriva de la detención policial. Por poner un ejemplo concreto, en una tarjeta de memoria de 8GB inserta en un telefono móvil 3G pueden almacenarse en formato electrónico libros que, impresos en papel, supondrían vários millones de páginas, o también puede contener, en fotografias, el equivalente a toda uma estantería llena de álbumes de fotos reveladas. […] Por ello, el acceso a la información contenida en cualquier dispositivo electronico o informático no puede ser considerado como una injerencia 'leve' en la esfera de la privacidad de las personas. Es más, hoy en día, u indivíduo puede considerar que su intimidad resulta menos afectada si registran su domicílio en vez de registrar el contenido de su ordenador personal, pues la información más íntima, confidencial y reveladora de su personalidad puede no estar guardada en cajones ni armarios, sino en chips, memorias USB y en el disco duro de su ordenador"*

[321] Id. p, 78. "*En los documentos 'en papel', la información contenida puede ser directamente percetible por los sentidos. En cambio, para acceder a la información digital, habrá que proceder a realizar determinadas operaciones (encendido del aparato, búsqueda de archivos, apertura de los mismos, descifrado de los misos, superación de contraseñas, etc.) que modifican, a su vez, las características de los datos. De ahí nuestra preferencia por garantizar la integridad de dichas pruebas mediante el oportuno aseguramiento de los objetos intervenidos y su posterior examen pericial con las debidas garantías legales".*

[322] Id. p, 79. "*Habría que delimitar con mayor detalle los supuestos en los que se entiende que existe tal urgencia, como por ejemplo, en aquellos casos en los que exista un peligro inminente para la vida, la liberdad o la integridad física de las personas, o cuando se trate de delitos flagrantes. De lo contrario, y sin el debido respaldo legal,*

São preocupações que, em maior ou menor medida, assolam a todos. Torre[323], a seu turno, afirma que existem dois requisitos fundamentais para prosseguir uma investigação informática. O primeiro é a "confiabilidade do método de tratamento dos dados", o segundo, refere-se à "verificabilidade da idoneidade do método". Isso porque a confiabilidade da prova digital no processo penal depende de uma complexa garantia que abarque tanto a originalidade do dado, em termos de conservação, como a cópia deste ao ponto de sua "genuinidade" e "não modificação". Tais resultados podem ser alcançados através de um protocolo procedimental metodologicamente guiado, cujo objetivo é a prevenção do risco de comprometer o resultado final.

Estes procedimentos são atualmente aprimorados pela *digital forensics science*, ou seja, decorrem de uma evolução e diversificação de serviços técnicos (*Computer Forensics*) desenvolvidos inicialmente pelo *FBI* com objetivos investigativos e jurídicos para o tratamento e análise dos resultados da Tecnologia da Informação (TI). Uma proposição que ampliava o manual de preservação das fontes de prova tradicionais da investigação criminal, mas que se expandiu a outros setores de negócios profissionais ou de entidades não governamentais no âmbito da produção de estudos sobre a coleta e o armazenamento de fontes de provas informatizadas em casos de violação da segurança[324].

Em linhas mais gerais traçadas por Britz[325], a *computer forensics* agrega mecanismos na investigação de crimes relacionados a computadores, adequadamente às disposições constitucionais e às leis de Direito Processual Penal. Protege-se a integridade daquilo que pode vir a servir de prova, mantendo sua cadeia de custódia.

A *Digital forensics*, portanto, volta sua atenção para os diversos setores de evolução tecnológica relacionados aos dados transportados em rede, tornando-se mais ampla e como ciência abarcando os ramos da *computer forensics, forensics data analysis, mobile devices forensics* e da *database forensics*[326].

---

corremos el riesgo de justificiar posibles fraudes y abusos en las garantías de los derechos fundamentales en aras de una falaz eficacia en la persecución criminal".

[323] TORRE, Marco. ***Indagini informatiche e proceso penale.*** *Università degli studi Firenze. Dottorado di ricerca in scienze giuridiche. Anni 2012/2015.* p, 35.

[324] GAMMAROTA, Antonio. ***Informatica forense e processo penale: la prova digitale tra innovazione normativa e incertezze giurisprudenziali.*** *Università di Bologna. Dottorato di ricerca in Diritto e nuove tecnologie.* 2016. p, 14 – 17.

[325] BRITZ, Marjie T. ***Computer forensics and cyber crime: na introduction.*** Clemson University. 3ª ed. 2013. p, 268 – 269. Um detalhe interessante exposto por Britz, é também da necessidade de assegurar que vírus ou *malwares* não sejam introduzidos no dispositivo objeto da investigação durante sua execução, de modo que também seja assegurada a integridade da prova ou daquilo que possa ser potencialmente uma prova.

[326] GAMMAROTA, Antonio. ***Informatica forense e processo penale: la prova digitale tra innovazione normativa e incertezze giurisprudenziali.*** Op. cit. p, 17. Pela limitação do espaço, não abordar-se-á todas estas formas "periciais", contudo é importante distingui-las. A *Forensics data analysis* volta-se à análise específica de

É uma ciência capaz de analisar e tratar todos os arquivos relevantes para a investigação dos dispositivos-alvos, desde os arquivos abertos, os ocultos, protegidos por senha, criptografados e alguns outros arquivos ainda que já excluídos. Segundo Britz, a partir da análise do sistema investigado é possível alcançar uma amplitude de informações como a estrutura dos arquivos, dados e informações de autoria, bem como o resgistro de qualquer manipulação de dados e qualquer outra manipulação de informações que possam ser relevantes[327].

Nas palavras de Torre, a *digital forensics* é uma ciência que possui como objeto de estudo o tratamento dos dados digitais para fins judiciais de modo a salvaguardar os "valores processuais" de determinado fato com o objetivo de assegurar a representação deste fato como "prova". Neste aspecto, a investigação deve obedecer a etapas que consistem desde o reconhecimento e individualização da fonte probatória, perpassando pela aquisição e conservação do dado, a análise forense e por fim, a apresentação de resultados[328].

3.1.3 A permanente negligência metodológica e procedimental de Investigação e Obtenção da Prova Digital na legislação brasileira

A influência tecnológica incide na legislação pátria desde a década de 1990 e teve um avanço significativo até então. Contudo o que se nota é a ausência do tratamento adequado às peculiaridades da prova penal decorrente das coletas nas investigações tecnológicas. No ano de 1996 por meio da Lei nº. 9.296 – cujo objetivo era a regulamentação do inciso XII, parte final, do artigo 5º da Constituição Federal de 1988[329] –, inaugura-se uma nova forma de investigação oculta, tanto por meio das interceptação de comunicações telefônicas, como comunicações em sistemas informática e telemática, para a prova em investigação criminal e em instrução processual penal.

De acordo com a interpretação de Badaró[330], o dispositivo constitucional atingido pela Lei nº 9.296/96 trata de quatro formas de comunicação, sendo-as comunicação postal ou

---

dados; a *Mobile devices forensics* atende aos dados de dispositivos de aparelho móveis de telefonia; a *Database forensics* atende a análise de bases de dados.

[327] BRITZ, Marjie T. ***Computer forensics and cyber crime: na introduction.*** Op. cit. p, 269.

[328] TORRE, Marco. ***Indagini informatiche e proceso penale.*** Op. cit. p, 37. A abordagem mais detalhada de todas as etapas proposta pelo autor terá espaço próprio quando se tratar da preservação da cadeia de custódia da prova.

[329] BRASIL, Art. 5º, XII, da CF: 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.

[330] BADARÓ, Gustavo Henrique. **Interceptação de comunicações telefônicas e telemáticas: limites ante o avanço da tecnologia.** *In:* J. Corrêa de Lima e Rubens R. R. Casara (coords.), Temas para uma Perspectiva Crítica do Direito, Rio de Janeiro: Lumen Juris, 2010. p, 4.

de correspondência, comunicação telegráfica, comunicação de dados e a comunicação telefônica. Entretanto, não há nenhuma menção no texto da lei federal que verse sobre a recolha da prova decorrente da interceptação requisitada. A limitação legislativa discorre tão somente quanto à possibilidade da autoridade policial requisitar serviços e pessoal técnico especializado às concessionárias de serviço público, quando dos procedimentos de interceptação[331].

Como observa Giacomolli[332], pouco se investiga e se discorre acerca da confiabilidade dos mecanismos de interceptação, reclamada evidentemente pela norma constitucional que impõe "o registro fiel do que foi interceptado, para que tudo isso seja escutado em contraditório e após, com a mesma garantia, transcrito o que interessa aos fatos".

Em um salto de uma década o legislador brasileiro se mantém negligente. A atenção legislativa se volta ao emprego do meio eletrônico na tramitação de processos judiciais, comunicação de atos e transmissão de peças processuais conforme a Lei nº. 11.419/06. Todavia, não se avança quanto à temática relativa às provas penais eletrônica, informática ou digital, exceto quando da inclusão de conteúdos probatórios via documentação digital de atos processuais[333].

Em tramitação, o Projeto de Lei do Senado de nº 330/2013 dispõe sobre a proteção, o tratamento e o uso dos dados das pessoas naturais e jurídicas de direito público ou privado. O texto legislativo traz algumas definições conceituais importantes, atribuindo a dado pessoal a concepção de toda informação, de qualquer natureza e independentemente do respectivo suporte, passível de ser armazenada, processada ou transmitida, relativa a pessoas identificadas ou identificáveis.

Quanto ao conceito de tratamento de dados pessoais, define o texto normativo como sendo qualquer operação ou conjunto de operações, em um ou mais bancos de dados, independentemente do mecanismo utilizado. De acordo com o texto original do PLS, Artigo 3º, § 2º, configura-se tratamento de dados pessoais a pesquisa, o recolhimento, o registro, a organização, a classificação, a comparação, a valoração, a conservação, a modificação, a adaptação, a alteração, a recuperação, a consulta, a utilização, a transferência, a transmissão, por difusão ou por qualquer outra forma de comunicação, a interconexão, o bloqueio, o descarte e a destruição da informação.

---

[331] BRASIL, Art.7º, Lei nº 9.296/96 - Para os procedimentos de interceptação de que trata esta Lei, a autoridade policial poderá requisitar serviços e técnicos especializados às concessionárias de serviço público.
[332] GIACOMOLLI, Nereu José. **A fase preliminar do processo penal.** Op. cit. p, 141.
[333] PRADO, Geraldo. **A produção da prova penal e as novas tecnologias: o caso brasileiro.** 2015. Disponível em: http://emporiododireito.com.br/a-producao-da-prova-penal-e-as-novas-tecnologias-o-caso-brasileiro-por-geraldo-prado/. Acesso em jun 2017.

Muito embora seu artigo 6º preceitue que o tratamento de dados pessoais para fins de segurança pública, investigação criminal ou instrução penal, administrativa ou tributária poderá ser feito exclusivamente pelos órgãos da administração pública direta ou pessoa jurídica de direito público, conforme a competência prevista em lei (inciso I), por motivos de prevenção ou repressão de infração penal, administrativa ou tributária (inciso II), há uma lacuna significativa quanto aos procedimentos formais específicos para tal tratamento, de modo que mesmo pretendendo proteger dados pessoais de acessos e tratamentos indesejados não limita a atuação dos próprios órgãos de controle do Estado no tratamento de dados individuais, e deste modo se mostra desde seu nascedouro ineficiente na proteção que pretende.

Não é preciso dizer que sem um procedimento metodologicamente guiado para o tratamento destes dados, e assim o estabelecimento de um padrão procedimental, não há que se falar em confiabilidade e integridade do dado que se julga fundamental à elucidação de um caso penal. O artigo 6º, também prevê a hipótese de compartilhamento de informações para fins de segurança do Estado e da sociedade (inciso III) e a hipótese do tratamento de dados para atender aos termos de acordo, tratado ou convenção internacional de que o Estado brasileiro seja parte (inciso IV).

Além do mais, o Artigo 9º, § 1º, desconsidera uma série de direitos básicos do titular de dados (Artigo 7º), bem como deveres no tratamento de dados pessoais, relativos ao proprietário e ao gestor de banco de dados (Artigo 8º), quando o tratamento de dados por bancos de dados públicos atender ao auxílio na atividade de segurança nacional ou pública, investigação criminal ou instrução processual penal[334].

O Projeto Lei também versa sobre a interconexão de dados, incluída a interconexão internacional quando houver tratado ou acordo internacional autorizativo que o Brasil seja parte, ou promessa de reciprocidade, e tiver por objetivo coibir crime organizado transnacional,

[334]Especificadamente os direitos e deveres não aplicados: **Art. 7º -** São direitos básicos do titular de dados: II – o acesso à origem e ao conteúdo de dados pessoais coletados e tratados em banco de dados; III – a ciência prévia, e por escrito, como requisito à inclusão de informações pessoais em banco de dados; IV – a retificação, a título gratuito, de dados pessoais inexatos, incompletos, omissos, inverídicos ou desatualizados; V – o consentimento prévio como requisito à coleta e ao tratamento de dados pessoais sensíveis, bem como à interconexão internacional de dados realizada por banco de dados privado (art. 10); VI – o cancelamento, a título gratuito, de dados que deixarem de ser necessários à consecução da finalidade para a qual foram coletados; VIII – a exclusão ou a dissociação gratuitas de dados pessoais sensíveis inseridos em banco de dados, se manifesto o interesse; **Art. 8º -** Constituem deveres do proprietário e do gestor de banco de dados, no tratamento de dados pessoais: I – informar aos titulares de dados pessoais: a) a inclusão e o tratamento de suas informações; b) a extensão de seus direitos; c) a finalidade da coleta; d) as categorias de usuários da informação; e) a identidade do proprietário e do gestor do banco de dados; as quais foram coletados; VI – não inserir dados oriundos de fontes acessíveis ao público sem que prévia ciência seja conferida ao titular dos dados; VII – não inserir dados pessoais sensíveis sem o consentimento prévio e expresso do titular dos dados; VIII – apreciar, no prazo máximo de dez dias, a contar da solicitação, pedido de retificação, oposição, cancelamento e exclusão de dados.

tráfico de seres humanos, crime de corrupção, terrorismo, financiamento ao terrorismo, narcotráfico, lavagem de dinheiro, extorsão mediante sequestro ou crimes contra o sistema financeiro nacional, desde que haja (I) expressa solicitação de autoridade competente estrangeira, (II) existência de pedido fundado na necessidade de investigação policial, instrução ou persecução criminal, (III) segurança assumida pelo Estado ou organismo internacional destinatário de nível adequado de proteção dos dados e informações.

As disposições do PLS 330/2013 permanecem silentes quanto ao procedimento protocolizado e metodologicamente guiado para que vislumbre a confiança necessária reclamada pelo texto constitucional, mesmo após parecer da comissão de ciência, tecnologia, inovação, comunicação e informática do Senado Federal que propôs algumas modificações ao texto original.

Por sua vez, a Lei de nº 12.850/2013 que define as chamadas organizações criminosas segue a tendência atual quanto ao acesso de dados, principalmente quanto aos meios ocultos de investigação. Estabelece em seu artigo 3º um rol de meios de obtenção de prova, dentre os quais se destacam – em relação ao tema aqui tratado – a captação ambiental de sinais eletromagnéticos, ópticos ou acústicos, acesso a registros de ligações telefônicas e telemáticas, a dados cadastrais constantes de bancos de dados públicos ou privados, interceptação de comunicações telefônicas e telemáticas.

A Lei que define organização criminosa e regulamenta os métodos de investigação e obtenção de provas consoantes aos crimes praticados, tem espaço dedicado exclusivamente à manutenção do sigilo sobre a investigação. O legislador regulamentou a necessidade de manter o sigilo sobre a capacidade investigatória, dispensando licitação para contratação de serviços técnicos especializados, aquisição ou locação de equipamentos destinados à polícia judiciária para o rastreamento e obtenção de provas referentes à captação ambiental e sinais eletromagnéticos, ópticos ou acústicos, bem como para a interceptação de comunicação telefônica e telemática.

Contudo, na oportunidade não se dispôs sobre quais exigências serão necessárias para que se eleja equipamentos ou instrumentos para a obtenção destas provas como "confiáveis". A lacuna existente possibilita a utilização de equipamentos comerciais inapropriados, desde *hardwares* a *softwares* de comercialização aberta ao público em geral, cuja confiabilidade não preenche a exigência constitucional, principalmente quanto à possibilidade de se verificar a idoneidade da coleta probatória.

No ano de 2014, por meio da Lei nº 12.965, comumente chamada de Marco Civil da Internet, na qual estabelece princípios, garantias, direitos e deveres para o uso da Internet no

Brasil, trouxe a possibilidade da parte processual interessada, com propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que fosse ordenado ao responsável pelo armazenamento de dados, o fornecimento de registros de conexão ou de registros de acesso a aplicação de internet.

Pela referida Lei, Art. 5º, inciso VI e VIII, entende-se por registro de conexão, o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados. Também trata o registro de acesso a aplicações de internet, como o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP.

Nesta linha, o Projeto de Lei nº 5.276/2016 que dispõe sobre o tratamento e a proteção de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural, cujo objetivo é proteger os direitos fundamentais de liberdade e de privacidade, excetua sua aplicabilidade ao tratamento de dados realizado para fins exclusivos de segurança pública, de defesa nacional, de segurança do Estado ou de atividades de investigação e repressão de infrações penais (Art. 4º, III). Ainda, o § 1º do artigo 4º dispõe sobre a necessidade de legislação específica para o tratamento de dados pessoais atinentes ao inciso III, devendo ser observados os princípios gerais de proteção e os direitos do titular dos dados. Na sequência, por força do § 2º fica vedado às pessoas de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, o tratamento dos dados pessoais para fins de segurança pública, de defesa nacional e de segurança do Estado ou de atividades de investigação e repressão de infração penal.

Cumpre informar que o Projeto de Lei nº 8.045/2010, que versa sobre o novo Código de Processo Penal, em seu artigo 241 e seguintes, prevê o acesso a informações sigilosas para a utilização como prova no processo penal quando autorizado por ordem judicial. Em sede de investigação preliminar caberá à autoridade policial ou ao Ministério Público formular o pedido para o acesso às informações, e no curso do processo penal, caberá a qualquer das partes a formulação do pedido ao juiz do caso.

Em ambas as hipóteses deve ser indicado (I) a existência de indícios razoáveis da prática de infração penal que admita a providência, (II) a necessidade da medida, diante da impossibilidade de obtenção da prova por outros meios, e (III) a pertinência e a relevância das informações pretendidas para o esclarecimento dos fatos. Contudo, não há menção concreta sobre qual seria a natureza das “informações sigilosas” as quais se terá acesso caso deferido o pedido pelo Poder judiciário.

Ademais, quanto a obtenção de dados informáticos, o artigo 245 e seguintes, traz a possibilidade de interceptação do fluxo de comunicação em sistemas de informática e telemática para fins de investigação criminal ou instrução processual penal. O artigo 246, §3º, inciso II preceitua que as disposições da seção sobre interceptação das comunicações telefônicas também serão aplicadas à interceptação de outras formas de comunicação por transmissão de dados, sinais, sons ou imagens. Logo, a seção abarca toda forma de comunicação e transmissão de dados, desde o registro de dados estáticos, referentes à origem, destino, data e duração. O tratamento uno não observa as especificidades que cada metodologia exige.

O artigo 249 dispõe sobre o pedido de interceptação a ser formulado ao Juiz competente. Proceder-se-á a interceptação mediante requerimento do Ministério Público ou da defesa, ou por meio de representação do delegado de polícia, devendo constar (I) a descrição precisa dos fatos investigados, (II) a indicação de indícios suficientes de materialidade do crime investigado, (III) a qualificação do investigado ou acusado, ou esclarecimento pelos quais se possa identifica-lo, (IV) a demonstração da estrita necessidade da interceptação e de que informações essenciais à investigação ou instrução processual não poderiam ser obtidas por outros meios. Neste último, salvo melhor interpretação é possível notar a estrita e necessária ligação (nexo causal) entre o ilícito investigado e o elemento de prova a ser alcançado, tendo liame essencial com meio de obtenção de prova a ser executado.

Quanto ao cumprimento da ordem judicial que decreta a interceptação, o artigo 254 prevê que caberá a prestadora de serviços de telecomunicação a disponibilização, gratuita, de recursos e meios tecnológicos necessários à interceptação, indicando ao juiz o nome do profissional que prestará tal colaboração. Neste aspecto, não há nenhuma menção aos requisitos alusivos ao meio tecnológico para prosseguir com a interceptação, seja telefônica ou de dados, não sendo possível vislumbrar a necessária confiabilidade do meio a ser empregado e, consequentemente, do material probatório obtido.

O material produzido após as operações técnicas deve ser encaminhado ao Juiz acompanhado de auto circunstanciado, que detalhará todas as operações realizadas (art. 256). Não há, entretanto, nenhuma menção ao protocolo metodológico da coleta de dados interceptados. O legislador penal, na oportunidade, não disponibilizou (ainda) nenhuma garantia de segurança à cadeia de procedimentos para uma produção de prova válida.

Ademais, também não se faz menção acerca das peculiaridades da prova penal técnica a ser produzida, considerando-a em linhas gerais, seja relacionada a interceptação telefônica, seja a produção probatória decorrente de sistemas de informática e telemática, seja

àquela relacionada a obtenção de dados. Discorrer sobre a prova penal digital observando suas especificidades é objeto da próxima seção da pesquisa.

3.2 Prova Penal e(m) tecnologia científica

Antes de avançar no estudo e com o intuito de sanar algumas lacunas que por ventura possam ter sido originadas até aqui, faz-se fundamental discorrer sobre as controversas e variadas noções acerca da terminologia "prova" no Direito Processual Penal brasileiro. Não se pretende esmiuçar todo o tema, tão somente se busca definir alguns termos demasiadamente caros ao objeto principal da pesquisa.

Também se buscará definir os diferentes institutos da prova irrepetível, prova cautelar e prova antecipada, tendo em vista que cada um destes institutos processuais corresponde a uma natureza jurídica específica referente ao material probatório. De tal modo que o tratamento processual dado também deve ser singularizado. Somente após, será possível expor a prova digital como produto recolhido, preservado e analisado através de um método guiado cientificamente que vise a manutenção de sua confiabilidade e integralidade.

3.2.1 Prova Penal: Definição de categorias

Recordar a partir de Carnelutti[335] é fundamental para o clarificar do tema. Dirá o autor que o processo penal busca compreender a ocorrência ou não de determinado fato. Portanto, sobre fato é preciso se entender como um pedaço da história; e esta, por sua vez, uma trajetória que se percorre deste o nascimento até a morte dos homens e da humanidade. Logo o fato é um pedaço do percurso. Carnelutti ensina que o crime, por sua vez, é um pedaço do percurso histórico no qual aquele que o pratica trata de destruir seus rastros[336]. Sobre "Fato", dirá Gonzalez Lagier[337], com o auxílio de Russell, que se trata daquilo que faz uma proposição verdadeira ou falsa. Pois bem, as provas – sob este aspecto – servem precisamente para reconstruir um pedaço da história, a história ou a existência do fato, para atestar uma proposição como verdadeira ou falsa.

---

[335] CARNELUTTI, Francesco. ***Las miserias del proceso penal.*** Buenos Aires: *Ediciones juridicas europa-america*, 1959. p, 71 – 73.
[336] CARNELUTTI, Francesco. ***Las miserias del proceso penal.*** Op. cit. p, 71 – 73. "*el delito es um trozo de camino, del cual quien lo ha recorrido trata de destruir las huellas*".
[337] GONZALEZ LAGIER, Daniel. ***Hechos y argumentos (racionalidad epistemológica y prueba de los hechos en el proceso penal* (I)**. *Jueces para la democracia.* Madrid: vol. 46, marco/2003, pp. 17-26.

Quando Carnelutti[338] trata sobre a prova penal o faz desconstruindo a ideia da certeza como resultado processual. Dirá o autor que a certeza é a existência do presente, e este somente o é enquanto percepção sob os sentidos do observador. A existência de algo não é o "ser" deste algo mas tão somente "parte do ser" alcançado pelos sentidos ou pelo pensamento. Logo a certeza, a partir de Carnelutti, é uma mera percepção. Não existe certeza mas um determinado grau de certeza ao qual se denominará de probabilidade.

É a prova como fundamento do processo que permite alcançar este alto grau de probabilidade, comumente descrito como certeza. Portanto, é a prova que proporciona ao julgador a obtenção de experiências que o capacita ao julgamento[339].

Neste sentido, dirá Tornaghi que a atividade probatória tem como finalidade principal formar a convicção do juiz, ou seja, "a demonstração da veracidade ou falsidade da imputação feita ao réu e das circunstâncias que possam influir no julgamento da responsabilidade e da periculosidade, na individualização das penas e na aplicação das medidas de segurança que se faz a prova"[340].

Entretanto, conforme aponta Ferrer Beltran[341], a dicotomia entre verdade material ou verdade formal e sua relação com a prova penal, ou nos termos acima, a veracidade ou falsidade dos fatos, por vezes se apresenta inócua. Se verdade somente pode ser verdade enquanto una e total, e certeza somente será a partir do grau de probabilidade, logo a tomada de decisão exige um grau ou uma quantidade de elementos probatórios capazes de motivarem a decisão racionalmente no sentido de aceitar uma proposição como provada ou não.

Dirá o autor que "para que possa se dizer que uma proposição está provada é necessário e suficiente que se disponha de elementos probatórios suficientes em seu favor, que fazem aceitável essa proposição como descrição do caso fático"[342]. Este portanto, é o critério máximo a ser observado para enfrentar o problema referente à irracionalidade da decisão judicial, a quantidade de elementos probatórios que atestem um enunciado probatório relacionando-o com o enunciado fático.

O argumentação perpassa pela desvinculação ideal do processo penal com o conceito de averiguação da verdade ou, em certa medida, de alguma relação guardada entre a

---

[338] CARNELUTTI, Francesco. ***Lecciones sobre el proceso penal Vol. I.*** Ediciones Jurídicas Europa-America. Bosch y Cia. Editores Chile 2970, Buenos Aires, 1950. p, 288. "*Como la certeza es captada inmediatamente por virtud de los sentidos, la probabilidad es existencia captada, mediatamente, por virtud del juicio*".
[339] CARNELUTTI, Francesco. ***Lecciones sobre el proceso penal Vol. I.*** Op. cit. p, 290.
[340] TORNAGHI, Hélio. **Compêndio de processo penal: tomo II.** Rio de Janeiro, 1967. p, 678 - 679.
[341] FERRER BELTRAN, Jordi. ***Motivacion y racionalidad de la prueba.*** Editora y Libreria Jurídica Grijley. 1 ed., 2016. p, 191 – 196.
[342] FERRER BELTRAN, Jordi. ***Motivacion y racionalidad de la prueba.*** Op.cit. p, 197.

prova e a verdade que se busca provar, ou a verdade dos fatos. Ferrer Beltran[343], sob este aspecto, afirma então parecer óbvio que a decisão judicial para a qual os elementos probatórios são destinados deve se ater aos enunciados fáticos formulados pelas partes no processo. O autor elabora uma distinção baseada em duas máximas "estar provado" ou "ser tido por provado" que possibilita sustar as distorções entre o que se entendia por "ser verdadeiro", "ser tido por verdadeiro" ou "aceito como verdadeiro". O elemento chave, portanto, dirá o autor é a suficiência dos elementos probatórios.

Contudo, não se pode dizer que a (alta ou baixa) quantidade de *elementos* probatórios é fundamental para que se tenha como provado (ou não) o fato que se alega, tão pouco que a probabilidade à qual se refere deriva de cálculos matemáticos. Conforme Haack[344], a partir da epistemologia se verifica que os elementos probatórios que se mostram suficientes e são capazes de sustentar a conclusão sobre o caso em concreto decorrem de regras acerca da carga probatória e dos estándares de prova, ou seja, as regras de quem está obrigado a desenvolver e como desenvolver a atividade probatória e o grau ou o nível de prova que deve se satisfazer ou alcançar nos processos penais.

Feito o esclarecimento inicial, partir-se-á para a definição de categorias acerca da prova. Primeiramente, é preciso dizer que o termo "prova" no processo penal brasileiro e no estudo do processo penal global abarca diversos sentidos. Isto porque tanto a legislação como a doutrina processual penal traz atrelado ao significado de "prova" o que denomina-se por *fontes* de prova, *meios* de prova, *elementos* de prova e *resultados* de prova.

Gomes Filho[345] afirma que a linguagem processual emprega três acepções ou sentidos ao termo prova. O primeiro sentido é atribuído à demonstração de um fato tido como processualmente verdadeiro a partir de dados de conhecimentos idôneos obtidos por meio de procedimentos racionais. A demonstração como um estopim para provar, um suporte que constrói a prova com a intencionalidade de obter a convicção de seu destinatário[346].

O segundo sentido se refere a uma experimentação, uma pesquisa feita na fase de instrução probatória que se destina a recolher e analisar os elementos necessários para confirmar ou refutar as hipóteses sobre os fatos. A experimentação se relaciona com a busca do tipo de

---

[343] FERRER BELTRAN, Jordi. ***Motivacion y racionalidad de la prueba.*** Op.cit. p, 198 - 199. "*Parece razonable sostener que el éxito de la intervención de las partes en la fase de prueba, aportando médios de prueba, etc., se produce si logran convencer al juez de que su "descripción" de los hechos (su historia, si se prefiere) es verdadera. Con ello, estarán en buenas condiciones de ganar el caso*".

[344] HAACK, Susan. ***El probabilismo jurídico: una disensión epistemológica.*** *In*: VAZQUEZ, Carmen. *Estándares de prueba y prueba científica: ensayos de epistemologia jurídica.* Marcial Pons, 2013. p, 68 – 69.

[345] GOMES FILHO, Antônio Magalhães. **Notas sobre a terminologia da prova (reflexos no processo penal brasileiro).** Op. cit. p, 303 – 304.

[346] CUNHA MARTINS, Rui. **O ponto cego do direito.** Op. cit. p, 5.

prova que se julga capaz de demonstrar a existência do *thema probandum*. Como afirma Prado[347], antes mesmo de obter os resultados práticos decorrentes do tipo de prova que se pretende incorporar no processo, se tem uma consideração psicológica relacionada aos possíveis rumos que a processo pode tomar a partir da juntada daquele tipo de prova. É fazer um exercício mental no qual se estabelece um objetivo pretendido e como se pretende construir o percurso para alcançá-lo. A experimentação faz parte da construção deste percurso.

Por fim, como terceiro sentido atrelado ao termo "prova" no âmbito processual, tem-se a ideia de desafio ou obstáculo a ser superado, denominado por Gomes Filho de ônus probatório[348], cuja melhor definição em âmbito de processo penal, e aqui adotada, atrela-se à noção de carga probatória[349].

Pois bem, se um dos sentidos dados à terminologia "Prova" refere-se à carga de provar o fato alegado (enunciado fático) pela acusação (na completude de seus elementos) e à oportunidade dada a defesa de provar sua hipótese, em sentido adverso é impossível dizer que se pode provar o fato a partir do protagonismo da atividade judicial. A atividade das partes impõe a inércia jurisdicional.

Conforme Cordero[350] tal inércia é consequência extrema decorrente do princípio acusatório, que impõe ao julgador a posição estática de espectador imparcial, ou seja a prioridade é estabelecer, a partir de uma atividade dialética das partes, um procedimento concebido no levantamento de hipóteses e nos contributos das provas trazidas tanto pela acusação quanto pela defesa. Neste prisma, a atividade probatória com atuação das partes somente deveria alcançar o julgador pelo (e a partir do) contraditório que incide nos *meios* de provas ou meios de provar os fatos, cuja função é inserir no processo as *fontes* de provas.

Não por outro motivo que Prado afirma: "quem procura sabe ao certo o que pretende encontrar e isso, em termos de processo penal condenatório, representa uma inclinação ou

---

[347] PRADO, Geraldo. **Sistema acusatório: a conformidade constitucional das leis processuais penais.** 3ª ed. Editora Lumen juris: Rio de Janeiro, 2005. p, 218.

[348] GOMES FILHO, Antônio Magalhães. **Notas sobre a terminologia da prova (reflexos no processo penal brasileiro).** Op. cit. p, 306.

[349] Carga probatória e ônus da prova não se confundem e não se aproximam. Como define Lopes Jr. carga no processo penal é um conceito vinculado à noção de unilateralidade, logo não é passível de distribuição, mas sim de atribuição. Logo não há que se falar em carga para a defesa, mas em sede de processo penal tão somente se terá carga probatória atribuída ao acusador, devendo este se liberar desta carga (LOPES JR. Aury. **Fundamentos do processo penal: introdução crítica.** 2 ed. São Paulo: Saraiva, 2016. p, 201). Sobre a carga da prova, acentua Goldschmidt que esta se apresenta sob os aspectos formal e material, cujo primeiro regula a relação entre as partes e o juiz, dispensando este de informar-se de ofício e de praticar as diligências necessárias a fim de averiguar a verdade. Quanto ao aspecto material da carga probatória, regula a relação mútua das partes designando a parte à qual incumbe a prova de um fato determinado (GOLDSCHMIDT, James. ***Principios generales del proceso Vol. II.*** Ediciones Jurídicas Europa-America, Buenos Aires, 1961, 88 – 89).

[350] CORDERO, Franco. ***Tre studi sulle prove penale.*** Op. cit. p, 200.

tendência perigosamente comprometedora da imparcialidade do julgador"[351]. É dizer ao menos duas premissas, a primeira afeta àquele que recai a carga de provar a acusação, cuja parcialidade lhe é inerente e por conta disto, neste primeiro ponto, não compromete a imparcialidade daquele que julga; a segunda, volta-se ao procedimento pelo qual – em um processo penal acusatório – se submete esta introdução da informação decorrente da *fonte* de prova nos autos processuais.

Tendo em vista a introjeção desta informação pelo seu destinatário (ou seja a pretendida absorção da informação probatória pelo julgador) e sendo a introdução da *fonte* de prova ao processo decorrente da atividade daquele que quer provar (ou seja a adoção de *meios* de prova em um contexto construído pela narratividade da parte), por evidente que a informação trazida ao processo, não pode alcançar o julgador sem antes ser submetida ao contraditório[352], sob pena da tomada de decisão, ou a adesão por uma das hipóteses levantadas pelas partes, ocorrer bem antes do momento oportuno para o pronunciamento judicial. É, portanto, a imparcialidade da tomada de decisão que se pretende proteger com o exercício do contraditório, bem como a promoção da originalidade cognitiva judicial.

Até que a parcialidade do *meio* de prova seja confrontada, mediante contraditório, para a extração de uma informação de relevância ao processo, este não pode(ria) alcançar o julgador. O contraditório portanto é o instituto processual que permite maior qualidade à prova. Não por acaso é que Gomes Filho[353] afirma que é justamente o antagonismo entre as falas dos interessados no provimento final que garante a imparcialidade do juiz. O autor ressalva que "sem que o diálogo entre as partes anteceda ao pronunciamento estatal, a decisão corre o risco de ser unilateral, ilegítima e injusta; poderá ser um ato de autoridade, jamais de verdadeira justiça".

Por óbvio que a imparcialidade judicial se esvai quando da adesão do julgador a uma das hipóteses (acusatória ou defensiva) fundadas nos *elementos* de prova colhidos. Mas para que se extraia *elementos* probatórios das *fontes* de provas trazidas aos autos, exige-se o contraditório como opção de civilidade e reconhecimento da dignidade do acusado[354]. Não é demais (re)afirmar que a prática do contraditório evita o contágio do julgador por uma informação sem qualidade probatória necessária.

---

[351] PRADO, Geraldo. **Sistema acusatório: a conformidade constitucional das leis processuais penais.** Op. cit. p, 218.

[352] Neste mesmo sentido LOPES JR. Aury. **Direito processual penal**. Op. cit. p, 568. dirá que o julgador deve "dar 'ouvida' a ambas as partes, sob pena de parcialidade, na medida em que conheceu apenas metade do que deveria ter conhecido.

[353] GOMES FILHO, Antônio Magalhães. **Direito à prova no processo penal.** São Paulo: Editora Revista dos Tribunais, 1997. p, 135 – 137.

[354] GOMES FILHO, Antônio Magalhães. **Direito à prova no processo penal.** Op. cit. p, 136.

Quanto as diferentes concepções entre *meios* de prova e *fontes* de prova, afirma Maier[355] que os primeiros se referem às distintas maneiras segundo as quais, as partes processuais podem incorporar ao processo os conhecimentos determinados e necessários, certos ou prováveis sobre as hipóteses defendidas (ex. testemunho, perícia, juntada de documentos). São canais de informação de que se serve o julgador[356].

Sobre *fonte* de prova, assevera Maier[357] se tratar de pessoas que introduzem no processo penal um conhecimento determinado sobre um objeto de prova[358] ou *thema probandi*[359]. Somadas às pessoas, Gomes Filho irá dizer que também serão fontes de prova coisas das quais se pode conseguir um *elemento* de prova, ou seja, as fontes de provas podem ser divididas em fontes pessoais e fontes de prova reais[360].

Conforme leciona Badaró[361], tais fontes decorrem do fato ilícito, são anteriores ao início do processo, portanto não guardam relação de existência com este. Será fonte de prova tudo o que puder servir para esclarecer algo sobre a existência do fato apurado, tudo que é idôneo a fornecer resultado apreciável para a decisão do juiz[362], mesmo que não chegue ao conhecimento deste[363]. O detalhe esclarecido pelo autor, a partir de Sentís Melendo, é que as *fontes* de prova têm como destinatários as partes, vez que servem para substanciar as alegações

---

[355] MAIER, Julio B. ***Derecho procesal penal Tomo III: parte general: actos procesale.*** 1 ed. Ciudad Autónoma de Buenos Aires: Del puerto, 2011**.** p, 82 – 96.

[356] GOMES FILHO, Antônio Magalhães. **Notas sobre a terminologia da prova (reflexos no processo penal brasileiro).** Op. cit. p, 308 – 309. No mesmo sentido, Badaró irá afirmar que meios de prova são os instrumentos por meio dos quais as fontes de prova são levadas para o processo. "Assim, a testemunha de um fato é a fonte de prova, enquanto suas declarações em juízo são o meio de prova. O documento é uma fonte de prova, a sua incorporação ao processo é o meio de prova". Conclui o autor que os meios de prova somente existem no processo. (BADARO, Gustavo. **Ônus da prova no processo penal.** São Paulo: Editora Revista dos Tribunais, 2003. p, 2003.

[357] Julio B. Maier define as pessoas que trazem informações ou conhecimento ao processo penal de *órgãos de prova.*

[358] Ainda segundo Julio B. Maier, objeto da prova é o tema ou situação real a que a própria prova se refere. Em algumas ocasiões irá referir-se ao fato punível em si mesmo com todos os seus elementos, em outras referir-se-á a circunstâncias meramente valorativas e normativas que não pertencem ao acontecimento fático em si. É comum segundo o autor, o objeto da prova se referir a apenas um elemento que constitui o fato punível.

[359] CORDERO, Franco. ***Procedimiento penal* Tomo II.** Op. cit. p, 9. "*las partes enuncian los diferentes temas y aducen las pruebas: en cuanto al ministério público, son los hechos objeto de la acusación; luego los defensores indican los hechos que se proponen probar y piden que se admitan determinadas pruebas*".

[360] GOMES FILHO, Antônio Magalhães. **Notas sobre a terminologia da prova (reflexos no processo penal brasileiro).** Op. cit. p, 308.

[361] BADARO, Gustavo. **Ônus da prova no processo penal.** Op. cit. p, 165 – 166.

[362] BADARO, Gustavo. **Processo penal.** 4 ed. rev. atual. e ampl. São Paulo: Editora Revista dos Tribunais, 2016. p, 386.

[363] Um documento que ateste a veracidade da hipótese (acusatória ou defensiva) mas que não foi carreado aos autos processuais por *meios* de prova, e portanto não se tornou conhecido pelo julgador. Uma pessoa que presenciou o fato ilícito, mas que não testemunhou sobre o ocorrido no processo.

ou hipóteses levantadas no processo[364]. Razão assiste Sentís Melendo[365]. Portanto, mesmo que exista passagens no texto legal em que o legislador processual penal atribua o sentido de *fonte* de prova à palavra "prova", não se pode vincular o julgador como seu destinatário.

Os dados objetivos de conhecimento e informação que confirmam ou negam determinada hipótese processual são denominados por Gomes Filho[366] de *elementos* de prova. Conforme já explicado acima, entende-se que estes *elementos* de prova, ou dados objetivos colhidos, somente os são após a submissão dos *meios* de provas ao contraditório. É o conjunto destes *elementos* probatórios que proporcionará o alto grau de certeza, ou a probabilidade de estar provado ou não o enunciado acusatório, alcançando-se assim a convicção judicial.

Sob este aspecto, o *resultado* de "estar provado" extraído dos diversos *elementos* de prova, demostra que o fundamental, ou crucial para o processo é o aspecto epistemológico acarretado à força ou o peso da prova, afastando para um local secundário o grau de confiança

---

[364] BADARO, Gustavo. **Ônus da prova no processo penal.** Op. cit. p, 167. Na obra, Badaró direciona seu raciocínio para a hipótese de que caberá ao juiz também o papel de destinatário da fonte de prova. Fundamenta sua posição "dentro do que se denominou ativismo judicial, no qual os poderes do juiz vêm sendo ampliados, os juízes também podem ser destinatários das fontes de provas". Justifica o autor que: "o que não parece adequado é que o juiz saia averiguando e buscando fontes, pois neste caso, transformar-se-ia em um juiz instrutor, ao mesmo tempo em que seria o julgador da causa, com seríssimos riscos de perda da imparcialidade". Ademais, para o autor "se o juiz tiver conhecimento das fontes, seja porque as partes as levaram para o processo mediante um meio de prova, seja porque a produção de um meio de prova revelou uma nova fonte de prova, nada impedirá que o juiz determine a normal produção daquela prova". Conclui que "pode também ser determinada a produção de ofício de um meio de prova, sem que sobre o mesmo haja qualquer fonte no processo, como, por exemplo, quando o juiz determina que se junte aos autos a certidão de antecedentes criminais do acusado". Não se concorda com este pensamento, com o risco de expor apenas uma síntese dos motivos da discordância, estes se embasam pela essência do sistema acusatório que impede o julgador de atuar como parte. Questiona-se ademais qual seria a relevância de se juntar ao processo uma certidão de antecedentes criminais do acusado, senão apenas para justificar a tomada de decisão que se pauta na presunção da culpabilidade. Tal postura esbarra em um dos princípios norteadores do processo, a presunção de inocência. Por fim, não é possível permitir ao julgador dispor de fontes de provas que não foram trazidas ao processo pelas partes. O motivo de tal impedimento é a relação direta com a criação de expectativas e resultados já discorridos acima, mas que para elucidação recomenda-se a obra de CUNHA MARTINS, Rui. **O ponto cego.** Op. cit.

[365] SENTIS MELENDO, Santiago. ***La prueba: los grandes temas del derecho probatorio.*** Ediciones Juridicas Europa-America, Buenos Aires, 1979. p, 170 – 171. De fato razão assiste o autor, principalmente quando este diferencia *fontes* de prova e *meios* de prova. Contudo, não passa despercebido o erro cometido por Sentis Melendo quando se posiciona em acordo com o princípio da oficialidade do julgador no direcionamento e ordenação dos meios de prova. Para o autor o princípio inquisitório deve ter prevalência ao dispositivo na produção dos meios de prova, tendo em vista que estes se direcionam ao juiz. Discorda-se deste ulterior pensamento pelo risco à imparcialidade e violação do sistema processual penal acusatório.

[366] GOMES FILHO, Antônio Magalhães. **Notas sobre a terminologia da prova (reflexos no processo penal brasileiro).** Op. cit. p, 307. Também em "**Limites ao compartilhamento de provas no processo penal**", GOMES FILHO irá explicitar seu entendimento acerca do contraditório *para* a prova e *sobre* a prova, de modo a admitir que na primeira situação o elemento probatório é somente formado após o contraditório, sendo o contraditório condição de existência *para* a formação da prova (ex. prova testemunhal); na segunda situação trazida pelo autor, na qual há o contraditório existe *sobre* a prova, afirma o autor se tratar do contraditório exercido sob os elementos probatórios (ex. prova documental) colhidos antes do processo. Ao nosso ver, não é acertado diferenciar as constituições probatórias a depender do momento em que se colhe a (fonte de) prova. Mesmo sendo uma prova documental colhida antes do processo, trata-se de fonte de prova sob a qual em contraditório irá se produzir os *elementos* de prova a serem adotados – se relevantes ao processo – na tomada de decisão que deverá ser congruente ao *resultado* da prova. (GOMES FILHO, Antônio Magalhães. **Limites ao compartilhamento de provas no processo penal.** Revista Brasileira de Ciências Criminais. RBCCRIM VOL. 122 (Agosto 2016).

ou de crença do julgador[367]. Como salienta Haack[368], o grau de crença do julgador é uma questão distinta e claramente secundária, contudo diretamente relacionada à força dos elementos de prova, quanto mais as provas avalizam o enunciado, mais o julgador terá confiança de o tomar como verdadeiro ou provado.

Feitas as ressalvas sobre a terminologia "Prova", passar-se-á a análise acerca das provas antecipadas, irrepetíveis e cautelares (Art. 155, CPP). Para Soares[369] "trata-se de *elementos* de prova colhidos antes da instauração de processo penal e trazidos aos autos sem o adequado contraditório em sua produção, cuja valoração judicial a lei excepcionalmente admite".

Porém, não nos parece se tratar exclusivamente de *elementos* de prova, muito menos a flexibilização do exercício adequado do contraditório como afirma o autor. Com efeito, se assim o fosse, seria em certa medida dispensável o exercício do contraditório para a produção de prova. No entanto, a premissa que rege a matéria é a de que a produção probatória que integra a estrutura dialética somente é formada pelo crivo do contraditório[370].

Pelas lições de Fazzalari[371] a estrutura processual consiste na participação dos contraditores em simétrica paridade de suas posições, de modo que possam exercitar um conjunto de escolhas, de reações, de controles e prestações de conta dos resultados. Se a atividade probatória é essencial para o processo e não há que se falar em processo sem a atuação das partes em contraditório, por evidente que a prova como elemento capaz de atestar uma hipótese fática processual não pode ser formulada sem a participação dos interessados na atividade probatória.

Logo, o fator que diferencia estas categorias probatórias não é a relativização do exercício do contraditório, mas tão somente o momento no qual deverá ser exercido, cujo critério é a possibilidade de preservação da (*fonte* de) prova ou a produção imediata ou antecipada de *elementos* de prova. Contudo, também não será possível uma abordagem aprofundada sobre tais categorias, mas ainda assim se faz fundamental a análise, mesmo com o risco da superficialidade. Principalmente por se entender de grande valia ao tema principal da pesquisa.

---

[367] HAACK, Susan. ***El probabilismo jurídico: una disensión epistemológica.*** Op. cit. p, 71.
[368] HAACK, Susan. ***El probabilismo jurídico: una disensión epistemológica.*** Op. cit. p, 71.
[369] SOARES, Gustavo Torres. **Investigação criminal e inovações técnicas e tecnológicas.** Op. cit. p, 58.
[370] GIACOMOLLI, Nereu. **Reformas (?) do processo penal: considerações críticas.** Editora Lumen Juris: Rio de Janeiro, 2008. p, 22.
[371] FAZZALARI, Hélio. **Instituições de Direito Processual**. 1ª ed. Campinas- SP: Bookseller Editora e Distribuidora. 2006. p, 119-120.

Lopes Jr. e Gloeckner[372] afirmam que, excepcionalmente, tendo em vista a urgência ou o risco de perecimento de uma prova importante, adotar-se-á o incidente de produção antecipada de provas[373] como procedimento a ser seguido para outorgar o *status* de ato de prova a determinado ato de investigação. Nada mais é que instrumentalizar uma forma de colher antecipadamente a prova, tendo em vista a impossibilidade de o fazê-lo em momento processual oportuno[374].

Para justificar a produção antecipada da prova deve se atentar para dois requisitos básicos, a "relevância e imprescindibilidade do seu conteúdo para a sentença" e a "impossibilidade de sua repetição na fase processual" (momento oportuno) devido ao provável perecimento da *fonte* de prova[375]. Antecipar a produção probatória não exclui a exigência do contraditório e do direito de defesa, ao contrário, simboliza o justo exercício antecipado de ambos para a produção da prova. A urgência jamais irá dispensar o contraditório como critério de produção da prova.

Não é a *fonte* da prova que se conserva urgentemente face ao perecimento, mas o que se tem é a produção – a partir do contraditório antecipado – da formação de *elementos* de prova que deveriam ser formados em momento processual oportuno, mas que pela urgência se antecipou sua formação.

Pode-se dizer que são provas antecipadas pela urgência, contudo caso os *elementos* de prova produzidos estejam eivados de vícios; e (ainda) não haja ocorrido o perecimento ou a perda da *fonte* de prova, nada impede que se repita a produção probatória. Afinal de contas, como lembra Lopes Jr[376], a partir de Pontes de Miranda, aquilo que foi feito com defeito, existe, mas pode – e deve, em se tratando de direito processual penal – ser refeito.

Não se pode confundir, nem misturar as categorias de prova antecipada e cautelar, nem coloca-las como espécies de um gênero denominado "prova cautelar em sentido amplo"[377]. Provas antecipadas não são cautelares pois não se prestam à conservação da *fonte* de prova para

---

[372] LOPES JR. Aury; GLOECKNER, Ricardo Jacobsen. **Investigação preliminar no processo penal brasileiro.** Op. cit. p, 209.

[373] Os autores alertam para a necessidade de revisar a legislação que versa – ainda que parcialmente – sobre o incidente probatório. Tal produção antecipada de provas está disciplinado no art. 225 que dispõe que "Se qualquer testemunha houver de ausentar-se, ou, por enfermidade ou por velhice, inspirar receio de que ao tempo da instrução criminal já não exista, o juiz poderá, de ofício ou a requerimento de qualquer das partes, tomar-lhe antecipadamente o depoimento".

[374] LOPES JR. Aury; GLOECKNER, Ricardo Jacobsen. **Investigação preliminar no processo penal brasileiro.** Op. cit. p, 211.

[375] LOPES JR. Aury; GLOECKNER, Ricardo Jacobsen. **Investigação preliminar no processo penal brasileiro.** Op. cit. p, 212.

[376] LOPES JR., Aury. **Direito Processual Penal.** Op. cit. p, 1181.

[377] ARANTES FILHO, Marcio Geraldo. **A interceptação de comunicação entre pessoas presentes.** 1 ed. Brasília, DF: Gazeta Jurídica, 2013. p, 53.

que se evite uma frustração probatória. A prova antecipada é o produto da antecipação da produção probatória. De igual modo, como se verá adiante, prova cautelar não é o mesmo que *meios de investigação de prova*. Separar estes institutos processuais também é fundamental para que seus proventos tenham tratamento adequado.

Meios de investigação de prova[378], como o próprio nome o define, são meios de investigação (de fontes de prova). Servem para a identificação de *fontes* de prova. Diligências que atendem ao esclarecimento do fato oculto, não tem capacidade de conservar cautelarmente nenhuma *fonte* de prova, mas identifica-la como tal e assim tornar possível que as partes processuais lancem mão de meios (meios de prova, meios de produção de prova) para as produzir como prova. Cumprida esta função, como meios de investigação, devem ser excluídos do processo.

Não se quer dizer que a natureza jurídica de um instituto não possa ser híbrida a partir da sua finalidade ou objetivo alcançado, mas ainda assim o tratamento é diferente. É possível que um mesmo instituto processual seja medida cautelar e meio de investigação de prova (ex. Busca e apreensão). Contudo, discorda-se de Arantes Filho, que embora afirme que a finalidade dos meios de investigação de prova seja a descoberta de fontes de prova e não a produção de elementos probatórios, admite que seja possível o contraditório postergado sob estes meios de investigação. O autor fundamenta o seu raciocínio a partir do fato de que destes meios de investigação de prova podem resultar elementos de informação que poderão ser utilizados como *fonte* de convencimento judicial para avaliação de objetos de prova, se confirmados por elementos probatórios produzidos em contraditório[379].

Como exemplo de prova cautelar – em sentido estrito de meio de investigação de prova – destaca o autor o instituto da interceptação telefônica, Lei nº. 9.296/96. Ora, não é demais reafirmar que conceder o contraditório diferido em relação a uma declaração autoincriminatória involuntária (como é o caso de interceptações telefônicas) é se utilizar da forma processual como maquiagem de legitimidade e constitucionalidade. Desconsidera-se a partir disto as finalidades peculiares dos institutos que funcionam como engrenagens de um sistema processual.

A face oculta deste específico contraditório diferido sob declarações autoincriminatórias é a subtração do princípio *nemo tenetur se detegere*. Não se pode dizer que

---

[378] O termo utilizado neste trabalho reflete ao exposto por Arantes Filho, em que a utilização do termo "meio de obtenção de prova" pressupõe ou induz equivocadamente a já existente fonte de prova que irá se obter, logo presumisse a culpabilidade do sujeito passivo da medida imposta. ARANTES FILHO, Marcio Geraldo. **A interceptação entre pessoas presentes.** Op. cit. p, 29 (nota de rodapé 58).

[379] ARANTES FILHO, Marcio Geraldo. **A interceptação entre pessoas presentes.** Op. cit. p, 53

o instituto da interceptação telefônica produz uma prova cautelar, não é possível vislumbrá-lo como um instrumento (medida cautelar probatória) mediante o qual se conserva qualquer fonte de prova, senão que tal argumento legitima o uso descabido da autoincriminação em um procedimento incriminatório.

Deve-se proteger o sujeito passivo da autoincriminação involuntária antes que esta produza seus efeitos nefastos no Processo Penal e na cognição judicial. Pela interceptação telefônica – como meio de investigação (de prova) - se identifica *fontes* de prova (ex. pessoas que compõe o esquema criminoso, objetos utilizados, proventos do crime), jamais será possível se conservar tais fontes. As declarações feitas, gravadas e transcritas, não são *fontes* de prova, o sujeito passivo (involuntariamente) não deve(ria) ser tratado como tal.

Porém, de tais declarações – evidentemente – se podem extrair informações que ajudem a esclarecer o fato oculto e identificar *fontes* probatórias. Cumpridas estas funções endoprocessuais, os registros decorrentes da interceptação devem ser excluídos, jamais servirão para convencimento judicial, ainda que confirmatórios de elementos já produzidos em contraditório. Parece óbvio que, se já produzidos elementos probatórios suficientes e satisfatórios para a condenação, não deveria se cogitar sua confirmação por outros meios.

Quanto às ditas provas cautelares, antes de defini-las é preciso entender o que são medidas cautelares penais. Isto porque uma tem ligação direta com a outra. De acordo com Gimeno Sendra[380] medidas cautelares são medidas dirigidas a garantir o cumprimento efetivo da sentença. Na mesma direção, aponta Badaró[381] que são instrumentos que asseguram o provimento final, o resultado de uma hipotética condenação (instrumentalidade hipotética). Tal concepção demonstra ainda uma severa influência civilista no âmbito do processo penal, de modo a desconsiderar a presunção de inocência como regra de tratamento ao acusado em todo o percurso processual até o provimento final. Assegurar o provimento final no processo civil corresponde à conservação do bem patrimonial em disputa, de modo que se ateste que à época da decisão, este bem – objeto da pretensão resistida – possa ser entregue ao seu real titular.

No processo penal porém, dizer isto acerca das medidas cautelares penais é desconsiderar a absolvição como resultado da sentença final, e portanto reconhecer a possível execução de uma hipotética condenação, uma presunção da culpa. Uma prisão preventiva – por exemplo – como medida cautelar pessoal poderia ser decretada como antecipação da punição,

---

[380] GIMENO SENDRA, Vicente. ***Derecho procesal penal.*** Op. cit. p, 472. "*Las medidas cautelares están dirigidas a garantizar el cumplimiento efectivo de la sentencia. [...] Para garantizar estos efectos o la futura y probable ejecución de la parte dispositiva de la sentencia surge la conveniência de adoptar, hasta que adquiera firmeza, las medidas cautelares*".

[381] BADARO, Gustavo. **Processo penal.** Op. cit. p, 988.

porquanto que hipotética seria a condenação[382]. Esta definição civilista importada para o Direito Processual Penal comina na confusão entre cautelaridade e antecipação de tutela, cuja inexistência no Processo Penal se impõe. Sem contar que tal concepção exclui de seu âmbito as medidas cautelares penais probatórias, pelo fato de permitir a partir da aplicação deste conceito antecipar-se a produção probatória sem a legitimidade ofertada pelo contraditório.

Apresenta-se mais acertada a definição sobre as medidas cautelares penais trazida por Pujadas Tortosa[383]. Medidas cautelares penais servem para a proteção do processo sobre vários perigos de frustração, ou seja, protege-se o processo do risco da frustração processual. Um risco que, segundo a autora, é aquele que eventualmente impossibilita a válida prossecução do processo e a realização de seu objetivo[384].

Quanto às provas penais e as ditas medidas cautelares penais, Pujadas Tortosa também afirma que deve se considerar também um risco à frustração processual a eventual indeterminação do fato ou do sujeito investigado proporcionada pela ausência de indícios que permitam se conhecer o fato ilícito (passado). Portanto, uma tutela cautelar probatória presta-se a evitar a ocultação, destruição ou manipulação de *fontes* e *meios* de prova[385].

Definitivamente, a prova cautelar não se apresenta semelhante às provas irrepetíveis ou antecipadas – muito menos aos *meios de investigação de prova* –, mas como *fontes* de provas recolhidas a partir da execução de uma medida cautelar probatória. Logo, recolhe-se a *fonte* de prova pela execução de medida cautelar (antes do processo ou no decorrer deste), conserva-se até inclui-la no processo penal por um *meio* de prova e, após, submete-se ao contraditório em momento processual oportuno. Não se pode dizer que executada uma medida cautelar

---

[382] MENDES, Carlos Hélder. **Do sentimento de impunidade à banalização da extrema ratio: uma análise discursiva das fundamentações dos decretos de prisão preventiva nas varas criminais de São Luís – MA.** 1ª ed. Florianópolis: Empório do Direito Academia, 2016. p, 34 – 35.

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

[384] PUJADAS TORTOSA, Virgínia. ***Para una teoria general de las medidas cautelares penales.*** Op. cit. p, 129.

[385] PUJADAS TORTOSA, Virgínia. ***Para una teoria general de las medidas cautelares penales.*** Op. cit. p, 213 – 214 Sobre os perigos cautelares elenca e discorre a autora: "1. *Imposibilidad de afirmar indicios suficientes de comisión delictiva por parte de un sujeto concreto (supuesto 2). La tutela cautelar acordada por esta causa tratará de evitar que la ocultación, destrucción o manipulación de fuentes de prueba, por parte del sujeto pasivo del proceso, obligue a sobreseerlo en virtud del art. 637.2º LECrim.* 2. *Imposibilidad de afirmar indicios suficientes que acrediten el carácter delictivo del hecho o su existencia (supuesto 4). Ante esta eventualidad, es factible acudir a la tutela cautelar para evitar que la ocultación, destrucción o manipulación de fuentes de prueba, por parte del sujeto pasivo del proceso, obligue a sobreseer el proceso de modo provisional (en caso de no poder acreditarse el carácter delictivo del hecho) o definitivo (en caso de no existir indicios racionales de haberse perpetrado el hecho que dio motivo a la formación de la causa).* 3. *Imposibilidad material de practicar alguna prueba en el juicio oral (supuesto 6). Este peligro debe combatirse evitando que el sujeto pasivo, con la intención de frustrar la práctica probatoria y forzar así una (quizás improcedente) sentencia absolutoria, destruya, oculte o manipule medios de prueba. Cabe advertir que el sujeto pasivo también puede impedir la práctica probatoria mediante la suspensión de la vista por ausencia del mismo. Pero este supuesto debe reconducirse, claramente, a la frustración del proceso por ausencia del acusado*".

probatória, cujos frutos foram (*fontes* de) provas recolhidas, se constitui a prova penal. Portanto, volta-se a afirmar: a constituição probatória é somente possível quando estabelecido o contraditório sob o *meio* de prova.

Diferente também é o instituto processual da prova irrepetível. Muito embora a doutrina[386] entenda que sejam semelhantes, sob outra óptica se percebe que não se trata de institutos de mesma peculiaridade. Provas não repetíveis "são aquelas que, por sua própria natureza, têm de ser realizadas no momento do seu descobrimento, sob pena de perecimento ou impossibilidade de posterior análise"[387]. Este conceito é o que se apresenta mais adequado em virtude de atestar o grau de emergência do perecimento da *fonte* de prova. Logo, conserva-se a informação desta *fonte* de prova através de seu registro e respectivos elementos. Um exemplo claro é o exame de corpo delito.

O contraditório será exercido, ainda que sob o registro da *fonte* de prova e de seus elementos, em momento processual oportuno para a formação de *elementos* de prova. Contudo por se tratar de prova irrepetível pela emergência do perecimento da *fonte* de prova, é importante permitir a manifestação da defesa na formação da documentação ou do registro da da *fonte* perecível, seja para solicitar outras provas, formulação de quesitos à perícia e etc. Pela "impossibilidade de repetição em iguais condições"[388], caso o registro de seus respectivos elementos seja feito com vícios não poderá ser refeito, por quanto irrepetível (ex. perícia em que consta juízos de valor do perito ou com conclusões alheias à sua competência).

3.2.2 A Prova Penal Digital: conceito e características

Diante do cenário global criado a partir do domínio de tecnologias de informação e comunicação, se impõe mudanças adaptativas às ciências jurídicas. Este cenário expôs a crise das normas e princípios tradicionais de modo a se exigir inovações em todos os ramos do direito[389]. No Direito Processual Penal não poderia ser diferente.

---

[386] GOMES FILHO, Antônio Magalhães. **Provas.** *In:* MOURA, Maria Thereza Rocha de Assis. **As reformas no processo penal: as novas leis de 2008 e os projetos de reforma.** São Paulo: Editora Revista dos Tribunais, 2008. p, 254 – 255.

[387] LOPES JR. Aury; GLOECKNER, Ricardo Jacobsen. **Investigação preliminar no processo penal brasileiro.** Op. cit. p, 326.

[388] LOPES JR. Aury; GLOECKNER, Ricardo Jacobsen. **Investigação preliminar no processo penal brasileiro.** Op. cit. p, p, 326.

[389] SALT, Marcos. ***Nuevos desafios de la evidencia digital: acceso transfornterizo y técnicas de acesso remeto a datos informáticos***. 1ª ed. Buenos Aires: Ad-hoc, 2017. p, 11.

Como explica Salt[390], os avanços tecnológicos permitem a utilização de mecanismos poderosos de investigação na obtenção de informações relevantes para processos penais. São inovações técnicas e tecnológicas de investigação que demandam conhecimentos específicos, tendo em vista que de tais investigações se possa recolher *fontes* cuja função é proporcionar o conhecimento de informações cada vez mais fidedignas e relevantes ao processo penal. *Fontes* de prova que, quando colhidas em ambiente digital ou informático, em virtude da complexidade metodológica e científica, também ostentam a característica do que se denomina de prova científica.

Antes de mais nada, entende-se por prova científica um fenômeno complexo, articulado e diversificado em suas múltiplas formas de manifestação. Para Dominioni[391] se trata de uma operação probatória pela qual, no momento de admissibilidade, de assunção e valoração, se usam instrumentos científicos e técnicos, ou seja, princípios e metodologia científica, métodos tecnológicos, aparatos técnicos cujo uso requer expertise. E sobre este prisma é que se deve evitar a excessiva valorização construída a partir do mito da confiabilidade inquestionável das provas científicas, portanto se fazendo necessário o estabelecimento de critérios de controle para a recolha e manutenção da qualidade da prova, que no presente estudo, trata-se da prova digital.

Neste interim é que se traz à baila a prova científica como gênero daquilo que denominar-se-á prova digital. Não por outra razão, mas pela exigência fundante de conhecimentos específicos de ciência da computação forense, que em definitivo se apresenta como uma disciplina científica aplicada para atender princípios de identificação, coleta, preservação e análise de (*fontes* de) provas, buscando-se assim garantir a admissibilidade da prova em processos judiciais[392].

No entanto, a tentativa da definição de um conceito acerca do que é verdadeiramente uma prova digital, embora relevante, trata-se de um trabalho árduo, pois se

---

[390] SALT, Marcos. ***Nuevos desafios de la evidencia digital.*** Op. cit. p, 11.

[391] DOMINIONI, Oreste. ***La prova penale scientifica: gli strumenti scientifico-tecnici nuovi o controversi e di elevata specializzazione.*** Milano: Giufre Editore, 2005. p, 12. "*espressione ellittica, che, esplicitata nei suoi contenuti, designa un complesso fenomeno, articolato e diversificato in molteplici forme di manifestazione. In generale si può dire che si trata di operazioni probatorie per le quali, nei momenti dell'ammissione, dell'assunzione e della valutazione, si usano strumenti di conoscenza attinti alla scienza e alla tecnica, cioè a dire principi e metodologie scientifiche, metodiche tencologiche, apparati tecnici il cui uso richiede competenze esperte*".

[392] WALKER, Cornell. ***Computer forensics: bringing the evidence to court***. Acesso em jun 2018. Disponível em: http://www.infosecwriters.com/text_resources/pdf/Computer_Forensics_to_Court.pdf. p, 1.

apresenta pendular entre a inoperatividade de um conceito possivelmente abstrato e a curta duração da força conceitual decorrente dos constantes avanços tecnológicos[393].

Por vezes, poderá haver confusão entre as definições acerca das provas de natureza digital e aquelas de origem eletrônica, contudo há que se fazer a dissociação entre ambas. Para Delgado Martín[394], prova eletrônica é "toda informação de valor probatório contida ou transferida por um meio eletrônico", ou seja qualquer classe de informação que possa ser produzida, armazenada ou transmitida por meios eletrônicos e que possa ter relevância para os fatos investigados.

Tal conceito engloba tanto as provas em formato digital como aquelas em formato analógico, como gravações em vídeo e áudio ou fotografias que embora digitalizáveis não tenham origem em formato digital[395]. O termo digital, segundo Ramalho[396], embora associado a tecnologias que utilizam a lógica binária, é mais amplamente vinculado à informática, e por este último aspecto é acertada a denominação de provas eletrônico-digitais por demonstrar a subespécie (digital) da prova eletrônica em formato digital.

De acordo com Daniele[397], tratam-se de "imaterialidades conceitualmente correspondentes a impulsos elétricos que se manifestam em uma sequência numérica pré-estabelecida e que são transmitidos em um suporte de computador com capacidade de memorização".

A definição daquilo que é chamado de prova digital, por vezes, se faz a partir de suas características principais. A imaterialidade como característica da prova digital, por exemplo, se dá pela informação de dados em *bits* sequenciais, que embora sua existência independa de um suporte físico, necessita de um transportador. O suporte físico tecnológico é necessário para que a torne percebível, mas a prova digital não se resume nem se limita ao seu suporte[398].

---

[393] RAMALHO, David Silva. **Métodos ocultos de investigação criminal em ambiente digital.** Almedina, 2017. p, 98 – 99.
[394] DELGADO MARTIN, Joaquin. ***La prueba electronica en el proceso penal.*** Diario La Ley, Nº 8167, Sección Doctrina, 10 Oct. 2013, Año XXXIV, Editorial La Ley. p, 1.
[395] RAMALHO, David Silva. **Métodos ocultos de investigação criminal em ambiente digital.** Op. cit. p, 99.
[396] RAMALHO, David Silva. **Métodos ocultos de investigação criminal em ambiente digital.** p, 101.
[397] DANIELE, Marcelo. ***La prova digitale nel processo penale.*** Rivista di Diritto Processuale Anno LXVI (Seconda Serie) – n. 2. Marzo – Aprile, 2011. p, 284. "*Di fronte alle prove digitali i processualisti si trovano a disagio, in quanto sono abituati a pensare alle prove come a degli oggetti fisici, dotati di un'evidente corporeità. Le prove digitali si presentano, invece, come entità immateriali. Ciò non significa che esse non abbiano una loro fisicità: concettualmente si tratta di impulsi elettrici che rispondono ad una sequenza numerica prestabilita e che, convogliati in un supporto informatico dotato di una memoria, originano informazioni intellegibili. È, però , una fisicità che, in assenza del supporto, non puo` essere percepita come tale*".
[398] Neste sentido, DANIELE, Marcelo. ***La prova digitale nel processo penale.*** Op. cit. p, 284 e RAMALHO, David Silva. **Métodos ocultos de investigação criminal em ambiente digital.** Almedina, 2017. p, 104.

É justamente por tal fato que a prova digital também se caracteriza pela sua volatilidade e fragilidade. A primeira se relaciona inversamente com a perenidade da prova, há uma facilidade de desaparecimento característica da prova digital que resulta da ocorrência de eventos como falta de bateria do dispositivo eletrônico, a gravação de informações novas em substituição às mais antigas, ou pelo simples fato de tais *fontes* de prova se tratarem de arquivos temporários[399]. Contudo, cabe ressaltar – conforme Vaz[400] – que a não durabilidade não é característica de toda prova digital, tendo em vista que os dados informáticos são armazenados em suportes eletrônicos por vezes submetidos a técnicas de preservação capazes de tornar a *fonte* probatória em uma fonte permanente.

Quanto à fragilidade, tal característica se relaciona com a grande possibilidade de contaminação dos dados que se pretende coletar, de tal modo que com a impropriedade do método de recolha utilizado se pode alterar suas características ou seu estado e com isso comprometer o material probatório[401]. Para evitar tal risco se atenta para a impossibilidade de fazer uso de analogias para o tratamento das provas digitais a partir do regime legislativo regulador de provas físicas. Requer-se, além dos requisitos formais para a utilização de mecanismos de meios de investigação de prova, normas que contemplem as peculiaridades da prova digital, tais quais a garantia da fidedignidade na sua coleta e a preservação de sua cadeia de custódia[402].

Neste sentido aponta Vaz para a necessária previsão e especificação de medidas investigativas e cautelares para que possibilite a coleta em tempo adequado e oportuno, de modo a considerar principalmente a elevada alterabilidade da *fonte* de prova digital e o perigo da sua volatilização[403].

3.2.3 Aquisição da fonte de Prova Digital

Todo o agir diário, voluntária ou involuntariamente, é registrado por diferentes formas de tecnologia de informação. Das mais diversas maneiras se conservam todos estes registros de vida em dispositivos de armazenamento de dados. Conforme Salt[404], os sistemas

---

399 RAMALHO, David Silva. **Métodos ocultos de investigação criminal em ambiente digital.** Op. cit. p, 104.
400 VAZ, Denise Provasi. **Provas digitais no processo penal: formulação do conceito, definição das características e sistematização do procedimento probatório.** Op. cit. p, 67.
401 SALT, Marcos. ***Nuevos desafios de la evidencia digital: acceso transfronterizo y tecnicas de acceso remoto a datos informáticos.*** Op. cit. p, 33.
402 RAMALHO, David Silva. **Métodos ocultos de investigação criminal em ambiente digital.** Op. cit. p, 104.
403 VAZ, Denise Provasi. **Provas digitais no processo penal: formulação do conceito, definição das características e sistematização do procedimento probatório.** Op. cit. p, 77.
404 SALT, Marcos. ***Nuevos desafios de la evidencia digital: acceso transfornterizo y técnicas de acesso remeto a datos informáticos***. Op. cit. p, 25.

informáticos – principalmente a partir da denominada "internet das coisas" – constituem uma fonte inestimável de potenciais provas utilizáveis para a averiguação dos fatos históricos no marco processual penal. Para o autor, as tecnologias da informática utilizadas no aprimoramento das investigações penais geram assim uma mudança de paradigma no Direito Processual Penal quanto as normas procedimentais diante desta nova realidade.

Esta mudança de paradigma não tem sido bem acompanhada pelo enquadramento dogmático e legislativo que tendencialmente propõe uma redução da complexidade temática. Primeiramente, é fundamental entender – em grau maior de importância – que além dos requisitos aplicáveis a cada técnica de obtenção da prova digital, trata-se de grande relevância a verificação da preservação da integridade da prova recolhida e a sua efetiva capacidade de demonstração da realidade a qual se propõe provar (*objeto* da prova)[405]. Deste modo, como as técnicas forenses de recolha da prova não são facilmente compreendidas pelos sujeitos processuais, somados a tais requisitos, também carecem de relatórios técnicos desenvolvidos e da possibilidade de comprovação da adequação dos métodos utilizados.

O procedimento de busca probatória em se tratando de provas digitais, segundo Kerr[406] é dividido na maioria das vezes em dois estágios. O primeiro voltado para a busca dos aparelhos ou dispositivos eletrônico-digitais de armazenamento de informação, ou seja, qualquer suporte físico que armazene dados com suposta relevância para a investigação criminal. O segundo, por sua vez, é a busca das *fontes* de provas digitais propriamente dita, cuja cópia integral e perfeita (*image*) do dispositivo se impõe para que – somente após – se possa identificar as provas relevantes e descritas na ordem jurisdicional. Uma vez obtido o acesso ao dispositivo informático, a busca por *fontes* probatórias através de *softwares* forenses incide na cópia autêntica ou *image* do dispositivo[407].

É possível afirmar que este procedimento em dois estágios é uma maneira até então usual de obtenção da prova digital, na qual se faz necessário um prévio e legítimo acesso ao suporte físico cuja *fonte* probatória está armazenada. Este procedimento sofre uma mudança significativa decorrente da influência direta das novas tecnologias de comunicação e

---

[405] RAMALHO, David Silva. **Métodos ocultos de investigação criminal em ambiente digital.** Almedina, 2017. p, 93.

[406] KERR, Orin S. ***Executing warrants for digital evidence: the case for use restrictions on nonresponsive data.*** Texas Tech School of Law Criminal Law Symposium, The Fourth Amendment in the 21st Century, on April 17, 2015, p. 6 – 10. Disponível em: http://texastechlawreview.org/wp-content/uploads/Kerr.PUBLISHED.pdf. Acesso em Jun 2018. É preciso destacar que a realidade investigada pelo autor é a prática norte americana, na qual a Quarta emenda constitucional é levada em consideração para o uso e restrições às buscas em dispositivos eletrônicos com o objetivo de obter dados de informação relevante para o processo penal. Ademais o autor enfrenta a problemática da possibilidade de mandados cumpridos de forma genérica. Esta é uma outra discussão fundamental, mas em que pese a relevância, pelo espaço limitado não poderia ser aprofundado com o rigor necessário.

[407] No mesmo sentido WALKER, Cornell. ***Computer forensics: bringing the evidence to court***. Op. cit. p, 1.

informação. Assim, novos instrumentos de recolha de material probatório digital[408] surgem gradualmente e permitem através da distância que se capture a informação relevante para a investigação, seja àquela armazenada em um sistema informático seja em circulação pela *internet*[409].

Não que um procedimento exclua o outro, mas existem peculiaridades na atividade probatória que merecem uma atenção e uma adequação procedimental para aumentar sua efetividade. Portanto, constata-se que a investigação informática se divide em duas grandes categorias, sendo diferenciadas pela estaticidade ou dinamicidade da atividade[410]. Categorias distintas denominadas por Torre de *indagini palesi* e *indagini occulte*, cuja diferença fundamental é que a primeira se trata de atividade investigativa ostensiva efetuada fisicamente sob um suporte material de memorização de informações digitais com uso de instrumentos de recolha de prova essencialmente típico; e a segunda se pauta na atividade de aquisição de informações por acesso remoto. Em outras palavras, investigações informáticas *off-line* e *on-line*[411].

De maneira semelhante aduz Delgado Martin[412], o autor afirma existir uma multiplicidade de instrumentos e elementos tecnológicos que determinam certa heterogeneidade nas formas de aquisição da *fonte* de prova. A primeira destas é o já destacado acesso ao conteúdo do sistema a partir da apreensão do equipamento material ou dispositivo eletrônico (investigação *off-line*). Haverá também a possibilidade de se ter acesso às informações pretendidas, contidas em um sistema digital, sem a necessária apreensão do seu suporte físico, cuja denominação é "busca remota" (*remote search*). Contudo, somente servirão de *fontes de prova digital* quando houver a possibilidade de, a partir da aquisição por acesso remoto, se comprovar a confiabilidade e integralidade da prova.

Destaca-se ainda a modalidade de coleta dos materiais probatórios digitais por meio do acesso a um sistema ou servidor alvo a partir de outro sistema já previamente acessado, seja pela forma tradicional ou por via remota. Por fim, Delgado Martin aponta a peculiar espécie de aquisição probatória por meio do acesso a registros transfronteiriços, ou seja, dados armazenados em sistemas informáticos situados fora do território nacional[413].

---

[408] O que se quer denominar de material probatório digital é o conjunto de dados que são recolhidos diante de uma investigação criminal para a posterior identificação de *fontes* de provas relevantes ao processo penal.
[409] SALT, Marcos. ***Nuevos desafios de la evidencia digital***. Op. cit. p, 53.
[410] TORRE, Marcos. ***Il captatore informático: nuove tecnologie investigative e rispetto delle regole processual*****.** Op. cit. p, 11.
[411] TORRE, Marco. ***Il captatore informático: nuove tecnologie investigative e rispetto delle regole processual*****.** Op. cit. p, 12.
[412] DELGADO MARTIN, Joaquin. ***La prueba electronica en el proceso penal.*** Op. cit. p, 3.
[413] DELGADO MARTIN, Joaquin. ***La prueba electronica en el proceso penal.*** Op. cit. p, 3.

Quanto aos meios utilizados no procedimento de aquisição do material probatório digital, são destacados por Salt a preservação rápida de dados, a retenção de dados de tráfego de comunicação e, por fim, a "busca e apreensão" de dados informáticos[414]. A preservação rápida de dados é medida útil em face da volatilidade e fragilidade característica da prova digital, volta-se tanto para a preservação de dados de informação quanto aos dados de tráfego de comunicações. Atende à preservação de dados já existentes em algum suporte físico eletrônico, seja em sistema informático privado ou público, de pessoa física ou jurídica.

Imagine-se um caso cujo os órgãos de investigação penal tenham conhecimento da comunicação eletronico-digital entre dois suspeitos da prática delitiva. Na medida em que se volta para evitar a perda de material probatório devido a fragilidade e volatilidade, e deste modo a evitar a frustração da instrução processual, tem-se por evidente seu caráter cautelar. Segundo Salt, seria possível que o Delegado de Polícia ou o órgão Ministerial requeresse que tais dados fossem conservados por um tempo até obtida ordem judicial para acessar o conteúdo pretendido[415].

É neste aspecto que se estabelece a diferença entre a *preservação* rápida de dados e a *retenção* dos dados de tráfego. Esta última, consiste na obrigatoriedade imposta aos provedores de serviços de *internet*, a conservar, entregar informações ou dados de tráfego de comunicação por determinado lapso temporal sem qualquer necessidade prévia ou para atender qualquer investigação específica[416]. O que é característico de vigilâncias informáticas ou investigações prospectivas.

Não é difícil perceber que tal medida se apresenta muito mais intrusiva à privacidade e intimidade dos cidadãos quando comparada à *preservação dos dados*, principalmente por retirar os limites às investigações e à produção probatória impostos pelas normas constitucionais e convencionais.

Quanto à "busca e apreensão" de dados informáticos, dá-se no contexto de uma investigação criminal específica e consiste justamente na cópia ou sequestro de dados possivelmente úteis à constatação do objeto probatório[417]. Pela falta de regulação específica, por vezes tal ferramenta é empregada de maneira análoga à busca de provas físicas, o que como já afirmado, nem sempre apresenta soluções adequadas ou o respeito necessário a garantias

---

[414] SALT, Marcos. ***Tecnologia informática: un nuevo desafio para el derecho procesal penal?.*** Disponível em: https://drive.google.com/file/d/0BxHBGMLx4HZGbzhJQ0ozMFhYYXc/view. Acesso em jun 2018. p, 9.
[415] SALT, Marcos. ***Tecnologia informática: un nuevo desafio para el derecho procesal penal?.*** p, 9.
[416] SALT, Marcos. ***Tecnologia informática: un nuevo desafio para el derecho procesal penal?.*** p, 10.
[417] SALT, Marcos. ***Nuervos desafios de la evidencia digital.*** p, 39.

referentes à procura específica das *fontes* de prova digital, bem como a conservação e manuseio do material colhido.

A convenção de Budapeste – a qual o Brasil não é signatário –, por exemplo, cuja pretensão é dispor sobre medidas de combate ao cibercrime, prevê em seu artigo 19 a possibilidade da busca e apreensão de dados de computador. Chama atenção o fato de tal ordenamento estabelecer a possibilidade da busca e recolha de dados tanto em sistemas de computador, como outros meios de armazenamentos de dados.

Em ambos os casos o texto convencional impõe ao Estado signatário que se digne a regulamentar, por medidas legislativas e outras cabíveis, a garantir a necessária capacitação dos seus agentes para a atividade de apreensão e proteção de dados de computador acessados. De modo que a tais medidas serão incluídos "o poder de apreender ou similarmente proteger um sistema de computador, parte dele, ou um meio de armazenamento; fazer e manter uma cópia desses dados de computador; manter a integridade dos dados armazenados considerados relevantes; e tornar inacessível ou remover os dados do sistema"[418].

Ressalta-se que ao especialista forense não caberá elaborar juízos valorativos sobre as informações ou *fontes* de prova coletadas. Restringir-se-á unicamente a princípios estabelecidos e metodologia adotada, não contemplando as conclusões decorrentes da análise, de modo que a prova digital se apresente como relevante, resultante de um método e com garantia assegurada de validação[419].

Ainda que definida a ferramenta que se utilize para a aquisição de dados possivelmente úteis à investigação de determinado caso penal, o risco do manuseio de dados ou informações alheias aos fatos investigados por parte dos agentes do Estado é alto, principalmente por não haver limites claramente definidos para o controle das chamadas buscas subjetivas[420]. Ademais, existe uma imensa possibilidade da *fonte* probatória estar misturada a arquivos ou informações irrelevantes aos fatos investigados, originando-se um risco prejudicial

---

[418] Convention on Cybercrime, Budapest, 23.XI.2001 - Article 19 – Search and seizure of stored computer data: 3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to: a) seize or similarly secure a computer system or part of it or a computer-data storage medium; b) make and retain a copy of those computer data; c) maintain the integrity of the relevant stored computer data; d) render inaccessible or remove those computer data in the accessed computer system. Disponível em: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf

[419] WALKER, Cornell. ***Computer forensics: bringing the evidence to court***. Op. cit. p, 5.

[420] KERR, Orin S. ***Executing warrants for digital evidence: the case for use restrictions on nonresponsive data.*** Op. cit. O autor se refere à ausência de limites legais, bem como a ausência de limites estabelecidos pela própria jurisprudência quanto à matéria.

à confidencialidade de terceiros alheios às investigações[421]. Neste aspecto é que se impõe uma restrição maior ao uso de informações ou conhecimentos ocasionalmente encontrados sem a prévia suspeita.

Mais ainda, se impõe a exigência de cautelas básicas de controle para evitar abusos por parte dos agentes estatais[422], afinal de contas, a promiscuidade do dado[423] como característica da investigação informática decorre justamente da heterogeneidade de dados acessados em um sistema informático. Heterogeneidade marcada pelas distintas naturezas dos dados acessados, que podem ser considerados irrelevantes, relevantes para o caso ou constitucionalmente sensíveis (dados pessoais referentes a convicção religiosa, filosófica, política, sexual e etc).

Alguns requisitos úteis à preservação da confidencialidade são destacados por Daniele[424], mas não se mostram suficientes para uma tutela efetiva. A proposta do autor perpassa por estabelecer em rol taxativo as infrações penais passíveis de serem apuradas por determinados métodos tecnológicos, bem como indícios suficientes de autoria e materialidade do cometimento de qualquer destas infrações.

Evidentemente que por se tratar de uma restrição a direitos fundamentais, impõe-se como requisito a reserva jurisdicional. Além da justificação e motivação constitucionalmente imposta, a restrição às buscas subjetivas do agente estatal pode ser possível mediante imposição de um protocolo de busca (*search protocol*)[425] ainda em sede de ordem judicial.

Acredita-se que tal imposição para ser obrigatória deverá ser requisito também exigido por força de lei[426], de modo que ao legislador se inflige o dever de determinar um procedimento que busque o equilíbrio entre a proteção da privacidade e intimidade e os

---

421 DANIELE, Marcelo. ***La prova digitale nel processo penale.*** Op. cit. p, 288. "*Le indagini informatiche, dunque, sono sempre potenzialmente in grado di pregiudicare la riservatezza degli individui. La loro capacità lesiva della privacy è addirittura superiore a quella delle intercettazioni; queste ultime si limitano a carpire le informazioni che la persona intercettata ha deciso di rivelare ad altri, mentre l'analisi dei sistemi informatici e delle reti possono rivelare il contenuto di intere esistenze: abitudini, opinioni politiche, preferenze di ogni genere. In ogni caso, dati riservati che nulla hanno a che fare con la comissione dei reati, e che sono facilmente divulgabili proprio grazie alle tecnologie informatiche e ad internet, in grado di renderle conoscibili da un numero sterminato di persone*".

422 VELASCO NUÑEZ, Eloy. *Limites a las investigaciones y a la prueba en el proceso penal.* In: ***Delitos tecnológicos: definición, investigación, y prueba en el proceso penal.*** Madrid: Editorial Jurídica Sepín, 2016. 13 – 38. p, 20.

423 TORRE, Marco. ***Il captatore informatico: nuove tecnologie investigative e rispetto delle regole processuali.*** Giuffre Editore, 2017. p, 9. Promiscuidade do dado referida pelo autor decorre da diversidade de sua natureza, facilidade e rapidez em sua circulação, desmaterialização e duplicabilidade em seu suporte.

424 DANIELE, Marcelo. ***La prova digitale nel processo penale.*** Op. cit. p, 288.

425 KERR, Orin S. ***Executing warrants for digital evidence: the case for use restrictions on nonresponsive data.*** Op. cit. p, 8.

426 Destaca Orin Kerr que tal imposição ainda não é obrigatória, muito menos pacífica no entendimento das Cortes Americanas.

interesses legítimos da persecução criminal quanto à obtenção destas *fontes* probatórias. Vislumbra-se também a necessária intervenção legislativa "desejável, clara e inequívoca"[427] para punir de forma rigorosa agentes que desvie a finalidade do tratamento de dados recolhidos na atividade investigativa.

Em caso da existência de suporte(s) físico(s) de armazenamento das *fontes* de prova objetos da pretensão investigativa, também se faz fundamental sua identificação e determinação prévia ainda em decisão judicial. A determinação e identificação dos dispositivos físicos alvos da medida se mostra como requisito que além de proteger, em certo grau, a privacidade ou confidencialidade do investigado e de terceiros, fornece um direcionamento aos agentes do Estado quanto à procura de determinado dispositivo informático alvo de apreensão, ou até mesmo alvo da *remote search*.

A identificação dos dispositivos otimiza a busca, ao passo que se mostra demasiado relevante quando levado em consideração o risco de perecimento das *fontes* de provas digitais, seja pela fragilidade característica da própria *fonte* – vez que a exclusão de arquivos pode ser uma programação automática do próprio sistema informático –, seja pelos possíveis riscos de sabotagem à investigação proporcionada pelo investigado[428].

Além de diminuir a possível perda de fontes relevantes para a apuração dos fatos, estabelecer um foco ao investigador especialista é primordial para uma investigação ao mesmo tempo eficiente e efetiva. Por evidente que um foco determinado também se evita a recolha de um volume excessivo de material irrelevante à investigação, bem como se reduz os danos causados à intimidade, privacidade e autodeterminação informativa do sujeito investigado.

Como dito, para a coleta da *fonte* de prova digital é imprescindível que o investigador tenha conhecimentos específicos em Ciência Forense Digital. De acordo com Lund[429], é tão importante uma compreensão abrangente de conhecimentos técnicos quanto o conhecimento dos objetivos da investigação, pois o especialista atuará com instrumentos e procedimentos apropriados que o possibilitem, por exemplo, a recuperação de arquivos excluídos, registros de contas dentre outras informações possivelmente utilizadas, bem como a proteção de tudo aquilo colhido, a demonstração da validação (através da função *hash*),

---

[427] TORRE, Marco. ***Il captatore informatico: nuove tecnologie investigative e rispetto delle regole processuali.*** p, 10.

[428] LUND, Paul. ***An investigator's approach to digital evidence.*** *In: Digital evidence and Electronic Signature Law Review,* Vol. 6. Pario Communications Limited, 2009. p, 220.

[429] Id. Ibidem. "*Need to provide a focus to any forensic examination of digital information, and to integrate it with more traditional forms of investigation to enable digital evidence to be searched effectively. Material that is recovered increases in volume exponentially. As the proportion of irrelevant material increases, so do the chances of missing relevant evidence if investigators have failed to follow traditional investigative methods, such as researching the background and speaking to appropriate employees and others who have relevant information*".

confiabilidade e não contaminação de dados e arquivos[430]. Trata-se de garantir o que Walker[431] denomina de "*cleanliness*" dos dados coletados, ou seja o aspecto "puro" ou a "pureza" dos dados para a validação da informação a ser extraída.

Além de determinar "onde procurar?" as fontes, outros desafios também são impostos pela complexidade da matéria, dentre os quais – afora a admissibilidade da prova – "quais técnicas utilizar?". Walker, com o auxílio de Ryan e Shpantezer, afirma ainda que o especialista forense deve considerar tanto as normas legais, por evidente, como alguns pressupostos essenciais para que a prova digital não seja inutilizada.

Tais pressupostos citados pelo autor foram firmados pela Corte Norte Americana como "*Rule 702 of the Federal Rules of Evidence*" decorrente do julgamento no caso *Daubert v. Merrell Dow Pharmaceuticals*, sendo a própria Corte a sugerir que fossem considerados fatores como "testes prévios das teorias e técnicas empregadas pelo especialista científico", "se houve revisão por outros especialistas", "taxas de erros", "a sujeição da técnica utilizada aos *standards* definidos" e "se as técnicas e teorias aplicadas pelo especialista possui grande aceitação"[432].

Como salienta Gascon Abellan[433], não é que toda fonte de prova que se diga científica (e aqui a prova digital) deva cumprir todos os critérios mencionados, tais servem para que o julgador penal analise a prova de maneira mais acentuada, de modo que provas científicas que por vezes não são substancialmente questionadas assim se tornem. É preciso desmistificar a perfeição da prova cientifica e adequá-la aos postulados processuais penais que impõe o respeito a garantias elementares dos sujeitos[434].

---

[430] RAMALHO, David Silva. **Métodos ocultos de investigação criminal em ambiente digital.** Almedina, 2017. p, 103.

[431] WALKER, Cornell. ***Computer forensics: bringing the evidence to court***. p, 1.

[432] WALKER, Cornell. ***Computer forensics: bringing the evidence to court***. p, 4. "*In ruling on the Daubert case, the Court held that Rule 702 of the Federal Rules of Evidence, adopted in 1973, supplanted Frye. Rule 702 provides: "If scientific, technical, or other specialized knowledge will assist the trier of fact to understand the evidence or to determine a fact in issue, a witness qualified as an expert by knowledge, skill, experience, training, or education, may testify thereto in the form of an opinion or otherwise. [...] In other words, the court gave its suggestion of several factors to be considered: a) whether the theories and techniques employed by the scientific expert have been tested; b) whether they have been subjected to peer review and publication; c) whether the techniques employed by the expert have a known error rate; d) whether they are subject to standards governing their application; and e) whether the theories and techniques employed by the expert enjoy widespread acceptance*".

[433] GASCON ABELLAN, Marina. *Prueba Científica: mitos y paradigmas.* ***Anales de la Cátedra Francisco Suárez,*** 44 (2010), pp. 81 – 103. p, 83. A autora destaca que a prova tida por cientifica adquiriu uma sobrestimada valoração, tanto semântica como epistemológica, e como consequência criou-se um mito de infalibilidade relacionado a esta, uma "salto de fé" incompatível com os próprios critérios da ciência.

[434] TORRE, Marcos. ***Il captatore informático: nuove tecnologie investigative e rispetto delle regole processuali.*** Giufrré Editore, 2017. p, 3.

Os requisitos destacados possibilitam o retorno de um olhar mais crítico tomado pelo julgador penal diante das provas científicas que, pela ausência de cautela e controle na prática processual, paradoxalmente e gradativamente adquiriram "validade" e "valor probatório" com respaldo absolutamente "inquestionável" pelo mero fato de se apresentarem como "científicas".

Por entender que o legislador processual deve voltar sua atenção para as peculiaridades desta atividade probatória é que Kerr[435] afirma se mostrar fundamental a adequação legislativa para a aquisição de fontes probatórias no ambiente digital. Ressalta o autor que a atualização tecnológica constante necessita de uma lei que restaure o equilíbrio entre o fato investigado e a aplicação da norma quanto às formas de investigação.

3.2.4 A preservação da cadeia de custódia digital: A necessária comprovação do dado informático como fonte de prova confiável

O procedimento de manuseio e análise de *fontes* provas em uma investigação e sua documentação em eventos cronológicos, transforma a cadeia de custódia em parte fundamental no procedimento de inserção daquela *fonte* de prova no processo judicial. Trata-se do registro de termos relacionados ao "onde", "quando", "por que", "quem", "como" no uso das informações probatórias[436]. Ademais, antes de discorrer sobre a necessária preservação da cadeia de custódia da prova obtida por novas tecnologias informáticas é preciso (r)estabelecer duas premissas. A primeira delas diz respeito ao "material" obtido a partir da execução do dito método tecnológico. A segunda diz respeito à questionalibidade do próprio método tecnológico utilizado.

Como afirmado acima, quando o método tecnológico corresponder a funções de meio de investigação de prova, tratar-se-á de um método para o descobrimento e a identificação de *fontes* de prova, de modo que a informação adquirida a partir do material recolhido não

---

[435] KERR, Orin S. ***Executing warrants for digital evidence: the case for use restrictions on nonresponsive data.*** Op. cit. p, 10. Kerr propõe uma metodologia de ajustamento da Quarta Emenda às buscas digitais, para restaurar o equilíbrio entre atuação estatal e norma. O autor utiliza como análise o caso *Riley vs. California.* Trata-se de um caso no qual a Corte Estadunidense em pronunciamento tratou como similar, ou melhor "materialmente indistinguível", a busca de dados em aparelhos celulares (que atualmente são mini computadores com a função de telefonia aglutinada) das buscas em materiais físicos. A observação feita pelo autor é para a errônea indiscriminação feita pela jurisprudência norte americana quanto à invasão da privacidade a partir de buscas nestes aparelhos de armazenamento digitais e em itens físicos. Conclui Kerr pela adequação legislativa para uma abordagem peculiar em se tratando de buscas em dispositivos de armazenamento de informação digital.

[436] PRAYUDI, Yudi; SN, Azhari. ***Digital chain of custody: state of the art.*** International Journal of Computer Applications (0975 – 8887) Volume 114, Nº 5, March 2015, p. 1. "*The scope of chain of custody includes all individuals involved in the process of acquisition, collection, analysis of evidence, time records as well as contextual information, which includes case labeling, and the unit and laboratory that process evidence*".

possui nenhum valor probatório. O valor probatório que surgirá a partir do contraditório não está relacionado ao material probatório recolhido pelo *meio de investigação de prova*, mas se refere às *fontes* de provas identificadas por tais métodos e carreadas aos autos processuais por *meios de prova*. Não há possibilidade de se ventilar o material coletado para o processo sob a leviana forma das provas antecipadas, provas cautelares ou outra subespécie que – segundo alguns – dispensaria o contraditório ou o exerceria de modo diferido.

A segunda das premissas, é ensinada por Prado[437] e também possui como ponto fundante o estabelecimento do contraditório. Primeiramente, pelo simples fato de que os métodos ocultos traduzem e verbalizam para o julgador "as supostas qualidades epistêmicas como antídoto contra toda tentativa de enquadramento jurídico". A adoção de métodos ocultos de investigação, realiza-se a partir da não oitiva da parte contrária, de modo que a autoria e a materialidade do ilícito é – por vezes – alcançada pelo debate do significado das imagens e sons e, agora também, dos dados (por vezes auto incriminatórios).

Erroneamente, o meio digital, e incluído está a *fonte* de prova digital, se apresenta salvo da confrontação, ou ainda com uma tácita presunção de fidedignidade que se traduz na confiança injustificada em sistemas informáticos[438]. Como consequência destacada por Prado, trata-se – fundamentalmente – da possível prostração do processo penal como entidade epistêmica e sua disposição como instrumento formal incapacitado, ou subtraído, de possibilidades questionadoras e refutadoras da "verdade", que se coloca a partir da "evidência" gerada pela execução dos métodos de investigação de prova[439].

A "verdade" ou "presunção de fidedignidade" do sistema informático, bem como da *fonte* de prova digital retira equivocadamente o fato humano (proposital ou acidental)[440] da possível contaminação da prova, o que certamente prejudica a questionabilidade caracterizada pelo aspecto da possibilidade de reação presente no direito ao contraditório.

Razão assiste Prado[441] quando afirma que as inovações tecnológicas que conferem suporte a métodos ocultos de investigação também, elas próprias, devem ser objetos de questionamento pelas partes. Bastaria um simples descuido para que se cause modificações ou

---

[437] PRADO, Geraldo. **Prova penal e sistema de controles epistêmicos.** Op. cit. p, 73.
[438] RAMALHO, David Silva. **Métodos ocultos de investigação criminal em ambiente digital.** Op. cit. p, 259.
[439] PRADO, Geraldo. **Prova penal e sistema de controles epistêmicos.** Op. cit. p, 74.
[440] RAMALHO, David Silva. **Métodos ocultos de investigação criminal em ambiente digital.** Op. cit. p, 259.
[441] PRADO, Geraldo. **Prova penal e sistema de controles epistêmicos.** Op. cit. p, 74. "As técnicas de captação de som, imagem e até de captura de outros elementos originalmente produzidos em meio digital não estão imunes à corrupção em termos metodológicos. Muito menos há isenção de risco de manipulação do produto obtido por meios dos métodos ocultos de investigação".

perdas de difícil identificação na *fonte* probatória, que certamente a comprometerão[442]. A simples exploração do sistema de computador, se realizada sem a observação de procedimentos devidos, pode fornecer ao investigador resultados irreparavelmente comprometidos e não confiáveis.

Deste modo, cuidados com a "*impressão digital*" da *fonte* de prova digital devem ser tomados para que a torne admissível no processo. Conhecer o código *hash* dos arquivos digitais, a localização da *fonte* de prova, a assinatura eletrônica de cada objeto, o local certo onde ocorreu a análise do material probatório, o momento do acesso à prova, a identidade daqueles que mantiveram contato com o material recolhido, tornaram-se práticas auditáveis pelos tribunais e pelas partes processuais. Um relatório pormenorizado é fundamental para comprovação da preservação da cadeia de custódia da prova digital[443].

A contaminação da *fonte* probatória pode se dar de duas maneiras distintas. A primeira, mediante um contato físico inapropriado ao suporte ou dispositivo informático. Marshall esclarece que tal forma de contaminação ainda não ganhou preocupação devida, mas que os cuidados referentes à coleta de provas físicas podem beneficiar a investigação digital de modo a ser possível identificar a partir das impressões digitais de usuários, marcas de ferramentas em um disco rígido ou ainda, a identificação do(s) último(s) usuário(s) daquele dispositivo informático. Desta forma, evitar a contaminação física durante a apreensão do dispositivo informático pode ser demasiado importante[444].

Outra forma de contaminação da *fonte* probatória decorre do contágio digital. Esta se relaciona diretamente com o objeto central da presente pesquisa. Como dito acima a alterabilidade é característica fundante do dado informático, ou *fonte* de prova digital. Bastar-se-á o mínimo de dúvida acerca da integridade da *fonte* probatória, ou seja, o levantamento da hipótese de adulteração do material para transformá-la em fonte inconfiável. Portanto, a preservação da cadeia de custódia consiste em neutralizar a possível suspeita da alteração do dado, quer dizer, reduzir o risco da perda da originalidade do dado e com isso garantir confiabilidade e integridade.

---

[442] BARTOLI, Laura e MAIOLI, Cesare. ***La cadena di custodia del dato digitale: tra anelli solidi e anelli mancanti.*** In: *Trattamento e scambio della prova digitale in Europa.* BIASIOTTI, Maria Angela; EPIFANI, Mattia; TURCHI, Fabrizio (a cura di). Edizioni Scientifiche Italiane. 2016. p, 139. "*basta una disattenzione per causare modifiche o perdite difficili da individuare: la semplice esplorazione del sistema informatico, se non svolta con la debita cura, può consegnare all'investigatore risultati irrimediabilmente compromessi, inaffidabili*".

[443] GIOVA, Giuliano. ***Improving Chain of custody in forensic investigation of eletronic digital systems.*** IJCSNS International Journal of Computer Science and Network Security, VOL. 11 No. 1, January 2011. p, 2.

[444] MARSHALL, Angus. ***Digital forensics: digital evidence in Criminal Investigation.*** Wiley-Blackwell. 2008. p, 41.

Neste sentido, Ramalho[445] descreverá o direito a um contraditório qualificado voltado aos relatórios diligenciais da condução investigativa, ou da recolha da prova digital. A importância dada pelo autor a tais relatórios consiste na justa comprovação de diligências realizadas a fim de se obter *fontes* de prova, ou seja, (I) a compreensão da diligência de recolha das *fontes* de provas, (II) a garantia do cumprimento dos procedimentos forenses que asseguram a cadeia de custódia da prova e (III) o afastamento de hipóteses de contaminação da prova por terceiros[446]. Trata-se, de responder perguntas relacionadas à atividade probatória como "o que", "como", "quem", "quando", "por quê" e "onde"[447-448] e desta forma aprimorar métodos de preservação da cadeia de custódia da prova, preenchendo espaços no procedimento que prejudicam a confiabilidade do material probatório.

Como assevera Prado[449] no direito norte americano se impõe à acusação uma obrigatoriedade de estabelecer a cadeia de custódia identificando os elos entre as diversas atividades que compõem o procedimento probatório para aferir o valor da informação obtida. A cisão de qualquer destes elos pode causar a inadmissibilidade da prova e consequentemente destruir seu valor probatório. Isto posto que se trata de um procedimento capaz de evitar as práticas que ceifam a produção probatória com ilicitudes, de modo que a garantia da preservação da cadeia de custódia alcance um *status* constitucional[450].

---

[445] RAMALHO, David Silva. **Métodos ocultos de investigação criminal em ambiente digital.** Op. cit. p, 258.

[446] RAMALHO, David Silva. **Métodos ocultos de investigação criminal em ambiente digital.** Op. cit. p, 258. O autor destaca de modo não exaustivo alguns pontos de referência cujos relatórios devem constar desejavelmente, como "(1) notas preparadas durante a fase de exame; (2) detalhes sobre o modo como a investigação foi conduzida e o meio de obtenção de prova a partir do qual a informação foi recolhida; (3) detalhes sobre a técnica e o modo de garantia da cadeia de custódia; (4) a validade dos procedimentos técnicos utilizados, à luz dos requisitos impostos pelo estado da arte; e, (5) informação sobre o que foi descoberto a partir da informação recolhida. Entre a informação sobre os dados recolhidos deverão constar, entre outros elementos, (a) os ficheiros concretamente relacionados com o tema da investigação, bem como outros ficheiros aptos a sustentar as conclusões do especialista, como sejam ficheiros eliminados e recuperados; (b) o tipo de pesquisa efetuada, incluindo os termos de pesquisa, os programas objeto da pesquisa e os programas utilizados para recolher a prova; (c) informação relevante extraída a propósito do uso da *internet*, como o histórico de visitas e ficheiros de *logs*; (d) a eventual existência de técnicas anti-forenses no sistema informático, designadamente de eliminação e dissimulação de ficheiros; (e) o registro de datas e horas de todas as diligências efetuadas; (f) a possibilidade da prova ter sido fabricada por um terceiro, tendo inclusivamente em consideração o grau de segurança informática física e lógica do sistema visado; e (g) a fidedignidade do sistema e do processo de criação de registros e gravações".

[447] COSIC, Jasmin; COSIC, Zoran. ***Chain of custody and life cycle of digital evidence.*** Computer Technology and Application 3 (2012) 126-129 p, 127. Os autores propõe o conceito de *DEMF* (*Digital Evidence Management Framework*) que se baseia em uma estrutura composta por instrumentos e ferramentas que servem para garantir a segurança da cadeia de custódia da prova digital. A proposta consiste no uso de características biométricas para assinatura digital (quem), *timestamps* para adicionar um tempo registrado (quando), usar alguns serviços da web (ex. google maps, ou GPS) para a geo localização (onde) e *hashing* e assimetria criptográfica para garantir a confiabilidade das provas digitais.

[448] GIOVA, Giuliano. ***Improving Chain of custody in forensic investigation of eletronic digital systems.*** Op. cit. p, 4 – 5.

[449] PRADO, Geraldo. **Prova penal e sistema de controle epistêmicos.** Op. cit. p, 81 – 82.

[450] *Status* Constitucional por permitir o exercício do direito à ampla defesa e ao contraditório, tendo em vista que a comprovação da preservação da cadeia de custódia possibilita a garantia de que a prova sob a qual incide o contraditório possui "mesmidade" à *fonte* de prova coletada.

Em virtude da prova possuir natureza persuasiva[451], carreada aos autos processuais por *meios* de prova dotados de linguagem, há que se notar que a informação dela decorrente – ainda que não confiável pela quebra da cadeia de custódia – poderá influenciar[452] na formação cognitiva do juiz acerca do caso penal[453]. Este contágio prejudicaria a tarefa epistêmica do processo penal, uma vez que se é possível perceber uma "ilegalidade de base"[454] do material probatório – após o rompimento dos elos que ligam a cadeia de custódia – será inadmissível a *fonte* de prova digital. Sendo ilícita, pela ilegalidade de base, impõe-se o desentranhamento desta prova do autos processuais, porquanto que inadmissível[455] devido a violação da confiabilidade probatória e portanto de seu status constitucional.

Todavia, a regra imposta pelo artigo 157 do Código de Processo Penal brasileiro, ao mesmo tempo em que atribui a prova ilícita como inadmissível, a contrassenso impõe seu desentranhamento. Trata-se de verdadeira atecnia processual, pois se inadmissível a prova no processo, não poderia ser carreada aos autos, portanto, também não poderia ser desentranhada. Em outras palavras, somente poderá ser desentranhada do processo uma prova admissível, ou seja, provas inadmissíveis não podem ser entranhadas nos autos processuais.

A discussão, portanto, versa novamente acerca da qualidade do contraditório, de modo que em um primeiro momento, para que seja admissível uma *fonte* de prova digital no processo, em face à presunção de fidedignidade cega[456] que circunda os sistemas informáticos, deverá ser comprovada a fiabilidade da *fonte probatória* a partir do contraditório sobre os critérios adequados de recolha, preservação e análise dos dados. A preservação da cadeia de custódia da prova é requisito de admissibilidade da prova.

Um posterior contraditório será também efetivado. Contudo, este último voltado ao debate do conteúdo informacional trazido ao processo pela *fonte* probatória recolhida, que nesta

---

[451] Mas não meramente persuasiva, conforme a ressalva de Prado – com o auxílio de Taruffo – a prova também deve servir essencialmente ao conhecimento dos fatos.

[452] Não se pode descartar os efeitos que decorrem das informações trazidas para o processo mediante ilicitudes probatórias e sua relação com a formação cognitiva do juiz. Sobre os prejuízos decorrentes do chamado "efeito primazia" ler RITTER, Ruiz. **Imparcialidade No Processo Penal: Reflexões a partir da Teoria da Dissonância Cognitiva.** Porto Alegre, PUCRS. Dissertação de Mestrado, 2016.

[453] Para blindar a cognição judicial destes vícios que decorrem da aquisição probatória, aplicando-se um juízo de admissibilidade da prova penal, faz necessário a institucionalização de mecanismos processuais cabíveis para cumprir com tal função. Neste ponto, o debate acerca da implementação do Juiz de Garantias se mostra pertinente.

[454] PRADO, Geraldo. **Prova penal e sistema de controle epistêmicos.** Op. cit. p, 88.

[455] Artigo 157, CPP – São inadmissíveis no processo, devendo ser desentranhadas do processo, as provas ilícitas, assim entendidas as obtidas em violação a normas constitucionais ou legais.

[456] RAMALHO, David. Silva. **Métodos ocultos de investigação criminal em ambiente digital.** Op. cit. p, 261. "é comum atribuir-se aos sistemas informáticos e à prova digital uma tácita presunção de fidedignidade, por vezes em prejuízo da presunção de inocência. Tal facto deve-se, em parte a uma certa confiança injustificada em sistemas informáticos, à qual subjaz a ideia de que as máquinas tendem a não cometer erros".

oportunidade já admitida como *fonte* de prova lícita. Como afere Ramalho[457], não basta a mera possibilidade formal do exercício do contraditório, necessita-se dispor às partes a possibilidade de *controlar a prova*, aferindo sua pertinência, fidedignidade e aptidão para a demonstração de qualquer das hipóteses fáticas trazidas por elas.

Na legislação espanhola, segundo Velasco Nuñez[458], assegura-se a originalidade da *fonte* de prova pela clonagem do dado, ou seja a realização de uma cópia idêntica (*image*). Trabalha-se com a cópia autêntica do original e desta forma se assegura a inalterabilidade da fonte probatória, garante-se a integridade dos dados e a preservação de seu conteúdo. O manuseio da cópia na atividade investigativa permite a prova em contraste pela preservação da *fonte* originária, possibilitando-se assim novas análises. Caso a apreensão de suportes físicos de armazenamento de dados informáticos se realize no curso de uma busca e apreensão, por exemplo, se presente o investigado, e *el Letrado de la Administración de Justicia*, recomenda-se que o procedimento de clonagem se realize no local, no exato instante da apreensão.

Exceto quando o procedimento de clonagem se apresente demasiadamente longo, complexo ou que não esteja presente o investigado (pois sua presença é requisito formal de garantia processual), deve-se nestes casos se realizar em sede judicial na presença do *Letrado de la Administracion de Justicia*. Quando não for possível a clonagem do material probatório logo no local da apreensão do suporte eletrônico, ressalta Velasco Nuñez que a *LECrim* espanhola proíbe que o procedimento tecnológico de clonagem seja realizado sem a presença do *Letrado de la Administracion de Justicia*. O investigado deverá ser citado para que, se assim quiser, presencie o procedimento tecnológico de clonagem, por meio de seu defensor, garantindo-se seu direito de defesa[459].

---

[457] RAMALHO, David. Silva. **Métodos ocultos de investigação criminal em ambiente digital.** Op. cit. p, 261.

[458] VELASCO NUÑEZ, Eloy. ***Aseguramiento, custodia de la prueba tecnológica, análisis y valor.*** In: ***Delitos tecnológicos: definición, investigación y prueba em el proceso penal.*** Madrid. Editorial Jurídica Sepín, 2016. p, 89-93. "Art. 588 sexies c) 1. In fine LECRIM; Art. 479 LECRIM", O autor ressalta para o importante papel do "*Letrado de la Administración de Justicia*" – tais seriam os "Secretários Judiciais" existente no Poder Judiciário brasileiro – na diligência de clonagem, posto que atende à fé pública e à custódia original do efeito tecnológico. Assevera que a jurisprudência do STS, 15 de novembro de 1999, equivoca-se por afirmar não ser necessária a presença do "Letrado de la Administracion de Justicia" tendo em vista que não seria função do referido funcionário público, verificar a veracidade técnica da cópia de dados, mas o de ordenar as operações dos técnicos e custodiar as provas para verificar que não falhem em seu armazenamento. A veracidade técnica, portanto, segundo o entendimento do tribunal se daria a partir da garantia da utilização do algoritmo *hash* que se verifica ao final da clonagem, para contrastar a certeza de toda a transferência de dados e informações são fidedignas. Contudo, Velasco Nuñez afirma que a presença do *Letrado de la Administración de Justicia* resulta do seu papel de garantidor da legalidade. Não se tratando de sua presença, mera formalidade, mas uma forma de garantia procedimental.

[459] VELASCO NUÑEZ, Eloy. ***Aseguramiento, custodia de la prueba tecnológica, análisis y valor.*** Op. cit. p, 91.

Marshall[460] destaca quatro princípios que servem para a orientação acerca do manuseio e processamento de provas digitais, ou melhor dizendo, recolha e processamento de *fontes* de prova digital. O primeiro destaca que "nenhuma ação tomada pelas agências policiais ou seus agentes deve alterar os dados mantidos em um computador ou mídia de armazenamento que possam ser subsequentemente invocados no Tribunal"[461]. Um segundo princípio afirma que "nas circunstâncias em que uma pessoa acredite que seja necessário acessar os dados armazenados em um computador ou em mídia de armazenamento, tal pessoa deve ser competente para tanto, e ser capaz de fornecer provas explicando a relevância e as implicações de suas ações"[462].

A seu turno, destacado pelo terceiro princípio está a possibilidade de "através do registro de todos os procedimentos referentes ao computador ou a recolha da *fonte* de prova digital" um terceiro independente possa alcançar o mesmo resultado após análise. Ou seja, fundamental é o registro dos procedimentos, ou aquilo que se denomina de cadeia probatória[463]. Por fim, em se tratando de um quarto princípio, discorre Marshall acerca da "responsabilidade da pessoa competente para a investigação de garantir que a lei e estes princípios anteriores sejam cumpridos"[464].

A imaterialidade como característica da *fonte* de prova digital faz com que aumentem as dificuldades dos registros e documentações cronológicas necessárias para averiguar o não contágio no material probatório. O acesso remoto ao material digital recolhido também poderá permitir a análise probatória à distância e simultânea por diversos especialistas, de modo que regulamentar por meio de lei todo o procedimento de recolha, análise e preservação da *fonte* probatória digital se faz demasiadamente necessário. Não apenas a forma do procedimento de registro e relatório, mas fundamentalmente a implementação técnica do tratamento da *fonte* de prova digital[465].

---

[460] MARSHALL, Angus. ***Digital forensics: digital evidence in Criminal Investigation.*** Op. cit. p, 19-20. Destaca o autor que tais princípios são diretrizes propostas pela Associação de Chefes de Polícia da Inglaterra e dos Países de Gales relacionadas à recolha e o processamento de *fontes de prova* digital.

[461] "*No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court*".

[462] "*In circumstances where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions*".

[463] "*An audit trail or other record of all processes applied to computer based electronic evidence should be created and preserved. An independente third party should be able to examine those processes and achieve the same result*".

[464] "*The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to*".

[465] PRAYUDI, Yudi; SN, Azhari. ***Digital chain of custody: state of the art.*** International Journal of Computer Applications (0975 – 8887) Volume 114, Nº 5, March 2015, p. 2. Discorrem os autores que a lei deve exigir informações detalhadas quanto ao processo investigativo, desde a assinatura do objeto analisado, identidade das

Portanto, é fundamental a exigência de lei proporcional que estabeleça diretrizes e possibilite o cumprimento de enunciados de cabimento das medidas que garanta a fiabilidade probatória do método (ou do procedimento probatório) de recolha das *fontes* de prova[466]. De mesma importância é a complementar limitação e exigência da reserva de jurisdição quando se tratar da incidência de métodos investigativos ou probatórios que atentem diretamente contra direitos fundamentais.

Tais garantias constitucionais, voltadas a atender a preservação da fiabilidade do material probatório, decorrem do axioma *nulla poena sine probatione*. Comprovar a fiabilidade das *fontes* probatórias se traduz como remédio jurídico-processual que evita o uso subjetivo do material recolhido pela atividade probatória sem exigências razoáveis de idoneidade probatória[467].

Falar em cadeia de custódia da prova, a seu turno, é ter consciência de que esta deriva dos requisitos indispensáveis à atividade probatória, como a identidade, a integridade e a autenticidade[468]. Trata-se de alcançar a observância da manutenção integral, ou imodificabilidade, do material probatório digital, sua "mesmidade". De certa forma, é uma garantia de que não será valorada uma prova distinta daquela coletada, ou seja, uma garantia capaz de evitar uma contaminação, possíveis alterações, manipulações, substituições, destruições, ou trocas entre *fontes* probatórias[469].

---

partes que manuseiam ou interagem com a prova, o tempo de acesso e todas as descrições que se referem a transações e qualquer acesso necessário à fonte de prova.

[466] Nos EUA, por exemplo, a admissão da prova digital é regulada pela *Federal Rule Evidence 901*, combinado em alguns casos diversas outras normas sobre a busca e apreensão das provas digitais. Como ressalta Giova, (GIOVA, Giuliano. ***Improving Chain of Custody in Forensic Investigation of Electronic Digital Systems***. Op. cit. p, 3) o *USA Patriot Act* resultou em um número significativo de mudanças em diversos estatutos federais que versam sobre a busca e apreensão de computadores e da aquisição de provas digitais ou eletrônicas. De igual modo, o Canadá (*Canada Evidence Act*) tratou especificadamente da autenticação de provas informáticas impondo a carga de provar sua autenticidade. (***Authentication of electronic documents 31.1*** *Any person seeking to admit an electronic document as evidence has the burden of proving its authenticity by evidence capable of supporting a finding that the electronic document is that which it is purported to be*). Disponível em: https://laws-lois.justice.gc.ca/eng/acts/C-5/page-5.html#docCont. Acesso em out, 2018.

[467] PRADO, Geraldo. **Prova penal e sistema de controles epistêmicos.** Op. cit. p, 75.

[468] VELASCO NUÑEZ, Eloy. ***Aseguramiento, custodia de la prueba tecnológica, análisis y valor.*** Op. cit. p, 90.

[469] "Mesmidade" como qualidade de ser do mesmo. VELASCO NUÑEZ, Eloy. ***Aseguramiento, custodia de la prueba tecnológica, análisis y valor.*** Op. cit. p, 90.

Um modelo de procedimento minimamente adequado[470] deve conter as seguintes etapas: a recolha, a autenticação, o exame, a análise e o relatório[471]. A recolha é a etapa que corresponde à identificação e à coleta, cujos investigadores forenses devem buscar, entre o material disponível, *fontes* de prova relevantes. Como dito acima, trata-se de fase marcada pelo alto risco de impacto na cadeia de custódia da prova digital[472], sendo assim é que se reafirma a necessária capacitação daqueles sujeitos (investigadores especialistas, peritos ou policiais) que terão o primeiro contato com o dispositivo informático ou dado propriamente dito[473]. Marshall[474] vincula esta etapa procedimental à *pré-visualização* da *fonte* de prova digital que perpassa pelo contato direto do investigador com o dispositivo informático alvo.

A *Pré-visualização* (*Previewing*) se executará tanto de modo *on-line* como *off-line*. A pré-visualização *on-line* – relevante para a presente pesquisa – se mostra como método arriscado de análise probatória pelo fato de serem utilizados sistemas de visualização em tempo real (acesso remoto por *softwares*) que padecem da falta de confiabilidade. Isto porque alguns destes sistemas contém programações que ao permitirem o acesso remoto do dispositivo alvo pelo invasor, alteram os programas e sistemas já inseridos no dispositivo invadido, na intencionalidade de disfarçar a invasão.

Deste modo, sendo difícil demonstrar que os resultados proferidos a partir da utilização destes sistemas são completos, precisos e seguros. Assim, até que provada e demonstrada a confiabilidade do *software* empregado, este deverá ser considerado impreciso. Portanto, o objetivo principal do procedimento de *pré visualização online* é justamente a certificação de que aquele dispositivo alvo poderá ser relevante para a investigação, e deste modo, ser passível de uma apreensão física para análise aprofundada em laboratório.

---

[470] Fala-se aqui em modelo minimamente adequado para atestar a confiabilidade da cadeia de custodia da prova digital, pois não é possível – até o presente momento – afirmar categoricamente que exista um único modelo ideal. Existem diversos estudos em desenvolvimento sobre aquilo que possa vir a ser um modelo precisamente confiável, para tanto recomenda-se a leitura de COSIC, Jasmin; BACA, Miroslav. ***Do We Have Full Control Over Integrity in Digital Evidence Life Cycle?*** Proceedings of the ITI 2010 32nd Int. Conf. on Information Technology Interfaces, June 21-24, 2010, Cavtat, Croatia.

[471] GIOVA, Giuliano. ***Improving Chain of custody in forensic investigation of eletronic digital systems.*** Op. cit. p, 5.

[472] COSIC, Jasmin; COSIC, Zoran. ***Chain of custody and life cycle of digital evidence.*** Op. cit. p, 128.

[473] COSIC, Jasmin; BACA, Miroslav. ***Do We Have Full Control Over Integrity in Digital Evidence Life Cycle?*** Op. cit. p, 430. Os autores salientam que o processo de coleta de provas digitais não é tão simples e os sujeitos que executam o primeiro contato com o material devem saber o que devem fazer neste momento. "Isso não é trivial, se sabemos que apenas um passo em falso pode ser fatal". Ressaltam, por exemplo, que se se desligar o computador "ativo" com o sistema operacional Windows XP, mais de 50 arquivos serão alterados e 5 novos arquivos criados na próxima inicialização. Isso significa que um momento de desatenção é suficiente para perder evidências e violar sua integridade da prova.

[474] MARSHALL, Angus. ***Digital forensics: digital evidence in Criminal Investigation.*** Op. cit. p, 43.

A ressalva feita pelo autor[475] é justamente que, após a utilização do referido procedimento, será muito difícil a comprovação de que não houve alterações no sistema informático alvo, sendo assim, para fins de Processo Penal serão inconfiáveis as provas recolhidas, de modo a servirem tão somente aos procedimentos de investigação e inteligência.

Pois bem, recolhido o material probatório e nele contidas potenciais *fontes* de prova digital, na fase denominada "exame" se ocupará precisamente da identificação e a separação daquelas de maior relevância para o processo[476]. A *image*¸ como já se referiu, trata-se da operacionalização de uma fotografia digital, uma cópia mestra protegida, que evita o manuseio das *fontes* probatórias originais e assim se conserva sua integralidade.

O procedimento de cópia integral em modo *off-line* é um procedimento mais simples, cujo o dispositivo suspeito é conectado a uma estação de processamento e geração de *images* (*imaging workstation*) e a um bloqueador de gravações (*write-blocker*)[477] que consiste em uma ferramenta informática que evita a introdução ou alteração de dados por um sistema informático[478].

Quando não for possível apreender ou desligar o sistema alvo das "buscas" por *fontes* probatórias, ou ainda diante da impossibilidade de conectar o sistema informático às estações de processamento e geração de *images* (*imaging workstation*), poder-se-á utilizar-se de métodos de apreensão e geração de *images* de modo *online.* Nesta ocasião, afirma Marshall, que o dispositivo visado permanece no local em que foi apreendido e são utilizadas ferramentas de geração das cópias integrais "ao vivo", em tempo real. Esta metodologia pode apresentar riscos de contaminação semelhantes aos da pré-visualização *online*, porém o uso de ferramentas confiáveis pode reduzir estes problemas[479].

Criada a imagem fiel da *fonte* de prova digital, é preciso protege-la de alterações, confirmar sua integridade e validar sua autenticidade. Verificações podem ser efetuadas para demonstrar que os procedimentos sequenciais não incidiram no material probatório de modo a

---

[475] MARSHALL, Angus. ***Digital forensics: digital evidence in Criminal Investigation.*** Op. cit. p, 44-46.
[476] COSIC, Jasmin; COSIC, Zoran. ***Chain of custody and life cycle of digital evidence.*** Op. cit. p, 128.
[477] MARSHALL, Angus. ***Digital forensics: digital evidence in Criminal Investigation.*** Op. cit. p, 47. "*Offline imaging is the simplest procedure, although it can be time consuming depending on the size of the device to be imaged. In this process, the suspect device is connected to an imaging workstation using a write-blocker [...]. The imaging software is then used to read data fromthe device and store it to either a file or separate device. Once imaging is complete, the first copy is usually considered to be the master copy and further working copies can be generated as required. Of course, there is still a requirement to show that the master copy and working copies are completely accurate and have not been modified in any way during imaging or examination*".
[478] RAMALHO, David. **Métodos ocultos de investigação criminal no ambiente digital.** Op. cit. p, 124.
[479] MARSHALL, Angus. ***Digital forensics: digital evidence in Criminal Investigation.*** Op. cit. p, 47. "*The trusted tools allow the examiner to copy the device to either an external storage device, such as a USB hard disc, or across a network to a dedicated storage server*".

comprometer sua integridade, ou seja, não trouxeram efeitos adversos acidentais ou intencionais que comprometam a custódia da prova. Destacada técnica é possível por meio da utilização da função *hash*[480] que permite verificar "assinaturas digitais efetivamente exclusivas para qualquer parte dos dados digitais"[481].

Ramalho discorre que a função *hash* é aplicada a certos documentos ou a um conjunto de dados informáticos, de modo a criar um código alfanumérico que funciona como uma *impressão digital*, designada de *hash*[482-483]. Os algoritmos referentes à *image* produzida devem ser idênticos aos originais, tendo em vista a "mesmidade" dos dados copiados. A "mesmidade" é verificável pois a aplicação da função *hash* em um mesmo conjunto exato de dados, produz sempre o mesmo valor *hash*[484], de modo que "a modificação de até mesmo um único *bit* resulta radicalmente em diferentes valores calculados em *hash*"[485], tornando-se contestável a integridade da prova penal.

Por sua vez, a preservação, ou armazenamento, como terceira etapa também é necessária para efetivar o rastreamento das *fontes* de prova. Deste modo, ao mesmo tempo em que possibilita o conhecimento acerca das circunstâncias da recolha da prova, permite ao processo sua qualidade de entidade epistêmica. O armazenamento como etapa procedimental, bem como o transporte das *fontes* de provas, deve corresponder à manutenção da cadeia de custódia da prova digital[486] e o registro cronologicamente orientado de todas as análises deve ser observado[487].

---

[480] Calculo matemático que gera um valor numérico baseado no *input* de dados. Este valor numérico é referido como valor de *hash.* COSIC, Jasmin; BACA, Miroslav. ***(Im)Proving Chain of Custody and Digital Evidence Integrity with Time Stamp*.** 1226 - 1230. 10.13140/RG.2.1.1336.0725. 2010. p, 2. Disponível em: https://www.researchgate.net/publication/224163003_Improving_chain_of_custody_and_digital_evidence_integrity_with_time_stamp. Acesso em set 2018.

[481] MARSHALL, Angus. ***Digital forensics: digital evidence in Criminal Investigation.*** Op. cit. p, 47.

[482] RAMALHO, David. **Métodos ocultos de investigação criminal no ambiente digital.** Op. cit. p, 124. "Os algoritmos mais utilizados atualmente são o MD5 (*Message Digest 5*) e o SHA-1 (*Secure Hash Algorithm*)".

[483] Discorre Giuliano Giova (***Improving Chain of Custody in Forensic Investigation of Electronic Digital Systems***. Op. cit. p, 3) que alguns *softwares* forenses modernos além de descreverem onde cada arquivo está localizado e suas muitas propriedades, incluindo data de criação e datas de acesso, permitem a criação de chaves específicas de acesso a usuários. Adotam o conceito de autenticação central e permissão de concessão a servidores que concedem tais chaves de sessão para usuários autorizados, monitorando desta forma toda a atividade de exame da cadeia de custódia da prova digital.

[484] RAMALHO, David. **Métodos ocultos de investigação criminal no ambiente digital.** Op. cit. p, 125.

[485]MARSHALL, Angus. ***Digital forensics: digital evidence in Criminal Investigation.*** Op. cit. p, 48. "*Hashing algorithms similar to checksums are used to calculate digital "signatures" which are effectively unique for any piece of digital data. At the highest level, one or more hash values will be computed for the data on the original device. Because the image has been produced from this device, and contains identical data, the hash value for the image should match, exactly, the value for the original. Hashing algoriths such as MD5 [42], SHA-1 [36] and SNEFRU[31] are very sensitive to changes in data, and the modification of even a single bit (1/8 of a byte) in the largest image results in radically different hash values being calculated*".

[486] COSIC, Jasmin; COSIC, Zoran. ***Chain of custody and life cycle of digital evidence.*** Op. cit. p, 128.

[487] COSIC, Jasmin; BACA, Miroslav. ***(Im)Proving Chain of Custody and Digital Evidence Integrity with Time Stamp*.** Op. cit. p, 3.

A criação de um padrão para armazenamento é muito importante para que se tenha acesso universal aos dados recolhidos e armazenados, de modo que o formato de armazenamento (*Digital Evidence Container*) permita uma unicidade procedimental. A *Digital Evidence Bag*[488], como configuração de armazenamento abrangente, por exemplo, trata-se de um formato padrão que compreende provas digitais ou um conjunto de objetos incluídos em uma estrutura hierárquica de provas digitais. A padronização (*stantard*) dos procedimentos de tratamento e de armazenamento permite um processamento consistente e simplificado. Segundo Lim, Gyu Lee e Wook Han, este formato é projetado para incluir os metadados criados durante a investigação, tais como informações de auditoria para os dados das *fontes* de provas recolhidas. O conceito da *Digital Evidence Container* foi desenvolvido originalmente para comportar um formato simples de armazenamento de *image*, todavia passou a comportar um formato multifuncional que reduz o volume inicial (compactando-o) e garante a integralidade da *image*[489].

Cosic e Miroslav ressaltam a importância do registro das datas e dos horários referentes aos procedimentos condizentes com o material probatório digital. Afirmam que o *Time Stamp*[490] no mundo digital marca o momento específico do tempo na investigação criminal em formato digital. A preocupação da admissibilidade da prova digital faz com que se

---

[488] LIM, Kyung-Soo; GYU LEE, Deok; WOOK HAN, Jong. ***A New Proposal for a Digital Evidence Container for Security Convergence***. IEEE International Conference on Control System, Computing and Engineering. 2011. p, 172. "*This design concept aims to develop a standard format in which digital evidences from diverse devices, including computers, mobile devices, and network systems, can be stored*".

[489] LIM, Kyung-Soo; GYU LEE, Deok; WOOK HAN, Jong. ***A New Proposal for a Digital Evidence Container for Security Convergence***. Op. cit. p, 172. "Os metadados são armazenados em texto simples e todos os dados são registrados no formato binário bruto para garantir seu uso universal". Os autores propõe um novo formato de Digital Evidence Container que denominaram de *XeBag*, não adentraremos nas peculiaridades do formato desenvolvido, mas basicamente se trata de uma melhor programação de padronização de informações coletadas como *fontes* de prova e armazenadas em um formato universalmente acessível. Contudo, os requisitos elencados pelos autores para um formato padronizado merecem destaques: *Generalidade*: O design deve ser baseado em tecnologia de modo que possa ser geralmente usado para diversas fontes de dados; *Preservação*: ambos os metadados relevantes e dados originais deve ser coletados e preservados; *Integridade*: deve haver um dispositivo para garantir a integridade dos dados da evidência original; *Unificação*: Diversos tipos de dados de evidência devem ser manipulados em um formato unificado; *Escalabilidade*: o formato deve ser escalável com o aumento do volume de dados, e o tamanho total dos dados não devem aumentar significativamente; *Compressibilidade*: o projeto deve fornecer um recurso para reduzir o tamanho dos dados originais; *Segurança*: O design deve fornecer um mecanismo de segurança para proteger o formato de armazenamento de evidências.

[490] São ferramentas utilizadas para marcar o exato horário referente a um *log* (data/hora). Em sistemas de arquivos, a data e a hora podem se referir às datas e horas relacionadas à criação do arquivo ou a modificação do arquivo. (COSIC, Jasmin; BACA, Miroslav. ***(Im)Proving Chain of Custody and Digital Evidence Integrity with Time Stamp*.** Op. cit. p, 3).

imponha o registro do exato momento de acesso à *fonte* de prova, quem a acessa, onde a acessa[491] e quando é transportada[492].

Os autores explicam que o registro do tempo se dá desde o primeiro contato com a *fonte* de prova digital, de modo que após a criação de uma numeração de identificação do arquivo (*hashing*), envia-se a numeração *hash* a um terceiro competente (*Time Stamps Authority*) que a relaciona com um registro de data e hora, calcula um novo valor *hash* e assina digitalmente o arquivo gerado com uma chave de assinatura digital protegida.

O *TSA* envia o arquivo registrado para o investigador, que também possui uma chave de acesso e assinatura protegida. O procedimento se repete em todas as etapas de análise do material probatório, desta forma é possível comprovar cronologicamente todos os acessos às *fontes* de prova em qualquer fase da investigação criminal[493].

A fase que fecha o ciclo da cadeia de custódia é o relatório ou publicação, fecha o ciclo da cadeia de custódia, contudo não significa dizer que se trata da fase final. O relatório da análise probatória deve servir como documento idôneo capaz de sustentar as hipóteses defensivas ou acusatórias no processo judicial. A linguagem técnico-informática referentes aos procedimentos adotados devem ceder espaço para uma forma especificada de linguagem acessível aos sujeitos processuais. A descrição dos procedimentos não deve ser resumida, mas minunciosamente elaborada para que cumpra com sua função de reforçar as garantias de controle do sujeito investigado[494]. De modo que a etapa final, propriamente dita, é marcada pelo arquivamento do material probatório (ou destruição das *fontes* irrelevantes)[495].

---

[491] COSIC, Jasmin; BACA, Miroslav. ***Do We Have Full Control Over Integrity in Digital Evidence Life Cycle?*** Op. cit. p, 432. Os autores afirmam que quanto à localização de "onde" o acesso à *fonte* de prova ocorre ainda é difícil de se precisar. Para a preservação da cadeia de custódia, é importante saber onde ocorreu o acesso à prova digital. Contudo, "há falta de pesquisas sobre este tema, e algumas organizações (IOCE, SWGDE, DRWS, etc) apenas propõe a documentação de "onde" estava a prova descoberta, coletada, arquivada, armazenada, e transferida. Não havendo detalhes sobre como implementar tal proposta".

[492] "*Time stamp and digital time stamping play a very important role in the digital forensics, because there is a need for knowing the time of certain moments in the investigation process. It is very important to know the answer to the question which we can be asked in the courtroom: "When was the digital evidence accessed, how long the staffs have been in touch with the evidence? Next question could be:"How long can we prove the integrity of the digital evidence that we signed*". COSIC, Jasmin; BACA, Miroslav. ***Do We Have Full Control Over Integrity in Digital Evidence Life Cycle?*** Op. cit. p, 432.

[493] COSIC, Jasmin; BACA, Miroslav. ***(Im)Proving Chain of Custody and Digital Evidence Integrity with Time Stamp*****.** Op. cit. p, 5.

[494] RAMALHO, David Silva. **Métodos ocultos de investigação criminal em ambiente digital.** Op. cit. p, 145.

[495] COSIC, Jasmin; COSIC, Zoran. ***Chain of custody and life cycle of digital evidence.*** Op. cit. p, 128.

4 *MALWARE* DO ESTADO: UMA (NOVA) METODOLOGIA DE INFILTRAÇÃO NAS INVESTIGAÇÕES INFORMÁTICAS

O cenário atual de complexidades protagonizado pela informática impregna o âmbito jurídico e gera um impacto significativo no Direito Processual Penal, de modo que técnicas de investigação criminal atreladas a novas tecnologias se mostram carentes de uma legislação adequada que estabeleça balizas à prática processual. Mesmo que a intervenção estatal por meio da tecnologia se mostre sutil, por vezes fronteiras intransponíveis são rompidas durante a persecução penal e portanto, se faz necessário o reestabelecimento de (novos) limites para preservar garantias individuais.

Aliás, uma das mudanças mais perceptíveis entre a investigação tradicional[496] e a investigação informática[497] é justamente o salto expressivo na qualidade das informações colhidas decorrente principalmente da criação de novos instrumentos de investigação que se voltam à busca e recolha de informações ou dados que circulam na *internet* ou estão armazenados nos dispositivos informáticos[498]. Contudo, este salto é acompanhado de uma enorme dificuldade de equilíbrio entre as exigências constitucionais de tutela individual dos direitos fundamentais do investigado e a própria atividade de investigar o delito.

A discussão que se pretende traçar neste momento objetiva buscar o equilíbrio entre a utilização de modalidades de infiltração possibilitadas pelo uso de novas tecnologias informáticas e a tutela de direitos fundamentais do sujeito, sem cair na armadilha do engano proporcionado pela famigerada necessidade de prevenir ou reprimir delitos considerados demasiadamente lesivos à sociedade e com isso incorrer na aceitação de métodos exploratórios travestidos de constitucionais.

O argumento baseado na necessidade de mais segurança esconde o risco do controle absoluto de indivíduos e, mais além, torna possível o risco da subtração de suas personalidades singulares. O debate se justifica principalmente porque as inovações investigativas que serão tratadas já são utilizadas na prática processual de alguns países e pouco a pouco serão inseridas no Direito Processual Penal brasileiro, o que impõe de maneira imediata a reflexão acerca dos limites exigidos para a atividade investigativa que faz uso de tais técnicas.

---

[496] Talvez o termo tradicional não seja o mais apropriado, mas pela falta de outro, será o utilizado neste espaço

[497] TORRE, Marco. ***Il captatore informatico: nuove tenologie investigative e rispetto delle regole processuali***. Op. cit. p, 13.

[498] ORTIZ PRADILLO, Juan Carlos. "***Hacking" legal al servicio de la investigación criminal: nuevos instrumentos para la investigación y prueba de la delincuencia informática*.** In: Castrillo, Eduardo de Urbano. **Delincuencia informática: tiempos de cautela y amparo.** Editora Aranzadi, 2012. p, 185.

As espécies de infiltração informática derivam de técnicas ocultas de intrusão à distância em sistemas[499] mediante a utilização ou não de *softwares.* Embora sejam metodologias similares em suas funcionalidades investigativas, o "*Hacking"* e o uso de *Malware* pelo Estado se diferenciam justamente pelo fato de que a primeira não se procede mediante a instalação de *software* em dispositivos informáticos, se tratando de um "acesso remoto não autorizado" possível e vinculado à utilização da *internet*. Por tal aspecto é limitado ao período de conexão, o que diferencia substancialmente as duas espécies[500].

Malware, em definição simples, refere-se a um programa malicioso instalado clandestinamente por terceiro em um sistema de processamento, uma ameaça destinada a quebra da confidencialidade e integralidade dos dados nele contidos[501]. Trata-se de um *software* previamente programado cuja função é infectar dispositivos eletrônicos (*smartphone, tablet* ou *PC*) para tornar possível o acesso remoto às informações, comunicações ou arquivos neles armazenados ou acessar suas funcionalidades (áudio, vídeo, *e-mail*, câmera, *web* e etc) independentemente de estarem ativas ou não[502].

Na visão de Ortiz Pradrillo e Torre[503] quando utilizado pelo Estado se trata de instrumento sofisticado, um programa informático utilizado por agentes estatais que possui capacidade de interceptação e gravação em tempo real de dados transmitidos, recebidos ou armazenados em equipamentos eletrônicos.

Velasco Nunez[504] afirma que a introdução do *software* malicioso no sistema informático alvo pode ser levada a cabo somente pela facilitação das tecnologias de conexão via *web*. Para o autor a introdução de um *software* espião se daria, ou a partir do acesso a páginas da *web* destinadas a atividades ilícitas – terrorismo, tráfico de drogas, pornografia infantil e etc

---

499 RAMALHO, David Silva. **Métodos ocultos de investigação criminal em ambiente digital.** Op. cit. 313.
500 RAMALHO, David Silva. **Métodos ocultos de investigação criminal em ambiente digital.** Op. cit. p, 313.
501 VACIAGO, Giuseppe e RAMALHO, David Silva. ***Online searches and online surveillance: the use of trojans and other types of malware as means of obtaining evidence in criminal proceedings*****.** *Digital evidence and eletronic signature Law Review,* 13 (2016), p. 88. "*Malware is short for malicious software and it may be briefly described as a 'a simple or self-replicating program, which discreetly installs itself in a data processing system, without the users' knowledge or consent, with a view to either endangering data confidentiality, data integrity and system availability or making sure that the users are framed for a computer crime'.1 In broad terms, it includes all kinds of software installed surreptitiously by third parties on a computer system, which can be used to somehow compromise its functions, circumvent its access controls, be detrimental to its user or to the infected computer system, monitor the user's activity or appropriate, corrupt, delete and change computer data*".
502 TESTAGUZZA, Alessandra. ***Exitus acta probat trojan di Stato: la composizione di un conflitto*****.** *Orientamenti. Archivio Penale,* 2016, n. 2. p, 2.
503 ORTIZ PRADILLO, Juan Carlos. "***Hacking" legal al servicio de la investigación criminal: nuevos instrumentos para la investigación y prueba de la delincuencia informática*****.** Op. cit. p, 185. No mesmo sentido TORRE, Marco. ***Il captatore informatico: nuove tenologie investigative e rispetto delle regole processuali***. Op. cit. p, 13.
504 VELASCO NUÑEZ, Eloy. *Limites a las investigaciones y a la prueba en el proceso penal.* In: ***Delitos tecnológicos: definición, investigación, y prueba en el proceso penal.*** Madrid: Editorial Jurídica Sepín, 2016. 13 – 38. p, 34.

– por indivíduos até então indeterminados, de modo que o *malware* instalado inicialmente nestas páginas infectaria de maneira sub-reptícia os dispositivos informáticos dos usuários; ou mediante um correio eletrônico dirigido ao suspeito conhecido para que este, em atividade consequente, de modo involuntário, instale o programa espião em seu dispositivo informático[505].

Porém, a instalação de *malware* em um dispositivos não se vincula ao modo *online*, podendo ocorrer sem o uso da *internet*, isto é, com um acesso físico direto ao *hardware* alvo mediante qualquer suporte físico removível (*pen-drive*, *CD*, *USB*). Ramalho destaca que embora menos expressiva, tal modalidade de infecção de sistemas mantém certa relevância para as investigações criminais. Infectar redes locais permite que se assegure a precisão da infiltração em um sistema específico e determinado[506]. De qualquer sorte, seja pela instalação remota, seja pelo acesso físico ao *hardware*, o resultado é idêntico, cria-se um portal de acesso (*backdoor*) que possibilita uma comunicação oculta e remota entre o dispositivo monitorado e o centro de comando[507]. *Backdoors* são formas ocultas de acessar o sistema do computador infectado de maneira remota, enviando os mecanismos de autenticação existente, possibilitando assim, que o terceiro – investigador – acesse informações (como senhas e *logins*) ou monitore as atividades do usuário do sistema alvo infectado[508].

Tanto o recurso *hacking* como a utilização de *malware* nas investigações permitem ao centro de comando um posicionamento à distância do dispositivo alvo, um controle remoto capaz de realizar de maneira oculta o monitoramento em tempo real, do áudio, vídeo, das funções de microfone e câmeras, do fluxo de dados e comunicações, da memória e armazenamento, da geo localização do dispositivo móvel alvo dentre outras funcionalidades por vezes disponíveis[509]. Mesmo com todas as semelhanças, este trabalho se voltará apenas ao estudo detido da utilização de *Malware* pelo Estado, mas é possível salientar que a maior parte das críticas e apontamentos são compatíveis ao recurso *Hacking* de investigação.

Pois bem, a sistematização de todos as funcionalidades destacadas a cima, em um controle ordenado somente é possível mediante o uso de um *software* pré programado destinado a tal objetivo. Um "sistema de controle remoto" que inclusive possibilita aos investigadores o

---

[505] VELASCO NUÑEZ, Eloy. *Limites a las investigaciones y a la prueba en el proceso penal.* In: ***Delitos tecnológicos: definición, investigación, y prueba en el proceso penal.*** Op. cit. p, 35.
[506] RAMALHO, David Silva. **Métodos ocultos de investigação criminal em ambiente digital.** Op. cit. p, 315.
[507] TORRE, Marco. ***Il captatore informatico: nuove tenologie investigative e rispetto delle regole processuali***. Op. cit. p, 16.
[508] VACIAGO, Giuseppe e RAMALHO, David Silva. ***Online searches and online surveillance: the use of trojans and other types of malware as means of obtaining evidence in criminal proceedings*.** Op. cit. p, 89.
[509] TORRE, Marco. ***Il captatore informatico: nuove tenologie investigative e rispetto delle regole processuali***. Op. cit. p, 17 – 18.

acesso a senhas de usuários do sistema informático alvo, documentos, correio eletrônico, histórico de páginas *web*, ou seja todos os acessos disponíveis a partir do dispositivo informático alvo, de modo a reduzir dificuldades na obtenção de material probatório que sirva na identificação de *fontes* provas[510].

Como descreve Torre[511], está-se diante de um instrumento de alto potencial tecnológico capaz de um controle total e uma verdadeira e própria capacidade de criação de perfis (*profiles*) mediante aquisição de dados dos indivíduos atingidos. Ademais, servem para burlar mecanismos de auto segurança do dispositivo, como por exemplo os *antivírus* presentes nos dispositivos informáticos ou recursos como a *criptografia* de mensagens que por vezes não são captadas por uma interceptação tradicional. Tal é o nível de intrusão na esfera privada do indivíduo que a regulamentação deste instrumento se faz necessária para que sua utilização não venha a lesionar em demasia direitos individuais[512] e se compatibilize com garantias processuais.

Em linhas gerais, o *software* utilizado em um sistema de controle remoto é composto por dois módulos principais, um programa *servidor* e um programa *cliente*, em que o primeiro se refere à faceta do sistema que atinge ou infecta o dispositivo alvo e o segundo – *client* – constitui o programa cujo investigador utiliza para controlar o dispositivo infectado[513].

Justamente pela complexidade da utilização deste instituto na investigação criminal é que se torna muito difícil a definição específica da sua natureza jurídica. No atual momento, por consistir no monitoramento intensivo e remoto, ou na captação oculta de toda atividade desempenhada pelo usuário, corresponderá a natureza jurídica de meio oculto de investigação, ou meio de investigação de prova[514]. A prejudicialidade em termos de comprovação da confiabilidade e integralidade do material probatório coletado impede – ainda que momentaneamente – outra definição de sua natureza jurídica, isto pelo fato de que a utilização de um sistema invasor altera configurações no sistema visado.

---

[510] SALT, Marcos. ***Nuevos desafios de la evidencia digital.*** Op. cit. p, 57.

[511] TORRE, Marco. ***Il captatore informatico: nuove tenologie investigative e rispetto delle regole processuali***. Op. cit. p, 18. Sobre os sistemas de controle remoto definidos pelo autor, cumpre salientar que se tratam de sistemas complexos que necessariamente sofrem modificações constantes para não se tornarem obsoletos. Com o avanço exponencial das tecnologias informáticas, incluindo as defensivas instaladas em sistemas informáticos particulares para bloquear invasões, é preciso ter em mente que o "sistema de controle remoto" é um conceito genérico composto por diversas espécies de programas tecnico-informáticos.

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

[513] TESTAGUZZA, Alessandra. ***Intercettazione telefônica 2. Trojan.*** *Diritto on line*, 2017. Disponível em: http://www.treccani.it/enciclopedia/intercettazione-telefonica-2-trojan_(Diritto-on-line). Acesso em Set/2018.

[514] Neste mesmo sentido TORRE, Marco. ***Il captatore informatico: nuove tenologie investigative e rispetto delle regole processuali***. Op. cit. p, 18.

No entanto, em um futuro poderá ser identificado como medida cautelar probatória. Para tanto, deverá ocorrer um avanço na atual conjuntura técnica e tecnológica de comprovação da integridade e fiabilidade das *fontes* de provas digitais recolhidas pelo *software* invasor e conservadas posteriormente (preservação cadeia de custódia da prova digital). Ou seja, quando for possível a comprovação da fiabilidade probatória do material recolhido por acesso remoto a partir de um *software* invasor, tal instituto processual possa vir a corresponder a uma natureza jurídica híbrida.

É de se notar que a capacidade de colheita de informações ou *fontes* de prova proporcionada pela utilização de um *software* próprio é muito alta, principalmente pelo funcionamento semi autônomo vinculado tão somente à sua pré configuração e à autorização judicial que determina sua execução. O procedimento investigativo pautado nesta nova tecnologia reduz custos à investigação (dentre os quais com pessoal) de maneira substancial e no aspecto econômico atende à eficiência[515].

Evidentemente que pelo funcionamento automático alguns problemas vão ocorrer, principalmente quanto ao volume massivo de dados recolhidos que não se mostram relevantes à investigação dos fatos. A solução para isto pode estar por vir, como explica Salt a tecnologia de programação destes *softwares* pode direciona-los à colheita de provas específicas, por um certo período de tempo, visando formatos de arquivos próprios e determinados[516].

Ainda assim, como instrumento investigativo, parte procedimental da investigação criminal – e portanto devendo se adequar ao fundamento existencial desta –, a pergunta a ser feita diante da possibilidade da utilização de *malware* pelo Estado como *meio de investigação de fontes de prova* é se tal método atende aos preceitos constitucionalmente impostos para a proteção nuclear de direitos fundamentais (?).

4.1 Uso de *Malware* pelo Estado, a reserva de lei e a (a)tipicidade probatória na lei Processual Penal

Antes de discorrer sobre a possibilidade de se admitir provas atípicas em um processo penal constitucional, primeiramente é preciso distinguir alguns conceitos que por vezes podem resultar em confusões. Falar-se-á, pois necessário, tanto sobre seu viés de *meio de investigação de prova* como da possível e futura função *cautelar*. Novamente a terminologia

[515] SALT, Marcos. ***Nuevos desafios de la evidencia digital.*** Op. cit. p, 68.
[516] SALT, Marcos. ***Nuevos desafios de la evidencia digital.*** Op. cit. p, 69.

prova volta a causar posturas equivocadas quanto ao seu tratamento, que mudará sobremaneira a depender do que significar.

Alguns esclarecimentos já foram feitos acima, contudo, no tocante a esta matéria se faz necessário observar que quando a doutrina processual penal trata de meios atípicos de prova[517], refere-se à atipicidade ou ausência de regulamentação em lei de determinados *meios* de prova. Estes em nada se assemelham aos *meios de investigação* de prova, que são instrumentos que permitem se descobrir *fontes*, chegar-se à *fonte* de prova[518].

A possível atipicidade da lei processual penal se relaciona ao rol de *meios* de prova presentes no Código de Processo Penal. Em verdade, e como regra, o rol de *meios* de prova é taxativo, contudo sendo aceitáveis os *meios* de prova que cumprem requisitos constitucionais e processuais. Quer-se dizer que ao lado dos *meios* de prova típicos, admitir-se-á *meios* de provas atípicos, isso porque como afirmado acima, *meios* de prova se destinam ao julgador e servem para carregar *fontes* de prova ao processo, não devem incidir ao ponto de restringir ou violar, efetivamente, direitos fundamentais ou garantias processuais.

O mesmo não ocorre com os *meios de investigação* de prova que se tratam de instrumentos processuais que auxiliam na descoberta de *fontes* de prova e o registro de sua existência[519]. Moraes[520] afirma que a determinação advinda do preceito processual *nulla coactio sine lege* traduz como necessariamente típicas as intervenções processuais, tanto em relação à sua aplicabilidade como em relação ao seu conteúdo pertinente ao âmbito dos direitos fundamentais do cidadão. Deve-se falar primeiramente em tipicidade processual da medida de coerção ou ingerência para poder utilizá-la[521].

Toda intervenção em direitos fundamentais deve ter fundamento na lei e ser proporcional, ou seja, resguardada em balizas. Do contrário, carece de justificativa sendo portanto uma lesão ou violação de direitos[522]. Destaca Greco – com total compatibilidade ao

---

517 CORDERO, Franco. ***Procedimiento penal II.*** Op. cit. p, 46 "*es admisible todo signo útil al juicio histórico con tal que su adquisición no viole prohibiciones explícitas o deducibles del sistema*".
518 LOPES JR. Aury. **Direito processual penal.** 13ª ed. São Paulo. Saraiva, 2016. p, 366.
519 ARANTES FILHO, Marcio Geraldo Britto. **A interceptação de comunicação entre pessoas presentes.** 1 ed. Brasilia, DF: Gazeta Jurídica, 2013. p, 30.
520 MORAES, Maurício Zanoide de. **Presunção de inocência no processo penal brasileiro: análise de sua estrutura normativa para a elaboração legislativa e para a decisão judicial.** Rio de Janeiro: Lumen Juris, 2012. p, 315 – 316.
521 BRUZZONE, Gustavo. ***La nulla coactio sine lege como pauta de trabajo en matéria de medidas de coerción en el proceso penal.*** Estudios sobre Justicia Penal: Homenaje al Profesor Julio B. J. Maier. Editores del Puerto Buenos Aires, 2005. p, 248.
522 GRECO, Luis. **Introdução – o inviolável e o intocável no direito processual penal.** In: WOLTER, Jürgen. **O inviolável e o intocável no direito processual penal: reflexões sobre dignidade humana, proibições de prova, proteção de dados (e separação informacional de poderes) diante da persecução penal.** Luis Greco (org.). 1ª ed. São Paulo: Marcial Pons, 2018. p, 32 – 33.

tema aqui tratado, e como será adiante mais profundamente explorado – que a categoria especial destes direitos, que não são passíveis de violação sem justificativa consistente, é denominada de *inviolável*[523].

Suscintamente aduz de outro modo, que sem lei específica que disponha de forma relativamente clara a intervenção e lhe estabeleça limites materiais e procedimentais, não é possível dizer que a intervenção a um direito fundamental será lícita. A intervenção em direitos dos cidadãos por parte do Estado, sem previsão legal, é uma intervenção sem consentimento, portanto não autorizada. Destarte, a dita lei específica se pautará como *fundamento legal*[524] da intervenção.

Sobre o tema, a crítica feita pelo autor ao Direito brasileiro se direciona ao não questionamento sobre a disposição de *normas autorizadoras*[525] que intervenham em direitos fundamentais. Greco salienta que no regime jurídico brasileiro, somente se debate sobre as normas de regulamentação – "como se apenas se tratasse de legislar sobre o como, e não sobre o se"[526]. Reflete a partir disto, que se toda intervenção em direito fundamental necessita de *fundamento legal* (norma autorizadora), "até a exigência de informação por meio de perguntas dirigidas a um cidadão significa intervir em sua esfera e necessita de uma autorização legal; isto quer dizer que o direito processual penal tem que ser fundamentalmente revisto para atender a essas exigências da reserva de lei".

Consoante ao que Prado explica, somente "a legalidade processual (constitucional) penal instaura um nexo funcional, no campo processual, equivalente ao que se verifica no direito material", sendo que nesta, a legalidade se volta para tipificar condutas proibidas aos indivíduos, e naquela – processual –, a legalidade ou melhor a tipicidade processual penal dirige-se aos responsáveis pela persecução criminal[527].

---

[523] GRECO, Luis. **Introdução – o inviolável e o intocável no direito processual penal.** Op. cit. p, 32 – 33. "É a própria redação da Lei Fundamental alemã que faz essa diferenciação: alguns direitos, como a liberdade de locomoção (art. 2 II 2 GG), a liberdade de consciência e de religião (Art. 4 I GG), o sigilo de telecomunicações (art. 10 I GG), o domicílio (art. 13 I GG), são invioláveis (*unverletzlich*), já a dignidade humana (art. 1 I GG) e o conteúdo essencial (Wesensgehalt) de um direito fundamental (art. 19 II GG) são intocáveis".

[524] GRECO, Luis. **Introdução – o inviolável e o intocável no direito processual penal.** Op. cit. p, 37 – 39.

[525] Salienta o autor para que não se confunda uma *norma autorizadora* com uma mera *norma de competência*. *Norma de competência* é a simples distribuição interna de tarefas, sem que se estabeleça o direito a alguém de adentrar na esfera de um terceiro. Estabelecida uma norma de competência sem outra que autorize a execução de uma intervenção, a primeira permanece inócua, posto que a medida que compete à autoridade não poderá ser utilizada. As *normas autorizadoras* preveem a concreta medida interventiva, descrevem o concreto meio de que as instâncias de persecução se valerão para cumprir a função que lhes é legalmente atribuída.

[526] GRECO, Luis. **Introdução – o inviolável e o intocável no direito processual penal.** Op. cit. p, 40 – 41.

[527] PRADO, Geraldo. **Prova penal e sistema de controles epistêmicos.** Op. cit. p, 63. A imposição advêm do texto constitucional, no qual ressalva em seu artigo 5º, II, que "ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei".

Portanto, sobre a utilização de *Malware* pelo Estado, duas questões iniciais devem se fazer presente. A primeira delas corresponde à afirmação acerca da inexistência de *norma autorizadora*, isto acarreta dizer que a utilização deste instrumento não condiz em similitude com a interceptação telemática disposta na Lei nº 9.296/96, posto que – como se verá a seguir – são dois institutos que atuam em direitos fundamentais diferentes. Quanto aos direitos fundamentais diretamente atingidos pela infiltração de *malware* em dispositivos informáticos, por não existir norma que fundamente e autorize a intervenção estatal nos moldes que se pretende, ou seja, um *fundamento legal* para a intervenção por *software*, será ilícita tal infiltração e consequentemente tudo que a partir dela decorrer.

A segunda, corresponde ao aspecto da reserva de lei como *norma reguladora*. É a tipicidade processual o critério de definição da qualificação da prova em típica ou atípica. Na visão de Arantes Filho o tipo processual probatório impõe uma delimitação legal para espécies de prova (tipicidade probatória) que quando ausente – não regulamentação legal – se estará diante de uma prova atípica. A tipicidade probatória, portanto, é integrada pela admissibilidade (por sua vez composta pela nominação e requisitos), pelos limites impostos, pelo procedimento probatório e também denominado rito probatório ou método probatório. Logo será típica a prova que tiver previsto em lei seu procedimento probatório próprio ou a remissão a um[528].

As considerações acima não se vinculam somente à faceta investigativa do instrumento analisado. Não é preciso dizer que as medidas cautelares penais também necessitam obedecer a reserva legal. Sob este aspecto assim deve se proceder a recolha cautelar de *fontes* de prova a partir do uso de *malware* pelo Estado. Desde que, como afirmado acima, seja possível a confirmação da integralidade e confiabilidade do material probatório a partir dos avanços tecnológicos e a utilização destes *softwares*.

Como relembra Pujadas Tortosa[529] de acordo com a divisão dos poderes, o julgador penal possui a função de aplicar, caso proceda, o que o poder legislativo dispõe como lei penal, em outras palavras não será o poder judiciário a quem compete decidir qual tratamento cabe dispensar ao indivíduo e que considerações se exige para ser feito. A reserva legal impõe que a restrição a um direito fundamental tenha habilitação legal prévia.

Salienta a autora, contudo, que a previsão legal que disponibiliza um instrumento cautelar penal não deixa de simbolizar uma vertente que vincula a medida cautelar penal não à

---

[528] ARANTES FILHO, Marcio Geraldo Britto. **A interceptação de comunicação entre pessoas presentes.** 1 ed. Brasilia, DF: Gazeta Jurídica, 2013. p, 41.

[529] PUJADAS TORTOSA, Virginia. ***Para una teoria general de las medidas cautelares penales.*** Op. cit. p, 357 – 358.

presunção de inocência como direito, mas como regra de tratamento ao imputado[530]. Se a medida cautelar penal deve respeitar uma regra de tratamento ao imputado, legislativamente devem estar previstos alguns requisitos para que seja possível sua execução, tais como *os motivos* para impor determinado tratamento, o respectivo *tratamento* (que identifica-se com a própria medida cautelar suas circunstancias), *os fins* que justifiquem seu uso e os *requisitos de proporcionalidade, legalidade, jurisdicionalidade e motivação*[531].

Algumas outras consequências se observa a partir do princípio da legalidade em matéria de cautelares penais. Notadamente a lei penal exige taxatividade, ou seja "não pode se impor mais medidas cautelares penais que as previstas na lei, nem por motivos, fins, nem procedimentos distintos aos que essa mesma disposição normativa estabeleça"[532]. Ademais, a legalidade como princípio impõe que o conteúdo da lei penal seja determinado, de modo que a previsão penal deve ser certa e precisa, seja relacionada aos pressupostos de aplicação, seja quanto às consequências da norma.

Destarte, por mais que se insista no argumento que a medida cautelar de busca e apreensão de *fontes* de provas físicas poderá ser usada na busca de *fontes* de prova digital, tal não deve prosperar. Para além de não possuir procedimento peculiar que atenda critérios de recolha e armazenamento das ditas *fontes* digitais, a própria reserva legal impede sua utilização para outros fins que não os dispostos na lei penal.

De tal forma, Torre[533] propõe requisitos indicativos para a admissibilidade da utilização de *softwares* maliciosos como meios de investigação de prova (que servirão também para indicativos de admissibilidade quanto ao *malware* como medida cautelar, quando possível a confiabilidade e integralidade do material coletado), a partir de um balanceamento entre os bens jurídicos objetos da tutela. A definição do instituto e a delimitação do seu perímetro de utilização (rol taxativo de crimes passíveis da utilização deste instrumento investigativo), bem como a individualização dos requisitos probatórios que devem ser alcançados para iniciar o poder de investigação são os dois pressupostos fundamentais destacados pelo autor.

A determinação de condutas ilícitas em rol taxativo de crimes, sem dúvidas permite com que se restrinja a utilização do *malware* do Estado nas investigações criminais. Principalmente por que o exercício feito pelo legislador para que se estabeleça os tipos penais

---

[530] Desenvolver a vinculação de uma medida cautelar penal com o direito à presunção de inocência para a autora seria contradizer a argumentação utilizada para determinar que o fundamento de uma tutela cautelar é a noção de *perigo cautelar abstrato*. De tal modo, a execução de uma medida cautelar penal deve respeitar a faceta de regra de tratamento da presunção de inocência do imputado. Id. p, 364.
[531] PUJADAS TORTOSA, Virginia. ***Para una teoria general de las medidas cautelares penales.*** Op. cit. p, 365.
[532] PUJADAS TORTOSA, Virginia. ***Para una teoria general de las medidas cautelares penales.*** Op. cit. p, 373.
[533] TORRE, Marcos. ***Il captatore informatico.*** Op. cit. p, 149.

em rol, deve ser o da equiparação entre o dano possivelmente alcançado pelo ilícito, a tutela de um bem jurídico relevante para o direito penal e, também, o grau de lesividade que este instituto processual pode acarretar a bens jurídicos pertencentes ao sujeito passivo da medida, igualmente relevantes sob a óptica constitucional.

Fator demasiadamente importante é o segundo ponto, que basicamente trata da eleição de critérios objetivos na determinação de quando serão considerados suficientemente alcançados os indícios – individualização de requisistos probatórios – que autorizam a execução do método de investigação. Neste ponto, cabe a ressalva de que a afirmativa que a medida deve ser executada quando existirem indícios suficientes de materialidade e autoria não é digna para autorizar a restrição de direitos fundamentais, pois o termo "suficiente" cumpre papel abstrato que faz com que a execução da medida atenda somente a critérios judiciais subjetivos. Por vezes, em virtude de tais abstrações, medidas excepcionais tendem à banalização.

Em seguida, Torre[534] aponta para a importância da disciplina concreta do método de execução da atividade, seja esta voltada para atender preceitos de monitoramento, ou quando se voltar para a modalidade técnica de aquisição de dados. Neste ponto, também se mostra fundamental para o cumprimento do princípio da legalidade, a determinação de procedimentos técnicos, ou seja, diretrizes mínimas capazes de orientar os sujeitos processuais quanto à valoração sobre a licitude procedimental da execução da medida, e consequentemente a admissão dos seus proventos no processo penal como *fontes* legítimas de prova.

4.1.1 Interceptação telemática efetuada mediante Malware

Antes de adentrar nas peculiaridades da interceptação efetuada mediante a utilização de *softwares* em dispositivos informáticos por parte do Estado em investigações criminais de cunho informático, é preciso estabelecer linhas breves sobre as interceptações telefônicas e telemáticas regulamentadas pela lei nº 9.296 de 1996. A justificativa para adentrar na temática não é outra senão a necessidade de compreender que se tratam de *meios de investigação de prova* diferentes, que pela nomenclatura utilizada podem gerar certos equívocos, principalmente pela ligeira e errada impressão de que a interceptação efetuada mediante *malware* pelo Estado, no Brasil, possa ter guarida na respectiva lei que tutela a proteção das comunicações em matéria penal.

[534] TORRE, Marcos. ***Il captatore informatico.*** Op. cit. p, 149.

Iniciar esta exposição não será possível de outra forma senão mencionando, a partir de Prado[535], a lição de Jorge Miranda que ressalta que "as normas sobre direitos, liberdades e garantias têm caráter preceptivo e não programático, fundando-se na Constituição e não na lei" sendo assim, "não são os direitos fundamentais que se movem no âmbito da lei, mas a lei que deve mover-se no âmbito dos direitos fundamentais". Talvez este seja o ponto nevrálgico que o debate se trava quando falamos destas modalidades de interceptações, de um lado a regulamentada pela Lei nº 9.296/96 que no tocante aos dados informáticos, trata-se de interceptação telemática, e de outro uma nova modalidade. Afinal, ambas incidem sobre o mesmo direito fundamental? Como afirmado acima, a resposta é negativa.

O entendimento acerca do conceito de interceptação refere-se à "atividade efetuada por um terceiro, captando, mediante instrumentos técnicos de percepção, o conteúdo de uma conversação ou de uma comunicação em curso, entre duas ou mais pessoas"[536]. Tanto a interceptação telefônica quanto a telemática possui em comum a utilização de mecanismos de intrusão nas relações interpessoais, com o objetivo de tomar conhecimento das declarações ou de outros elementos úteis à prova de um fato ilícito, como os dados. Ademais, a natureza jurídica deste instituto processual penal é notadamente de meio de investigação de prova[537], e portanto, compartilha de consequências e finalidades já expostas acima.

A telemática pela definição de Giacomolli[538] é a área do conhecimento humano que reúne um conjunto e o produto das combinações de tecnologias associadas à eletrônica, informática e telecomunicações, aplicados aos sistemas de comunicação. O conceito jurídico de telemática, portanto, segundo Sidi, tratar-se-á da comunicação que se realize em forma digital, a partir da utilização da conversão em séries binárias, seja qual for a infraestrutura utilizada, exceto quando se enquadrar na modalidade telefônica ou telegráfica[539].

Um sistema telemático "é constituído de mais de um sistema informático, necessariamente interligados entre si, para trocar informações e conhecimento, com conexão de caráter permanente ou, pelo menos, não ocasionais" [540]. Todo dispositivo eletrônico digital pode se enquadrar no conceito de sistema informático caso entendido como um sistema de

---

[535] PRADO, Geraldo. **Limites às interceptações telefônicas e a jurisprudência do Superior Tribunal de Justiça.** 2ª ed. Editora Lumen Juris, 2006. p, 22.
[536] GIACOMOLLI, Nereu. **A fase preliminar do processo penal.** Op. cit. p, 141.
[537] SIDI, Ricardo. **A interceptação das comunicações telemáticas no processo penal.** Belo Horizonte: Editora D'Plácido, 2016. p, 230.
[538] GIACOMOLLI, Nereu. **A fase preliminar do processo penal.** Op. cit. p, 143 – 144.
[539] SIDI, Ricardo. **A interceptação das comunicações telemáticas no processo penal.** Belo Horizonte: Editora D'Plácido, 2016. p, 72. Na visão do autor, "não faria sentido, igualmente, sustentar que as ligações telefônicas atuais, digitais, passaram a se enquadrar no conceito constitucional de comunicação 'de dados'.
[540] GIACOMOLLI, Nereu. **A fase preliminar do processo penal.** Op. cit. p, 143 – 144.

recursos composto por dispositivos de elaboração eletrônica digital, programas de memorização e grupos de dados que, sob o controle de tais programações trata de emitir automaticamente os dados que possam memorizar e recuperar para restituir a este último a tutela legal[541].

Nesta concepção, se um sistema telemático se forma a partir da conexão de dois ou mais sistemas informáticos, a interceptação telemática é a atividade desempenhada por um terceiro alheio e externo aos dois sistemas que alcança a comunicação entre ambos. Neste sentido, é também o conceito adotado por Sidi, de modo a afirmar que a interceptação, diferentemente da obtenção de dados que repousem em servidores, constitui a captação de uma comunicação contemporânea, ou seja, que esteja ocorrendo durante a medida[542].

O que ocorre é a restrição da comunicabilidade, da intimidade e vida privada, da pessoa alvo da interceptação, cujo terceiro autorizado pelo Estado – como fantasma – passa a acompanhar os passos do sujeito que se investiga[543]. Evidente que em todo o processo de interceptação, seja telefônica, seja telemática, o direito fundamental restringido – portanto – é da livre telecomunicação, tido como direito inviolável salvo mediante autorização judicial[544].

De modo completamente distinto é a interceptação efetivada mediante *malware* levada a cabo pelo Estado em investigações criminais. Primeiramente, há que se notar que não se trata de uma interceptação como a referida acima, difere-se principalmente por se efetivar na própria fonte emissora/receptora das informações. Não é que não haja interceptação telemática a partir do uso do *malware*, mas esta interceptação não ocorre de maneira externa ao dispositivo informático, e sim pela intrusão mediante *software* malicioso no próprio sistema informático alvo.

Tal técnica possibilita maior recolha de informações, pois como assevera Torre[545], a interceptação "tradicional" – denominada de passiva – não possui uma alta capacidade para fornecer dados que possam servir aos interesses investigativos. Converter as ondas capturadas pela interceptação para um formato acessível é o que se denomina de decodificação, contudo capturar as ondas de frequência, por si só, não possibilita alcançar o conteúdo que possuem[546].

---

[541] GIACOMOLLI, Nereu. **A fase preliminar do processo penal.** Op. cit. p, 144.
[542] SIDI, Ricardo. **A interceptação das comunicações telemáticas no processo penal.** Op. cit. p, 73.
[543] PRADO, Geraldo. **Limites às interceptações telefônicas e a jurisprudência do Superior Tribunal de Justiça.** 2ª ed. Editora Lumen Juris, 2006. p, 32.
[544] BRASIL, Constituição Federal. Art. 5º, XII - 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;
[545] TORRE, Marcos. ***Indagini informatiche e processo penale.*** *Dottorato di ricerca in scienza giuridiche, ciclo XXVIII.* Università degli studi Firenze. Anni 2012/2015. p, 151.
[546] SIDI, Ricardo. **A interceptação das comunicações telemáticas no processo penal.** Op. cit. p, 75. A criptografia, hoje, é ferramenta inerente às comunicações digitais de modo que os Governos, as agências de segurança e companhias de telecomunicação passaram a utilizar formas mais fáceis de espionar comunicações. De

Isto porque, atualmente, uma grande quantidade dos dados emitidos encontram-se protegidos por criptografia. Assevera Torre que na prática, a interceptação (telemática) passiva permite apenas verificar que os dispositivos alvos estão sendo utilizados pelos suspeitos, embora – na grande maioria dos casos – não fornece dados relevantes para a investigação criminal[547].

Diz-se interceptação pois ocorre a captação em tempo real, mas é certamente uma captação de dados (*bit*) possibilitada pela intrusão de *software* que corrompe a integridade de um sistema informático. O *malware* a serviço da investigação não incide no fluxo comunicacional que se encontra por vezes protegido pela técnica criptográfica, mas transforma aquela interceptação passiva em "ativa" (*intercettazioni attive*), na medida em que permite a interceptação da informação após sua decodificação internamente nos dispositivos informáticos. Em suma, a utilização do *malware* transforma a interceptação do fluxo da informação em uma captura dos dados receptados pelo dispositivo alvo[548]. Portanto, sua efetivação incide em um novo direito fundamental, destacado por Greco como uma nova concretização do direito geral da personalidade, qual seja a integridade do sistema informático[549].

Como ressalta Mendes e Branco[550] inexiste no direito brasileiro, lei específica que regule e autorize a infiltração sub-reptícia em sistemas de tecnologia da informação para investigação criminal. Não há efetivamente qualquer legislação que assegure de maneira inequívoca tal método investigativo, entretanto, se acaso existir a indagação acerca do possível uso análogo dos procedimentos estabelecidos pela Lei nº 9.296/96, conforme os autores, ressalta-se que a infiltração através de *malware* em computadores pessoais se mostra de difícil conformação com a garantia constitucional do direito à privacidade. Deste modo, indispensável

---

acordo com Sidi, "agências de inteligência adotaram uma bateria de métodos em sua atuação para superar aquilo que elas enxergam como uma das maiores ameaças à sua capacidade de acessar comunicações, a saber, o uso da criptografia, onipresente em toda a internet. Esses métodos incluem medidas para assegurar o controle da *National Security Agency* (NSA) norte-americana sobre os padrões internacionais de criptografia, o uso de supercomputadores para violar criptografias e [...] a colaboração de empresas desenvolvedoras de tecnologia e dos próprios provedores de serviços de *internet*. Foi por meio desta parceria secreta que as agências inseriram nos sistemas comerciais de criptografia, que perante o mercado se anunciam seguros e confiáveis, vulnerabilidades propositais e secretas conhecidas como *backdoors* ou *trapdoors*".

[547] TORRE, Marcos. ***Indagini informatiche e processo penale.*** *Dottorato di ricerca in scienza giuridiche, ciclo XXVIII*. Università degli studi Firenze. Anni 2012/2015. p, 151.

[548] TORRE, Marcos. ***Indagini informatiche e processo penale.*** p, 151.

[549] GRECO, Luis. **Introdução – o inviolável e o intocável no direito processual penal.** Op. cit. p, 39.

[550] MENDES, Gilmar; BRANCO, Paulo Gustavo Gonet. **Curso de Direito Constitucional.** 10 ed. rev. e atual. São Paulo: Saraiva, 2015. p, 558 – 559. "Embora a Lei nº 9.296/96 indique os procedimentos a serem observados nas interceptações por ela disciplinadas, há que se ponderar que, em razão da diversidade de tecnologias que podem ser empregadas nesse tipo de espionagem [...]. Tendo com conta o elevando grau de ingerência de medida dessa natureza na intimidade e na vida privada, com o consequente incremento dos riscos de abuso, afigura-se indispensável a sua disciplina pela lei".

será sua disciplina em lei, observadas as peculiaridades, indicação de requisitos, procedimentos e cautelares a serem observados quando do deferimento em ordem judicial.

4.1.2 Roving Bug: Interceptação entre presentes mediante Malware

Com o advento de novas tecnologias, a possibilidade de se ter o acionamento remoto do microfone do dispositivo informático, por meio de *softwares* específicos é real. A técnica se denomina de *Roving Bug* e possibilita ao investigador o acesso ao microfone do dispositivo alvo para fins de captação ambiental[551]. De acordo com Odell trata-se de técnica à distância, executada de modo sub-reptício que funciona mesmo com o dispositivo alvo desligado[552], de modo a possibilitar a recolha de elementos fonéticos ainda que o proprietário do aparelho não esteja efetuando uma ligação[553]. Trata-se de interceptação ambiental e como tal, possui natureza jurídica de meio de investigação de prova.

A definição daquilo que se denomina de comunicação entre pessoas presentes é trazida por Arantes Filho como a forma de concretização por meio da reprodução da voz, com a inerente emissão de sinais sonoros – conversações – que se propagam no "fluido aéreo", ou seja, em um âmbito estruturalmente livre. De modo que a interceptação desta comunicação se perpassa pela tentativa de captar o conteúdo da comunicação, as informações verbalizadas pelos respectivos interlocutores. Sendo portanto subespécies da interceptação da comunicação entre pessoas presentes aquelas denominadas de domiciliares e ambientais, cujo aspecto que diferencia, por evidente, é o local de sua ocorrência[554]. Esta captação, necessariamente deve ser efetivada por um terceiro alheio à comunicação, com o emprego de meios técnicos, utilizados

---

[551] SIDI, Ricardo. **A interceptação das comunicações telemáticas no processo penal.** Op. cit. p, 87.

[552] No mesmo sentido, Declan Mccullagh ressalta que o *FBI* já havia inaugurado esta técnica cuja aprovação se deu pelo Departamento de Justiça dos Estados Unidos que visavam alvos membros de uma família inserida no contexto de organização criminosa (Genovese Family). Conforme narra Mccullagh, a decisão proferida pelo juiz Lewis Kaplan destacou que para o magistrado tal técnica de vigilância seria legal porque a lei federal de escutas telefônicas é ampla o suficiente para permitir a interceptação até de conversas que acontecem perto do celular, a espionagem funcionaria tanto enquanto o aparelho estivesse ligado, como desligado. Segundo Mccullagh, o departamento de segurança dos Estados Unidos alerta que um telefone celular pode ser transformado em um microfone e um transmissor com a finalidade de ouvir conversas nas proximidades do telefone. MCCULLAGH, Declan. ***FBI taps cell phone mic as eavesdropping* tool.** *Agency used novel surveillance technique on alleged Mafioso: activating his cell phone's microfone and the just listennig.* December 4, 2006. Disponível em: https://www.cnet.com/news/fbi-taps-cell-phone-mic-as-eavesdropping-tool/. Acesso em 24 Set 2018.

[553] ODELL, Mark. ***Use of mobile helped police keep tabs on suspect and brother.*** Financial Times. Mark Odell, Telecoms Correspondent, *august 1, 2005.* Disponível em: https://www.ft.com/content/7166b8a2-02cb-11da-84e5-00000e2511c8. Acesso em 24 set 2018.

[554] ARANTES FILHO, Marcio Geraldo. **A interceptação de comunicação entre presentes.** Op. cit. p, 97, 153.

em operações ocultas e simultâneas à comunicação, sem o conhecimento dos interlocutores ou o conhecimento de um ou de alguns deles[555].

A obtenção da comunicação pela utilização desta espécie de sistema de controle remoto demonstra o avanço técnico investigativo capaz de monitorar verdadeiramente o áudio e as câmeras do aparelho alvo, desde uma instalação quase sempre furtiva. Certamente, torna-se capaz de reduzir os riscos de descobrimento da execução da medida, por isto mesmo que se trata de um meio oculto de investigação. Todavia, não se trata de um ponto de captação ambiental fixo, mas o oposto, um monitoramento perene e itinerante de áudio e vídeo do sujeito investigado e dos demais em que aquele mantém contato[556].

Na legislação brasileira a captação ambiental de sinais eletromagnéticos, ópticos ou acústicos em investigações criminais é disposta na Lei nº 12.850/2013, que embora omissa quanto à exigência de circunstanciada autorização judicial (como dispunha a legislação revogada – Lei nº 9.034/95), evidentemente não a dispensa. Tal interpretação, de acordo com Mendes e Branco condiz com as garantias constitucionais inerentes à privacidade, "cujo alcance há de ser aquilatado em consonância com os riscos decorrentes do indiscriminado uso de novas tecnologias invasivas"[557].

Contudo, há que se ressaltar a insuficiência da legislação brasileira quanto ao tratamento sobre a matéria, principalmente quando diante de novas tecnologias disponíveis ao serviço de investigação como o monitoramento remoto no interior de residências ou em outros ambientes privados, seja pelo uso de *scanners* ou *drones* cujo alcance de sons e imagens é demasiado sofisticado[558], ou ainda, seja pelo uso de *softwares* atualmente utilizáveis para tais fins.

Farley e Wang desenvolveram um programa *bugbot* e demonstram as funcionalidades incorporadas neste sistema. A título meramente exemplificativo, discorrer-se-á sobre a programação desenvolvida, contudo é preciso entender que a variação de programação destes *software* é ampla. O objetivo da exemplificação é, precisamente, estabelecer um ponto de partida sobre as possibilidades da referida metodologia[559].

---

[555] ARANTES FILHO, Marcio Geraldo. **A interceptação de comunicação entre presentes.** Op. cit. p, 157.
[556] TORRE, Marco. ***Il captatore informático.*** Op. cit. p, 37.
[557] MENDES, Gilmar; BRANCO, Paulo Gustavo Gonet. **Curso de Direito Constitucional.** 10 ed. rev. e atual. São Paulo: Saraiva, 2015. p, 562.
[558] MENDES, Gilmar; BRANCO, Paulo Gustavo Gonet. **Curso de Direito Constitucional.** 10 ed. rev. e atual. São Paulo: Saraiva, 2015. p, 564. Importante ressaltar conforme os autores, que quanto à gravação ambiental clandestina realizada com o intuito de obter a confissão de crime em conversa mantida entre agentes policiais e presos, por violar o direito ao silêncio (art. 5º, LXIII), é considerada ilícita pelo Supremo Tribunal Federal.
[559] FARLEY, Ryan e WANG, Xinyuan. ***Roving Bugnet: Distributed Surveillance Threat and mitigation.*** *Comput. Security*, vol. 29, no. 5, pp. 592-602, 2010. Disponível em: https://pdfs.semanticscholar.org/3ce7/f7d7b852fdf82876887bc01ca51b9a462284.pdf. Acesso em 30 set 2018.

Para o acesso ao microfone através do *Bug*, desenvolveram um sistema composto por dois componentes funcionais[560] para a realização do controle remoto da captação de áudio. O primeiro voltado a realizar o sequestro do microfone[561] e o segundo programado para manter o próprio controle remoto do sistema alvo. Segundo Farley e Wang o sistema de desenvolvimento do *bug* pode permitir um controle remoto interativo que servirá para iniciar e interromper uma gravação, captar dados de áudio ao vivo ou a gravação e armazenamento de dados para análise posterior.

O programa desenvolvido pelos autores pode detectar o nível do sinal de conexão. Se a conexão cair, o sistema executa um teste de acessibilidade automaticamente, de modo que caso o teste falhe, o *software* emitirá um arquivo de gravação até que a conexão seja restaurada. Restaurada a conexão, ter-se-á acesso ao arquivo gerado para a reprodução. Instalado o referido *software* (*bot*), o invasor poderá executar programas de vigilância e ativar o *bug* em qualquer dos sistemas alvos. O invasor – neste exemplo – precisaria especificar por quanto tempo registrar-se-á os áudios almejados, bem como o armazenamento de arquivos e opções de transmissão de rede[562].

Muito mais que uma interceptação entre presentes, trata-se de uma interceptação itinerante, de modo a proporcionar uma excessiva vigilância face ao sujeito alvo, monitorando assim, tudo o que se passa ao seu redor, mediante a captação de áudio, em qualquer lugar por onde este se desloque. Conforme ressalta Mele, trata-se de uma evidente violação da liberdade e do segredo da comunicação[563], mais ainda, uma violação pelo impedimento no livre desenvolvimento da personalidade do indivíduo que resta incapaz de expressar sentimentos sensações, opiniões, reflexões e experiências sem o receio de que agências de persecução penal do Estado estejam o monitorando[564].

Sobre a matéria discorre Mele que há necessidade de especificação da localização na qual irá ocorrer a interceptação. A justificativa é precisamente a imposição de limites ao

---

[560] FARLEY, Ryan e WANG, Xinyuan. ***Roving Bugnet: Distributed Surveillance Threat and mitigation.*** Op. cit. p, 3.
[561] *Microphone hijacking*.
[562] FARLEY, Ryan e WANG, Xinyuan. ***Roving Bugnet: Distributed Surveillance Threat and mitigation.*** Op. cit. p, 6. "*At a minimum, the attacker would need to specify how long to record as well as file storage and network transmission options. In our implementation the attacker can specify: the UDP server listening port number; how long to record for; whether to use a file, network stream, or both; the output filename; and, the network broadcast stream destination host IP address and port number. For run time controls, the attacker can send commands to the bug program through its UDP server*".
[563] MELE, Anderson. ***Trojan horse e limiti dell'intercettazione ambientale.*** *Diritto Penale. Fondatore Francesco Brugaletta.* 2017. p, 2.
[564] MENDES, Gilmar; BRANCO, Paulo Gustavo Gonet. **Curso de Direito Constitucional.** 10 ed. rev. e atual. São Paulo: Saraiva, 2015. p, 566.

alcance na utilização do *software* para a captação de elementos sonoros, posto que a utilização de tal instrumento, se não balizada, pode tomar proporção demasiadamente ampla e lesiva a direitos fundamentais de investigados e terceiros alheios à investigação dos fatos[565].

Este não é o sentido adotado pela Corte de Apelação Italiana, que em sessão plenária entendeu ser inconciliável a referida modalidade técnica de interceptação com necessidade jurídica da prévia delimitação do local em que ocorrerá a captação[566]. Isto devido ao uso, quase contínuo, do dispositivo monitorado por diversos lugares que o sujeito investigado transita. Deste modo, segundo a Corte se aplicaria as regras de inutilidade[567] das captações ambientais adquiridas dentro do domicílio do investigado, exceto quando se tratar de crimes que envolvam a investigação de organizações criminosas, posto que na legislação italiana em tal hipótese se derrogaria a disciplina que distingue "uma interceptação dentro do domicílio" da "interceptação fora do domicílio".

Em outras palavras, como esclarece Torre[568], a Corte definiu ao menos um critério para a utilização de *software* em investigações criminais, qual seja de que a utilização desta metodologia investigativa (salvo se tratando de delitos de criminalidade organizada) não poderá ocorrer para realizar uma interceptação itinerante de modo a alcançar todos os ambientes que o sujeito investigado transita, como o domicílio.

De fato, o *roving bug* permite interceptar conversas em locais que não são facilmente acessíveis. Neste sentido, ensina o caso Estados Unidos vs. Jorge Ortiz Oliva[569] que o *roving bug* somente será passível de utilização quando se estabelecer uma completa

---

[565] MELE, Anderson. ***Trojan horse e limiti dell'intercettazione ambientale.*** Op. cit. p, 2. "*Si è così iniziato ad intravedere, dunque, la necessità di una specificazione della localizzazione o comunque di uma precisazione della portata nell'utilizzo di tale strumento che, se non in considerazione di reati appartenenti al binario parallelo nel processo penale che è quello inerente la criminalità organizzata, apparve di portata assolutamente straripante per i reati comuni*".

[566] TORRE, Marco. ***Il captatore informático***. Op. cit. p, 39.

[567] Id. p, 41. "*In realtà, a ben guardare le posizioni assunte dalla giurisprudenza di legittimità sul captatore informatico (utilizzato per effetuare intercettazioni ambientali) non divergono po cosí tanto. Un dato appare infatti come constante: nei procedimenti che hanno ad oggetto "reati comuni" (ossia reati non qualificabili come di "criminalità organizzata), il captatore informatico non può essere impiegato; processualmente la sanzione che scatta in ipotesi di violazione di tale divieto è la più drastica, ossia la inutilizzabilità di tutte le informazioni eventualemente ottenute. Sulla regola, dunque, la giurisprudenza di legittimità è compatta: divieto di utilizzo del captatore informatico per fini di intercettazione ambientale. È sull'eccezione, ossia sulla legittimità dell'utilizzo del captatore nei procedimenti per reati di criminalità organizzata, che si riscontra il contrasto, ma questo è un altro discorso che può essere agevoltamente affrontato e chiuso avallando (ovviamente) la scelta delle Sezioni unite: l'art 13 del d.l. n. 152 del 1991, derogando al co. 2 dell'art. 266 c.p.p., esclude la necessità di dimostrare il fondato motivo di ritenere che nei luoghi domiciliari si stia svolgendo l'attività criminosa e rende di fatto irrilevante la caratteristica itinerante dell'intercettazione ambientale mediante captatore*".

[568] TORRE, Marco. ***Il captatore informático***. Op. cit. p, 42.

[569] *United State of America vs. Jorge Ortiz Oliva*. No. 10-30126, D.C. No.3:07-cr-00050-BR-1. July, 20, 2012. p, 8375. Disponível em: http://cdn.ca9.uscourts.gov/datastore/opinions/2012/07/20/10-30126.pdf. Acesso 30 set 2018.

especificação do motivo pelo qual se pretende fazer uso desta metodologia investigativa. Além do mais, deve se identificar a pessoa alvo da referida medida, cujas comunicações devem ser captadas.

A potencialidade invasiva desperta enorme interesse das autoridades investigativas. Sobre a matéria, o governo dos Estados Unidos – por exemplo – através do FBI (*Federal Bureau of Investigation*)[570] pretendeu discutir o alcance e o acesso a sistemas de carros luxuosos que forneciam utilidades de telecomunicação a seus usuários. Ter acesso aos serviços de telecomunicação interligados aos carros de usuários permitiria – através da colaboração da empresa fornecedora de serviços – alcançar uma conexão de celular no veículo alvo para ouvir as comunicações orais ocorridas dentro do automóvel.

Originalmente, segundo conta o caso, o sistema foi desenvolvido para auxiliar na navegação e trânsito, através da combinação entre um sistema de *GPS* e a tecnologia celular, servindo também para auxiliar nas buscas investigativas quando diante do furto ou roubo de veículos equipados com este sistema. O modo de recuperação de veículos roubados permite que a empresa se conecte com o sistema através de uma chamada celular. Quando a chamada do sistema é atendida, permite que o operador ou terceiros ouvintes possam ouvir o som de dentro do veículo sem que os ocupantes do automóvel tomem conhecimento da conexão do telefone celular, de modo que também não saberão da escuta executada.

A conexão entre o sistema e a empresa permanece enquanto não desligada a ignição do veículo ou haja uma queda na conexão[571]. O FBI pretendeu e obteve uma série de ordens

---

[570] *United State of America vs. The company*. *In re: In the matter of the application of the United States, for an order authorizing the roving interception of oral communications.* No. 02-15635. D.C. No. CV-01-01495-LDG Opinion. November, 18, 2003. Disponível em: https://www.steptoe.com/images/content/3/7/v1/374/629.pdf. Acesso em 02 out, 2018.

[571] As companhias alegam a impossibilidade de auxiliar nas investigações por diversos motivos, dentre os quais a possibilidade do usuário tomar conhecimento de que o sistema de recuperação está em operação. Duas coisas podem acontecer quando o sistema está em modo de recuperação do veículo. A primeira é quando o rádio multimídia do veículo estiver ligado, situação em que aparecerá em seu *display* a mensagem [*System Active*]; A segunda é quando o rádio multimídia estiver desligado, em que o próprio sistema emite um sinal sonoro, independentemente de o veículo estar ligado ou não. A empresa esclarece que "não há como impedir tais sinais de que o carro está em modo de recuperação". Id. p, 16136. A empresa ainda justifica que conceder acesso ao FBI para investigações, utilizando o sistema de chamada celular, não será possível a execução das demais funcionalidades do sistema, como por exemplo as chamadas de emergência. Nenhum operador estiver na linha, somente o FBI esteja escutando, não haverá resposta à emergência do usuário assinante sinalizada pelo sistema. [*When the System is in stolen vehicle recovery mode, the customer cannot use any of the other System services. If a customer presses any of the non-emergency buttons — for example, the roadside assistance or information buttons — nothing will happen. If the customer presses the emergency button or the airbags deploy while the recovery mode is enabled, it appears to the user that the system is attempting to open up a cellular phone connection to the response center but it is not. Instead, an audio tone is sent over the already open connection. The Company is concerned that if no operator is on the line and only the FBI is listening in, there will be no response to the subscriber's emergency signaled by the transmitted tone*].

judiciais que exigiam da empresa fornecedora deste serviço o auxílio na captação das conversas que ocorriam no automóvel, através do uso do "*bug*" para escutas de investigados.

O caso emblemático de *Roving Bug* em aparelhos celulares é descrito em *United States Vs. Tomero*[572] cujas investigações pretendiam desarticular uma organização criminosa. O governo estadunidense solicitou a utilização do *bug* no aparelho celular de John Ardito, para interceptar suas conversas em locais que este utilizava para se reunir com demais membros da organização. O juiz deferiu o requerimento do meio de obtenção de prova, de modo que foi possível captar conversas do indivíduo alvo em locais nada comuns, sem que houvesse a necessidade do dispositivo permanecesse ligado.

A mesma medida foi requerida ao juiz competente para que instalasse o *roving bug* no aparelho telefônico do advogado Peter Peluso, suspeito de ser um colaborador de Ardito e de transmitir mensagens a familiares e membros da família criminosa que – àquela altura – já desconfiavam das investigações por meio de interceptação. A discussão acerca da constitucionalidade das conversas interceptadas mediante *Roving Bug* foi parar na Corte dos Estados Unidos na tentativa de serem suprimidas as conversas captadas pelos aparelhos auditivos nos telefones de Ardito e Peluso.

A argumentação gira em torno da ausência de aplicabilidade constitucional relacionada à execução da referida medida[573], tendo em vista a inexistência de descrição adequada e particular do local a ser executada a captação da comunicação. Permitir-se-ia ao governo a interceptação de comunicações sem antecipadamente identificar o local a se realizar, ou seja a possibilidade de execução de mandados gerais de interceptação.

De acordo com o caso estadunidense uma vigilância eletrônica dessa natureza deveria incluir "uma descrição completa sobre os outros procedimentos investigativos tentados anteriormente, bem como suas falhas, ou os motivos pelos quais parecem não alcançarem êxito

---

[572] *United States of America Vs. John Tomero, et al. Defendants.* No. S206Crim.0008(LAK). 462 F.supp.2d565(2006), November, 27, 2006. Disponível em: https://www.leagle.com/decision/20061027462fsupp2d5651976. Acesso em 01 out, 2018.

[573] Id. p, 569. "*In 1986, Congress amended Title III to "update and clarify Federal privacy protections and standards in light of dramatic changes in new computer and telecommunications technologies."[6] One of the amendments was Section 2518(11), which permits "roving" electronic surveillance. It provides that: The requirements of subsections (1)(b)(ii) and (3)(d) of this section relating to the specification of the facilities from which, or the place where, the communication is to be intercepted do not apply if —(a) in the case of an application with respect to the interception of an oral communication —(i) the application is by a Federal investigative or law enforcement officer and is approved by the Attorney General, the Deputy Attorney General, the Associate Attorney General, an Assistant Attorney General, or an acting Assistant Attorney General;(ii) the application contains a full and complete statement as to why such specification is not practical and identifies the person committing the offense and whose communications are to be intercepted; and(iii) the judge finds that such specification is not practical. Section 2518(12) further provides that an agent implementing a roving intercept under subsection 11 must ascertain the place of the communication in advance of interception*".

nas investigações, ou ainda pelo excesso de perigo que proporcionam". Contudo, estes requisitos são flexibilizados pela Corte americana, segundo o argumento de que não seriam um obstáculo insuperável, bastando o cumprimento na demonstração de que técnicas investigativas normais seriam difíceis de alcançarem êxito. Tudo o que é necessário, segundo o entendimento da Corte, é uma "explicação fundamentada".

Ademais, segundo a argumentação dos réus no caso em tela, dever-se-ia ter uma identificação em concreto dos sujeitos interceptados, bem como dos assuntos que se pretende alcançar através da aplicação da medida. De acordo com a argumentação, a norma específica limitaria o uso de *roving bug* a situações em que o indivíduo ou os indivíduos específicos utilizam vários aparelhos celulares ou locais para discutir crimes, como meio a se evitar uma vigilância estatal. Contudo, a identificação dos sujeitos exigível – como requisito para a medida –, segundo a Corte é apenas a do sujeito alvo singular a ser interceptado, não sendo exigível, portanto, a identificação prévia de terceiros interlocutores.

Quanto à impraticabilidade da determinação dos locais frequentados pelos sujeitos a serem interceptados, segundo o entendimento da Corte Americana, não é necessário que o governo mostre completa imprevisibilidade no movimento dos sujeitos, bem como que outros métodos de vigilância falharam ou falhariam na interceptação. Tão somente seria necessário mostrar que os investigados se mudam com frequência suficiente para que os procedimentos regulares de interceptação restassem prejudicados.

Ainda no caso em tela, traz-se à baila a argumentação da "boa-fé" do Estado persecutor na utilização do referido método para obtenção de provas. Contudo, neste ponto específico se trata de argumentação apelativa para a flexibilização de garantias constitucionais que protegem o sujeito investigado de abusos na persecução penal. Não se discorrerá sobre o absurdo que é confiar na "boa-fé" de agentes em persecução penal, apenas um argumento basta para tanto. "Boa-fé" dos agentes jamais poderá ser tratada como requisito a ser observado na execução de medidas que restringem e violam direitos fundamentais, principalmente quando se tratar de flexibilização de garantias constitucionais. Em suma, o Estado atua em cumprimento da norma e não ao seu bel prazer e conveniência, afinal "quem nos salvará da bondade dos bons?"[574].

[574] MARQUES NETO, Agostinho Ramalho. **O Poder Judiciário na Perspectiva da Sociedade Democrática: O Juiz Cidadão.** Texto publicado originalmente: Revista ANAMATRA. Órgão Oficial da Associação Nacional dos Magistrados do Trabalho. Ano VI, nº 21, p. 30 – 50. Brasília: ANAMATRA, outubro a dezembro de 1994. p, 44. "[...] do ponto de vista do cidadão comum, nada me garante, em relação às boas intenções do Juiz – eu não digo em relação às más intenções, digo em relação às boas. Uma vez perguntei: quem nos protege da bondade dos bons? Do ponto de vista do cidadão comum, nada nos garante, "a priori", que nas mãos do Juiz estamos em boas mãos,

De qualquer sorte, no Brasil devido ao caráter extremamente vago quanto à legislação sobre captações ambientais, não especificando procedimentos adequado a serem observados, não parece conter razoáveis condições de assegurar adequadamente e suficientemente a proteção do direito à privacidade[575]. Como ressalta Mendes e Pinheiro, dizer que a lei de proteção é insuficiente talvez não retrate com o rigor apropriado o seu descompasso com o surgimento de novas tecnologias, para os autores o apropriado é destacar o verdadeiro grau de "ineficiência de todo um modelo de regulação fundado nas tradicionais garantias de inviolabilidade do domicílio e do sigilo das comunicações"[576]. Em se tratando de garantias – vale relembrar – é certo dizer "inefetividade" de todo este modelo.

4.1.3 Buscas on-line: A recolha de dados por acesso remoto

A recolha de dados mediante *malware* serve à investigação de *fontes* de prova correspondentes aos fatos ilícitos. Logo, como explicitado acima, a natureza jurídica adequada a esta funcionalidade é de meio de investigação de (*fonte* de) prova[577]. Deste modo, executada a aquisição de dados por acesso remoto, aos investigadores caberá a análise e identificação das informações e dos documentos colhidos para que, a partir destes, se possa tomar conhecimento de *quais* e *onde* se situam as *fontes* de prova relevantes para o processo penal.

Os dados obtidos mediante acesso remoto não correspondem, eles próprios, às *fontes* de provas utilizáveis. Em verdade, até pode haver algum dado digital relevante para o processo penal no caso concreto, mas em virtude do elevado risco eminente de contaminação do material probatório a partir da metodologia de acesso remoto por *malware*, perde-se confiabilidade, consequentemente se torna inutilizável como *fonte de prova*.

O uso da técnica investigativa, inevitavelmente, faz com que sejam alteradas configurações do sistema informático alvo. Por tal fato, a recomendação dos especialistas é que esse procedimento se destine tão somente à aquisição e análise daqueles dados considerados voláteis (*cache* do sistema, histórico, páginas da web, arquivos temporários, banco de dados em

---

mesmo que essas mãos sejam boas. [...] Enfim, é necessário, parece-me, que a sociedade controle o Estado, mas o lugar do Juiz não pode ser dissolvido nesse controle".

[575] MENDES, Gilmar; BRANCO, Paulo Gustavo Gonet. **Curso de Direito Constitucional.** 10 ed. rev. e atual. São Paulo: Saraiva, 2015. p, 566.

[576] MENDES, Gilmar; PINHEIRO, Jurandi Borges. **Interceptações e privacidade: novas tecnologias e a Constituição.** In: MENDES, G. F; SARLET, I. W; COELHO, A. Z. P. **Direito, inovação e tecnologia.** São Paulo: Saraiva, 2015. p, 249.

[577] Nesse sentido TROGU, Mauro. ***Sorveglianza e "perquisizione" on-line su materiale informatico.*** In: (a cura di) SCALFATI, Adolfo. *Le indagini atipiche.* G. Giappichelli Editore. Torino. 2014. p, 444.

uso, caixas de mensagens e bate-papo, mídias descriptografadas, sistemas de armazenamento virtualizados)[578].

A recolha de dados mediante *software* implica em uma mudança substancial na forma de se obter dados contidos em sistemas informáticos pertencentes ou utilizados pelos indivíduos-alvos da persecução penal. Seja pelo aspecto da economia de pessoal (descolamento de investigadores para a apreensão de suportes físicos), seja pela economia de tempo e efetividade da medida, a utilização de *malware* põe em crise a aplicação de mecanismos tradicionais de obtenção de materiais probatórios digitais que anteriormente necessitavam exclusivamente da apreensão de suportes físicos.

Possibilita-se a busca e obtenção tanto de dados concretos (arquivos, documentos, dados de tráfico, correios eletrônicos) como também de chaves de acesso ou fórmulas de encriptação em sistemas informáticos[579]. Ademais, a busca *online* em ambiente digital permite acessar dados armazenados não somente em suportes físicos, mas em sistemas informáticos dispostos em "nuvens" (*Cloud*)[580].

Neste sentido é que Salt destaca duas vantagens técnicas inerentes à metodologia de recolha de dados por acesso remoto. A primeira delas se refere, justamente, à efetividade da investigação e produção probatória, de modo que pela volatilidade da *fonte* de prova digital – bem como a existência de mecanismos de segurança que permitem esconder ou destruir os dados – poderia se tornar contraproducente ou infrutífera uma busca e apreensão do suporte físico antes da identificação e localização das *fontes* relevantes. A segunda se relaciona diretamente com o segredo no emprego da medida, que pela subrepticialidade se obtém informações sem o conhecimento do sujeito alvo nem de terceiros[581].

Do ponto de vista jurídico, parece mais adequado a execução da medida ainda na fase investigativa, mas desde que já elaborado relatório criminal pela autoridade policial, de modo que neste se tenham preenchidos requisitos suficientes de identificação do sujeito passivo e do sistema informático visado (autoria e materialidade delitiva). Isto retrata também que a

---

[578] BUSO, Diego; PISTOLESI, Daniele. ***Le perquisizioni e i sequestri informatici.*** In: (a cura di) RUGGIERI, Francesca; PICOTTI, Lorenzo. *Nuove tendenze della giustizia penale di fronte alla criminalità informática Aspetti sostanziali e processuali.* G. Giappichelli Editore – Torino. 2010. p, 189.

[579] SALT, Marcos. ***Nuevos desafios de la evidencia digital***. Op. cit. p, 53-55. "*Implica también la posibilidad de que los investigadores puedan obterner las claves de todo tipo que el usuário para aceder a documentos, sitios de Internet, lugares de almacenamiento de información en la nube, servidores de correo electrónico, evitando las dificultades que enfrentan hoy muchas investigaciones penales en las que, producido un allanamiento y obtenido el acceso a los dispositivos físicos de almacenamiento de información, resulta problemático el acceso a los datos protegidos por claves y sistemas de encriptación cada vez más efectivos*".

[580] Sobre o tema RAMALHO, David Silva. **A recolha de prova penal em sistemas de computação em nuvem.** Revista de Direito Intelectual n. 02, 2014. p, 123-162.

[581] SALT, Marcos. ***Nuevos desafios de la evidencia digital***. Op. cit. p, 57-58.

natureza do instituto se refere à identificação de *fontes* de prova, que após a sua aquisição, servirão para a construção das hipóteses fáticas das partes. Retrata Marcolini[582] que a medida decorre dos relatórios criminais e não o inverso, desta forma evitar-se-ia cenários de *inquisitio generalis.*

A metodologia empregada deve se constituir sob orientação constitucional, de modo que como meio de investigação de prova, há que possuir demarcação temporal para cumprir sua finalidade. Não é possível que um direito fundamental seja demasiadamente restringido sem que possua prazo legalmente especificado para que cesse a ingerência estatal que o restringe. Tanto a recolha dos dados por acesso remoto, como a análise do material probatório devem ser concluídas no tempo estritamente necessário para verificar a presença ou a ausência da *fonte* de prova, no lugar ou relacionada à pessoa indicada no mandado judicial que autoriza a medida[583].

A ilustração da metodologia de recolha de dados por acesso remoto pode ser feita a partir da análise da *sentenza "Virruso"*[584] que derivou da primeira hipótese de utilização do *malware*[585] em investigações criminais para fins de buscas online[586]. De tal sorte que alguns problemas foram enfrentados pela Suprema Corte Italiana (*Corte Suprema di Cassazione*).

---

[582] MARCOLINI, Stefano. ***Le cosiddette perquisizioni on line (o perquisizioni elettroniche).*** In: a cura di) RUGGIERI, Francesca; PICOTTI, Lorenzo. *Nuove tendenze della giustizia penale di fronte alla criminalità informática Aspetti sostanziali e processuali.* G. Giappichelli Editore – Torino. 2010. p, 191.

[583] TROGU, Mauro. ***Sorveglianza e "perquisizione" on-line su materiale informatico.*** Op. cit. p, 444.

[584]ITALIA, Cass. Pen., sez. V, 29 abril 2010, n. 16556, Virruso. Disponível em: http://www.penale.it/stampa.asp?idpag=1228. Acesso em out 2018.

[585] Em italiano "*captatore informatico*".

[586] Outro caso que serve para ilustrar a efetivação da medida de busca online é o caso "*Bisignani*". Neste, iniciado pelo Ministério Público, a suspeita era de que os investigados teriam, por meio da utilização de tráfico de influências, adquirido mecanismos de obtenção de informações sigilosas, como noticias relativas a casos penais em trâmite, ou dados pessoais sensíveis de terceiros, que os possibilitava sustar ou reveter prejuízos nas investigações judiciais que eram submetidos ou outros benefícios (TESTAGUZZA, Alessandra. ***Il sistemi di controlo remoto: fra normativa e prassi.*** Mezzi di prova. Diritto penale e processo 6/2014. p, 760). O *software* utilizado na investigação, além de adquirir dados informáticos armazenados nos dispositivos informáticos visados, possibilitou efetivação de interceptações ambientais por meio do controle remoto tanto dos microfones quanto das webcams integradas aos sistemas informáticos infectados. Marcos Torre salienta que as autoridades competentes reconheceram a necessidade de conciliação entre os fins objetivados pal investigação e o direito de defesa dos investigados, de modo que requereram autorização judicial tanto para o acesso remoto (buscas *online*) dos dados armazenados em tais dispositivos, como para execução da vigilância *online* (***Il captatore informático*****.** Op. cit. p, 103). A autoridade judicial deferiu os requerimentos salientando a semelhança da vigilância *online* com a interceptação ambiental, e de tal forma, regulada pelo artigo 266 do Código de Processo Penal Italiano. Quanto ao segundo efeito, o acesso a dados sensíveis mediante a "busca online", restou limitado em exigir que o Ministério Público garantisse a confidencialidade dos sujeitos que tivessem acesso aos referidos dados. Dispõe o artigo 266 do *Codice di Procedura Penale: "1) L'intercettazione di conversazioni o comunicazioni telefoniche e di altre forme di telecomunicazione è consentita nei procedimenti relativi ai seguenti reati: a) delitti non colposi per i quali è prevista la pena dell'ergastolo o della reclusione superiore nel massimo a cinque anni determinata a norma dell'articolo 4; b) delitti contro la pubblica amministrazione per i quali è prevista la pena della reclusione non inferiore nel massimo a cinque anni determinata a norma dell'articolo 4; c) delitti concernenti sostanze stupefacenti o psicotrope; d) delitti concernenti le armi e le sostanze esplosive; e) delitti di contrabbando; f) reati di ingiuria, minaccia, usura, abusiva attività finanziaria, molestia o disturbo alle persone col mezzo del telefono*

No caso, o Ministério Público determinou em decreto de "busca e apreensão" de documentos nos termos do artigo 234, do Código de Processo Penal Italiano[587], uma cópia da documentação informatizada armazenada no computador visado, situado nos escritórios da empresa responsável pela sistema de água potável do município de *Villafrati*. Contudo, o decreto do Ministério Público não autorizava apenas a cópia documental como prevê o artigo utilizado, mas uma extensão. O objetivo abarcava tanto a coleta de arquivos existentes nos discos rígidos do computador, como também todos os dados relacionados à investigação que poderiam surgir futuramente, produzidos ou incluídos, na memória do sistema informático[588].

O *software* invasor (*gosth*) utilizado pelos investigadores era capaz de se apropriar de todos os dados do sistema, seja daqueles já armazenados na memória, seja daqueles arquivos processados em tempo real. Neste ponto em destaque, sob as alegações da defesa, os requisistos necessários para a execução da medida não foram obedecidos, porquanto que tal atividade devia obediência ao artigo 266-*bis* e seguintes do Código de Processo Penal Italiano[589], que versam sobre a interceptação telefônica e telemática.

Tratava-se portanto de um acompanhamento oculto e contínuo do conteúdo produzido e acessado pelo usuário do sistema informático, e deste modo a alegação defensiva era de que haveria um fluxo de informações dentro do sistema informático alvo, desta feita fazendo *jus* a obediência de requisitos presentes dos artigos referidos sobre a matéria[590]. Portanto, imprescindível seria uma prévia autorização judicial contendo os procedimentos operacionais cabíveis e os limites de duração da medida de interceptação. Desta forma, o

---

(1). 2. Negli stessi casi è consentita l'intercettazione di comunicazioni tra presenti. Tuttavia, qualora queste avvengano nei luoghi indicati dall'articolo 614 del codice penale, l'intercettazione è consentita solo se vi è fondato motivo di ritenere che ivi si stia svolgendo l'attività criminosa.

587 ITALIA, ***Codice di Procedura Penale*** *– articolo 234*: *Prova documentale. 1) E' consentita l'acquisizione di scritti o di altri documenti che rappresentano fatti, persone o cose mediante la fotografia, la cinematografia, la fonografia o qualsiasi altro mezzo. 2) Quando l'originale di un documento del quale occorre far uso è per qualsiasi causa distrutto, smarrito o sottratto e non è possibile recuperarlo, può esserne acquisita copia. 3) E' vietata [c.p.p. 191] l'acquisizione di documenti che contengono informazioni sulle voci correnti nel pubblico intorno ai fatti di cui si tratta nel processo o sulla moralità in generale delle parti, dei testimoni, dei consulenti tecnici e dei periti.*

588 TORRE, Marco. ***Il captatore informatico.*** Op. cit. p, 101.

589 ITALIA, ***Codice di Procedura Penale – articolo 266-bis***: *Nei procedimenti relativi ai reati indicati nell'articolo 266, nonché a quelli commessi mediante l'impiego di tecnologie informatiche o telematiche, è consentita l'intercettazione del flusso di comunicazioni relativo a sistemi informatici o telematiciovvero intercorrente tra più sistemi;* ***articolo 267:*** *1. Il pubblico ministero richiede al giudice per le indagini preliminari l'autorizzazione a disporre le operazioni previste dall'articolo 266. L'autorizzazione è data con decreto motivato quando vi sono gravi indizi di reato e l'intercettazione è assolutamente indispensabile ai fini della prosecuzione delle indagini (1) (2). Il decreto che autorizza l'intercettazione tra presenti mediante inserimento di captatore informatico su dispositivo elettronico portatile indica le ragioni che rendono necessaria tale modalità per lo svolgimento delle indagini; nonché, se si procede per delitti diversi da quelli di cui all'articolo 51, commi 3-bis e 3-quater, i luoghi e il tempo, anche indirettamente determinati, in relazione ai quali è consentita l'attivazione del microfono[...]*.

590 TORRE, Marco. ***Il captatore informático*****.** Op. cit. p, 101.

material coletado deveria ser considerado prova inconstitucional e, portanto, inutilizável conforme o artigo 271 do Código de Processo Penal Italiano.

Negada a tese defensiva, a Corte decidiu que não se tratava de interceptação, tendo em vista a não ocorrência de comunicação entre interlocutores e deste modo não haveria uma gravação do "fluxo das comunicações", mas uma relação direta entre o sistema informático e o *software* captador de dados, um "fluxo unidirecional de informações"[591]. As fontes de provas coletadas na investigação foram fundamentais para a condenação dos réus pelo Tribunal de Palermo, que admitiu ser legítima a atividade investigativa realizada, constituindo-se prova atípica regulamenta pelo artigo 189 do Código de Processo Penal Italiano[592].

Acertadamente a Corte afastou a tese de que a utilização de recolha de material probatório digital mediante *softwares* maliciosos corresponderia a interceptação de fluxo de comunicação telemática. Como afirmado acima, não se trata de interceptações de fluxo de comunicação, mas a recolha unilateral a partir da invasão de um *software* em um sistema informático, corrompendo desta forma a integridade e segurança do sistema alvo, para que assim seja possível o acesso remoto pelo Estado investigador.

Por outro lado, não se pode olvidar que a utilização de *vírus spy* como medida de alta incidência em direitos fundamentais dos investigados deve ser somente executada obedecendo a requisitos mínimos de legalidade (ainda que no ordenamento jurídico italiano se entenda pela utilização de provas atípicas) e limites impostos por autorizações judiciais[593]. Salt adverte que a medida decretada pelo Ministério Público e levada a cabo pelas autoridades de investigação, além de dispensar mandado judicial, utilizou-se de disposições análogas de execução que, no caso em tela, versam sobre a obtenção de documentos físicos e não virtuais. Ademais, no entendimento da Corte italiana também justificou que a medida não se tratava de uma medida irreptível, dispensando garantias previstas como a comunicação da defesa para que se estabelecesse o contraditório. De modo que assim se procederia em momento oportuno no curso processual.

Em ambos os vértices de análise, tal entendimento não seria legítimo no ordenamento jurídico brasileiro. A despeito de já ter se falado sobre a necessidade de critérios

---

[591] ITALIA, Cass. Pen., sez. V, 29 abril 2010, n. 16556, Virruso.

[592] ITALIA, ***Codice di Procedura Penale*** *– articolo 189*: 1) *Quando è richiesta una prova non disciplinata dalla legge, il giudice può assumerla se essa risulta idonea ad assicurare l'accertamento dei fatti [187] e non pregiudica la libertà morale della persona [642, 188]. Il giudice provvede all'ammissione, sentite le parti sulle modalità di assunzione della prova*.

[593] Neste mesmo sentido SALT, Marcos. ***Nuevos desafios de la evidencia digital***. Op. cit. p, 100.

mínimos de legalidade[594] – *nulla coactio sine lege* – e o fundamental controle judicial sobre medidas de investigação de prova que incidem demasiadamente em direitos fundamentais dos sujeitos passivos, deve-se também levar em consideração o Direito Processual Penal como entidade epistêmica e, consequentemente, tornar-se necessária a devida comprovação da integridade e fiabilidade do material probatório recolhido.

A utilização análoga de disposições que regulamentam as buscas e apreensões de documentos físicos refletem uma atecnia processual que lesiona significativamente o direito de defesa do sujeito passivo. Não é possível tratar institutos processuais distintos como se de mesma natureza jurídica fossem. A busca e apreensão de provas físicas, em que pese corresponder a uma natureza híbrida, qual seja meio de investigação de prova e medida cautelar probatória, somente assim o é, devido a possibilidade de se confirmar a "mesmidade" por procedimentos de recolha e conservação da *fonte* de prova. Desta forma, se possibilita incluir a *fonte* de prova cautelar no processo para que em momento oportuno se estabeleça o contraditório judicial.

Tal capacidade não é percebida atualmente pela execução de *buscas online* mediante *malware*. Do ponto de vista técnico, o *software* invasor modifica o sistema alvo, possibilitando até mesmo a inclusão de arquivos neste sistema informático[595]. De tal sorte, jamais será possível se estabelecer o contraditório judicial sobre às informações constantes nas *fontes* de prova decorrentes das *buscas online* pela incapacidade da comprovação da "mesmidade" do material probatório. Portanto, como não se trata de cautelar probatória, não há que se falar em conservar as fontes de prova recolhidas e inseri-las no processo penal para que se exerça o contraditório judicial.

Semelhantes foram as discussões que levaram o legislativo espanhol a optarem pela regulamentação dos denominados "*registros remotos*". A experiência espanhola quanto ao tema reflete a necessidade de determinações normativas atinentes às medidas de investigação que se fundam na utilização de tecnologias de informação. As razões expressadas no preâmbulo da reforma da *Ley de Enjuiciamento Criminal*, promovida em 2015 pela *Ley Organica* 13/2015[596], afirmam que haveria uma necessidade de adequação legislativa a um novo modelo processual

---

[594] Semelhante ressalva também é feita por AIGE MUT, Mª Belén. Boletín de la Academia de Jurisprudencia y Legislación de las Illes Balears, ISSN 2254-2515, Nº. 17, 2016, págs. 221-230. p, 230. "[...] *pero ese programa al introducirlo en el ordenador podría afectar a otros derechos fundamentales de la persona investigada porque podría actuar como un programa espía, una especie de troyano federal17 y por eso es muy importante contar con una norma habilitante que regule esta posibilidad de acceso remoto, pero a la vez con una serie de limitaciones y restricciones importantes*".

[595] TROGU, Mauro. ***Sorveglianza e "perquisizione" on-line su materiale informatico.*** Op. cit. p, 454.

[596] ESPANHA. *BOE* Núm. 239. Martes 6 de octubre de 2015. Sec I. Pág. 90192. Disponível em: https://www.boe.es/boe/dias/2015/10/06/pdfs/BOE-A-2015-10725.pdf Acesso em out 2018.

penal que se dedicasse a questões enquadradas na regulação de medidas de investigação tecnológica que incidem no âmbito de direitos da intimidade, segredo das comunicações a proteção de dados pessoais tutelados pela Constituição e o fortalecimento de garantias processuais[597]. Antes da dita reforma as discussões no contexto espanhol se voltavam à possível utilização de interpretações análogas quanto à recolha de dados mediante acesso remoto[598].

A nova lei, a seu turno, incluiu um capítulo dedicado ao uso de *malware* e demais tecnologias de invasão de sistemas informáticos[599]. O artigo 588 *septies* a., elenca os pressupostos que devem ser observados pelo juiz antes de decretar a execução da medida de "registro remoto" através da instalação de *software* em dispositivos eletrônicos, sistemas informáticos, instrumentos de armazenamento de dados ou bases de dados, sem o conhecimento de seu titular. O primeiro pressuposto que restringe a utilização da referida medida é a disposição, na lei espanhola, de rol taxativo dos delitos passíveis de serem investigados através do acesso remoto[600].

Na sequência, o legislador espanhol optou pela imposição à autoridade judicial de especificar requisitos que direcionem os investigadores na execução da apreensão de dados mediante acesso remoto. Primeiramente, deverá constar na decisão judicial, especificadamente, a identificação dos computadores, dispositivos eletrônicos, sistemas informáticos ou partes destes, meios informáticos de armazenamento de dados ou bases de dados que serão, efetivamente, objetos da medida. Ademais, também constará o alcance do método de investigação, a forma em que se procederá o acesso e a apreensão dos dados e arquivos informáticos, bem como a especificação do *software* pelo qual se executará o controle da informação.

Caberá ao juiz a determinação das autoridades competentes para a realização da medida, a autorização para a realização e a conservação das cópias dos dados informáticos

---

[597] SALT, Marcos. ***Nuevos desafios de la evidencia digital.*** Op. cit. p 103.
[598] RAMALHO, David Silva. **Métodos ocultos de investigação criminal em ambiente digital.** Op. cit. p, 333.
[599] ESPANHA. *BOE*.Op. cit. CAPÍTULO IX ***Registros remotos sobre equipos informáticos.***
[600] ESPANHA, Id. *Artículo 588 septies a.) pressupostos.* 1) *[...]: a) Delitos cometidos en el seno de organizaciones criminales. b) Delitos de terrorismo. c) Delitos cometidos contra menores o personas con capacidad modificada judicialmente. d) Delitos contra la Constitución, de traición y relativos a la defensa nacional. e) Delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación o servicio de comunicación*. Marcos Salt afirma que esta última alínea (*e*) pode derivar a interpretação de que seja possível a utilização da na investigação de delitos de menor gravidade pelo simples fato de que estes tenham sido cometidos através de meios informáticos. Contudo, tal interpretação vai de encontro com a intencionalidade do legislador, qual seja, limitar o uso da medida processual de "registro e sequestro de dados" devido ao âmbito de proteção de garantias constitucionais afetados por tal ingerência (SALT, Marcos. ***Nuevos desafios de la evidencia digital***. Op. cit. p, 108). No mesmo sentido que Salt, QUEVEDO GONZALEZ, Josefina. ***Técnicas de investigación de los ciberdelitos.*** In: *Investigación y prueva del ciberdelito.* Madrid: Editorial Jurídica Sepín, 2017. p, 200.

objetivados, bem como as medidas precisas para a preservação da integridade destes dados. Ademais, determinará medidas para possibilitar a inacessibilidade dos dados ou a sua supressão quando necessário.

O conhecimento judicial acerca da execução das medidas de acesso remoto a dados, pela lei espanhola, é constante. O artigo 588 *septies a 3* ressalta que no momento da efetivação do acesso remoto, caso os investigadores percebam que os dados relevantes, objetos da busca, estejam armazenados em outro sistema informático, ou em outra parte do sistema acessado, deverão comunicar o juiz para que este, entendendo ser cabível, autorize uma ampliação nos termos da execução do "*registro remoto*".

4.1.4 Malware e a vigilância online

A vigilância *online* é modalidade investigativa permitida a partir da utilização de *software* espião invasor em um sistema informático visado. Abarca o monitoramento de diversas atividades executadas pelos sujeitos alvos da medida, desde o fluxo de dados transmitidos pelos sistemas informáticos em geral ao monitoramento de email, *chats*, localização dos dispositivos, monitoramento em tempo real do acesso aos navegadores de internet (*screenshot*), identificação de senhas de acesso, bem como as teclas digitadas no teclado (*keylogger*) e etc. Ademais, é possível o monitoramento do momento e da duração das atividades realizadas[601].

De tal forma, esta parece ser a diferença basilar entre a *vigilância online* e *a pesquisa online* ou *recolha de dados por acesso remoto*, a primeira pressupõe a ocorrência de fluxos de dados, esta última volta-se ao alcance de dados constantes no dispositivo informático. A vigilância *online* se volta ao controle contínuo, ou seja, um sistema de controle remoto relacionado ao sistema informático e telemático[602].

Monitorar a atividade do usuário através de *software* espião que capta tudo que for digitado, seja em teclados físicos ou digitais, é possível pela infiltração de um *keylogger*. Conforme Torre, trata-se de *software* capaz de interceptar tudo e armazenar secretamente tudo o que foi digitado por meio de cadeias de caracteres alfanuméricos, ou mesmo permitir o acesso

[601] TORRE, Marcos. ***Indagini Digitale y Processo Penale.*** Op. cit. p, 94.
[602] COLAIOCCO, Sergio. ***Nuovi mezzi di ricerca della prova: l'utilizzao dei programmi spia.*** Orientamenti: Archivo penale. 2014, n.1. p, 4.

daquilo que foi digitado em tempo real ou periodicamente por uma central de controle remoto[603-604].

Segundo o autor, a vigilância exercida contempla uma diversidade de atividades desenvolvidas pelo usuário, desde o acesso por meio de senhas em sistemas restritos, até o monitoramento na elaboração de documentos digitais. Por sua vez, as funcionalidades *sreenshot* e *screencast* se referem à possibilidade de registrar seja – no primeiro caso – as imagens visualizadas no écran dos dispositivos informáticos, seja – no segundo caso – os vídeos reproduzidos no dispositivo[605].

Possibilita ao investigador o acesso à privacidade do indivíduo-alvo de maneira expressiva. Como consequência, permite-se ao Estado persecutor tirar conclusões muito precisas sobre a privacidade das pessoas cujos dados acessados fazem referência, "tais como hábitos diários, locais frequentados (permanente ou temporariamente), viagens diárias e não diárias, atividades realizadas, as relações sociais das pessoas e os ambientes sociais que frequentam"[606].

Neste aspecto, afeta certeiramente o direito constitucional de proteção da privacidade, de modo que a recolha ou o simples acesso ao registro de dados do sistema informático pode indicir no direito ao desenvolvimento livre da personalidade, e mais precisamente a uma vida privada livre. Portanto, sendo medida investigativa que restringe direitos fundamentais, além do critério da legalidade, deverá haver necessária autorização judicial que imponha controles, limites e consequências quanto a ocorrência de abusos investigativos[607]. Este é, certamente, um dos pontos fundamentais da problemática sobre a matéria, a possibilidade (e a necessidade) de estabelecer limites específicos quanto às múltiplas funcionalidades desempenhadas pelo *malware* que permite a constante vigilância estatal perante o indivíduo.

Interessante caso ocorrido nos Estados Unidos chama atenção. Trata-se do caso *United States v. Nicodemo S. Scarfo*[608] no qual há forte tensão entre os direitos de privacidade e interesses na persecução penal guiada pelo uso de novas tecnologias aqui tratadas.

---

[603] TORRE, Marco. ***Il captatore informático*****.** Op. cit. p, 114.
[604] CONTI, Carlotta; TORRE, Marco. ***Spionaggio informatico nell'ambito dei social network*****.** In: (a cura di) SCALFATI, Adolfo. *Le indagini atipiche.* G. Giappichelli Editore. Torino. 2014. p, 416.
[605] TORRE, Marco. ***Il captatore informático*****.** Op. cit. p, 115.
[606] TROGU, Mauro. ***Sorveglianza e "perquisizione" on-line su materiale informatico.*** Op. cit. p, 445.
[607] TROGU, Mauro. ***Sorveglianza e "perquisizione" on-line su materiale informatico.*** Op. cit. p, 446.
[608] ESTADOS UNIDOS DA AMERICA, **ESTADOS UNIDOS, v. Nicodemo S. SCARFO, et al.** Ação Criminal No. 00-404 (NHP). **180 F. Supp. 2d 572 (2001). Tribunal Distrital dos Estados Unidos, D. New Jersey.** 26 de dezembro de 2001. Disponível em: https://law.justia.com/cases/federal/district-courts/FSupp2/180/572/2475159/. Acesso em out 2018.

Especificadamente, o *FBI* em janeiro de 1999, no cumprimento de uma busca e apreensão efetivada no escritório de Scarfo e Paolercio, tinha como objetivo coletar provas relativas a operações ilegais de jogos ilícitos e agiotagem. Na ocasião o *FBI* apreendeu um computador pessoal, contudo não logrou êxito quanto ao acesso aos dados do dispositivo informático devido à proteção *antiforensic* de criptografia dos arquivos.

Diante deste cenário, e suspeitando que um dos arquivos denominado "*Factors*" guardava *fontes* de prova relevantes para a investigação, o *FBI* resguardado por autorização judicial instalou entre o teclado e o *CPU* (*Central Process Unit*) um dispositivo *Key Logger System* (*KLS*), para que fosse possível coletar informações digitadas pelos usuários e desta forma, decifrar as senhas de acesso para o arquivo criptografado. Pelo acesso às *fontes* de prova, moveu-se acusações penais em face de Scarfo que cuminaram em uma sentença condenatória[609].

A principal discussão à época era se o Governo norteamericano teria violado as então normas que regulavam as interceptações telefônicas ao utilizar o *KLS*, pois o sistema transmitia as informações para a central através de moldem conectado a linhas telefônicas. Contudo, a tentativa da defesa na supressão das provas colhidas pela investigação a partir do uso do *KLS* foi negada, pelo argumento de que não houve abusos na investigação quanto ao acesso a demais informações, principalmente por não ser necessário uma autorização judicial especificada, pois a metodologia empregada não estaria regulamentada. No caso em tela, nos parece que o direito fundamental não se trata de integridade do sistema informático por evidente, o dispositivo não se integralizava ao sistema visado, mas era instalado por *hardware* externo.

De todo modo, como salienta Carrell[610] o *FBI* passou a desenvolver um *software* denominado *Magic Latern* que cumpre basicamente com as funções do *KLS*, somadas à possibilidade de ser ativado por acesso remoto com a invasão do dispositivo informático visado mediante *malware*[611]. A investida tem como mote a vigilância *online* de dados por vezes

---

[609] No caso em tela, o dispositivo instalado não se tratava de um *software key logger*, mas sim de um dispositivo físico (*hardware*). Contudo, a funcionalidade do dispositivo físico e dos atuais *malwares key loggers* é a mesma.

[610] CARRELL, Nathan E. ***Spying on the mob: United Sta Tes v. Scarfo - a constitutional analysis***. JOURNAL OF LAW, TECHNOLOGY & POLICY. Vol. 2002. p, 194.

[611] Em paralelo, desenvolveu um programa de interceptação denominado *Carnivore* que basicamente tinha a capacidade de filtrar as informações em mensagens transmitidas pelos provedores de serviços de internet (*ISP – Internet Service Providers*). A partir dos acontecimentos do 11 de setembro de 2001, a *CIA* buscou autorização para que para que fosse possível a interceptação de todos os e-mails (*e-mail surveillance*) enviados do exterior para os Estados Unidos. Contudo, a investida por vezes se mostrou inócua devido a utilização de técnicas *antiforensics* como a criptografia. GEORGITON, Peter J. ***The FBI's Carnivore: How Federal Agentes may be viewing your personal e-mail and why there is nothing you can do about it.*** Ohio State Lawjournal. Vol. 62. p,

impedida pela utilização massiva de medidas anti-forenses de encriptação de arquivos e mensagens. O *Magic Lantern* perde espaço para o *CIPAV* (*Computer and Internet Protocol Address Verifier*)[612] que também se projeta como *software* cuja função é a recolha de informações sobre o endereço *IP* (*Internet Protocol*) ou *MAC* (*Media Access Control*) do dispostitivo alvo, bem como sua localização, o sistema operacional utilizado, lista de programas em funcionamento, último site acessado pelo dispositivo informático[613].

Um curioso caso[614] demonstra a atual funcionalidade e o alto grau de vigilância e alcance de dados que estes *softwares* podem obter. Em 2012 após o recebimento de diversas ameaças de explosões por bombas compostas de nitrato de amônio em aeroportos e unidades prisionais, foi solicitado aos agentes do *FBI* que efetivassem uma investigação técnica com a utilização de *software NIT* (*Network Investigative Technique*). As informações importantes para que se identificasse o suspeito da prática de falsa informação relacionada a terrorismo e crimes de violência, resumia-se ao endereço do *e-mail* pelo qual se comunicou com as autoridades policiais, não havendo portanto, uma identificação concreta da pessoa suspeita.

Desta forma, requereu-se a implantação de *software* capaz de coletar dados informacionais que pudessem facilitar na identificação, seja do suspeito inominado, ou do dispositivo informático que este utilizava para se comunicar. A *NIT*, portanto, deveria ser programada para identificar: a) o endereço *IP*[615]*;* b) o endereço *MAC*[616]; c) as portas de comunicações do computador[617]; d) A lista de programas em execução no computador; e) o tipo de sistema operacional instalado no computador e o número de série; f) o navegador da *web* e a versão em execução no computador; g) a codificação do idioma do computador e o idioma padrão; h) informações de fuso horário do computador; i) o nome de registro do

1834. Disponível em: https://kb.osu.edu/bitstream/handle/1811/70480/OSLJ_V62N6_1831.pdf. Acesso em nov 2018.

612 Sobre a operatividade do *CIPAV*: https://archive.org/details/CIPAV

613 RAMALHO, David Silva. **Métodos ocultos de investigação criminal em ambiente digital.** Op. cit. p, 326.

614 ESTADOS UNIDOS DA AMÉRICA. ***UNITED STATES DISTRICT COURT for the District of Colorado***. Case 1:12-sw-05685-KMT Document 7 Filed 12/11/12 USDC Colorado. Disponível em; https://pt.scribd.com/document/189641401/Colorado-NIT-Doc-7. Acesso em nov 2018.

615 Id. p, 3. "Um endereço IP é um numérico exclusivo endereço usado para direcionar informações pela Internet e é escrito como uma série de quatro números, cada um no intervalo 0 - 255, separados por períodos (por exemplo, 121.56.97.178)". Tradução livre.

616 Id. Ibidem. "Cada vez que um computador se comunica através de uma rede local (ou "LAN"), ele usa um dispositivo de hardware chamado placa de interface de rede. Fabricantes de cartões de interface de rede atribuem a cada um identificador numérico exclusivo chamado controle de acesso à mídia ou endereço *MAC*". Tradução livre.

617 Id. Ibidem. "Um número de comunicação da porta é uma informação que ajuda os computadores a associar uma comunicação a um determinado programa ou processo de *software* executado em um computador de forma eficiente. Por exemplo, se uma comunicação for enviada para a porta 80, o computador receptor geralmente a associa com o tráfego da *World Wide Web* e o envia para o servidor *web*, que pode enviar de volta uma página *web* para o computador solicitante". Tradução livre.

computador e o nome de registro da companhia; j) o nome do usuário atual e a lista de contas do usuário; k) as informações de conexão da rede com fio e sem fio do computador; l) a *URL* (*Uniform Resource Locator*) que o computador tinha acesso; m) outras informações de identificação semelhantes na ativação do computador que possam auxiliar na identificação do computador, sua localização, outras informações sobre o dispositivo informático e seu usuário que possam ser acessadas pela *NIT*.

Semelhante investida do *FBI* é retratada no caso, também de suspeita desconhecida, ocorrido no Estado do Texas[618]. Os crimes supostamente cometidos se tratavam de fraudes em bancos federais, roubo de identidades e violação de leis de segurança de computadores. A informação mais próxima à identificação das pessoas suspeitas também era uma conta de *e-mail*. De tal forma que a busca por mais informações também seria pela utilização de *software* malicioso instalado sub-repticiamente com o intuito de se extrair registros telefônicos armazenados, gerar fotografias dos usuários pela ativação das câmera instalada no dispositivo e extrair informações de localização (latidude e longitude)[619].

É notória a característica de uma investigação prospectiva quando solicitada expressamente o monitoramento de um período de trinta dias com o objetivo de recolher dados referentes a "lançamentos contábeis" com identificação de novas vítimas da fraude, fotografias extraídas pelo *malware* com o uso da câmera acoplata ao dispositivo informático visado, e a identificação de terceiros que utilizem o computador alvo.

A análise feita pelo magistrado competente se embasa nas regras de limites territoriais para emissão de mandados judiciais de busca e apreensão. Desta forma, salienta o julgador que mesmo diante da alegação de cumprimento da regra 41 (b)[620] pelo Governo

---

[618] ESTADOS UNIDOS DA AMÉRICA. ***United States District Court Southern District Of Texas Houston Division***. *In re warrant to search a target computer at premises unknown*. CASE NO. H-13-234M. Document 3 Filed in TXSD on 04/22/13. Disponível em: http://pt.scribd.com/doc/137842124/texas-order-denying-warrant. Acesso em no 2018.

[619] São as informações requeridas após a instalação do *software*: a) endereço *IP;* b) registros de atividade da Internet, incluindo logs de firewall, caches, navegador histórico e cookies, páginas da Web "marcadas como favoritos" ou "favoritas", termos de pesquisa que o usuário inseriu em qualquer mecanismo de pesquisa da Internet e registros de endereços da Web digitados pelo usuário; c) registros que evidenciam o uso dos endereços do Protocolo da Internet (*IP*) para se comunicar com os servidores de e-mail do [banco da vítima]; provas de quem utilizou o dispositivo informático como entradas de registro de logs, configuração arquivo, nomes de usuário e senhas salvos, documentos, histórico de navegação, perfis de usuário, conteúdo de e-mail, contatos de e-mail, "bate-papo", registros de mensagens, fotografias e correspondência; d) provas da existencia de outros *software* que pudessem permitir o acesso remoto ao dispositivo informatico por terceiros; e) provas da duração do uso do computador; f) registros de aplicativos executados.

[620] *Rule 41. Search and Seizure – b) Venue for a Warrant Application. At the request of a federal law enforcement officer or an attorney for the government: (1) a magistrate judge with authority in the district—or if none is reasonably available, a judge of a state court of record in the district—has authority to issue a warrant to search for and seize a person or property located within the district; (2) a magistrate judge with authority in the district has authority to issue a warrant for a person or property outside the district if the person or property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant*

estadunidense, também foi expressado na solicitação o desconhecimento da localização do dispositivo informático visado. Como ressaltado na decisão, os dados informáticos são reconhecidos como propriedade e como tal estão armazenados em dispositivos localizados em um território[621]. Evidente que o impasse ocorre quando a incursão do Estado extrapola a competência jurisdicional no que tange ao limite territorial, se não se conhece a localização do computador, a seu turno se desconhece também a localização dos dados informacionais requeridos[622].

Para além das inconstitucionalidades de mandados judiciais gerais, a priori os pontos levantados quanto a competência territorial merecem atenção. Embora esteja se tratando da conexão global de computadores, não é possível o Estado persecutor ultrapassar limites de competência jurisdicional por motivos de combate à criminalidade. De fato, não nos suscita dúvidas de que a jurisdição em termos de competência territorial na persecução penal estabelece limites e controle ao poder punitivo. Nesta óptica, a competência territorial como garantia deve ser (re)pensada a partir das possibilidades ofertadas pela conexão mundial de computadores, de modo a evitar que abusos na investigação criminal informática.

Outro aspecto levantado pela decisão que merece reflexão é a forma precária de se inserir o *malware* nos dispositivos informáticos pelo envio de correios eletrônicos. A diligência empregada não leva em consideração a possibilidade de que o *e-mail* alvo pode ser clonado, ou

---

is executed; (3) a magistrate judge—in an investigation of domestic terrorism or international terrorism—with authority in any district in which activities related to the terrorism may have occurred has authority to issue a warrant for a person or property within or outside that district; (4) a magistrate judge with authority in the district has authority to issue a warrant to install within the district a tracking device; the warrant may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both; and (5) a magistrate judge having authority in any district where activities related to the crime may have occurred, or in the District of Columbia, may issue a warrant for property that is located outside the jurisdiction of any state or district, but within any of the following: (A) a United States territory, possession, or commonwealth; (B) the premises—no matter who owns them—of a United States diplomatic or consular mission in a foreign state, including any appurtenant building, part of a building, or land used for the mission's purposes; or (C) a residence and any appurtenant land owned or leased by the United States and used by United States personnel assigned to a United States diplomatic or consular mission in a foreign state. (6) A magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if: (A) the district where the media or information is located has been concealed through technological means; or (B) in an investigation of a violation of 18 U.S.C. § 1030(a)(5), the media are protected computers that have been damaged without authorization and are located in five or more districts. Disponível em: https://www.law.cornell.edu/rules/frcrmp/rule_41. Acesso nov 2018.

[621] "*It is true that Rule 41(a)(2) (A) defines "property" to include "information," and the Supreme Court has long held that "property" under Rule 41 includes intangible property such as computer data [...]By the Government's logic, a Rule 41 warrant would permit FBI agents to roam the world in search of a container of contraband, so long as the container is not opened until the agents haul it off to the issuing district. The court has found no case willing to stretch the territorial limits of Rule 41(b)(1) so far". **United States District Court Southern District Of Texas Houston Division***. CASE NO. H-13-234M. p, 5.

[622] A exceção para a limitação territorial quanto a emissão de mandados judiciais, como salientado na nota 125, *Rule 41 (b)(3),* é quando da investigação de crimes de terrorismo doméstico ou internacional.

ainda que possa ser acessado em diversos dispositivos informáticos com proprietários diferentes.

Estas buscas por suspeitos "não-suspeitos", ou seja, uma pessoa não implicada[623] desde a ruptura de seus direitos à intimidade, privacidade e demais, coloca pessoas diversas em um local de "suspeitos em potencial". O suspeito em potencial é aquele que de imediado tem sua presunção de inocência vilipendiada, e durante a persecução – após a devassa feita na personalidade externada pelos dados acessados – deverá se desencubir de cargas para provar sua inocência. O cenário inquisitorial é remontado.

Não é demais lembrar que o usuário do email ou do dispositivo digital (ainda que sendo um "não suspeito"), ao se infectar com o *malware* corresponderá às máximas expectativas dos investigadores e desta forma, pela expectativa gerada a partir da evidência esquizofrênica, também se projeta na pessoa do "não suspeito" o resultado: o culpado.

De tal sorte que os limites e critérios empregados pelo legislador processual penal deve atender a tais possibilidades, de modo que – se constitucionalmente aceita – a vigilância investigativa por meio de *malware*, mantenha-se minimamente à pessoa visada, respeitando direitos fundamentais e garantias processuais deste, mas também sem que direitos fundamentais de terceiros sejam afetados. Nas palavras de Wolter[624] deve se exigir que a utilização dos dados seja detalhadamente regulada.

4.1.5 Investigação por gravação de vídeo ou observação em tempo real

Uma das potenciais formas de se investigar proporcionadas pelo advento da utilização de *software* invasivos em dispositivos informáticos é a investigação por meio de gravação de vídeo. Como dito acima, a partir da configuração do *malware* utilizado para obtenção de *fontes* de prova na investigação criminal, pode-se ativar por acesso remoto ao dispositivo diversas funcionalidades dentre as quais sua câmera.

Trata-se de mais uma forma de monitoramento próprio, desta vez, executado mediante gravação ou observação por vídeo de tudo aquilo que pode ser captado através da câmera integrada ao dispositivo alvo[625]. Também é, certamente, um método oculto de investigação de substancial lesividade a direitos fundamentais do investigado.

---

[623] WOLTER, Jürgen. **O inviolável e o intocável no direito processual penal.** Op. cit. p, 172.
[624] WOLTER, Jürgen. **O inviolável e o intocável no direito processual penal.** Op. cit. p, 164.
[625] TORRE, Marco. ***Il captatore informático*.** Op. cit. p, 110.

No ordenamento jurídico brasileiro, esta modalidade investigativa esbarra na proteção constitucional da intimidade e da vida privada, bem como em garantias processuais já mencionadas acima como o princípio da legalidade processual. De acordo com a jurisprudência italiana, estão estabelecidas na categoria de prova atípica, utilizáveis se realizadas em local público[626] mas determinado[627].

Conforme destaca Torre[628], há duas formas de vídeo vigilância que merecem distinção. A primeira se trata do registro do comportamento comunicativo que representa uma nova forma de interceptação de comunicação entre pessoas presentes, cuja captação se dá mediante o registro do áudio e vídeo, demonstrando-se demasiadamente lesivo à direitos como a privacidade do sujeito investigado[629]. Sobre a matéria a Corte Suprema de Cassazione Italiana manifestou a necessária determinação do lugar onde deve ocorrer as gravações, de modo que do contrário afrontaria o sistema jurídico constitucional, pois se incluiria a possibilidade de uma captação de qualquer lugar em que o sujeito se mova[630].

A segunda, por sua vez, trata-se do vídeo registro de comportamento não comunicativo. Esta definição impõe a diferenciação dos espaços cujo registro é efetivado. Torna-se necessário estabelecer a distinção entre a investigação por vídeo em local domiciliar, em local reservado ou em local público[631]. A importância de tais distinções é, definitivamente, as consequências relacionadas ao material coletado.

No ordenamento jurídico italiano, por exemplo, a vídeo vigilância domiciliar possui sanção que afeta o material investigativo recolhido, inutilizando-o no processo penal. Em se tratando de *fontes* de prova adquiridas por gravações de vídeos em ambiente domiciliar, "tal prova se baseia em uma atividade que a lei proíbe"[632]. A proibição decorre de mandado Constitucional que, a partir do art. 14 da Constituição Italiana, prevê a inviolabilidade do domicílio, sendo nele proibida a ocorrência de inspeções ou sequestros, salvo nos casos e

---

[626] DANIELE, Marcelo. ***Contrasto al terrorismo e captatori informatici.*** Revista di Diritto Processuale. Marzo – Aprile, 2017. p, 400.

[627] ITALIA, ***Repubblica Italiana In Nome Del Popolo Italiano La Corte Suprema Di Cassazione***. Sez. 6, Sentenza n. 27100 del 2015, MUSUMECI. Disponível em: http://questionegiustizia.it/doc/sentenza-27100-2015.pdf. Acesso em out 2018.

[628] TORRE, Marco. ***Il captatore informático*.** Op. cit. p, 111.

[629] De acordo com a Corte Constitucional Italiana, a referida interceptação possui natureza de instrumento investigativo e como tal, possui consequências dispostas nas normas dos artigos 266 e seguintes do Código que determina o rito das interceptações tradicionais. TORRE, Marco. ***Il captatore informático*.** Op. cit. p, 111.

[630] ITALIA, ***Repubblica Italiana In Nome Del Popolo Italiano La Corte Suprema Di Cassazione***. Op. cit., MUSUMECI.

[631] TORRE, Marco. ***Il captatore informático*.** Op. cit. p, 111-112.

[632] DANIELE, Marcelo. ***Contrasto al terrorismo e captatori informatici.*** Revista di Diritto Processuale. Marzo – Aprile, 2017. p, 400.

formas estabelecidas em lei. De modo a assegurar as garantias prescritas para a tutela da liberdade pessoal[633].

Quando se tratar de investigação a partir da gravação de vídeo em locais reservados, configurar-se-á prova atípica cuja utilização necessita de prévia motivação da autoridade judicial. Deste modo, quando protegido o âmbito da confidencialidade dos sujeitos, a prova atípica poderá ser utilizada[634].

Tal argumento, segundo Daniele[635], demonstra uma forma arbitrária de investigação de *fontes* de prova, pois se trata de um método igualmente invasivo que não possui critérios estabelecidos ou requisitos de elegibilidade que devem estar presentes na motivação judicial, para que esta se mostre idônea. A leitura do dispositivo 189 do Código de Processo Penal italiano revela uma impropriedade quanto à regulamentação da aquisição de provas atípicas, principalmente por não estabelecer qualquer garantia voltada à proteção mínima a direitos do acusado.

Dirá a referida normativa processual que, excepcionalmente, uma prova não regulada por lei poderá ser tomada como adequada pelo juiz competente caso sirva para assegurar o esclarecimento dos fatos e quando não afetar a liberdade moral da pessoa[636]. Para cumprir com requisitos mínimos de garantia, conforme Daniele[637], a leitura do dispositivo deve ser combinada com a Convenção Europeia dos Direitos Humanos[638]. Segundo o autor, as

---

633 Constituição da República Italiana. *Costituzione Italiana edizione in língua portoghese*. Senato della Repubblica. 2018. p, 11. Disponível em: https://www.senato.it/application/xmanager/projects/leg18/file/repository/relazioni/libreria/novita/XVII/COST_PORTOGHESE.pdf. Acesso em 04 set, 2018.

634 TORRE, Marco. ***Indagini informatiche e processo penale.*** Op. cit. p, 157.

635 DANIELE, Marcelo. ***Contrasto al terrorismo e captatori informatici.*** Revista di Diritto Processuale. Marzo – Aprile, 2017. p, 400-401. "*Le Sezioni unite hanno aggiunto che le videoriprese in luoghi meramente riservati – i quali, a differenza dei luoghi privati, non fruiscono della tutela apprestata dall'art. 14 Cost. – sarebbero dal canto loro utilizzabili solo qualora venissero disposte con un provvedimento motivato dell'autorità giudiziaria. Si tratta, però, di un assetto normativo arbitrariamente costruito dall'interprete, e comunque incompleto. Perché, in particolare, l'autorizzazione dell'autorità giudiziaria, e non di un vero e proprio giudice, come invece previsto dall'art. 266 c.p.p. in rapporto alle intercettazioni (ossia un mezzo investigativo altrettanto intrusivo per la privacy)? Quali, inoltre, i requisiti di ammissibilita` su cui dovrebbe cadere la motivazione?*"

636 Italia, Codice di Procedura Penale. Art. 189 - Prove non disciplinate dalla legge. 1. Quando è richiesta una prova non disciplinata dalla legge, il giudice può assumerla se essa risulta idonea ad assicurare l'accertamento dei fatti e non pregiudica la libertà morale della persona. Il giudice provvede all'ammissione, sentite le parti sulle modalità di assunzione della prova.

637 DANIELE, Marcelo. ***Contrasto al terrorismo e captatori informatici.*** Revista di Diritto Processuale. Marzo – Aprile, 2017. P 402.

638 Convenção Europeia de Direitos do Homem, Art. 8º Direito ao respeito pela vida privada e familiar 1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência. 2. Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem - estar económico do país, a defesa da ordem e a prevenção das infracções penais, a protecção da saúde ou da moral, ou a protecção dos direitos e das liberdades de terceiros.

garantias que parecem socorrer o método de investigação substanciado pela gravação de vídeo se encontram nos dispositivos disciplinares da interceptação telefônica[639].

O uso análogo da norma que disciplina as interceptações telefônicas à investigação pela gravação de vídeo mediante *malware* não nos parece adequado. Para além da incidência em outro(s) direito(s) fundamental(is), pelo uso de *software* malicioso, a aplicação análoga de normas não cumpre com requisitos que limitam a ocorrência de abusos estatais. Tornar-se visível em estado de privacidade e intimidade, coloca a investigação em condição potencial de *voyeurismo*, no contínuo desejo daquele que investiga em alcançar visualmente seu alvo investigado em ato ilícito.

Uma constante busca pelo *gozo*. Como esclarece Coutinho[640], deseja-se o que não se tem, [ou ainda não se tem; e o "ainda" é que motiva a busca], e por isso se persegue, "afinal, não teria sentido seguir vivendo se não fosse para tentar encontrar, amanhã, o gozo que hoje não se encontrou". Evitar o abuso pelo tempo de investigação também deve ser requisito estabelecido pela lei processual penal. Limites temporais são importantes para delimitar a atuação do Estado quando este incide na esfera de proteções constitucionais, de tal forma que o prazo estabelecido como adequado e necessário para a investigação por vídeo deve ser fixado pelo legislador processual.

Ademais, ainda que não se trate de invasões domiciliares propriamente ditas[641], devem ser objeto de tutela judicial as vídeo gravações que atentem aos comportamentos de

---

639 DANIELE, Marcelo. ***Contrasto al terrorismo e captatori informatici.*** Op. cit. p, 402. "*Come si è già detto, la Corte europea esige che le attività di captazione occulta di dati riservati nei procedimenti penali siano regolate da norme di legge conoscibili e prevedibili, nonché in grado di conseguire un bilanciamento proporzionato fra i valori in gioco, mediante la previsione di adeguate ed effettive garanzie volte ad evitare abusi di potere. Ma garanzie del genere sono rinvenibili nelle norme sulle intercettazioni di comunicazioni; le quali, considerata la somiglianza fra le intercettazioni e le videoriprese, potrebbero essere integralmente applicate anche a queste ultime, nella ragionevole convinzione che si tratti di una disciplina in linea con la volonta` del legislatore e compatibile con la Cedu*".

640 COUTINHO, Jacinto Nelson de Miranda. **Sonhocídio: estragos neoliberais no ensaio do direito ou "la busqueda del banquete perdido", como diria Enrique Marí.** Revista Crítica Jurídica – Nº 21. Jul – Dez/2002, p, 103.

641 Sobre o direito à inviolabilidade domiciliar é fundamental, tendo em vista a serventia para o estudo, a decisão proferida pelo Tribunal Supremo Espanhol em 20 de abril de 2016. No caso, investigadores sem a devida autorização judicial conseguiram ter acesso óptico a um dos cômodos do domicilio do investigado por meio de um binóculo. Na decisão, embora se utilize diversos outros argumentos para reformar a anterior sentença condenatória, trata-se da análise da validade da observação realizada pelos investigadores quanto ao interior do domicílio. Deste fato decorre a argumentação de que "o agente não vulnera nenhum direito fundamental quando percebe com seus próprios olhos aquilo que está alcançável por qualquer um. [...] Com efeito, a tutela constitucional do direito problamado no inciso 2 do artigo 18 da CE protege, tanto frente a inrrupção inconsentida do intruso no cenário doméstico, como a observação clandestina do que acontece em seu interior, se para isso é preciso se valer de um arificício técnico de gravação ou aproximação de imagens. O estado não pode adentrar sem autorização judicial no espçao de exclusão que cada cidadão impõe a terceiros. O disposto no artigo 18.2 da CE. E se vulnera essa proibição quando sem autorização judicial e para superar os obstáculos próprios da tarefa de fiscalização, se recorre a um utensílio óptico que permite ampliar as imagens e salvar a distância entre o observante e o observado".

privacidade pessoal, como por exemplo gravações obtidas em banheiros públicos. Deste modo, tratando-se não da proteção ao domicílio propriamente e isoladamente, mas essencialmente na intenção de proteger a liberdade geral da personalidade, bem como a privacidade pessoal do sujeito e de terceiros afetados.

Na Itália, o material recolhido em ambiente domiciliar deve ser inutilizado. Por sua vez no ordenamento jurídico brasileiro, entende-se como prova ilícita posto que viola direito fundamental sem a necessária reserva legal e todas as suas circunstâncias. Como já exposto, quando ocorrer a investigação por vídeo em locais públicos, na realidade jurídica italiana, se configurará como prova atípica, de modo a ser efetuado por própria iniciativa da polícia investigativa, tratando-se de ato não repetível utilizável na fase processual de debates.

De acordo com a jurisprudência italiana[642], a regulamentação da investigação a partir do acesso remoto e ativação da vídeo câmera acoplada ao dispositivo informático, com a utilização de *malware*, deve se voltar a tutelar a (in)utilização do material adquirido em detrimento da privacidade pessoal e não, somente, a legitimação da técnica investigativa[643]. Contudo, deve-se antes de rechaçar qualquer ingerência em direito fundamental, pela tão somente ausência de lei que preveja limites à atividade estatal, proceder com a indagação de ser possível ou não a restrição deste direito fundamental a partir de métodos ocultos de investigação como o aqui tratado. Ou seja, embora haja previsão legal que impõe determinado limite a intervenção estatal por meios ocultos de investigação que incidem em direitos fundamentais, necessita-se questionar primeiramente se o direito fundamental pode ser restringido por dita ingerência.

4.1.6 Investigação por acesso a geolocalização dos dispositivos informáticos

A amplitude investigativa a partir da utilização de *malware* em dispositivos informáticos alvos contempla também o alcance de informações por dados referentes à longitude e latitude, consequentemente sua coordenada espaço temporal no globo[644]. Talvez a informação despertasse ligeiro interesse quando relacionadas a dispositivos fixos em locais determinados mas não conhecidos. Contudo, revela uma grande preocupação quando tais

Tradução livre (ESPANHA, **STS 329/2016, 20 de Abril de 2016,** Número do Recurso: 1789/2015. Disponível em: https://supremo.vlex.es/vid/637465649. Acesso em nov 2018).
642 ITALIA. Op. cit. Sentenza n. 27100 del 2015, MUSUMECI.
643 TORRE, Marco. ***Il captatore informático.*** Op. cit. p, 112.
644 BENE, Teresa. ***Il pedinamento elettronico: truismi e problemi spinosi***. In: (a cura di) SCALFATI, Adolfo. *Le indagini atipiche.* G. Giappichelli Editore. Torino. 2014. p, 348.

dispositivos informáticos são dotados de tecnologia móvel. A este custo, o acesso à localização do dispositivo reflete também no alcance constante da localização de seu usuário.

Em um cenário que novas tecnologias de informação e comunicação são utilizadas massiva e constantemente por invíduos, a ingerência sub-reptícia empregada pelo Estado sob estes dispositivos serve à "tecnovigilância". Como ressalta Velasco Nuñez[645] é a técnica e não a pessoa propriamente que se aproveita da informação captada pelo máquina, contudo a técnica serve ao investigador e sua aplicação não pontual, mas prolongada no tempo, afeta a direitos fundamentais do suspeito, dando lugar a vigilâncias tecnológicas.

A tecnologia usada na investigação, segundo o autor[646], por mais que possua inibidores do delito acaba produzindo uma espécie de paranôia em parte da população que deve ser racionalizada pela norma. De tal sorte que a norma deve proteger o cidadão ao definir o direito de não estar localizado de maneira contínua, exigindo sobretudo que os cidadãos não sejam submetidos a ingerências constantes em sua vida privada.

O sistema de geolocalização e sua utilização na investigação criminal não se equipara à mera observação por inspeção, ou o "seguir alguém" como diligência policial na modalidade eletrônica, ao contrário, não possui outra utilidade que não a localização e o monitoramento constante do sujeito visado[647]. Enquanto que na inspeção se busca uma constatação atual ou pré-existente do lugar[648], bem como no seguir alguém se esbarra em limitações físicas que acabam por preservar parcela da privacidade do sujeito visado.

O *GPS* (*Global Positioning System*) é uma aplicação incorporada a diversos dispositivos de comunicação e consiste no identificação do posicionamento espaço temporal sob qualquer condições meteorológicas[649]. O monitoramento, portanto, decorre da comunicação via satélite, de modo que é possível determinar a localização do referencial ainda que esteja em movimento.

Quando se tratar de dispositivos informáticos móveis como *smartphones* o monitoramento da localização ocorre de maneira distinta. Conforme Torre a localização de celulares utiliza o sistema de "células" que corresponde a uma distribuição territorial de corbetura do sinal de telefonia móvel. "A potência do sinal de rádio de cada célula telefônica é

---

[645] VELASCO NUÑEZ, Eloy. *Limites a las investigaciones y a la prueba en el proceso penal.* In: ***Delitos tecnológicos: definición, investigación, y prueba en el proceso penal.*** Op. cit. p, 21.
[646] VELASCO NUÑEZ, Eloy. *Limites a las investigaciones y a la prueba en el proceso penal.* In: ***Delitos tecnológicos: definición, investigación, y prueba en el proceso penal.*** Op. cit. p, 21.
[647] BENE, Teresa. ***Il pedinamento elettronico: truismi e problemi spinosi***. Op. cit. p, 349.
[648] SERRANI, Alessandro. ***Sorveglianza satellitare GPS: un'attività investigativa ancora in cerca di garanzie.*** Archivio Penale 2013, n. 3 p, 6.
[649] VELASCO NUÑEZ, Eloy. *Limites a las investigaciones y a la prueba en el proceso penal.* In: ***Delitos tecnológicos: definición, investigación, y prueba en el proceso penal.*** Op. cit. p, 25.

analisada em relação à respectiva Estação Rádio Base conectada ao dispositivo móvel ou terminal e sua distância é determinada com base no conhecimento de atenuação do ambiente de radiopropagação". De tal sorte que a investigação pautada no alcance da localização deste dispositivo não necessita de suporte, basta uma conexão móvel ao celular ou *smartphone*[650].

A modalidade de investigação por geolocalização não corresponde a qualquer forma de interceptação[651]. Primeiro, pelo fato de que monitorar as coordenadas espaço-temporais do sujeito não corresponde a interceptação de fluxo de dados entre pessoas. De um lado se tem como objeto de aquisição o conteúdo de uma comunicação entre duas ou mais pessoas, de outro a posição e o movimento de uma pessoa ou coisa[652].

Ademais, o prejuízo da restrição à privacidade pela interceptação, bem como o direito ao segredo de comunicações, não é comparável à tecnovigilância desempenhada pelo *malware* na apropriação de dados de geolocalização. Não é preciso de muito esforço para compreender que os dados de localização constante do sujeito fazem parte do complexo de dados que correspondem à sua personalidade e de tal forma, somente por tal motivo, não é comparável a interceptação de um fluxo de dados em um determinado contexto específico, com alcance do histórico de dados de localização do indivíduo e ou a sua localização constante em tempo real.

A apropriação dos dados informativos de localização do dispositivo informático pode influenciar não apenas na investigação preliminar, mas também em toda a construção do lastro probatório que servirá à instrução processual. Se quanto a investigação preliminar já surgem questionamentos quanto à possibilidade do Estado se utilizar de tecnologias para monitorar o sujeito passivo, quanto ao processo penal, no que tange à atividade probatória, também surgirão.

Se os dados informáticos que se referem à localização do dispositivo utilizado podem ser armazenados constantemente em bases de dados administradas por servidores, de tal forma que se torne possível o levantamento histórico dos percursos transcorridos pelo dispositivo, estes mesmos dados podem servir de lastro probatório para instruir um processo penal? Quais os limites de incidência da investigação tecnológica ou informática no direito a não ser localizado constantemente, ou ainda à liberdade? A complexidade das perguntas reflete à forma complexa de se responde-las.

---

650 TORRE, Marco. ***Indagini digitali e processo penale.*** Op. cit. p, 159.
651 BENE, Teresa. ***Il pedinamento elettronico: truismi e problemi spinosi***. Op. cit. p, 350.
652 Também neste sentido TORRE, Marco. ***Indagini digitali e processo penale.*** Op. cit. p, 161.

O primeiro passo é retomar a ideia de que o processo penal e a investigação preliminar serve ao controle do poder punitivo, de modo que para a incidência do Estado sobre direitos fundamentais do indivíduo há que se estabelecer limites. Para Torre[653], "a disciplina constitucional assume uma tripla importância, ao mesmo tempo atua como limite hermenêutico, como parâmetro de legitimidade e, ainda que de maneira mais controversa, como fonte de regras excludentes".

Não por acaso que a Constituição Espanhola estabelece que a lei limitará o uso da informática para garantir a honra e a intimidade pessoal e familiar dos cidadãos e o exercícios de seus direitos[654]. Uma norma constitucional que tutela a incidência da técnica informática em direitos fundamentais é bastante significativa por representar uma postura constitucional frente aos avanços tecnológicos. Trata-se de uma restrição autorizada pelo constituinte – quanto ao uso da informática sob seus diversos aspectos – para que o legislador infraconstitucional a restrinja diante de demais direitos fundamentais conflitantes[655]. De tal sorte que a restrição abarca efetivamente a utilização da informática nas investigações tecnológicas.

A Constituição Federal Brasileira de 1988 não dispõe expressamente a autorização de restrições infraconstitucionais ao uso da informática. Ainda assim, a norma constitucional – por dispor sobre proteções a liberdades e direitos fundamentais – opera substancialmente na (re)leitura de todo o ordenamento jurídico, de modo que novas tecnologias informáticas – de investigação – são passíveis de sofrer restrições diante da colisão com outros direitos fundamentais.

Ainda sem expressa restrição autorizada é papel do legislador infraconstitucional conciliar a utilização de novas tecnologias possivelmente utilizadas em investigações criminais com direitos fundamentais afetados do sujeito passivo. Não se trata de presunção da vontade constitucional, mas da obrigatoriedade de uma aplicação processual consoante ao equilíbrio do ordenamento jurídico guiado pela Carta Maior. Neste sentido, concorda-se com Bene[656], a investigação afeta a proteção da liberdade pessoal, e isto implica dizer que a legitimidade deste

---

653 TORRE, Marco. ***Indagini digitali e processo penale.*** Op. cit. p, 163.

654 ESPANHA, ***Constitución Española***, artículo 18.4 - *La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.* Disponível em: https://www.boe.es/buscar/doc.php?id=BOE-A-1978-31229. Acesso em nov 2018.

655 SARLET, Ingo. **A eficácia dos direitos fundamentais: uma teoria geral dos direitos fundamentais na perspectiva constitucional.** 12 ed. rev. atual e ampl. Porto Alegre: Livraria do Advogado Editora, 2015, p. 409.

656 BENE, Teresa. ***Il pedinamento elettronico: truismi e problemi spinosi***. Op. cit. p, 348. "*Se il pedinamento è in grado di comprimere la libertà di circolazione di cui all'art. 16 Cost, intesa anche come diritto a 'non essere localizzati'. Se può ipotizzarsi che l'attività di indagine incide sulla libertà personale tutelata dall'art. 13 Cost., poiché, intesa anche come libertà morale, comporterebbe che eventuali limitazioni cella stessa possono avvenire solo "per atto motivato dell'autorità giudiziaria e nei soli casi e modi previsti dalla legge".*

ato se relaciona diretamente com o cumprimento da forma prevista em lei e embasado pelos limites impostos na motivação da autorização judicial.

Conforme Velasco Nuñez a preocupação do sistema jurídico quanto à incidência da geolocalização na privacidade do sujeito se volta a dois critérios básicos, a intensidade e a duração. Ou seja, para que se evite a usurpação de direitos do investigado a partir de abusos que extrapolam os limites autorizados à empreitada investigativa, "a lei deve habilitar e definir em abstrato os supostos em que cabe o sacrifício do direito face a benefícios sociais maiores de uma concreta investigação delitiva, e deve também regular as garantias que permitam ao investigado exercer uma efetiva defesa" [657-658].

4.2 Direitos do indivíduo-alvo diretamente afetados pela utilização de *Malware* na investigação criminal tecnológica

4.2.1 Direito à proteção da intimidade

Uma adequada definição do conceito daquilo que seria a intimidade em relação ao tema aqui trabalhado é: a necessidade de encontrar na solidão a paz e equilíbrio continuamente comprometidos pelo ritmo da vida moderna. A capacidade da pessoa, querendo, se manter isolada ou resguardada da curiosidade dos olhares e dos ouvidos ávidos[659].

Costa Jr. define a intimidade distinguindo-a por meio de seu aspecto interno e externo. O primeiro sendo a possibilidade de abstrair-se da multidão, afastando-se

---

[657] VELASCO NUÑEZ, Eloy. *Limites a las investigaciones y a la prueba en el proceso penal.* In: ***Delitos tecnológicos: definición, investigación, y prueba en el proceso penal.*** Op. cit. p, 23-24. "*Al derecho deben preocupar más variables como la intensidad de la injerencia y su duración: los ciudadanos, potenciales afectados, necessitamos que se sepa previamente em qué casos y como se nos injiere, lo que la ley reserva a la proporcionalidad y las garantias que deben reducir los errores para que el ejercicio del derecho sea la regla y su inmisión la excepción, y para evitar todo atisbo de arbitrariedad en el receptor inicial de la información con la disculpa de que se está combatendo el delito. Esto es, que controlemos también a quien nos controla*".

[658] No mesmo sentido Marco Torre (TORRE, Marco. ***Indagini digitali e processo penale.*** Op. cit. p, 166.) "*la soluzione migliore sarebbe, de iure condendo, l'introduzione di una disciplina specifica idonea a realizzare un equo bilanciamento tra esigenze dell'accertamento penale e diritti individuali coinvolti in tale accertamento. Infatti, alla luce di un progresso tecnologico foriero di mezzi di indagine sempre più penetranti e invasivi, la supplenza giurisdizionale può diventare rischiosa. Ed allora, anche con riferimento al rilevamento mediante g.p.s. sarebbe opportuno un intervento legislativo che si occupasse di specificare le tipologie di reato per le quali consentire il monitoraggio, le modalità preparatorie ed esecutive, la riserva di giurisdizione, la forma della documentazione delle operazioni, le sanzioni processuali in ipotesi di violazione dei presupposti legittimanti l'uso dello strumento investigativo"*.

[659] COSTA JR., Paulo José da. **O direito de estar só: tutela penal da intimidade.** Editora Revista dos Tribunais Ltda. 1970, p, 8.

materialmente. Já o segundo, trata-se de natureza psíquica, "o homem a estabelece no burburinho da multidão"[660].

A impossibilidade do sujeito de permanecer reservado em seu íntimo é a contraprestação da comodidade e praticidade proporcionadas pelas novas tecnologias. Ambos os aspectos, interno e externo, da intimidade sofrem um processo constante de corrosão devido à massiva utilização das tecnologias de comunicação e informação. Desta forma o direito à intimidade por vezes sofre incidência e restrições que ultrapassam determinados limites alcançando seu núcleo intocável[661].

A determinação do fundamento intocável que compõe o direito à intimidade decorre da "teoria das esferas", cuja visualização de três círculos concêntricos com diâmetros progressivamente menores permite entender os níveis de restrições possíveis de ocorrerem na esfera privada do sujeito. O círculo externo representa a esfera social em que há maiores possibilidades de intervenções. Inserem-se neste âmbito, processos, situações e condutas de natureza pública[662]. O círculo intermediário corresponde à intimidade, esfera da confiança ou sigilo, ou seja, neste círculo se inserem conversas ou acontecimentos íntimos que se excluem do público em geral[663].

A seu turno, no terceiro círculo, que representa o âmago da esfera privada, ou seu núcleo intocável, não há possibilidade de se justificar uma intervenção. Conforme Greco, trata-se de uma expressão da ideia de dignidade humana, e para Costa Jr. compreende uma parcela da vida privada conservada em segredo pelo indivíduo[664]. Sob este prisma, o Tribunal Constitucional Alemão entendeu que restou afetado este núcleo intocável da privacidade ao decidir sobre um caso em que se gravou um solilóquio travado por uma pessoa que se encontrava sozinha em seu automóvel[665]. É difícil estabelecer com exatidão o conteúdo concreto deste núcleo intocável, mas nos parece evidente que abarca situações

---

[660] COSTA JR., Paulo José da. **O direito de estar só: tutela penal da intimidade.** Editora Revista dos Tribunais Ltda. 1970, p, 8.
[661] GRECO, Luis. **Introdução – o inviolável e o intocável no direito processual penal.** Op. cit. p, 34.
[662] COSTA JR., Paulo José da. **O direito de estar só: tutela penal da intimidade.** Editora Revista dos Tribunais Ltda. 1970, p, 31. Neste sentido Luis Greco (**Introdução – o inviolável e o intocável no direito processual penal.** Op. cit. p, 34.) exemplifica as incidências como "falar ou perguntar sobre a profissão de alguém".
[663] Id. Ibidem. Também GRECO, Luis. **Introdução – o inviolável e o intocável no direito processual penal.** Op. cit. p, 34. "Aqui, trata-se de informações, por ex., sobre as compras de uma pessoa, o local em que ela passa férias, o seu círculo de amigos".
[664] COSTA JR., Paulo José da. **O direito de estar só: tutela penal da intimidade.** Op. cit. p, 32 – 33. GRECO, Luis. **Introdução – o inviolável e o intocável no direito processual penal.** Op. cit. p, 34
[665] GRECO, Luis. **Introdução – o inviolável e o intocável no direito processual penal.** Op. cit. p, 34. " BGHSt 57, 71 (74 e ss.)"

comportamentais, sentimentais ou intelectuais diversas em que o sujeito, em seu íntimo, acredita não estar alcançável por terceiros.

Embora o direito à intimidade seja material e autônomo, é estritamente vinculado ao respeito a vida privada e familiar, ao direito a honra e à própria imagem[666]. Configura-se bem jurídico elevado à categoria de direito fundamental, vinculado essencialmente ao direito geral do livre desenvolvimento da personalidade[667].

A ressalva feita por Costa Jr.[668] é que o indivíduo busca satisfazer tanto o interesse da livre existência como o de livre desenvolvimento na vida de relação social, deste modo "enquanto os direitos que se destinam à proteção da 'esfera individual' servem para preservação da personalidade dentro da vida pública, na proteção da 'esfera privada' cogita-se da inviolabilidade da personalidade dentro de seu retiro, necessário ao seu desenvolvimento e evolução, em seu mundo particular, margem da vida exterior". A esfera individual, portanto, se contrapõe à esfera privada na qual se insere a intimidade ou a reserva do cidadão[669].

É possível verificar que na esfera privada se distinguem o direito de impedir que a atividade de terceiros se enderece a conhecer, descobrir as particularidades da vida privada alheia[670] e, por sua vez, o direito de defender a pessoa diante da divulgação de notícias particulares, mas legitimamente conhecidas pelo divulgador[671], ou seja, de um lado se tutela a vida privada diante da invasão ilegítima e de outro, se tutela a divulgação de informações privadas[672].

Sob este primeiro aspecto, ou seja, da interferência ou ingerência física ou à distância pelo uso de tecnologias – diante da possibilidade de se levar a cabo uma investigação criminal por meio de novas tecnologias que possibilitam uma ingerência mais ampla por parte do Estado face ao sujeito passivo – há que se levar em consideração a potencial lesividade da investigação informática que conta com mecanismos de captação visual, oral e de dados mediante dispositivos eletrônico-digitais perante o direito à proteção da intimidade. Desta

---

666 BRASIL, Constituição Federal. Artigo 5º, X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação.
667 QUEVEDO GONZALEZ, Josefina. ***Derechos y libertades que resulta afectados.*** In: *Investigación y prueba em el proceso penal.* Madrid: Editorial Jurídica Sepín, 2017. p, 109.
668 COSTA JR., Paulo José da. **O direito de estar só: tutela penal da intimidade.** Editora Revista dos Tribunais Ltda. 1970, p, 24.
669 Se contrapõe pois os interesses tutelados são diferentes. Costa Jr. afirma que na esfera individual é a reputação como atributo de respeitabilidade que se insere na vida de relação. A seu turno, na esfera da intimidade, trata-se ao aspecto da individualidade, ou seja a intencionalidade do indivíduo em se conservar diante de intromissões indesejadas.
670 *Diritto alla segretezza.*ou *Diritto al rispetto della vita privata*.
671 *Diritto alla riservatezza* ou *Diritto alla riservatezza della vita privata.*
672 COSTA JR., Paulo José da. **O direito de estar só: tutela penal da intimidade.** Editora Revista dos Tribunais Ltda. 1970, p, 29.

forma, salienta Quevedo Gonzalez[673] que a aplicação das garantias processuais que legitimam tal intervenção estatal é obrigatória, tendo em vista a possível produção ilícita da prova penal.

Deste modo, a premissa trazida à baila é que se torna possível uma restrição do direito à intimidade, desde que legítima, diante de justificativas condicionadas aos preceitos da investigação criminal constitucionalmente orientada. Ou seja, desde que haja autorização legalmente constituída para a incidência do Estado na esfera privada da intimidade do sujeito. A legitimidade da atuação estatal se pauta na legalidade e nos pressupostos de respeito à dignidade humana, que no tocante à intimidade, impõe o respeito ao seu núcleo *intocável*.

Restrições ao direito à intimidade podem decorrer do consentimento do sujeito passivo. Deste modo, a ilicitude ocorrerá se a intervenção à intimidade se deslegitimar pelo abuso. Por mais que se diga que alguém que tenha o direito de permanecer recolhido em sua esfera privada, pode tanto sair do seu isolamento, quanto permitir que terceiros tenham acesso à sua soledade[674], a licitude advinda do acesso consentido deverá ser restrita a um fim determinado[675]. De tal forma, o consentimento autorizativo se vincula a um sujeito determinado (público ou privado) e às limitações exatas inerentes ao fim expressamente especificado[676].

Este duplo aspecto vinculativo do consentimento, portanto, se mostra como um mecanismo processual de proteção, ou seja, uma regra de vinculação das informações a determinada finalidade, como exemplo, o apagamento de dados, o levantamento de dados, ou o uso de dados do sujeito passivo. Destaca Wolter, que tais mecanismos de proteção permitem a condução da prevenção de perigos a direitos fundamentais, diante do possível esvaziamento de seu conteúdo[677].

Ademais, não há que se falar em consentimento do sujeito a ingerências em sua intimidade diante uma investigação criminal, tal atuação estatal deve se pautar nos limites

---

673 QUEVEDO GONZALEZ, Josefina. ***Derechos y libertades que resulta afectados.*** In: *Investigación y prueba em el proceso penal.* Madrid: Editorial Jurídica Sepín, 2017. p, 110.

674 COSTA JR., Paulo José da. **O direito de estar só: tutela penal da intimidade.** Editora Revista dos Tribunais Ltda. 1970, p, 45.

675RODOTÁ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje.** Rio de Janeiro: Renovar, 2008. p, 74. Rodotá tenta estabelecer "rumo a um renascimento do consentimento" cujo desfecho não será abordado aqui, posto que adiante será explorado o direito à proteção de dados e à autodeterminação informativa, que em linhas breves se perfaz em mecanismos de proteção à privacidade. O autor aponta para o surgimento de uma outra definição de privacidade que consubstancia-se no "direito do indivíduo de escolher aquilo que está disposto a revelar aos outros", ou seja, o direito que a pessoa possue de determinar a circulação de informações a seu respeito.

676 Um exemplo para ilustrar o que se discorre é justamente a hipótese de um sujeito consentir à determinada empresa gerenciadora de aplicativos informáticos o acesso a câmera, ao microfone, aos álbuns de fotografias, aos demais arquivos e ficheiros do dispositivo informático, para em contrapartida ter comodidades quanto à compartilhamentos de informações pessoais, localizações geográficas, e etc. O consentimento dado pelo titular da intimidade não poderá ser desvirtuado de sua finalidade, muito menos alcançar terceiros não contemplados, dentre estes o Estado ou seus órgãos de controle penal.

677 WOLTER, Jürgen. **O inviolável e o intocável no direito processual penal.** Op. cit. p, 86-87.

estabelecidos legalmente. A intervenção estatal incidente no direito à intimidade deve portanto obediência a requisitos objetivos legalmente estabelecidos e verificados na decisão penal que a autorize. Pelas lições de Quevedo Gonzalez[678] e Velasco Nuñez[679] se pode extrair ao menos alguns "determinantes de validade" obrigatoriamente exigidos diante da autorização judicial. São eles o princípio da especialidade, idoneidade e excepcionalidade[680].

Por especialidade da medida se entende a relação imediata entre o método investigativo adotado e um fato delitivo concreto, ou seja, a vedação de medidas de investigação que tenham por objeto prevenir ou descobrir delitos, ou ainda, esclarecer suspeitas sem uma base objetiva. Neste aspecto, dirá Quevedo Gonzalez[681] e Velasco Nuñez[682], que não poderá ser dirigida uma medida tecnológica que busque exclusivamente obter meros indícios ou suspeitas de criminalidade. Proibidas, portanto, estão as medidas de natureza prospectiva. Para a autora, a idoneidade da medida investigativa versa sobre o âmbito objetivo e subjetivo e a duração da medida em virtude de sua utilidade. Por conseguinte, "deve existir uma relação de adequação entre o meio de investigação e o fim perseguido"[683], uma combinação constitucional do interesse investigativo e a legitimidade do instrumento probatório, e consequente utilidade de seu resultado[684].

---

[678] QUEVEDO GONZALEZ, Josefina. ***Derechos y libertades que resulta afectados.*** In: *Investigación y prueba em el proceso penal.* Madrid: Editorial Jurídica Sepín, 2017. p, 111.

[679] VELASCO NUÑEZ, Eloy. **Investigación tecnológica: medidas concretas**. In: **Delitos tecnológicos: definición, investigación y prueba en el proceso penal.** Op. cit. p. 70

[680] Discorrem a autora e o autor, a partir da interpretação do Supremo Tribunal Constitucional Espanhol acerca do Artigo 588 *bis* a.) *LECrim*, também sobre o princípio da proporcionalidade, admitindo que este se relaciona com a medida empregada quando, levada em consideração todas as circunstâncias do caso, e o sacrifício dos direitos e interesses afetados não sejam superiores ao benefício trazidos pela adoção da medida diante do interesse público e de terceiros. Ainda, discorre que para a ponderação dos interesses em conflito, a valoração do interesse público se baseará na gravidade do fato, sua transcendência social ou o âmbito tecnológico de produção, a intensidade dos indícios existentes e a relevância do resultado perseguido com a restrição do direito. No mesmo sentido, Velasco Núñez, (Investigación tecnológica: medidas concretas. In: **Delitos tecnológicos: definición, investigación y prueba en el proceso penal.** Op. cit. p. 70) afirma se tratar de evitar impor excessos absurdos ou arbitrários para a resolução de delitos, ou seja, a violação de direitos fundamentais não tolerável em uma democracia. Sobre o princípio da proporcionalidade, Jürgen Wolter – a partir da situação jurisprudencial alemã – afirma que a sua má aplicação e entendimento proporcionou a experiência retrograda para a dignidade humana e a liberdade no processo penal, de modo que este se converteu "em um instrumento para arrostar os perigos para a administração da justiça penal". Assevera que "com a ajuda do princípio da proporcionalidade, a dignidade humana e a liberdade são, ao fim e ao cabo, anuladas". WOLTER, Jürgen. **O inviolável e o intocável no direito processual.** Op. cit. p, 84.

[681] QUEVEDO GONZALEZ, Josefina. ***Derechos y libertades que resulta afectados.*** In: *Investigación y prueba em el proceso penal.* Madrid: Editorial Jurídica Sepín, 2017. p, 112.

[682] VELASCO NUÑEZ, Eloy. Investigación tecnológica: medidas concretas. In: **Delitos tecnológicos: definición, investigación y prueba en el proceso penal.** Op. cit. p. 70

[683] QUEVEDO GONZALEZ, Josefina. ***Derechos y libertades que resulta afectados.*** Op. cit. p, 112. "*Debe existir una relación de adecuación entre el médio de investigación y el fin perseguido. De esta forma, aquel debe servir objetivamente para la finalidad constitucionalmente legitima: conseguir datos útiles para investigar las circunstacias del delito*".

[684] TORRE, Marco. ***Il captatore informatico*****.** Op. cit. p, 80.

A aplicação do princípio da excepcionalidade do método investigativo, a seu turno, decorre da indisposição de outras medidas menos gravosas face ao direito à intimidade do investigado e igualmente úteis para o esclarecimento do fato investigado. A excepcionalidade da medida, deste modo, é demarcada pela cláusula de subsidiariedade[685]. Dirá Velasco Nuñez que a excepcionalidade retrata a impossibilidade de se alcançar as informações pretendidas com medidas menos gravosas ao direito fundamental, ou ainda, quando seja "gravemente" dificultoso a comprovação do ilícito por outros meios[686].

Neste ponto, porém, há que se levar em consideração o risco de banalização de tais métodos pela busca incessante da eficiência no processo penal. Sendo assim, necessária é a imposição de um critério mais adequado ao processo penal constitucional, tendo em vista que a excepcionalidade como conceito abstrato pode ser satisfeita a partir de subjetivismos, evidenciando assim um conjunto de procedimentos e discursos pautados pela exceção[687].

De tal sorte, é possível se pensar em um critério de imprescindibilidade. O método de investigação tecnológica deve ser utilizado quando, diante dos demais métodos, se mostrar imprescindível para a apuração dos fatos ou a busca de *fontes* de prova, que no tocante ao digital, tratam-se de dados. Logo, a imprescindibilidade do método marca sua singularidade diante dos demais métodos utilizáveis, tendo em vista que estes últimos são carentes de efetividade, seja pela impossibilidade de alcançar o fim pretendido, seja pela lesão inapropriada a um direito fundamental. Ou seja, pelo alto grau de lesividade da investigação tecnológica, o método de investigação adotado deve ser o único capaz de satisfazer os interesses investigativos.

Os critérios vinculantes capazes de estabelecerem limites concretos face à restrição do direito à intimidade por parte de novas tecnologias de investigação ainda não estão postos na lei processual penal. Contudo, é impossível não se perceber que há – pela pretensa incidência ao núcleo essencial íntimo do sujeito passivo por novas tecnologias de investigação – uma

---

685 QUEVEDO GONZALEZ, Josefina. ***Derechos y libertades que resulta afectados.*** Op. cit. p, 113.

686 VELASCO NUÑEZ, Eloy. Investigación tecnológica: medidas concretas. In: **Delitos tecnológicos: definición, investigación y prueba en el proceso penal.** Op. cit. p. 69.

687 A exceção é uma constante inserida nos quadros da própria legalidade. Um "Estado de exceção" semelhante àquele exposto por Agamben, no qual "tende cada vez mais a se apresentar como o paradigma de governo dominante na política contemporânea e que nessa perspectiva, se apresenta como um patamar de indeterminação entre a democracia e absolutismo". Esclarece o autor que o Estado de exceção está intimamente ligado ao fator necessidade, e que aparentemente o caráter de ser "necessário" parece atribuir à "necessidade" uma capacidade de tornar lícito algo ilícito, ou ainda, mais que tornar lícito, a necessidade atua como justificativa para uma transgressão, por meio da exceção à regra. Não há, no critério da necessidade, um interesse objetivo e claro, mas sim "um juízo subjetivo", no qual será necessário ou excepcional, tudo aquilo que se quiser declarar como tal, relativo ao objetivo que se quer atingir. Suspende-se a norma para que se possa abrir espaço para a exceção. AGAMBEN, Giorgio. **Estado de exceção**. São Paulo: Boitempo, 2004, p. 13.

inversão do objeto do processo penal, e isto deve ser rechaçado. Ora, se em um processo penal oriundo do liberalismo está proibido que o sujeito passivo se torne objeto do processo e sofra, com isso, as perseguições mais perversas, por evidente que da mesma forma se proíbe a incidência do Estado no *intocável* âmbito da vida privada[688].

O núcleo intocável da vida privada, como dito, não admite qualquer justificativa para incidência, trata-se da essência digna da humanidade em termos de intimidade e privacidade. Portanto, quando se discorre acerca da possível ingerência estatal na intimidade dos indivíduos, refere-se à "esfera intermediária" da vida privada. Esta, deve ser protegida por lei, pois se trata de bem tutelado pela Constituição Federal e pela Convenção Americana de Direitos Humanos[689], de modo que a ingerência deve se sustentar em um fundamento legal.

Uma dupla proteção, portanto. De um lado, exige-se uma predeterminação legislativa dos casos e dos modos de incidência, bem como as hipóteses da inadmissibilidade do método investigativo, consequentemente a inutilidade do material probatório adquirido[690]. Neste ponto, não se trata da lei processual penal atentar as peculiaridades do método, mesmo porque o progresso tecnológico constante tornaria obsoleta a lei processual. Contudo, há que se pensar em uma legislação que regule a atuação estatal mediante determinado método de investigação. Ora, regulamentar a utilização de *malware* na investigação criminal não é o mesmo que discorrer sobre peculiaridades técnicas de recolha das *fontes* de provas digitais obtidas pelo método, trata-se de estabelecer diretrizes. A tecnicidade procedimental será objeto de discussão das partes processuais e não pelo legislador ordinário, como se observará adiante.

---

[688] WOLTER, Jürgen. **O inviolável e o intocável no direito processual.** Op. cit. p, 84.

[689] No tocante à Convenção Americana de Direitos Humanos, o próprio ordenamento internacional afirma que é a lei que protege o sujeito de ingerências abusivas e arbitrárias, de modo que ao interpretar tal dispositivo se verifica que a lei deve impor os limites que o legislador entenda serem legítimos e constitucionalmente recepcionados. CADH, Artigo 11 – Proteção da honra e da dignidade: 1. Toda pessoa tem direito ao respeito da sua honra e ao reconhecimento de sua dignidade. 2. Ninguém pode ser objeto de ingerências arbitrárias ou abusivas em sua vida privada, em sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais à sua honra ou reputação. **3. Toda pessoa tem direito à proteção da lei contra tais ingerências ou tais ofensas.** (grifo nosso).

[690] TORRE, Marco. ***Il captatore informatico.*** Op. cit. p, 83. "*la conseguneza è ovvia: le perquisizioni online incidono sul bene giuridico della riservatezza della vita privata, la cui lesione, all luce del nuovo combinato constituzionale-sovranazionale, esige le predeterminazione da parte del legislatore ordinario dei casi e dei modi di agressione di quel bene. Con conseguente inammissibilità dello strumento e, comunque, inutilizzabilità degli elementi acquisiti*". Ressalta o autor que pela impossibilidade de previsão legislativa precisa diante do progresso tecnológico, o Tribunal Europeu optou pela flexibilização a expulsão automática dos dados ilegitimamente obtidos como material probatório. A utilização destes dados depende de três condições: que a prova seja legitima diante do direito interno (mesmo que tenha sido considerada ilegítima em relação à CEDH); que os dados ofensivos não representem o único elemento disponível para o juiz; que não seja considerado decisivo para fins de condenação no presente caso.

De outro lado, a proteção se fará mediante motivação judicial constitucionalmente adequada[691]. Neste aspecto ensina Quevedo Gonzalez que a resolução judicial deverá conter obrigatoriamente: a) o fato punível objeto da investigação e sua qualificação jurídica, com expressão dos indícios razoáveis nos quais se funde a medida; b) a identidade dos investigados e de qualquer outro afetado pela medida; c) a extensão da medida, especificando-se o alcance assim como a motivação relativa ao cumprimento dos princípios acima ditados (especialidade, idoneidade, excepcionalidade); d) a unidade da polícia investigativa que executará a medida; e) a duração da medida; f) a forma e a periodicidade com a qual o juiz será informado sobre os resultados alcançados; g) a finalidade perseguida com a medida; h) o sujeito que executará a medida, com expressa menção de seu dever de colaborar e guardar segredo[692].

4.2.2 Do Direito a autodeterminação informativa ao Direito à proteção de dados.

O conceito de autodeterminação, segundo Hassemer[693], aparenta ser de um tempo passado não relacionado com a globalização, a liberdade de mercado, mercancias e serviços, ou com a multiculturalidade. Trata-se de algo relacionado ao século XVIII, referido à pessoa, dirigido à sua interioridade com seu próprio sentido. O pré-moderno, conforme o autor, é marcado como uma pura ausência de autodeterminação, um submetimento imperial.

Contudo, esta reflexão de Hassemer que possui a antropologia cristã como ponto de partida, o leva a discorrer que o ser humano, como pessoa diante de Deus, é pensado e aceito em sua particularidade, ou seja, aceito pela em sua diferença perante os demais. De tal modo, que a diferença se vincula à consciência do ser humano e neste ponto, não se poderia entender a consciência sem algum tipo de concepção da autodeterminação[694].

A autodeterminação como característica do ser humano consciente é autovinculativa na medida em que o possibilita intervir nas coisas de modo consequente. Da mesma forma, Hassemer explica que a liberdade cristã que influenciou diretamente a inclusão do ser humano individual no Direito, também no que se refere à reforma da atividade probatória, destacou a impossibilidade de se encontrar aquilo que não se procura. Explica-se: "nunca se

[691] BRASIL, Constituição Federal. Artigo 93, IX - todos os julgamentos dos órgãos do Poder Judiciário serão públicos, e fundamentadas todas as decisões, sob pena de nulidade, podendo a lei, se o interesse público o exigir, limitar a presença, em determinados atos, às próprias partes e a seus advogados, ou somente a estes.
[692] QUEVEDO GONZALEZ, Josefina. ***Derechos y libertades que resulta afectados.*** Op. cit. p, 114. Tais requisitos destacados pela autora constam no artigo 588 *bis* c) da LECrim espanhola.
[693] HASSEMER, Winfried. ***Es la autodeterminación todavia actua?*** Revista Internacional de Pensamiento Político, II Época. Vol 3, 2007.
[694] HASSEMER, Winfried. ***Es la autodeterminación todavia actua?*** Op. cit. p, 242.

pode saber por antecipado, o que a procura exigirá todo dia", é dizer, nas palavras do autor, "primeiro se deve procurar o que depois deve ser encontrado". E quanto a liberdade do sujeito, neste aspecto, também se percebe algo vinculado à autodeterminação[695].

Com a modernidade, a autodeterminação surge como o "cantar dos cantares". Uma nova época marcada pelo contrato social posiciona o ser humano como aquele que determina o que vai acontecer a partir das legislações[696]. Os afetados pelo sistema normativo se põem em livre autodeterminação sobre este sistema, ou seja, entregam uma parte de sua liberdade para a manutenção da existência de todos em uma liberdade cidadã segura, proporcionada por uma autoridade superior que vigie os limites de tal liberdade. O que não significa dizer que os seres humanos se colocam submissos à autoridade, justo o contrário, é esta autoridade superior que tem que servir e medir seu poder para prestar serviços aos seres humanos.

Na "realidade real" descrita por Hassemer, a autodeterminação não funciona desde um princípio[697]. Em se tratando de globalização e a velocidade nela constante o conceito de autodeterminação corre sérios riscos. Deste modo, a autodeterminação possui limites em si mesma, um bem obrigatoriamente compartilhado e necessariamente limitado[698]. O Direito a seu turno não poderá suprimir a autolimitação da autodeterminação, somente poderá criar e dispor as condições sob as quais é possível uma concordância entre a autodeterminação e o caso em concreto.

Quando se tratar do direito a autodeterminação informativa, portanto, versar-se-á sobre o direito que assiste às pessoas de saberem quem e de que forma se tem acesso aos seus dados pessoais, com quais objetivos e sob quais circunstâncias. Garantindo-se assim a transparência no processamento de dados[699], de modo a se permitir desenvolver medidas de proteção que possibilitem o sujeito a intentar na adequação e exatidão das bases de dados, bem como efetuar seu cancelamento quando os dados deixarem de ser necessários[700].

---

695 HASSEMER, Winfried. ***Es la autodeterminación todavia actua?*** Op. cit. p, 243.

696 HASSEMER, Winfried. ***Es la autodeterminación todavia actua?*** Op. cit. p, 244. "*Ya com ello se abría la puerta a una legislación y a uma creación del derecho, de la que eran responsables los seres humanos, porque sólo ellos eran responsables, porque no había nadie más que pudiera ser hecho responsable. De lo vertical habia surgido la horizontalidad, de la deducción la constitución; los seres humanos quedaban sólos ante la cuestión de qué es lo que había que hacer*".

697 HASSEMER, Winfried. ***Es la autodeterminación todavia actua?*** Op. cit. p, 247. "*Pero en el hervidero de las sociedades entrelazadas y de los estados abiertos la autodeterminación lleva a al caos, al derrumbamiento de las instituciones y a la frustración de los ciudadanos enganados*".

698 HASSEMER, Winfried. ***Es la autodeterminación todavia actua?*** Op. cit. p, 248. "*La autodeterminación, igual que la libertad y la arbitrariedad, choca con la autodeterminación de los demás y termina en ella*".

699 ROMERO SANCHEZ, Angelica. *Proceso penal, privacidad y autodeterminación informativa en la persecución penal de la delincuencia organizada. Un análisis desde la perspectiva del derecho procesal penal alemán*. In: ***Revista Criminalidad,*** 57 (2): 319-333. 2015. p, 326.

700 QUEVEDO GONZALEZ, Josefina. ***Derechos y libertades que resulta afectados.*** Op. cit. p, 125.

Do direito a informação se deu origem à uma categoria específica de dados, tidos por representarem determinados tipos de informação que, caso conhecidas e processadas, resultariam em uma potencial utilização discriminatória, ou seja apresentaria maiores riscos de lesão ao seu titular, são dados sensíveis[701]. O direito a autodeterminação informativa se apresenta como medida de proteção a tais dados[702], ou ainda, como direito específico da pessoa, desenvolvido para determinar o destino de seus dados[703].

Contudo, a proteção de tais dados não parece suficiente somente pela expansão do "núcleo" da privacidade, atingir um maior âmbito de proteção perpassa pelo asseguramento de uma tutela mais intensificada. Conforme Rodotá se deve além da mudança na concepção da privacidade e de seu "núcleo" intocável, adotar medidas de proteção ou de controle destes dados[704].

O direito à proteção de dados se constitui em um desdobramento do direito à privacidade, podendo assim ser denominado de direito à privacidade informacional[705]. Contudo, mesmo sendo um desdobramento, há substancial distinção entre o direito à vida privada e o direito à proteção de dados. Como esclarece Rodotá[706], o primeiro reflete um componente individualista de natureza negativa capaz de impedir uma interferência na vida privada, ou seja, uma proteção estática. Em contrapartida, o direito à proteção de dados se estabelece a partir de regras acerca do processamento de dados e deste modo, estabelece um tipo de proteção dinâmica.

Evidente que a proteção de dados como direito fundamental é passível de restrições, pois não absoluto, contudo se trata de regra constitucional, de modo que a intervenção estatal em seu âmbito será a exceção. Desde que, evidentemente, haja previsão constitucional para tanto[707]. Do núcleo da disciplina jurídica da proteção de dados derivam princípios norteadores e instrumentais, tais quais o princípio da correção, exatidão, finalidade, da publicidade, do acesso individual e da segurança. Todavia, é o princípio do acesso, que marca um plano diferente, de modo que se mostra como instrumento para a atuação direta de um interesse

---

[701] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais.** Rio de Janeiro: Renovar, 2006. p, 160 – 161.
[702] RODOTÁ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje.** Op. cit. p, 37.
[703] HASSEMER, Winfried; CHIRINO SANCHEZ, Alfredo. ***El derecho a la autodeterminación informativa y los retos del procesamiento automatizado de datos personales.*** Editores del Puerto: Buenos Aires, 1997. p, 33.
[704] RODOTÁ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje.** Op. cit. p, 37
[705] RUARO, Regina Linden. **Privacidade e autodeterminação informativa: obstáculos ao Estado de vigilância?** Arquivo Jurídico – ISSN 2317-918X – Teresina-PI – v. 2 – n. 1 – p. 41-60. Jan./Jun. de 2015. p, 43.
[706] RODOTÁ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje.** Rio de Janeiro: Renovar, 2008. p, 17.
[707] RUARO, Regina Linden. **Privacidade e autodeterminação informativa: obstáculos ao Estado de vigilância?** Op. cit. p, 45.

individual e para garantir a efetividade de um princípio geral[708]. Desta forma, o princípio do acesso representa – a seu turno – a passagem da proteção estática para a proteção dinâmica e ativa.

O conceito de autodeterminação informativa foi construído pelo Tribunal Federal Constitucional Alemão[709] em um cenário de compilação dos dados de cidadãos que, isoladamente acessados não representava tamanha necessidade de tutela constitucional, mas que pela compilação ameaçava-os de um excessivo controle estatal. Diante da compilação de todos os dados resta inócua a discussão sobre graus de importância e relevância de determinado dado em um contexto individualizado, já que se torna possível a criação de perfis completos de personalidades[710].

O catálogo dos cidadãos, bem como dos grupos sociais que compõem, é característico de nações que possuem regimes políticos autoritários. A construção destas bases de dados da personalidade se mostra um risco capaz de impedir ou reduzir drasticamente a possibilidade das pessoas cumprirem seu papel social ativamente. A criação de tais bases é medida anterior àquelas tomadas de medidas de prevenção social ou medidas de controle dos corpos indesejáveis[711].

---

[708] RODOTÁ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje.** Op. cit. p, 59-60. "1) princípio da correção na coleta e no tratamento das informações; 2) princípio da exatidão dos dados coletados, acompanhado pela obrigação de sua atualização; 3) princípio da finalidade da coleta dos dados, que deve poder ser conhecida antes que ocorra a coleta, e que se especifica na relação entre os dados colhidos e a finalidade perseguida (*princípio da pertinência*); na relação entre a finalidade da coleta e a utilização ou na transformação em dados anônimos das informações que não são mais necessárias (*princípio do direito ao esquecimento*); 4) princípio da publicidade dos bancos de dados que tratam as informações pessoais, sobre os quais deve existir um registro público; 5) princípio do acesso individual, com a finalidade de conhecer quais são as informações coletadas sobre si próprio, obter a sua cópia, obter a correção daquelas erradas, a integração daquelas incompletas, a eliminação daquelas coletadas ilegitimamente; 6) *princípio da segurança* física e lógica da coletânea dos dados".

[709] O conceito de autodeterminação informativa compõe a decisão proferida pelo Tribunal Federal Constitucional Alemão que julgou a aplicação parcialmente constitucional da chamada "Lei do Censo" (*Volkzählungsurteil*) que seria aplicada em 1983 impondo diversas alterações. A *BVerfGE* 65 se dirigia concretamente contra a "recolha total" de dados dos cidadãos pretendida pelas autoridades estatais. Ressalta Hassemer e Chirino Sanchez que se pedia aos cidadãos informações sobre seus nomes, seus apelidos, seus endereços, telefone, sexo a data de nascimento, a ideologia política, a religião, a nacionalidade, o tipo de convivência com outras pessoas, os domicílios, o tipo de trabalho, a renda, a profissão, a duração do período de estudos realizados, com indicação dos estudos médios e a duração do período universitário, o endereço profissional, os meios de locomoção utilizados para ir ao trabalho, o tempo médio no deslocamento até o trabalho, duração da jornada de trabalho, classe, extensão, costumes, número e uso dos imóveis, quantia de alugueis mensais (HASSEMER, Winfried; CHIRINO SANCHEZ, Alfredo. ***El derecho a la autodeterminación informativa y los retos del procesamiento automatizado de datos personales.*** Op. cit. p, 161). Como explica Ruaro, "julgou-se nulo os dispositivos relacionados à comparação e à transmissão dos dados para repartições públicas, reconhecendo a Corte o direito do cidadão de negar informações de caráter pessoal, sendo desta forma uma faculdade subjetiva de consentir ou não na coleta, no armazenamento e no compartilhamento de dados pessoais". RUARO, Regina Linden. **Privacidade e autodeterminação informativa: obstáculos ao Estado de vigilância?** Op. cit. p, 44.

[710] CHIRINO SANCHEZ, Alfredo. ***Las tecnologias de la informacion y el proceso penal: analisis de una crisis anunciada.*** Revista de Ciencias Penales de Costa Rica. p, 44.

[711] HASSEMER, Winfried; CHIRINO SANCHEZ, Alfredo. ***El derecho a la autodeterminación informativa y los retos del procesamiento automatizado de datos personales.*** Op. cit. p, 168-169.

Deste modo, a Corte estabeleceu bases para a construção futura da proteção de dados pessoais[712-713]. Sobre o julgado, Hassemer salienta que a Corte identificou o direito à autodeterminação informativa como sendo decorrente do centro da ordem constitucional, local ocupado pelo valor e pela dignidade da pessoa que atua em livre autodeterminação como membro de uma sociedade livre.

De tal forma, entendendo o ser humano como ser comunicante, ou seja, "uma pessoa obrigada a comunicação, que se desenvolve dentro da comunidade social", elevou a autodeterminação informativa ao *status* de direito fundamental vinculado ao livre desenvolvimento da personalidade[714].

Conforme esclarece Menke, o Tribunal Federal Constitucional Alemão definiu o direito geral da personalidade distinguindo três categorias que o compõe, sendo elas, além do direito à autodeterminação, o direito à autopreservação e à autoapresentação. O primeiro se relaciona ao direito do próprio individuo de determinar a sua identidade, neste sentido abarcando o direito do conhecimento da origem biológica, o direito a ter um nome, uma orientação sexual. Quanto ao direito à autopreservação, garante ao indivíduo o direito de se recolher para si e ficar só, por exemplo o direito ao sigilo dos diários pessoais, dos documentos médicos e dos materiais biológicos. Por fim, a autoapresentação, como direito, possibilita que o indivíduo se insurja contra as falsas, não autorizadas, degradantes ou deturpadas representações de sua pessoa, "bem como o protege das observações secretas e indesejadas de sua personalidade". De tal modo, compondo portanto, o direito geral da personalidade, a autodeterminação informativa está protegida – como elemento da personalidade – ainda que não esteja coberto pelas garantias especiais de liberdade da lei fundamental[715].

---

712 ROMERO SANCHEZ, Angelica. **Proceso penal, privacidad y autodeterminación informativa en la persecución penal de la delincuencia organizada. Un análisis desde la perspectiva del derecho procesal penal alemán.** Op. cit. p, 326.

713 HOFFMAN-RIEM, Wolfgang. ***Innovaciones en la Jurisprudencia del Tribunal Constitucional Alemán, a Propósito de la Garantía de los Derechos Fundamentales en Respuesta a los Cambios que Conducen a la Sociedad de la Información*.** RDU, Porto Alegre, Volume 12, n. 64, 2015, 40-61, jul-ago 2015. p, 48.

714 HASSEMER, Winfried. ***Es la autodeterminación todavia actua?*** Op. cit. p, 249-250. "*Todos tienen derecho al libre desarrollo de su personalidad, siempre que no lesione los derechos de otro y no infrinja el orden constitucional o la ley moral*".

715 MENKE, Fabiano. **A proteção de dados e o novo direito fundamental à garantia da confiadencialidade e da integridade dos sistemas técnico-informacionais no direito alemão.** Op. cit. p, 210. O autor, em tradução livre da decisão proferida, traz as definições do Tribunal Federal Constitucional Alemão acerca da autodeterminação informativa: "aquele que, com segurança suficiente, não pode vislumbrar quais informações pessoais a si relacionadas existem em áreas determinadas de seu meio social, e que aquele que não pode estimar em certa medida qual o conhecimento que um possível interlocutor tenha da sua pessoa, pode ter sua liberdade consideravelmente tolhida"; "Aquele que tem insegurança acerca de o seu modo comportamental desviante ser, a todo momento, registrado, e como informação, ao longo do tempo armazenado, utilizado ou disponibilizado a terceiros, tentará não incidir em tal modo comportamental. Aquele que parte do pressuposto de que, por exemplo, a participação em uma reuni~~ao ou em uma iniciativa do exercício de cidadania seja registrado por um órgão

Se as comodidades proporcionadas por novas tecnologias de comunicação e informação decorrem dos avanços tecno-científicos não ameaçados por retrocessos tecnológicos, ou seja, não marcados pela possibilidade de sustação do avanço da tecnologia, resta se perceber o perigo destes avanços representados proporcionalmente pelos benefícios que são concendidos aos seus usuários. Logo, reconhecer o direito à autodeterminação informativa representa a faculdade colocada nas mãos dos interessados de utilizarem instrumentos que os permitam recuperar, parte, do controle sobre as informações cedidas em contraprestação aos benefícios tecno-informacionais percebidos[716].

Não impede dizer, desta forma, que pela quantidade de dados pessoais produzidos e armazenados pelos usos de novas tecnologias não torne possível a construção de uma identidade virtual, e desta forma necessitando sua tutela. Esta abordagem é trazida por Quevedo Gonzalez[717-718], a partir da jurisprudência do Supremo Tribunal Constitucional Espanhol, na qual admite a construção de um novo direito à identidade virtual oriundo precisamente da utilização massiva de novas tecnologias. Tratar-se-ia de um "direito ao próprio entorno virtual" que abarca "uma serie de elementos comuns do direito à intimidade, ao segredo das comunicações e do direito de proteção de dados pessoais", ou seja, dados integrados relativos a um mesmo titular.

De tal sorte, conforme argumenta a autora, o "entorno virtual próprio" foi incluído como direito fundamental de nova geração em julgamento STS 204/2016[719] em que se declarou que "o legislador outorga um tratamento unitário aos dados contidos nos computadores e nos telefones móveis, reveladores do perfil pessoal do investigado, configurando um direito constitucional de nova geração que é o direito à proteção do próprio entorno virtual".

---

público, e que a partir dessas atividades possam lhe advir riscos, provavelmente abdicará do exercício dos direitos fundamentais relativos a essas atividades".

[716] MURILLO DE LA CUEVA, Pablo Lucas; PIÑAR MAÑAS, José Luis. ***El derecho a la autodeterminacón informativa.*** Fundación Coloquio Jurídico Europeo, Madrid. 2009. p, 16.

[717] QUEVEDO GONZALEZ, Josefina. ***Derechos y libertades que resulta afectados.*** Op. cit. p, 127. "*la información em formato electrónico que, a través del uso de las nuevas tecnologias, ya sea de forma consciente o inconsciente, com voluntariedade o sin ella, va generando el usuário, hasta el punto de dejar um rastro susceptible de seguimento por los poderes públicos*" (SSTS 985/2009, de 13 de diciembre; 342/2013, de 17 de abril, y 97/2015, de 24 de febrero).

[718] Neste mesmo sentido PEREA, Inmaculada Lopez-Barajas. ***Nuevas tecnologías aplicadas a la investigación penal: el registro de equipos informáticos***. Revista de los Estudios de Derecho y Ciencia Política. IDP N.º 24 (Febrero, 2017) I ISSN 1699-8154 p, 68.

[719] QUEVEDO GONZALEZ, Josefina. ***Derechos y libertades que resulta afectados.*** Op. cit. p, 127. "*El Legislador otorga un tratamiento unitario a los datos contenidos en los ordenadores y teléfonos móviles, reveladores del perfil personal del investigado, configurando un derecho constitucional de nueva generación que es el derecho a la protección del propio entorno virtual*". Disponível em: https://supremo.vlex.es/vid/631962729. Acesso out/2018.

A discussão que perpassa sobre a matéria impõe a reflexão acerca de mutações que o uso de novas tecnologias tem acarretado ao processo penal. Por esta óptica, o processo penal deixa de ser uma ordem de proteção e liberdade e se converte, sobretudo, "em um instrumento operativo das autoridades responsáveis pela persecução penal"[720]. Portanto, há uma necessidade de se entender a dimensão desta mutação que afeta o papel do processo penal diante, principalmente, do direito à autodeterminação informativa de modo a alcançar temas como a presunção de inocência, a proibição de produzir provas contra si, a utilização de métodos enganosos ou sub-reptícios de investigação de prova, bem como outros temas mais tradicionais que dizem respeito a proteções constitucionalmente impostas, tais como a privacidade domiciliar.

A afetação da autodeterminação informativa e proteção de dados incide no conceito de domicílio, de modo a se alargar os limites semânticos que dizem respeito ao físico, para que se alcance também dimensões virtuais. Os dados referentes ao indivíduo necessitam de proteção face à intrusão de estranhos nas esferas de pensamento ou atividade contida no domicílio virtual[721]. Conforme Torre, e semelhante ao já acima apontado, a intromissão em dados informáticos pode representar algo mais pessoal e íntimo do que a tradicionalmente conhecida como invasão de domicílio. Uma extensão da nossa mente é mantida e preservada, de modo que o passado, o presente e o futuro do usuário "materializam-se" em representações através dos dados confidenciais que formam o denominado "domicílio virtual".

No que toca ao tema central do trabalho, a lesão ao domicílio é dupla. A imediata se trata do domicilio virtual, porquanto que este é composto por dados informáticos que dizem respeito a personalidade do sujeito. De maneira mediata, acaba por atingir também o domicílio físico a partir da utilização de mecanismos sub-reptícios de invasão da intimidade em ambientes privados com o objetivo principal de coletar informações que serviram para sustentar uma hipótese acusatória. A conclusão parcial a este respeito é que o domicílio virtual deve ser duplamente protegido, tanto mediante legislação que descreve claramente os limites do método, quanto pela autorização judicial na restrição de direitos fundamentais. Na atual conjuntura se trata de uma investigação de *fonte* de prova que se baseia em um meio atípico e de tal sorte, sem legislação clara, integra uma hipótese de prova inconstitucional[722], ou para o direito processual penal brasileiro, ilícita.

---

[720] HASSEMER, Winfried. ***Proceso penal sin protección de datos?***. La insostenible situación del derecho penal, ISBN 84-8151-967-7, págs. 103-128. 2000. p, 111-112.
[721] TORRE, Marco. ***Il captatore informatico.*** Op. cit. p, 86-87.
[722] Neste sentido, também é a conclusão de Marco Torre (***Il captatore informático***. Op. cit. p, 87).

4.2.3 Sigilo e proteção das comunicações: Direito Inviolável (?)

Todo o exposto até aqui não poderia desaguar em outro lugar que não na restrição do direito ao sigilo e proteção das comunicações. Os problemas situados no corpo desta pesquisa simbolizam que na realidade a proteção da livre comunicação é trazida para o centro do debate, de tal forma que também merece reflexão.

O desenvolvimento tecnológico permitiu que avanços técnicos a nível de vigilância fossem atingidos, os instrumentos tradicionais de controle se transformaram paulatinamente em tecno-instrumentos de vigilância ou mais precisamente instrumentos informáticos de vigilância para o controle, evidentemente.

Como ressalvado desde o início, é o controle da informação nas mãos do controlador que lhe assegura o poder da informação como capacidade de prever e assim evitar riscos. Pela informação se controla o sujeito, seu comportamento (e pensamento). Deste modo a reflexão vai mais além da afetação isolada do direito ao sigilo e proteção das comunicações, e atinge outros direitos fundamentais e princípios processuais diante destas cruzadas contra a criminalidade[723].

O direito da proteção à comunicação se enquadra entre os direitos de liberdade, compreendido como subjetivo e essencial de defesa[724], de modo que independentemente de seu conteúdo, as comunicações devem resultar protegidas[725], tal como impõe a constituinte brasileira, é inviolável o sigilo das comunicações. Sendo assim, assevera Quevedo Gonzalez que além da proteção constitucional se direcionar tanto a agentes públicos quanto privados, o segredo da comunicação – pela proteção do conteúdo – se pauta contra interceptações não autorizadas ou qualquer outra forma de conhecimento antijurídico do comunicado. Abarcando, ademais, a identidade subjetiva dos interlocutores, ou qualquer dado correspondente a elemento da cadeia de comunicação gerado por meio de um sistema informático, como a origem, o destino, a rota, o tamanho, a duração[726].

A premissa portanto é que a ingerência estatal face à proteção constitucional do sigilo das comunicações somente poderá ocorrer, quando autorizada por lei para fins de investigação criminal e instrução processual penal, desde que autorizada judicialmente. Como

[723] WOLTER, Jürgen. **O inviolável e o intocável no direito processual penal.** Op. cit. p, 160.
[724] GRINOVER, Ada Pellegrini. **Liberdades públicas e processo penal: as interceptações telefônicas.** 2ª edição atualizada. São Paulo: Editora Revista dos tribunais, 1982. p, 191.
[725] QUEVEDO GONZALEZ, Josefina. ***Derechos y libertades que resultan afectados.*** Op. cit. p, 118.
[726] QUEVEDO GONZALEZ, Josefina. ***Derechos y libertades que resultan afectados.*** Op. cit. p, 119.

ressalta Muñoz Conde[727], em se tratando de processo penal, a restrição do direito fundamental ao sigilo das comunicações pode ser imprescindível para a persecução penal, contudo os limites impostos reforçam a proibição da busca incansável e a qualquer preço daquilo que se entende por "verdade".

Talvez a assombração da "verdade" como suposto objetivo do processo penal tenha cedido espaço à busca pela "prevenção de delitos". A equação parece simples e verdadeira, mas se trata de um complexo paradoxo. Nesta lógica o processo penal perde serventia e utilidade, a lógica da guerra contra criminalidade, aniquila o Direito Processual Penal pois mina sua capacidade de controle e de reação ao poder punitivo. A prevenção pelo poder da informação prosta tanto a liberdade individual – aqui observada na sua face comunicativa resguardada pelo sigilo – que sujeita o indivíduo não à lei, mas ao controle, quanto a sua capacidade de reação frente a violência sub-reptícia da transparência.

A proteção quanto à inviolabilidade do direito ao sigilo das comunicações, na realidade tecnológica não se sustenta. Há, ao contrário, violações constantes em função de intervenções prospectivas do Estado para a prevenção de crimes. Como ressalta Cuerda Arnau, o exemplo paradigmático desta realidade se retrata no "controle estratégico das telecomunicações", ou seja, a recolha de informações de maneira aleatória e seu processamento mediante diversos filtros buscando palavras chaves. Esta tecnologia é controlada por países como Estados Unidos, Canadá, Gran Bretanha, Austrália e Nova Zelândia, e funciona na captura de comunicações por rádio, satélites, chamadas de telefone, *fax*, e *e-mails* em quase todo o mundo, incluindo ainda a análise automática e classificação das interceptações"[728].

A informação recolhida por novas formas de "tecnovigilância" que afetam a comunicação como direito fundamental não serve para compor material probatório que embase uma condenação. Se o texto constitucional impõe que a inviolabilidade do sigilo comporta exceções quando em contextos de investigação criminal ou processo penal, o faz determinando que antes da autorização judicial à quebra do sigilo comunicional, haja o início de uma persecução criminal.

Deste modo, parece irrazoável que informações anteriormente coletadas a partir das tecnologias de vigilância possam fazer parte do lastro probatório em um processo judicial.

---

[727] MUNOZ CONDE, Francisco. ***Prueba prohibida y valoración de las grabaciones audiovisuales en el proceso penal.*** Revista Penal, Nº 14, 2004. p, 102.

[728] CUERDA ARNAU, Mª Luisa. ***Intervenciones prospectivas y secreto de las comunicaciones. Cuestiones pendientes.*** In: GONZALEZ CUSSAC, José Luis; CUERDA ARNAU, María Luisa (Dir.); FERNANDEZ HERNANDEZ, Antonio (Coord). ***Nuevas amenazas a la seguridade nacional: terrorismo, criminalidad organizada y tecnologias de la información y la comunicación.*** Tirant lo Blanch, Valencia, 2013. p, 109.

Ademais é possível dizer que sequer seria admissível inaugurar uma investigação criminal a partir desta anterior violação ao sigilo comunicacional. Ou seja, o conteúdo das comunicações não servirão sequer a funções endoprocedimentais, pois sua aquisição não é sustentada por mandado judicial autorizativo, e portanto, carece de constitucionalidade. A utilização de informações veladas ao Estado, seja no processo penal judicial, seja na investigação preliminar, causa uma ruptura no ordenamento jurídico.

Diferente será quando já se iniciada uma investigação criminal ou quando o processo penal está em curso. Neste ponto, a violação do sigilo e da proteção das comunicações poderár ocorrer se previsto em lei e autorizada judicialmente. Vale ressaltar que em se tratando da utilização de *malware* para a quebra e colheita de informações referentes à comunicação não pode se embasar pelos ditames regulatórios de outros métodos de intervenção. A especificidade da lei deve atender às peculiaridades deste meio de investigação, pois a partir deste haverá a afetação de direitos fundamentais específicos além do direito ao sigilo das comunicações.

O processo de comunicação comporta três momentos, a transmissão, o armazenamento da informação no servidor receptor e o acesso do receptor à mensagem. Ademais, como faz Quevedo Gonzalez[729], é preciso identificar três situações distintas quanto à comunicação. Primeiramente, quando no caso concreto não está presente nenhum processo de comunicação, o acesso à informação constante em dispositivos eletrônicos não afeta ao direito ao sigilo comunicacional e sua proteção, mas ao direito à intimidade – quando em uma investigação informática por *malware*, a afetação se direciona a outros direitos abaixo elencados.

A segunda situação diz respeito a um claro processo de comunicação em curso. Ou seja, ocorre em dois casos: quando se acessa o conteúdo da mensagem que foi enviada ou recebida, mas que ainda não foi lida por seu destinatário; e quando a mensagem se encontra no processo de transferência. Nestes casos, evidentemente a afetação se dirige ao sigilo e a proteção da comunicação.

Por fim, uma terceira situação se refere a um processo comunicativo efetivamente consumado ou ainda não iniciado. Surgem duas hipóteses concretas, a primeira diz respeito ao acesso à informação não enviada, e a segunda se atenta ao acesso quando já enviada, recebida e lida, encontrando-se armazenada no dispositivo eletrônico. De fato, também nestas hipóteses, não haverá violação ao sigilo da comunicação por se tratarem de arquivos, que embora destinados ou decorrentes a/do processo comunicativo, trata-se de materiais de arquivo.

---

[729] QUEVEDO GONZALEZ, Josefina. ***Derechos y libertades que resultan afectados.*** Op. cit. p, 122.

4.2.4 A integridade e confiabilidade do sistema informático

Os direitos fundamentais garantem o *status* subjetivo dos indivíduos através do reconhecimento de faculdades ou possibilidades de atuação e pelo estabelecimento do equilíbrio dos poderes em uma sociedade democrática[730]. Portanto, medidas de dimensão democráticas devem comportar a previsão de equilíbrio entre poderes políticos, sociais e econômicos, transformando os direitos fundamentais não em mera garantia formal, mas – sobretudo – em garantia fática.

No tocante ao tema aqui tratado, o direito à livre personalidade combinado com a dignidade humana origina a construção do denominado direito geral de personalidade, que nas palavras de Greco[731], trata-se de "um direito que compreende em seu bojo uma série de direitos mais concretos, como os tradicionais direito ao próprio nome e à honra, e os mais modernos direitos à própria imagem, à própria voz".

Nesta senda, a tutela jurídica da personalidade a partir do advento de novas tecnologias deve ser ampliada, principalmente por permitirem um passo para novas formas de poder e controle dos cidadãos[732]. De acordo com Rodotá[733] as pessoas se apropriam da tecnologia através do corpo, vivem em uma realidade incrementada. Justamente pela tecnologia é que se dispõem à exploração, permite-se invadir muitas vezes de maneira invisível através dos dados que são constantemente recolhidos. O poder no contexto atual deriva do domínio da informação não mais se restringindo aos meios coativos[734].

Pode-se afirmar, portanto, que o direito geral da personalidade compreenderá também – se se disser que os dados são fragmentos da personalidade individual[735] – o direito da proteção de dados. Proteger dados pessoais, portanto, é sinônimo de proteger informações e isso, segundo Perez Luño, tornou-se critério de legitimação política dos "sistemas democráticos tecnologicamente desenvolvidos". Reconhecer isto é condição de funcionamento do próprio sistema democrático, a liberdade informática e a proteção de dados fazem parte do conjunto de direitos "que definem o *status constituens*" do cidadão[736].

---

[730] PEREZ LUÑO, Antonio Enrique. ***Los derechos humanos en la sociedad tecnológica*.** In: LOSANO, Mario G; PEREZ LUÑO, Antonio Enrique; GUERRERO MATEUS, Mª Fernanda. ***Liberdad informática y leyes de proteccion de datos personales.*** Cuadernos y Debates. Centro de estúdios constitucionales. Madrid, 1989. p, 138.
[731] GRECO, Luis. **Introdução - O inviolável e o intocável no direito processual.** Op. cit. p, 33.
[732] PEREZ LUÑO, Antonio Enrique. ***Los derechos humanos en la sociedad tecnológica*.** Op. cit. p, 138.
[733] RODOTA, Stefano. ***El derecho a tener derechos.*** Op. cit. p, 289.
[734] PEREZ LUÑO, Antonio Enrique. ***Los derechos humanos en la sociedad tecnológica*.** Op. cit. p, 139.
[735] RODOTA, Stefano. ***El derecho a tener derechos*.** Op. cit. p, 293. "*Estamos también ante identidades 'dispersas', por el hecho de que informaciones relacionadas con uma misma persona se hallan en bancos de datos diferentes y donde cada uno de ellos restituye solo una parte o un fragmento de la identidade en su conjunto*".
[736] PEREZ LUÑO, Antonio Enrique. ***Los derechos humanos en la sociedad tecnológica*.** Op. cit. p, 139.

Nesta nova compreensão da realidade, quando se pretende alcançar informações individuais privilegiadas (dados), os objetos tecnológicos tomam protagonismo na relação entre indivíduo e objeto. Não é mais necessário se direcionar ao indivíduo para se cumprir com este objetivo, basta se dirigir, ou melhor se intervir sob o objeto.

O indivíduo externaliza sua identidade pela comunicação, transformando-se em uma fonte de contínua extração de dados. Na visão de Rodotá[737] neste novo mundo a relação entre indivíduos e objetos se converte em um imenso fluxo de informações relacionadas às pessoas, de modo a permitir – inclusive – que haja um "diálogo" entre objetos (*internet das coisas*) a fim de que se incremente, se atualize, os dados individuais.

Resta evidente não se tratar unicamente da busca pela proteção de dados, mas há que se falar – em primeiro plano e máximo grau – na proteção fundamental das pessoas cujos dados fazem referência[738]. No que se refere ao Direito Processual Penal, proteger os dados é possivelmente proteger o sujeito passivo de invasões demasiadamente lesivas à sua intimidade. Invasões que acarretam no acesso a informações sensíveis, desafetas aos fatos investigados, ou que possuam conteúdo auto incriminatório que sequer poderia ser utilizado como *fonte* de prova em um processo penal constitucional, mas que pelo alto nível de evidência que o impregna, acaba por corromper a imparcialidade judicial, na tentativa da resolução eficiente do caso.

O Tribunal Constitucional Alemão definiu como um novo direito constitucional a confibialidade e integridade dos sistemas de tecnologia da informação, de modo a protegê-lo diante de ingerência estatais investigativas que buscassem alcançar o fluxo de informações de maneira oculta utilizando a *internet.* Investigações que se utilizam de expedientes que interfiram demasiadamente em direitos constitucionais, sem uma necessária justificação, ou seja, ausente de demonstração capaz de justificar a intervenção no âmbito de proteção e a proporcionalidade em seus impactos, tratar-se-á de investigação ilegal. A confiabilidade e integridade do sistema informático é um direito constitucional que protege de maneira explícita a privacidade e os direitos de personalidade dos cidadãos quando se referirem às novas tecnologias de informação e comunicação[739].

O direito à integridade dos sistemas passa, então, a garantir a proteção contra ingerências em sistemas de tecnologia da informação não assegurados por outros direitos fundamentais, como a privacidade de correspondência, correios e telecomunicações, ou a

---

[737] RODOTA, Stefano. ***El derecho a tener derechos.*** Op. cit. p, 296.
[738] PEREZ LUÑO, Antonio Enrique. ***Los derechos humanos en la sociedad tecnológica.*** Op. cit. p, 139.
[739] ABEL, Wiebke; SCHAFER, Burkhard. ***The German Constitutional Court on the Right in Confidentiality and Integrity of Information Technology Systems – a case report on BVerfG***, NJW 2008, 822. In Madhuri, V. (Ed.), Hacking. (pp. 167-91). Icfai University Press. Volume 6, Issue 1, April 2009. p, 120.

inviolabilidade do domicílio[740]. Em verdade, trata-se de uma atualização da proteção à personalidade em face da realidade tecnológica do século XXI[741]. Portanto, a partir da realidade atual em contexto de tecnologia da informação e comunicação e a utilização cada vez mais constante de sistemas de tecnologia, o Tribunal Constitucional Alemão adotou o conceito de sistema de tecnologia da informação "como um sistema com capacidade de conter dados técnicos a um ponto que fosse possível ter conhecimento de uma substancial parcela da vida de um indivíduo e noção significativa de sua personalidade"[742].

Identificando as lacunas existentes na proteção da personalidade, a Corte Constitucional Alemã estabeleceu que o âmbito de proteção deste novo direito se volta contra o acesso do Estado ao sistema de tecnologia e informação, não somente às comunicações individuais, nem aos dados já armazenados no dispositivo informático, mas ao próprio sistema em sua confiabilidade e integralidade[743]. Contudo, embora não taxando especificadamente quais sistemas informáticos são protegidos pelo direito fundamental, por ter conhecimento da obsolescência constante das novas tecnologias[744], sinalizou que tais sistemas condizem àqueles com poder de detalhamento acentuado quanto ao fornecimento de dados da personalidade.

Logo, a proteção atua em casos cuja intervenção estatal compreenda sistemas informacionais que, "considerados individualmente ou acerca de suas possibilidades de conexão técnica, contenham dados pessoais do indivíduo numa extensão e numa variedade que o acesso a esse sistema possibilite vislumbrar as diversas facetas da condução de sua vida pessoal ou até mesmo uma 'fotografia' de sua personalidade"[745].

A mera capacidade de armazenamento de dados pessoais já é suficiente, de modo que tal direito protege um sistema, que mesmo não contendo dados pessoais, desde que seja tecnicamente capaz de armazenar e processar tais dados, merece a referida proteção. Como

---

[740] MENDES, Gilmar; BRANCO, Paulo Gustavo Gonet. **Curso de Direito Constitucional.** 10 ed. rev. e atual. São Paulo: Saraiva, 2015. p, 557.

[741] MENKE, Fabiano. **A proteção de dados e o novo direito fundamental à garantia da confiadencialidade e da integridade dos sistemas técnico-informacionais no direito alemão.** In: MENDES, Gilmar F.; SARLET, Ingo W.; COELHO, Alexandre Z. P. **Direito, inovação e tecnologia.** São Paulo: Saraiva, 2015. p, 217.

[742] MENDES, Gilmar; BRANCO, Paulo Gustavo Gonet. **Curso de Direito Constitucional.** Op. cit. p, 558.

[743] ABEL, Wiebke; SCHAFER, Burkhard. ***The German Constitutional Court on the Right in Confidentiality and Integrity of Information Technology Systems – a case report on BVerfG***, NJW 2008, 822. In Madhuri, V. (Ed.), Hacking. (pp. 167-91). Icfai University Press. Volume 6, Issue 1, April 2009. p, 119.

[744] *The Court applies the guarantees of this right to information technology systems, but interestingly in doing so does not deliver a definition of such a system. Instead, it lists systems that are not protected by this right, and provides a description of minimum abilities an information technology system must possess to fall into the protection scope of this fundamental right. By doing so, it keeps the protection scope of this basic right very broad and deliberately avoids tailoring this new basic right to specific technologies. It thereby clearly acknowledges the rapid technological developments of information technology devices, and attempts to create technology neutral legislation with this judgement, hence trying to keep the new basic right "future-proof"*. p, 119.

[745] MENKE, Fabiano. **A proteção de dados e o novo direito fundamental à garantia da confiadencialidade e da integridade dos sistemas técnico-informacionais no direito alemão.** Op. cit. p, 222.

esclarece Ramalho[746], tratar-se-á de uma abrangência maior na proteção de dados que constem armazenados ou são propriamente gerados por sistemas, conectados ou não à *internet*, suscetíveis à possibilitar um conhecimento significativo da personalidade do sujeito. A tutela de proteção, segundo o autor, se estende ainda aos demais sistemas acessíveis através de um sistema concretamente afetado, como por exemplo *webmails*, sistemas de computação de armazenamento em nuvens e etc.

Abel e Schafer[747] esclarecem ainda que o referido direito fundamental visa a proteção de um interesse comum de usuários de sistemas de tecnologia da informação em garantir que dados criados, processados e armazenados pelo sistema permaneçam confidenciais. A Corte Alemã, neste sentido, estabeleceu a proteção face ao acesso clandestino do sistema, seja o acesso total ou em suas partes mais sensíveis, por exemplo, a memória de trabalho, dados temporários ou permanentes armazenados na mídia do sistema, principalmente quanto à aquisição de dados mediante procedimentos sub-reptícios, como a utilização de *key-loggers*, que como já retratado acima conta com o objetivo de monitorar as teclas digitadas para obtenção de senhas de acesso, *logins* e etc.

Contudo, a Corte Constitucional também observou critérios para a flexibilização deste direito. Por evidente, não se trata de um direito fundamental absoluto, podendo ser restringido para fins preventivos ao processamento de ilícitos penais desde que sua restrição seja proporcional. O critério de proporcionalidade determinado pela corte se refere à existência de evidência suficiente de que outros significativos valores fundamentais precisam ser protegidos, tais quais a vida e a integridade de outros cidadãos, os fundamentos do Estado e os valores da humanidade. A medida ainda, deverá sempre ser analisada caso a caso e confirmada por um juiz, para que seja garantido um controle objetivo de base jurídica constitucional.

Outro requisito para a restrição do direito a integridade e confidencialidade do sistema de informação é justamente a não supressão de seu núcleo fundamental que diz respeito à conduta central da vida privada (comunicação, sentimentos internos, relacionamentos). Como é difícil a separação entre estes dados sensíveis e aqueles de interesse das investigações, declara

---

[746] RAMALHO, David Silva. **Métodos ocultos de investigação criminal em ambiente digital.** op. cit. p, 247 – 248.

[747] ABEL, Wiebke; SCHAFER, Burkhard. ***The German Constitutional Court on the Right in Confidentiality and Integrity of Information Technology Systems – a case report on BVerfG***, NJW 2008, 822. In Madhuri, V. (Ed.), Hacking. (pp. 167-91). Icfai University Press. Volume 6, Issue 1, April 2009. p, 120. "*The Court specifies further that this basic right protects the right holder in particular from the clandestine access of an information technology system that is targeted at the system in its entirety or its major parts. The scope of protection of this right covers both the data kept on the working memory as well as data which is temporarily or permanently kept on the storage media of the system. It also protects against data acquisition that does not rely on the data processing procedures of the system itself, but nevertheless targets these, such as so-called key-loggers, which monitor the keystrokes of a user to gain passwords and other crucial login details*".

o Tribunal que os procedimentos devem se adequar às novas necessidades desta fase de análise dos dados. Se dados sensíveis forem detectados, estes devem ser excluídos imediatamente, de modo a estarem proibidos de serem utilizados pelo Estado[748].

A tentativa de adaptação dos meios de investigação de prova, por exemplo, quanto à sua aplicabilidade das *fontes* probatórias físicas para a investigação e obtenção de provas de natureza digital, como dito acima, é constante, por vezes ineficiente e inadequada, seja para a finalidade pretendida, seja pela desproporcionalidade do meio em virtude da alta incidência em direitos fundamentais.

Quanto ao tema, disporá Ramalho algumas questões[749] que objetivam uma reflexão acerca da proteção necessária do ambiente digital, que pela ingerência estatal em investigações criminais, não se mostra devidamente protegido, muito pelo fato da utilização de meios de investigação sem um juízo acertado de ponderação, ou seja, necessidade, adequação e proporcionalidade quanto à utilização do meio. De tal sorte, que consoante ao entendimento do Tribunal Alemão, afirma o autor que somente por via de Lei é que pode ser incluída a possibilidade excepcional[750] da utilização de métodos de investigação que incidem diretamente no direito à integridade e confiabilidade do sistema, como por exemplo a utilização de *software* maliciosos. Neste sentido, Bronzo conclui que sem uma base legal adequada, quanto à clareza e especificidade, destas intrusões investigativas não poderão ser recolhidas *fontes* probatórias para utilização no processo penal[751].

---

[748] ABEL, Wiebke; SCHAFER, Burkhard. ***The German Constitutional Court on the Right in Confidentiality and Integrity of Information Technology Systems – a case report on BVerfG***, NJW 2008, 822. In Madhuri, V. (Ed.), Hacking. (pp. 167-91). Icfai University Press. Volume 6, Issue 1, April 2009. p, 121 – 122. A ressalva feita pelos autores parece ser fundamental. Dirão que mesmo sendo de proibida utilização pelo Estado, ainda assim, a violação a um direito fundamental absoluto (dados da áera central da vida privada) existirá, e desta forma não será possível se desfazer a ocorrida violação do direito absoluto à dignidade humana.

[749] RAMALHO, David Silva. **Métodos ocultos de investigação em ambiente digital.** Op. cit. p, 242. "Mas que dizer, então, do ambiente digital? Da tutela da atividade do utilizador de um sistema informático *online* ou *offline*? Da expectativa de inviolabilidade de um sistema informático, independentemente do que nele se encontre armazenado? Dos dados automaticamente gerados pelo sistema informático; dos ficheiros aí armazenados ou dos dados guardados na *nuvem* em localização incerta? Haverá uma tutela distinta para cada sistema informático, consoante (i) o mesmo se encontre fisicamente no domicílio do visado ou noutro local, (ii) contenha dados pessoais ou mesmo íntimos, (iii) os dados se encontrem armazenados no sistema ou simplesmente sejam apreensíveis através dele, ou (iv) caso contenha correspondência digital?"

[750] Excepcional, posto que a utilização de determinados métodos de investigação em ambiente digital deve corresponder ao ilícito que se visa investigar. No caso Alemão, a utilização de *Malware* em investigações criminais dizem respeito a tão somente à defesa face aos perigos do terrorismo internacional, por exemplo.

[751] O autor destaca o grau de ilegitimidade da medida quando inexistente lei que regulamente, bem como a inutilidade – característica do Processo Penal italiano – para as provas que dela derivarem. No direito brasileiro, tratar-se-ão de provas ilícitas, posto que lesionam – sem autorização e controle legal – direitos fundamentais. BRONZO, Pasquale. ***Intercettazione Ambientale Tramite Captatore Informatico: Limiti Di Ammissibilità, Uso In Altri Processi E Divieti Probatori***. In: GIOSTRA, Glauco e ORLANDI, Renzo (a cura di). *Nuove Norme In Tema Di Intercettazioni Tutela Della Riservatezza, Garanzie Difensive E Nuove Tecnologie Informatiche*. G. GIAPPICHELLI Editore, Torino. 2018. p, 239.

No mesmo sentido a própria Corte Constitucional Alemã tratou de especificar requisitos e limitações para a restrição deste novo direito, impondo primeiramente a reserva legal de acordo com postulados normativos claros e precisos, acompanhados evidentemente de um juízo de proporcionalidade. Segundo ressalta Menke[752], para o referido Tribunal o monitoramento de sistemas informáticos é possível na medida em que os requisitos mínimos sejam possíveis de verificação na própria lei, ou seja, "a partir de parâmetros dos textos legais que eventualmente venham a ser editados prevendo medidas de monitoramento de sistemas informáticos".

Discorre o autor que somente quando a reserva legal autorizativa contemplar como condição a existência de perigo concreto "que ponha risco um bem jurídico de importância transcendental" é que seria possível o monitoramento remoto de sistemas técnico informacionais. De modo que o perigo concreto ou "prognóstico de perigo" corresponderia à probabilidade de, em tempo próximo e determinado, sejam causados danos a bens protegidos pela norma por meio de determinadas pessoas[753]. A análise do perigo concreto se dará mediante três fatores: a particularidade do caso concreto, a proximidade temporal da transformação do perigo em dano efetivo e o liame entre determinadas pessoas individuais como causadoras do dano iminente[754].

Deste modo, dever-se-ia considerar o direito à integridade e confiabilidade do sistema – ou tal como desenvolve Ramalho, a partir de Cuellar Serrano, *direito à não intromissão no ambiente digital* – como direito decorrente do princípio do Estado Democrático de Direito, e mais ainda, como expressão ou projeção do livre desenvolvimento da personalidade, reserva da intimidade da vida privada, sigilo das correspondências, utilização da informática, proibição de acesso a dados de terceiros. Ou seja, considerar sua abrangência estrutural para que haja efetiva proteção face a tutela fragmentária destes citados direitos, que não asseguram devidamente as garantias individuais e processuais diante de novas tecnologias probatórias ou de investigação em expansão[755].

---

[752] MENKE, Fabiano. **A proteção de dados e o novo direito fundamental à garantia da confiadencialidade e da integridade dos sistemas técnico-informacionais no direito alemão.** Op. cit. p, 223.

[753] Entende por bem jurídico de importância transcendental "o corpo, a vida e a liberdade da pessoa" ou ainda "bens da coletividade, cuja ameaça afeta os fundamentos ou a própria existência do Estado e das pessoas". MENKE, Fabiano. **A proteção de dados e o novo direito fundamental à garantia da confiadencialidade e da integridade dos sistemas técnico-informacionais no direito alemão.** Op. cit. p, 223.

[754] Id. p, 224. Esclarece o autor que mesmo que não seja possível verificar uma probabilidade da conversão do perigo em dano efetivo, o monitoramento poderá ser utilizado quando fatos determinados indiquem a iminência de ameaça concreta a bem jurídico de importância transcendental. Ademais, é fundamental que seja possível determinar quais as pessoas que estão envolvidas como causadoras da ameaça. A medida deve ser direcionada e limitada a estas pessoas, sem que o direito de outros indivíduos sejam violados.

[755] RAMALHO, David Silva. **Métodos ocultos de investigação em ambiente digital.** Op. cit. p, 251.

Pelo que dispõe a Constituição Federal do Brasil, artigo 5º, § 2º, como regra constitucional os direitos e garantias expressos no texto constitucional não excluem outros decorrentes do regime e dos princípios nele adotados, de igual modo se estendendo aos tratados internacionais cuja República Federativa do Brasil seja parte. Trata-se pois da denominada cláusula de abertura[756] que possibilita a incorporação de outros direitos que – em virtude do conteúdo – tenham *status* de fundamentais.

O conteúdo que compõe o direito incorpora-o ao conceito material de direitos fundamentais. Quer-se dizer que para além dos direitos fundamentais expressamente dispostos na Constituição Federal do Brasil (fundamentalidade formal), há que ser observada a fundamentalidade material do direito. Tal é caracterizada pelo conteúdo destes direitos "trazerem decisões fundamentais referentes à estrutura básica do Estado e da sociedade"[757].

De tal forma, pela análise do conteúdo do direito à integridade e confiabilidade dos sitemas informáticos, é possível verificar sua fundamentalidade material e como tal, figura um elemento constitutivo da Constituição material. Ou seja, um direito materialmente fundamental que pelo contéudo, compõe a estrutura básica do Estado Democrático Brasileiro[758].

---

[756] Sobre cláusula de abertura da Constituição Federal do Brasil ler SARLET, Ingo. **A eficácia dos direitos fundamentais.** Op. cit. p, 75 – 92.

[757] SARLET, Ingo. **A eficácia dos direitos fundamentais.** Op. cit. p, 76.

[758] Tal argumento se embasa na relação direta que o direito fundamental à integridade e confiabilidade do sistema informático possui com o demais direitos já mencionados neste trabalho, que compõe o Título II da Constituição Federal. Tais quais o direito à intimidade, privacidade, sigilo das comunicações, bem como o princípio dignidade da pessoa humana, inscrito no Título I do texto constitucional, que estrutura e norteia o Estado brasileiro.

5 CONSIDERAÇÕES FINAIS

As considerações finais trazidas ao leitor expõe justamente a importância da reflexão continuada a respeito da temática que se abordou em todo o texto. Isto reforça a importância atual da discussão que perpassa sobre a investigação criminal incrementada por novas tecnologias de informação e de comunicação. De fato, este talvez seja o aspecto que justifica a pesquisa elaborada.

Em verdade a temática da proteção de dados, bem como o surgimento de direitos fundamentais relacionados a ela, já conta com um acervo de pesquisas significativas. Contudo, por se tratar de tema de grande relevância atual, principalmente pela influência da sociedade da informação, percebida em todas as relações sociais, é possível que – a partir deste – surjam novas problemáticas que o envolvam. É disto que esta pesquisa se trata, o recorte dado à influência direta da sociedade de informação na sistemática processual penal.

A hipótese para a resolução do problema foi de fato confirmada tanto em seu aspecto geral, como nas especificidades. Os limites para a execução de um método oculto de investigação – o *malware* em específico –, bem como os requisitos necessários para que seja possível a sua decretação, são estabelecidos a partir do fundamento existencial do Direito Processual Penal e da Investigação Criminal Preliminar. Ou seja, o processo penal como um todo que atende às funções constitucionais e convencionais de garantia ao sujeito processado e de controle ao poder punitivo do Estado.

De tal sorte, a limitação do acesso a dados imposta aos órgãos de persecução penal decorre do envolucro de proteção individual que a legalidade impõe. Pode soar estranho esta consideração após a análise de estratégias estatais de segurança nacional e de legislações tendenciosamente lesivas à proteção de dados. Todavia, não se pode olvidar que é a legalidade processual penal que regulamenta a atuação do Estado, de tal forma que pela regulação se limita e se legitima a intervenção. Ademais, a leitura da legalidade processual não se faz isoladamente ou alheia aos ditames constitucionais e convencionais. O texto constitucional – por si só – é tido como mecanismo de proteção. Ou seja, quando em contextos de investigação criminal e processos penais, a atuação do Estado em violação aos dados, se legitima somente a partir de limites legalmente constituídos.

De fato não se desconsidera a hipótese da violação de todas estas proteções, contudo esta análise ultrapassa os recortes estabelecidos para a pesquisa que se realizou. O objeto de pesquisa, qual seja a investigação informática por meio do uso de *malware* pelo Estado, foi analisado por uma óptica processual penal constitucional, de modo que o descompromisso a

esta sistemática se trata de uma intervenção não legítima, uma intervenção característica de Estados de exceção.

A controvérsia percebida é que pela legalidade, como exigência processual, as exceções também surgem. As situações "excepcionais" que permitem o Estado lançar mão de métodos demasiadamente invasivos à privacidade e intimidade do investigado – o *malware* como método de investigação de *fontes* de prova – simbolizam falhas sistémicas (intencionais ou não). Contudo, como ficou demonstrado, a importância da tipicidade processual, ainda que verse sobre temas dinamicamente mutáveis como é o caso de novas tecnologias de investigação, possibilita o estabelecimento de diretrizes de tratamento procedimental.

Do fundamento existencial do Direito Processual Penal se deriva uma diversidade de institutos processuais que essencialmente se configuram também como mecanismos de proteção. O contraditório – por exemplo – é, além de técnica de defesa, elemento constitutivo do próprio processo, pois é somente a partir dele que se pode legitimar a produção probatória penal, qualquer que seja ela, incluindo neste espectro a produção de prova penal vinculada ao ambiente digital. Não há prova penal que não decorra da atuação dos contraditores, as partes do processo.

Deste modo, pelo contraditório possivelmente realizado a partir das diretrizes demarcadas pela lei processual é que se possibilita ainda o resgate do processo penal como entidade epistêmica de controle. As diretrizes irão servir de base para a questionabilidade, que em se tratando do tema proposto – *provas digitais* que carregam o caráter científico – demonstrou ser demasiadamente importante, principalmente pela "confiabilidade cega" inerente ao sistema informático e às provas tidas como científicas.

Provar a confiabilidade e a integridade do resultado probatório que derivou a partir de uma recolha de dados metodologicamente guiada pela ciência, no caso da pesquisa a ciência forense, é critério de admissibilidade probatória. De tal forma que não comprovada a confiança e integridade da *fonte* de prova digital, não há que se falar em produção probatória. Trata-se de prova ilícita por natureza inconstitucional, não por se referir à violação de um direito fundamental especificamente relacionado à obtenção dos dados, mas pelo prejuízo do exercício de defesa constitucionalmente garantido. A confiabilidade do método empregado na produção probatória da prova digital, bem como a integralidade do material recolhido, são limitações impostas à admissibilidade da prova.

Este elemento se volta à confirmação da hipótese em seu aspecto específico. Não é possível se falar na utilização do material probatório como *fonte de prova* a partir da recolha pelo acesso remoto mediante *malware*. Por tal motivo é que se tem a impossibilidade de

caracterizar o referido método investigativo como *medida cautelar probatória.* Ficou evidente que a medida cautelar probatória conserva fonte de prova, esta é a característica fundamental daquilo que se pretende como *medida cautelar probatória penal*. Conserva-se a fonte de prova para se evitar a frustração processual probatória.

Por evidente, antes da utilização do material probatório recolhido e conservado por uma medida cautelar probatória, há a comprovação da preservação de todos os elos da cadeia de custódia da prova. Somente assim se percebe admissível a *fonte de prova* cautelar. Como afirmado na pesquisa, a utilização de *malware* na recolha de material probatório (ainda) não atende a tais exigências. Trata-se, de um lado, à limitação pelo próprio desenvolvimento tecnológico, e de outro lado, uma limitação propriamente processual penal.

A natureza jurídica do instituto processual penal impede – em alguma medida – o uso do dado recolhido como *fonte de prova penal*. Uma reflexão que demarca a limitação do uso do material probatório recolhido pelo *malware* do Estado na investigação criminal, pautada na recolha de dados, decorre da natureza jurídica do instituto. A nomenclatura utilizada para defini-la pode variar de doutrina para doutrina, de legislação para legislação, contudo a essência não muda. Pode se denominar de *meios ocultos de investigação, meios de obtenção de prova* ou *meios de investigação de prova.*

Mas essencialmente se trata de um método que busca encontrar *fontes* de prova penal. O detalhe é que pelo método não se obtém propriamente as *fontes* de prova. O material probatório que se adquire não é ele mesmo a *fonte* de prova. Se assim fosse, por diversos modos seriam lesionados princípios processuais da produção de prova, como exemplo destacado no trabalho a proibição de provas contra si. É certo que o material colhido a partir da execução de tais métodos se refere ao material que será analisado, o qual poderá conter ou não informações acerca da existência de *fontes de prova.*

Caso identificadas as *fontes de prova*, o Estado persecutor – por nova autorização judicial – pode se valer de *medidas cautelares probatórias* para que se alcance as *fontes de prova* anteriormente identificadas no material recolhido e as conserve para que em momento processual oportuno se exerça o contraditório judicial.

O material probatório recolhido pela execução dos *métodos ocultos de investigação, meios de obtenção de prova*, ou *meios de investigação de prova* não possue nenhum valor probatório. Como ato de investigação que serve para a identificação de *fontes* de prova, somente será útil até cumprida sua função endoprocessual. Assim é a utilização do *malware* pelo Estado nas investigações criminais, serve a funções de investigação, e seus resultados não possuem

nenhum valor probatório. De tal modo que não devem ser incluídos aos autos processuais, mas descartados juntamente com os cadernos do inquérito policial.

Este tratamento não é o concedido ao material coletado pelo uso de *malware* na persecução penal. A análise dos casos nas experiências estrangeiras que ilustram as diversas funcionalidades do incremento informático, quanto ao acesso remoto aos dispositivos informáticos visados, demonstram justamente a utilização do material probatório coletado como *fonte de prova* digital.

Como demonstrado se considera um equívoco pelos diversos fatores elencados no texto acima. Desde a ausência de uma legalidade especificada, o uso análogo de legislações processuais referentes a outros métodos de investigação, a ausência da comprovação da fiabilidade e integralidade da suposta prova, a falta de autorização judicial necessária e precisa, a violação de direitos fundamentais propriamente relacionados com a invasão dos dispositivos informáticos, e também pela violação do preceito da proibição de produção de provas contra si – que retira do sujeito investigado seu *status* de dignidade, e o situa involuntariamente como possível *fonte* de prova.

Neste último ponto é que se ressalta que a utilização dos *métodos ocultos de investigação*, como o *Malware* do Estado, servem para alcançar a autoincriminação involuntária do sujeito investigado. Especificamente a utilização de *Malware*, como visto, decorre da necessidade do Estado de burlar medidas anti-forenses como a criptografia, e assim alcançar dados informáticos. Estes dados são equivocadamente utilizados como *fontes de prova penal.*

Ademais, pela análise dos casos que refletem as experiências estrangeiras, ficou comprovado que a taxatividade de tipos penais na lei que possibilita a investigação por meio do *Malware* se faz urgente. Os casos concretos não correspondiam apenas aos crimes informáticos, embora o método de investigação se trate de possibilitar a investigação por meio da informática. Se isto ficou comprovado, a hipótese da expansão da utilização de métodos investigativos pautados na informática é real.

O exemplo dos *EUA* é sintomático, verificou-se que a investida estatal se iniciou pela eleição dos sujeitos periodicamente tidos por “inimigos” como os alvos visados, mas posteriormente alcançou um caráter genérico de vigilância e controle, que transformou todos os indivíduos em potenciais suspeitos, ou como estalecido no texto, indivíduos “suspeitos não-suspeitos”. A intervenção estadunidense nos dados informáticos se inicia pelo combate à criminalidade de mafiosos, incrementando-se após os atentados terroristas do 11 de setembro

de 2001, e se expandindo à vigilância *online* por meio de programas governamentais de segurança nacional.

De todo o exposto, volta-se ao ponto de partida. A influência da Sociedade da Informação nos âmbitos do processo penal e investigação criminal, além dos incrementos tecnológicos, pauta-se na promoção de um imaginário coletivo da produtividade, o resultado como produto da óptica neoliberal é o resultado eficiente. A eficiência é colocada como preceito para a resolução de crimes ainda que pelo desrespeito às garantias processuais.

Por tal óptica se observa a utilização de mecanismos de controle e vigilância por meios tecnológicos para a prevenção de delitos. A vigilância compõe a sociedade da transparência. A eficiência jamais pode ser pressuposto de um processo penal que se veste como garantia constitucional, que limita e legitima a atuação do Estado. Demostrou-se que se trata de outra coisa, da efetividade. A eficiência causa degeneração processual.

6 REFERÊNCIAS

ABEL, Wiebke; SCHAFER, Burkhard. ***The German Constitutional Court on the Right in Confidentiality and Integrity of Information Technology Systems – a case report on BVerfG***, NJW 2008, 822. In Madhuri, V. (Ed.), Hacking. (pp. 167-91). Icfai University Press. Volume 6, Issue 1, April 2009.

AGAMBEN, Giorgio. **Estado de exceção**. São Paulo: Boitempo, 2004.

AGAMBEN, Giorgio. **Profanações.** São Paulo: Boi tempo, 2007.

AIGE MUT, Mª Belén. Boletín de la Academia de Jurisprudencia y Legislación de las Illes Balears, ISSN 2254-2515, Nº. 17, 2016, págs. 221-230.

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

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

ARANTES FILHO, Marcio Geraldo Britto. **A interceptação de comunicação entre pessoas presentes.** 1 ed. Brasilia, DF: Gazeta Jurídica, 2013.

AZEVEDO, Rodrigo Ghiringhelli de; VASCONCELLOS, Fernanda Bestetti de. **O Inquérito Policial em questão – Situação atual e a percepção dos delegados de polícia sobre as fragilidades do modelo brasileiro de investigação criminal.** Revista Sociedade e Estado. Volume 6 Número 1. Jan/Abr. 2011.

BADARÓ, Gustavo Henrique. **Interceptação de comunicações telefônicas e telemáticas: limites ante o avanço da tecnologia.** *In:* J. Corrêa de Lima e Rubens R. R. Casara (coords.), Temas para uma Perspectiva Crítica do Direito, Rio de Janeiro: Lumen Juris, 2010.

BADARO, Gustavo. **Ônus da prova no processo penal.** São Paulo: Editora Revista dos Tribunais, 2003. p, 2003.

BADARO, Gustavo. **Processo penal.** 4 ed. rev. atual. e ampl. São Paulo: Editora Revista dos Tribunais, 2016.

BARTOLI, Laura e MAIOLI, Cesare. ***La cadena di custodia del dato digitale: tra anelli solidi e anelli mancanti.*** In: BIASIOTTI, Maria Angela; EPIFANI, Mattia; TURCHI, Fabrizio (a cura di). *Trattamento e scambio della prova digitale in Europa*. Edizioni Scientifiche Italiane. 2016.

BAUDRILLARD, Jean. **Tela total: mito-ironias do virtual e da imagem.** 4 ed. Porto Alegre: Editora Sulinas. 2005.

BECK, Ulrich. **A metamorfose do mundo: novos conceitos para uma nova realidade.** 1ª ed. Rio de Janeiro: Zahar, 2018.

BECK, Ulrich. **Sociedade do risco: rumo a uma outra modernidade.** São Paulo: Ed. 34, 2010.

BENE, Teresa. ***Il pedinamento elettronico: truismi e problemi spinosi***. In: (a cura di) SCALFATI, Adolfo. *Le indagini atipiche.* G. Giappichelli Editore. Torino. 2014.

BINDER, Alberto. **Fundamentos para a reforma da justiça penal.** (Org.) GOSTINSKI, Aline; PRADO, Geraldo; GONZALEZ POSTIGO, Leonel. 1 ed. Florianópolis, SC: Empório do Direito, 2017.

BIZZOTO, Alexandre. **A mão invisível do medo e o pensamento criminal libertário.** 1ª ed. Florianópolis: Empório do Direito. 2015.

BRASIL. Presidência da República. **Código de Processo Penal.** Disponível em: http://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del3689.htm. Acesso em abr 2018.

BRASIL. Constituição (1988). **Constituição Federal do Brasil:** promulgada em 5 de outubro de 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em abr 2018.

BRASIL. **Superior Tribunal de Justiça.** STJ, RHC nº 89.981 – MG, Relator: Min. Reynaldo Soares da Fonseca. Quinta Turma, DJe 13/12/2017.

BRAUM, Stefan. ***La investigación encubierta como característica del proceso penal autoritário***. *In*: ROMEO CASABONA, Carlos Maria (org). ***La insostenible situacion del derecho penal.*** Instituto de Ciencias Criminales de Frankfurt (Ed.) Área de Derecho Penal de la Universidad Pompeu Fabra (ed. española). Granada, 2000.

BRITZ, Marjie T. ***Computer forensics and cyber crime: na introduction.*** Clemson University. 3ª ed. 2013.

BRONZO, Pasquale. ***Intercettazione Ambientale Tramite Captatore Informatico: Limiti Di Ammissibilità, Uso In Altri Processi E Divieti Probatori***. In: GIOSTRA, Glauco e ORLANDI, Renzo (a cura di). *Nuove Norme In Tema Di Intercettazioni Tutela Della Riservatezza, Garanzie Difensive E Nuove Tecnologie Informatiche*. G. GIAPPICHELLI Editore, Torino. 2018.

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

BUSO, Diego; PISTOLESI, Daniele. ***Le perquisizioni e i sequestri informatici.*** In: (a cura di) RUGGIERI, Francesca; PICOTTI, Lorenzo. *Nuove tendenze della giustizia penale di fronte alla criminalità informática Aspetti sostanziali e processuali*. G. Giappichelli Editore – Torino. 2010.

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

CARNELUTTI, Francesco. ***Las miserias del proceso penal.*** Buenos Aires: *Ediciones juridicas europa-america,* 1959.

CARNELUTTI, Francesco. ***Lecciones sobre el proceso penal Vol. I.*** Ediciones Jurídicas Europa-America. Bosch y Cia. Editores Chile 2970, Buenos Aires, 1950.

CARNELUTTI, Francesco. **Verdade, dúvida e certeza.** *Rivista di diritto processuale, Padova: Cedam,* 1965, vol. XX, p, 4 – 9. Tradução do Prof. Dr. Eduardo Cambi, publicada na Folha Acadêmica, n. 116, a. LIX, p. 5, 1997.

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

CASARA, Rubens R. R. **Mitologia processual penal.** São Paulo: Saraiva, 2015.

CASARA, Rubens R. R. **Processo penal do espetáculo: ensaios sobre o poder penal, a dogmática e o autoritarismo na sociedade brasileira.** 1ª ed. Florianópolis: Empório do Direito, 2015.

CASARA, Rubens R. R. **Estado pós-democrático: neo-obscurantismo.** 2 ed. Rio de Janeiro: Civilização Brasileira, 2017.

CASTELLS, Manuel. **A galáxia da internet: reflexões sobre a internet, os negócios e a sociedade.** Rio de Janeiro: Jorge Zahar Ed., 2003.

CASTELLS, Manuel. **A Sociedade em rede.** Vol. 1. 8ª ed. rev. e ampl. Tradução: Roneide Venâncio Majer. Editora: Paz e Terra. São Paulo, 2005. p, 67.

CONSELHO DA EUROPA. Tribunal Europeu dos Direitos do Homem. CEDH, **Convenção Europeia de Direitos do Homem**, Disponível em: https://www.echr.coe.int/Documents/Convention_POR.pdf. Acesso em out 2018.

CHAMAYOU, Grégore. **Teoria do drone.** São Paulo: Cosac Naify. Coleção Exit. 2015.

CHIRINO SANCHEZ, Alfredo. *Las tecnologias de la informacion y el processo penal: análisis de uns crisis anunciada.* ***Revista de ciências penales de Costa Rica*.** Rep. Fed. de Alemania 6 (1982): 275.

CHIRINO SANCHEZ, Alfredo. ***Proteccion de datos y moderno processo penal aspectos constitucionales y legales.*** *Conferencia presentada en el Seminario "Nuevo Ministério Público y Crisis de la Justicia Penal", que se celebró em la Ciudad de Buenos Aires, Argentina, auspiciado por la Procuraduría General de la Nación, los días 14 y 15 de diciembre de* 1998.

CHOUKR, Fauzi Hassan. **Garantias constitucionais na investigação criminal.** 3ª ed. Revista, ampliada e atualizada. Rio de Janeiro: Editora Lumen Juris, 2006.

COLAIOCCO, Sergio. ***Nuovi mezzi di ricerca della prova: l'utilizzao dei programmi spia.*** Orientamenti: Archivo penale. 2014, n.1.

CONTI, Carlotta; TORRE, Marco. ***Spionaggio informatico nell'ambito dei social network*.** In: (a cura di) SCALFATI, Adolfo. *Le indagini atipiche.* G. Giappichelli Editore. Torino. 2014.

CORDERO, Franco. ***Procedimiento Penal* Tomo I.** Editorial Temis S. A. Sanfa Fé de Bogotá – Colombia, 2000

CORDERO, Franco. ***Procedimiento penal* Tomo II.** Editorial Temis S. A. Sanfa Fé de Bogotá – Colombia, 2000

CORDERO, Franco. ***Tre studi sulle prove penali.*** Milano: Dott. A. Giuffrè Editore, 1963.

COSIC, Jasmin; BACA, Miroslav. ***(Im)Proving Chain of Custody and Digital Evidence Integrity with Time Stamp*.** 1226 - 1230. 10.13140/RG.2.1.1336.0725. 2010. p, 2. Disponível em: https://www.researchgate.net/publication/224163003_Improving_chain_of_custody_and_digital_evidence_integrity_with_time_stamp. Acesso em set 2018.

COSIC, Jasmin; BACA, Miroslav. ***Do We Have Full Control Over Integrity in Digital Evidence Life Cycle?*** Proceedings of the ITI 2010 32nd Int. Conf. on Information Technology Interfaces, June 21-24, 2010, Cavtat, Croatia.

COSIC, Jasmin; COSIC, Zoran. ***Chain of custody and life cycle of digital evidence.*** Computer Technology and Application 3 (2012) 126-129.

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

COUTINHO, Jacinto Nelson de Miranda. **Por que sustentar a democracia do sistema processual penal brasileiro?** *In: In*: SILVEIRA, Marco Aurélio Nunes da; DE PAULA, Leonardo Costa (org). Observações sobre os sistemas processuais penais: escritos do Prof. Jacinto Nelson de Miranda Coutinho Vol. 1. Curitiba: Observatório da mentalidade inquisitória, 2018.

COUTINHO, Jacinto Nelson de Miranda. **Efetividade do Processo Penal e Golpe de Cena: um problema às reformas processuais no Brasil.** *In*: SILVEIRA, Marco Aurélio Nunes da; DE PAULA, Leonardo Costa (org). Observações sobre os sistemas processuais penais: escritos do Prof. Jacinto Nelson de Miranda Coutinho Vol. 1. Curitiba: Observatório da mentalidade inquisitória, 2018.

COUTINHO, Jacinto Nelson de Miranda. **Sonhocídio: estragos neoliberais no ensaio do direito ou "la busqueda del banquete perdido", como diria Enrique Marí.** Revista Crítica Jurídica – Nº 21. Jul – Dez/2002.

CUERDA ARNAU, Mª Luisa. ***Intervenciones prospectivas y secreto de las comunicaciones. Cuestiones pendientes.*** In: GONZALEZ CUSSAC, José Luis; CUERDA ARNAU, María Luisa (Dir.); FERNANDEZ HERNANDEZ, Antonio (Coord). ***Nuevas amenazas a la seguridade nacional: terrorismo, criminalidad organizada y tecnologias de la información y la comunicación.*** Tirant lo Blanch, Valencia, 2013.

CUNHA MARTINS, Rui. **O ponto cego do direito.** 3 ed. São Paulo: Atlas, 2013.

DANIELE, Marcelo. ***Contrasto al terrorismo e captatori informatici.*** Revista di Diritto Processuale. Marzo – Aprile, 2017.

DANIELE, Marcelo. ***La prova digitale nel processo penale.*** Rivista di Diritto Processuale Anno LXVI (Seconda Serie) – n. 2. Marzo – Aprile, 2011.

DARDOT, Pierre; LAVAL, Christian. **A nova razão do mundo: ensaio sobre a sociedade neoliberal.** 1 ed. São Paulo: Boi tempo, 2016.

DELEUZE, Gilles e GUATTARI, Félix. **Mil platôs – capitalismo e esquizofrenia, vol. 1**. Rio de Janeiro: Ed. 34, 1995.

DELEUZE, Gilles. **Conversações, 1972 - 1990.** São Paulo: Ed. 34, 1992.

DELEUZE, Gilles. **O atual e o virtual**. *In:* ALLIEZ, Éric. **Deleuze filosofia virtual.** São Paulo: Ed; 34, 1996.

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

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

DOMINIONI, Oreste. ***La prova penale scientifica: gii strumenti scientifico-tecnici nuovi o controversi e di elevata specializzazione.*** Milano: Giuffrè Editore, 2005.

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

ESPANHA, ***Constitución Española***, artículo 18.4 - *La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.* Disponível em: https://www.boe.es/buscar/doc.php?id=BOE-A-1978-31229. Acesso em nov 2018.

ESPANHA, Supremo Tribunal Spanhol **STS 329/2016, 20 de Abril de 2016,** Número do Recurso: 1789/2015. Disponível em: https://supremo.vlex.es/vid/637465649. Acesso em nov 2018.

ESPANHA. *BOE* Núm. 239. Martes 6 de octubre de 2015. Sec I. Pág. 90192. Disponível em: https://www.boe.es/boe/dias/2015/10/06/pdfs/BOE-A-2015-10725.pdf Acesso em out 2018.

ESPANHA. ***Real decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal.*** *Ministerio de Gracia y Justicia.* <BOE> núm. 260, de 17 de septiembre de 1882. Referencia: BOE-A-1882-6036. Disponível em:

https://www.boe.es/buscar/pdf/1882/BOE-A-1882-6036-consolidado.pdf. Acesso em: 25 mai. 18.

ESTADOS UNIDOS DA AMERICA, ***ESTADOS UNIDOS, v. Nicodemo S. SCARFO,* et al.** Ação Criminal No. 00-404 (NHP). **180 F. Supp. 2d 572 (2001). Tribunal Distrital dos Estados Unidos, D. New Jersey.** 26 de dezembro de 2001. Disponível em: https://law.justia.com/cases/federal/district-courts/FSupp2/180/572/2475159/. Acesso em out 2018.

ESTADOS UNIDOS DA AMÉRICA. *Federal Rules of Criminal Procedure.* TITLE VIII. SUPPLEMENTARY AND SPECIAL PROCEEDINGS. *Rule 41. Search and Seizure* Disponível em: https://www.law.cornell.edu/rules/frcrmp/rule_41. Acesso nov 2018.

ESTADOS UNIDOS DA AMÉRICA. ***United States District Court Southern District Of Texas Houston Division***. CASE NO. H-13-234M. p, 5.

ESTADOS UNIDOS DA AMÉRICA, *United State of America vs. Jorge Ortiz Oliva.* No. 10-30126, D.C. No.3:07-cr-00050-BR-1. July, 20, 2012. p, 8375. Disponível em: http://cdn.ca9.uscourts.gov/datastore/opinions/2012/07/20/10-30126.pdf. Acesso 30 set 2018.

ESTADOS UNIDOS DA AMÉRICA, *United State of America vs. The company*. *In re: In the matter of the application of the United States, for an order authorizing the roving interception of oral communications.* No. 02-15635. D.C. No. CV-01-01495-LDG Opinion. November, 18, 2003. Disponível em: https://www.steptoe.com/images/content/3/7/v1/374/629.pdf. Acesso em 02 out, 2018.

ESTADOS UNIDOS DA AMÉRICA, *United States of America Vs. John Tomero, et al. Defendants.* No. S206Crim.0008(LAK). 462 F.supp.2d565(2006), November, 27, 2006. Disponível em: https://www.leagle.com/decision/20061027462fsupp2d5651976. Acesso em 01 out, 2018.

ESTADOS UNIDOS DA AMÉRICA. ***United States District Court for the District of Colorado***. Case 1:12-sw-05685-KMT Document 7 Filed 12/11/12 USDC Colorado. Disponível em; https://pt.scribd.com/document/189641401/Colorado-NIT-Doc-7. Acesso em nov 2018.

ESTADOS UNIDOS DA AMÉRICA. ***United States District Court Southern District Of Texas Houston Division***. *In re warrant to search a target computer at premises unknown*. CASE NO. H-13-234M. Document 3 Filed in TXSD on 04/22/13. Disponível em: http://pt.scribd.com/doc/137842124/texas-order-denying-warrant. Acesso em no 2018.

FARLEY, Ryan; WANG, Xinyuan. ***Roving Bugnet: Distributed Surveillance Threat and mitigation.*** *Comput. Security*, vol. 29, no. 5, pp. 592-602, 2010. Disponível em: https://pdfs.semanticscholar.org/3ce7/f7d7b852fdf82876887bc01ca51b9a462284.pdf. Acesso em 30 set 2018.

FAZZALARI, Hélio. **Instituições de Direito Processual**. 1ª ed. Campinas- SP: Bookseller Editora e Distribuidora. 2006.

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

FERRER BELTRAN, Jordi. ***Motivacion y racionalidad de la prueba.*** Editora y Libreria Jurídica Grijley. 1 ed., 2016.

FOUCAULT, Michel. **Em defesa da sociedade: curso no Collège de France (1975-1976).** São Paulo: Martins Pontes, 1999.

FOUCAULT, Michel. **História da sexualidade I: A vontade do saber.** 4ª ed. Rio de Janeiro/São Paulo: Paz e Terra, 2017.

FOUCAULT, Michel. **Microfísica do poder.** 19ª ed. Rio de Janeiro: Edições Graal, 1979.

FOUCAULT, Michel. **Segurança, território e população: curso dado no Collége de France (1977-1978).** São Paulo: Martins Fontes, 2008.

FOUCAULT, Michel. **Vigiar e punir: nascimento da prisão.** Petrópolis: Vozes, 1987.

FRANÇA, Leandro Ayres. **Cibercriminologias.** *In:* FRANÇA, L. A; CARLEN, Pat. **Criminologias Alternativas.** Porto alegre: Canal Ciências Criminais, 2017.

GAMMAROTA, Antonio. ***Informatica forense e processo penale: la prova digitale tra innovazione normativa e incertezze giurisprudenziali.*** *Università di Bologna. Dottorato di ricerca in Diritto e nuove tecnologie.* 2016.

GARAPON, Antoine. **Bem julgar: ensaio sobre o ritual judiciário.** Coleção: direito e direitos do homem. Instituto Piaget: Lisboa, 1997.

GARIBALDI, Gustavo E. L. ***Las modernas tecnologías de control y de investigación del delito: su incidencia en el derecho penal y los principios constitucionales.*** 1ª ed. Buenos Aires: Ad-Hoc, 2010.

GASCON ABELLAN, Marina. *Prueba Científica: mitos y paradigmas.* ***Anales de la Cátedra Francisco Suárez,*** 44 (2010), pp. 81 – 103.

GAUER, Ruth M. Chittó. **Falar em tempo, viver o tempo!** *In*: GAUER, Ruth (coord.); SILVA, Mozart Linhares da (org). Tempo/História. Porto Alegre: EDIPUCRS, 1998.

GEORGITON, Peter J. ***The FBI's Carnivore: How Federal Agentes may be viewing your personal e-mail and why there is nothing you can do about it.*** Ohio State Lawjournal. Vol. 62. p, 1834. Disponível em: https://kb.osu.edu/bitstream/handle/1811/70480/OSLJ_V62N6_1831.pdf. Acesso em nov 2018.

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

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

GIACOMOLLI, Nereu. **Reformas (?) do processo penal: considerações críticas.** Editora Lumen Juris: Rio de Janeiro, 2008.

GIMENO SENDRA, Vicente; MORENO CATENA, Victor; CORTÉS DOMÍNGEZ, Valentín. ***Derecho Procesal Penal*.** 3ª Edición 1999. Editorial COLEX, 1999.

GIOVA, Giuliano. ***Improving Chain of custody in forensic investigation of eletronic digital systems.*** IJCSNS International Journal of Computer Science and Network Security, VOL. 11 No. 1, January 2011.

GLOECKNER, Ricardo Jacobsen e AMARAL, Augusto Jobim do. **Criminologia e(m) crítica**. Curitiba: Editora Champagnat – PUC-PR; Porto Alegre, RS: Edipucrs, 2013.

GLOECKNER, Ricardo Jacobsen. **Autoritarismo e processo penal: uma genealogia das ideias autoritárias no processo penal brasileiro.** Vol. 1, 1ª ed. Florianópolis: Tirant lo blanch, 2018.

GLOECKNER, Ricardo Jacobsen. **Nulidades no processo penal: introdução principiológica à teoria do ato processual irregular.** 2ª ed., Editora Juspodivm. 2015.

GLOECKNER, Ricardo Jacobsen. **Risco e processo penal: uma análise a partir dos direitos fundamentais do acusado.** Editora: JusPodivm. 2015.

GOLDSCHMIDT, James. ***Principios generales del proceso Vol. II*.** Ediciones Jurídicas Europa-America, Buenos Aires, 1961.

GOMES FILHO, Antônio Magalhães. **Direito à prova no processo penal.** São Paulo: Editora Revista dos Tribunais, 1997.

GOMES FILHO, Antônio Magalhães. **Limites ao compartilhamento de provas no processo penal.** Revista Brasileira de Ciências Criminais. RBCCRIM VOL. 122 (Agosto 2016).

GOMES FILHO, Antônio Magalhães. **Notas sobre a terminologia da prova (reflexos no processo penal brasileiro).** *In*: YARSHELL, Flavio Luiz; MORAES, Maurício Zanoide de. (Coord.). **Estudos em homenagem à professora Ada Pellegrini Grinover.** 1 ed. São Paulo: DPJ Editora, 2005. p, 309.

GOMES FILHO, Antônio Magalhães. **Provas.** *In:* MOURA, Maria Thereza Rocha de Assis. **As reformas no processo penal: as novas leis de 2008 e os projetos de reforma.** São Paulo: Editora Revista dos Tribunais, 2008.

GOMEZ COLOMER, Juan-Luis. *In:* MONTERO AROCA, Juan *et* all. ***Derecho Jurisdiccional: III Proceso Penal.*** 10ª Edición. Valencia: Tirant lo Bllanch. 2001. p, 118.

GONZALEZ LAGIER, Daniel. ***Hechos y argumentos (racionalidad epistemológica y prueba de los hechos en el proceso penal* (I)**. *Jueces para la democracia. Madrid: vol.* 46, marco/2003, pp. 17-26**.**

GOZAINI, Osvaldo A. ***Pruebas científicas y verdad: el mito del razonamiento incuestionable..*** Disponível em: http://www.derecho.uba.ar/institucional/deinteres/2015-gozaini-pruebas-cientificas-y-verdad.pdf. Acesso em jun 2018.

GRECO, Luis. **As regras por trás da exceção – reflexões sobre tortura nos chamados "casos de bomba-relógio".** R. Jurídica, Curitiba, n. 23, Temática n. 7, p. 229-264, 2009-2.

GRECO, Luis. **Introdução – o inviolável e o intocável no direito processual penal.** In: WOLTER, Jürgen. **O inviolável e o intocável no direito processual penal: reflexões sobre dignidade humana, proibições de prova, proteção de dados (e separação informacional de poderes) diante da persecução penal.** Luis Greco (org.). 1ª ed. São Paulo: Marcial Pons, 2018.

GRINOVER, Ada Pellegrini. **Liberdades públicas e processo penal: as interceptações telefônicas.** 2ª edição atualizada. São Paulo: Editora Revista dos tribunais, 1982.
HAACK, Susan. ***El probabilismo jurídico: una disensión epistemológica.*** *In*: VAZQUEZ, Carmen. *Estándares de prueba y prueba científica: ensayos de epistemologia jurídica.* Marcial Pons, 2013.

HAN, Byung-Chul. **A sociedade da transparência.** Petrópolis, RJ: Vozes, 2017.

HAN, Byung-Chul. ***El agonia del Eros.*** Herder Editorial, S. L. 2014.

HAN, Byung-Chul. **No Enxame: reflexões sobre o digital.** Lisboa: RelógioD'Água, 2016.

HAN, Byung-Chul. **Psicopolítica: neoliberalismo e novas técnicas de poder.** Antropos. Lisboa: Relógio D'água Editores. 2015. p, 31

HAN, Byung-Chul. **Topologia da violência.** Petrópolis, Rio de Janeiro: Vozes, 2017.

HARDT, Michael e NEGRI, Antonio. **A produção biopolítica.** *In:* PARENTE, André (Org). **Tramas da rede: novas dimensões filosóficas, estéticas e políticas da comunicação.** Porto Alegre: Sulinas, 2013.

HASSEMER, Winfried. ***El destino de los derechos del ciudadano en un derecho penal eficaz.*** *Estudios Penales y Criminológicos, vol. XV (1992). Cursos e Congresos nº 71 Servizo de Publicacións da Universidade de Santiago de Compostela.* ISBN 84-7191-866-8, pp. 182-198.

HASSEMER, Winfried. ***Es la autodeterminación todavia actua?*** Revista Internacional de Pensamiento Político, II Época. Vol 3, 2007.

HASSEMER, Winfried. ***Proceso penal sin protección de datos?*.** La insostenible situación del derecho penal, ISBN 84-8151-967-7, págs. 103-128. 2000.

HASSEMER, Winfried; CHIRINO SANCHEZ, Alfredo. ***El derecho a la autodeterminación informativa y los retos del procesamiento automatizado de datos personales.*** Editores del Puerto: Buenos Aires, 1997.

HAWKING, Stephen. **O universo numa casca de noz.** 1 ed. Rio de Janeiro: Intrínseca, 2016.

HOFFMAN-RIEM, Wolfgang. ***Innovaciones en la Jurisprudencia del Tribunal Constitucional Alemán, a Propósito de la Garantía de los Derechos Fundamentales en Respuesta a los Cambios que Conducen a la Sociedad de la Información*.** RDU, Porto Alegre, Volume 12, n. 64, 2015, 40-61, jul-ago 2015.

ITALIA, ***Repubblica Italiana In Nome Del Popolo Italiano.*** *La Corte Suprema di Cassazione. Sezione Quinta Penal*. Cass. Pen., sez. V, 29 abril 2010, n. 16556, Virruso. Disponível em: http://www.penale.it/stampa.asp?idpag=1228. Acesso em out 2018.

ITALIA, ***Codice di Procedura Penale.*** D.P.R. 22 de settembre 1988, n. 477. Disponível em: https://www.brocardi.it/codice-di-procedura-penale/. Acesso em out 2018.

ITALIA, **Constituição da República Italiana**. *Costituzione Italiana edizione in língua portoghese.* Senato della Repubblica. 2018. p, 11. Disponível em: https://www.senato.it/application/xmanager/projects/leg18/file/repository/relazioni/libreria/novita/XVII/COST_PORTOGHESE.pdf. Acesso em 04 set, 2018.

ITALIA, ***Repubblica Italiana In Nome Del Popolo Italiano La Corte Suprema Di Cassazione***. Sez. 6, Sentenza n. 27100 del 2015, MUSUMECI. Disponível em: http://questionegiustizia.it/doc/sentenza-27100-2015.pdf. Acesso em out 2018.

KASTRUP, Virgínia. **A rede: uma figura empírica da ontologia do presente.** *In:* PARENTE, André (Org). Tramas da rede: novas dimensões filosóficas, estéticas e políticas da comunicação. Porto Alegre: Sulina, 2013.

KERCKHOVE, Derrick de. **A pele da cultura: uma investigação sobre a nova realidade electrónica.** São Paulo: Relógio D'Água Editores, 1997.

KERR, Orin S. ***Executing warrants for digital evidence: the case for use restrictions on nonresponsive data.*** Texas Tech School of Law Criminal Law Symposium, The Fourth Amendment in the 21st Century, on April 17, 2015.

LATOUR, Bruno. **Jamais fomos modernos: ensaios de antropologia simétrica.** Rio de Janeiro: Ed. 34. 1994.

LEVY, Pierre. **Cibercultura**. São Paulo: Ed. 34. 1999.

LEVY, Pierre. **O que é virtual?** São Paulo: Ed. 34, 1996.

LIM, Kyung-Soo; GYU LEE, Deok; WOOK HAN, Jong. ***A New Proposal for a Digital Evidence Container for Security Convergence***. IEEE International Conference on Control System, Computing and Engineering. 2011.

LIPOVETSKY, Gilles. **Os tempos hipermodernos.** São Paulo: Editora Barcarolla, 2004.

LOPES JR, Aury. **Fundamentos do processo penal: introdução crítica.** 2ª ed. São Paulo; Saraiva, 2016.

LOPES JR. Aury, GLOECKNER, Ricardo Jacobsen. **Investigação preliminar no processo penal.** 6 ed. rev., atual e ampl. São Paulo: Saraiva, 2014.

LOPES JR. Aury. **(Des)Velando o Risco e o Tempo no Processo Penal.** *In:* GAUER, Ruth M. Chittó (Org). **A qualidade do tempo: para além das aparências históricas.** Rio de Janeiro: Editora Lumen Juris, 2004. p. 139 - 177.

LOPES JR. Aury. **Direito processual penal.** 11. ed. São Paulo: Saraiva, 2014.

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

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

LUND, Paul. ***An investigator's approach to digital evidence.*** *In: Digital evidence and Electronic Signature Law Review*, Vol. 6. Pario Communications Limited, 2009.

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

MAIER, Julio B. ***Derecho procesal penal Tomo III: parte general: actos procesale.*** 1 ed. Ciudad Autónoma de Buenos Aires: Del puerto, 2011.

MARCOLINI, Stefano. ***Le cosiddette perquisizioni on line (o perquisizioni elettroniche).*** In: a cura di) RUGGIERI, Francesca; PICOTTI, Lorenzo. *Nuove tendenze della giustizia penale di fronte alla criminalità informática Aspetti sostanziali e processuali.* G. Giappichelli Editore – Torino. 2010.

MARQUES NETO, Agostinho Ramalho. **Neoliberalismo e gozo.** Conferência proferida sob o título *A Banalização da Lei: com que Direito Podemos Contar Hoje?*, por ocasião do Congresso Brasileiro de Direito e Psicanálise, sob o tema "A Lei em Tempos Sombrios", promovido pela Escola Lacaniana de Psicanálise de Vitória e pela Faculdade de Vitória. Vitória (ES), 29 de maio de 2008.

MARQUES NETO, Agostinho Ramalho. **Neoliberalismo: o declínio do Direito.** In: RUBIO, David Sanchez; FLORES, Joaquin Herrera; CARVALHO, Salo de. Direitos humanos e globalização: fundamentos e possibilidades desde a teoria crítica. 2. Ed. Porto Alegre: EDIPUCRS, 2010.

MARQUES NETO, Agostinho Ramalho. **O Poder Judiciário na Perspectiva da Sociedade Democrática: O Juiz Cidadão.** Texto publicado originalmente: Revista ANAMATRA. Órgão Oficial da Associação Nacional dos Magistrados do Trabalho. Ano VI, nº 21, p. 30 – 50. Brasília: ANAMATRA, outubro a dezembro de 1994.

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

MCCULLAGH, Declan. ***FBI taps cell phone mic as eavesdropping* tool.** *Agency used novel surveillance technique on alleged Mafioso: activating his cell phone's microfone and the just listennig.* December 4, 2006. Disponível em: https://www.cnet.com/news/fbi-taps-cell-phone-mic-as-eavesdropping-tool/. Acesso em 24 Set 2018.

MELE, Anderson. ***Trojan horse e limiti dell'intercettazione ambientale.*** *Diritto Penale. Fondatore Francesco Brugaletta.* 2017.

MENDES, Carlos Hélder. **Do sentimento de impunidade à banalização da extrema ratio: uma análise discursiva das fundamentações dos decretos de prisão preventiva nas varas criminais de São Luís – MA.** 1ª ed. Florianópolis: Empório do Direito Academia, 2016.

MENDES, Gilmar; BRANCO, Paulo Gustavo Gonet. **Curso de Direito Constitucional.** 10 ed. rev. e atual. São Paulo: Saraiva, 2015.

MENDES, Gilmar; PINHEIRO, Jurandi Borges. **Interceptações e privacidade: novas tecnologias e a Constituição.** In: MENDES, G. F; SARLET, I. W; COELHO, A. Z. P. **Direito, inovação e tecnologia.** São Paulo: Saraiva, 2015.

MENKE, Fabiano. **A proteção de dados e o novo direito fundamental à garantia da confiadencialidade e da integridade dos sistemas técnico-informacionais no direito alemão.** In: MENDES, Gilmar F.; SARLET, Ingo W.; COELHO, Alexandre Z. P. **Direito, inovação e tecnologia.** São Paulo: Saraiva, 2015.

MONTOYA, Mario Daniel. ***Informantes y técnicas de investigación encubiertas: análisis Constitucional y Procesal Penal***. Buenos Aires: Ad-Hoc, 1998.

MORAES, Maurício Zanoide de. **Presunção de inocência no processo penal brasileiro: análise de sua estrutura normativa para a elaboração legislativa e para a decisão judicial.** Rio de Janeiro: Lumen Juris, 2012.

MUNOZ CONDE, Francisco. ***Prueba prohibida y valoración de las grabaciones audiovisuales en el proceso penal.*** Revista Penal, Nº 14, 2004.

MURILLO DE LA CUEVA, Pablo Lucas; PIÑAR MAÑAS, José Luis. ***El derecho a la autodeterminacón informativa.*** Fundación Coloquio Jurídico Europeo, Madrid. 2009.

ODELL, Mark. ***Use of mobile helped police keep tabs on suspect and brother.*** Financial Times. Mark Odell, Telecoms Correspondent, *august 1, 2005.* Disponível em: https://www.ft.com/content/7166b8a2-02cb-11da-84e5-00000e2511c8. Acesso em 24 set 2018.

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

ORTIZ PRADILLO, Juan Carlos. ***Informática y derechos fundamentales: hacia un derecho fundamental a la confidencialidad e integridad de los equipos informáticos.*** *In:* BAUZÁ

REILLY, Marcelo; BUENO DE MATA, Federico (Coord.). *El derecho en la sociedad telemática: estúdios en homenaje a Valentín Carrascosa López*. 2012.

OST, François. **O tempo do direito.** Bauru, SP: Edusc, 2005.

PEREA, Inmaculada Lopez-Barajas. ***Nuevas tecnologías aplicadas a la investigación penal: el registro de equipos informáticos***. Revista de los Estudios de Derecho y Ciencia Política. IDP N.º 24 (Febrero, 2017) I ISSN 1699-8154.

PEREZ LUÑO, Antonio Enrique. ***Los derechos humanos en la sociedad tecnológica*.** In: LOSANO, Mario G; PEREZ LUÑO, Antonio Enrique; GUERRERO MATEUS, Mª Fernanda. ***Liberdad informática y leyes de proteccion de datos personales.*** Cuadernos y Debates. Centro de estúdios constitucionales. Madrid, 1989.

PRADO, Geraldo. **A produção da prova penal e as novas tecnologias: o caso brasileiro.** 2015. Disponível em: http://emporiododireito.com.br/a-producaotheo-da-prova-penal-e-as-novas-tecnologias-o-caso-brasileiro-por-geraldo-prado/. Acesso em jun 2017.

PRADO, Geraldo. **Limites às interceptações telefônicas e a jurisprudência do Superior Tribunal de Justiça.** 2ª ed. Editora Lumen Juris, 2006.

PRADO, Geraldo. **O dever de fundamentação reforçada das decisões no âmbito das medidas cautelares.** *In:* GRINOVER, Ada Pellegrini, *et all.* Verdade e prova no processo penal: Estudos em homenagem ao professor Michele Taruffo. Coordenador Flávio Cardoso Pereira. 1 ed. Brasília, DF: Gazeta Jurídica,2016.

PRADO, Geraldo. **Prova penal e sistema de controles epistêmicos.** 1 ed. São Paulo: Marcial Pons, 2014. p, 41.

PRADO, Geraldo. **Sistema acusatório: a conformidade constitucional das leis processuais penais.** 3ª ed. Editora Lumen juris: Rio de Janeiro, 2005.

PRAYUDI, Yudi; SN, Azhari. ***Digital chain of custody: state of the art.*** International Journal of Computer Applications (0975 – 8887) Volume 114, Nº 5, March 2015.

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

QUEVEDO GONZALEZ, Josefina. ***Derechos y libertades que resulta afectados.*** In: *Investigación y prueba em el proceso penal.* Madrid: Editorial Jurídica Sepín, 2017.

QUEVEDO GONZALEZ, Josefina. ***Técnicas de investigación de los ciberdelitos.*** In: *Investigación y prueva del ciberdelito.* Madrid: Editorial Jurídica Sepín, 2017.

RAMALHO, David Silva. **A recolha de prova penal em sistemas de computação em nuvem.** Revista de Direito Intelectual n. 02, 2014.

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

RITTER, Ruiz. **Imparcialidade No Processo Penal: Reflexões a partir da Teoria da Dissonância Cognitiva.** Porto Alegre, PUCRS. Dissertação de Mestrado, 2016.

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

RODOTA, Stefano. ***Cual derecho para el nuevo mundo?*** Revista de Derecho Privado, núm. 9, julio-diciembre, 2005, pp. 5-20. Universidad Externado de Colombia, Bogotá, Colombia.

RODOTA, Stefano. ***El derecho a tener derechos.*** Editorial Trotta, 2014.

ROMERO SANCHEZ, Angelica. **Proceso penal, privacidad y autodeterminación informativa en la persecución penal de la delincuencia organizada. Un análisis desde la perspectiva del derecho procesal penal alemán.** In: *Revista Criminalidad*, 57 (2): 319-333. 2015.

ROSA, Alexandre Morais da e MARCELLINO JR, Julio Cesar. **O processo eficiente na lógica econômica [recurso eletrônico]: desenvolvimento, aceleração e direitos fundamentais.** Itajaí: UNIVALI; FAPESC, 2012.

ROSA, Alexandre Morais da; AMARAL, Augusto Jobim do. **Cultura da punição: a ostentação do horror.** 2ª ed. Florianópolis: Empório do Direito, 2015.

ROSA, Alexandre Morais da ; LOPES JR., Aury. Limite Penal: Critérios de validade para vasculhar o celular – *whatsapp* – do preso. **Revista Consultor** Jurídico. 25 Mai. 2018. Disponível em: https://www.conjur.com.br/2018-mai-25/limite-penal-criterios-validade-vasculhar-celular-whatsapp-preso

ROSA, Alexandre Morais da; LOPES JR., Aury. Limite Penal: Vasculhar aparelho celular só é possível com autorização judicial. **Revista Consultor Jurídico.** 23 de fev. 2018. Disponível em: https://www.conjur.com.br/2018-fev-23/limite-penal-vasculhar-aparelho-celular-somente-autorizacao-judicial

ROXIN, Claus. ***Pasado, presente y futuro del derecho procesal penal.*** 1ªed. 1ªreimp. Santa Fé: Rubinzal Culzoni, 2009.

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

SAAD, Marta. **Exercício do direito de defesa no inquérito policial.** *In:* Boletim do IBCCRIM, nº 166, setembro de 2006.

SALT, Marcos G. ***Tecnológia informática: un nuevo desafío para el Derecho Procesal Penal?***. XXV Congreso Nacional de Derecho Procesal Penal, Rubinzal Editores, Argentina. Disponível em: https://drive.google.com/file/d/0BxHBGMLx4HZGbzhJQ0ozMFhYYXc/view. Acesso em jun 2018.

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

SAMPAIO, André Rocha. **A onipresença processual dos atos de investigação como sintoma biopolítico.** Tese (Doutorado em Ciências Criminais) Faculdade de Direito, Pontifícia Universidade Católica do Rio Grande do Sul. 2015.

SAMPAIO, André Rocha. **Profanando o dispositivo "inquérito policial" e seu ritual de produção de verdades**. Revista Brasileira de Ciências Criminais. Vol 134/2017. p. 351 – 383. Ago/2017.

SARLET, Ingo. **A eficácia dos direitos fundamentais: uma teoria geral dos direitos fundamentais na perspectiva constitucional.** 12 ed. rev. atual e ampl. Porto Alegre: Livraria do Advogado Editora, 2015.

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

SENTIS MELENDO, Santiago. ***La prueba: los grandes temas del derecho probatorio.*** Ediciones Juridicas Europa-America, Buenos Aires, 1979.

SERRANI, Alessandro. ***Sorveglianza satellitare GPS: un'attività investigativa ancora in cerca di garanzie.*** Archivio Penale 2013, n. 3.

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

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

SOARES, Gustavo Torres. **Investigação criminal e inovações técnicas e tecnológicas.** Belo Horizonte: Editora D'Plácido, 2017.

TESTAGUZZA, Alessandra. ***Exitus acta probat trojan di Stato: la composizione di un conflitto*****.** *Orientamenti*. *Archivio Penale,* 2016, n. 2.

TESTAGUZZA, Alessandra. ***Il sistemi di controlo remoto: fra normativa e prassi.*** Mezzi di prova. Diritto penale e processo 6/2014

TESTAGUZZA, Alessandra. ***Intercettazione telefônica 2. Trojan.*** *Diritto on line*, 2017. Disponível em: http://www.treccani.it/enciclopedia/intercettazione-telefonica-2-trojan_(Diritto-on-line). Acesso em Set/2018.

TESTAGUZZA, Alessandra. ***Schizofrenia itálica (prevenzione dei fenomeni terroristici e hipertrofia intercettiva)*****.** L'opinione. *Archivio Penale, 2015.* N.3. p, 3. Acesso em jun 2018. Disponível em: http://www.archiviopenale.it/File/DownloadArticolo?codice=59e97fba-e5eb-4b35-8fad-c8115d4d03bd&idarticolo=9304.

TORNAGHI, Hélio. **Compêndio de processo penal: tomo II.** Rio de Janeiro, 1967.

TORRE, Marco. ***Indagini informatiche e proceso penale.*** *Università degli studi Firenze. Dottorado di ricerca in scienze giuridiche. Anni 2012/2015*.

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

TROGU, Mauro. ***Sorveglianza e "perquisizione" on-line su materiale informatico.*** In: (a cura di) SCALFATI, Adolfo. *Le indagini atipiche.* G. Giappichelli Editore. Torino. 2014.

VACIAGO, Giuseppe e RAMALHO, David Silva. ***Online searches and online surveillance: the use of trojans and other types of malware as means of obtaining evidence in criminal proceedings.*** *Digital evidence and eletronic signature Law Review,* 13 (2016).

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

VAZ, Denise Provasi. **Provas digitais no processo penal: formulação do conceito, definição das características e sistematização do procedimento probatório.** Tese de doutorado. Faculdade de Direito da Universidade de São Paulo. São Paulo, 2012.

VAZQUEZ-ROJAS, Carmen. ***Sobre la cientificidad de la prueba científica en el proceso judicial.*** Anuário de Psicologia jurídica, vol. 24. pp. 65-73. Colégio Oficial de Psicólogos de Madrid, Madri. Espanha. enero-diciembre, 2014.

VEGAS TORRES, Jaime. ***Las medidas de investigación tecnológica*** *In:* CEDEÑO HERNAN, M. (Coord.). *Nuevas tecnologías y derechos fundamentales en el proceso.* Aranzadi, 2017.

VELASCO NUÑEZ, Eloy. ***Aseguramiento, custodia de la prueba tecnológica, análisis y valor.*** In: ***Delitos tecnológicos: definición, investigación y prueba em el proceso penal.*** Madrid. Editorial Jurídica Sepín, 2016.

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

VIRILIO, Paul. **A inércia polar.** Tradução de Ana Luísa Faria. Lisboa: Publicações Dom Quixote, 1993.

VIRILIO, Paul. ***El cibermundo, la política de lo peor*****.** Entrevista con Philippe Petit. *Traducion* Mónica Poole. Teorema, Madrid: Ediciones Catedra S.A, 1997.

VIRILIO, Paul. **O espaço crítico**. Rio de Janeiro: Ed. 34, 1993.

VIRILIO, Paul. **Velocidade e política.** São Paulo: Estação Liberdade, 1996.

WALKER, Cornell. ***Computer forensics: bringing the evidence to court***. Acesso em jun 2018. Disponível em: http://www.infosecwriters.com/text_resources/pdf/Computer_Forensics_to_Court.pdf.

WEISSBERG, Jean-Louis. **Paradoxos da teleinformática.** *In:* PARENTE, André (Org). Tramas da rede: novas dimensões filosóficas, estéticas e políticas da comunicação. Porto Alegre: Sulina, 2013.

WHITAKER, Reg. ***El fin de la privacidad.*** Buenos Aires: Paidós, 1999.

WOLTER, Jürgen. **O inviolável e o intocável no direito processual penal: reflexões sobre dignidade humana, proibições de prova, proteção de dados (e separação informacional de poderes) diante da persecução penal.** Luis Greco (org.). 1ª ed. São Paulo: Marcial Pons, 2018.

Pontifícia Universidade Católica do Rio Grande do Sul
Pró-Reitoria de Graduação
Av. Ipiranga, 6681 - Prédio 1 - 3º. andar
Porto Alegre - RS - Brasil
Fone: (51) 3320-3500 - Fax: (51) 3339-1564
E-mail: prograd@pucrs.br
Site: www.pucrs.br