13 – Esboço de Proposta sobre Dispositivo de Controle da Investigação Digital: O "Aspecto Dinâmico da Prova Digital" [287]

Draft Proposal on the Control Mechanism for Digital Investigation: The "Dynamic Aspect of Digital Evidence"

Geraldo Prado[288]

> Com referência a tal tipologia de atividade [investigação digital], podemos falar do 'aspecto estático' da prova informática ou da prova digital *off line*.
>
> A investigação digital oculta, por sua vez, representa o aspecto dinâmico da prova digital (prova digital *on line*) e a esse vai reconduzido, entre outros, o fenômeno do 'captor informático', cada vez mais usado pelos investigadores devido a imensa quantidade e qualidade de informação que pode ser extraída.
>
> Marco Torre[289]

RESUMO

O artigo apresenta os fundamentos de um esboço de tratamento legal relativamente aos cuidados visando a preservação da integridade,

[287] Artigo "Esboço de Proposta sobre Dispositivo de Controle da Investigação Digital: o 'Aspecto Dinâmico da Prova Digital'", elaborado para compor o Dossiê sobre Crime Organizado, publicado na Revista do Sistema Único de Segurança Pública (Revista SUSP) e organizado pela Secretaria Nacional de Segurança Pública do Ministério da Justiça e Segurança Pública (Senasp/MJSP). Na oportunidade, foram apresentados resultados parciais da pesquisa levada a cabo sobre o fenômeno da transnacionalidade do processo penal, tema abordado no contexto do Projeto de I&D Corpus Delicti – Estudos de Criminalidade Organizada Transnacional [Ratio Legis - Centro de Investigação e Desenvolvimento em Ciências Jurídicas da Universidade Autónoma de Lisboa - UAL].

[288] Doutor em Direito. Investigador do Ratio Legis - Centro de Investigação e Desenvolvimento em Ciências Jurídicas, da Universidade Autónoma de Lisboa, e professor visitante da Universidade Autônoma de Lisboa. Membro do Comité de Aconselhamento do Instituto de Direito Penal e Ciências Criminais da Faculdade de Direito da Universidade de Lisboa. Consultor Sênior Associado do Justicia LatinoAmerica – JusLat. Integra o Núcleo de Investigação Defensiva da Defensoria Pública do Estado do Rio de Janeiro - NIDEF. Consultor Jurídico. Ex-Professor Associado de Direito Processual Penal da Universidade Federal do Rio de Janeiro (UFRJ). Consultor Jurídico. Currículo Lattes disponível em: http://lattes.cnpq.br/0340918656718376.

[289] TORRE, Marco. Il captatore informatico: nuove tecnologie investigative e rispetto delle regole processuali. Milano: Giuffrè, 2017. p. 12. Marco Torre é doutor em direito penal pela Università di Firenze.

autenticidade e auditabilidade da prova digital obtida por meio de acesso remoto aos sistemas informáticos.

Palavras-chave: investigação digital; investigação intrusiva; acesso remoto a dispositivos digitais; prova *online*; controle judicial; cadeia de custódia.

ABSTRACT

The article presents the foundations of a draft legal framework regarding procedures to preserve the integrity, authenticity, and auditability of digital evidence obtained through remote access to computer systems.

Keywords: digital investigation; intrusive investigation; remote access to digital devices; online evidence; judicial control; chain of custody.

1. INTRODUÇÃO

É consensual que a criminalidade transnacional se beneficia, cada vez mais, de recursos derivados das modernas aplicações tecnológicas, que asseguram o resultado de crimes cometidos mesmo fora do ambiente cibernético. Além disso, tal criminalidade se vale desse ambiente para tornar especialmente difícil a apuração das infrações penais, assim como para evitar a reparação do dano causado por elas.[290]

Esperado, portanto, que as agências de investigação criminal igualmente recorram às aplicações tecnológicas para superar os obstáculos criados pelas práticas delituosas, o que deve ocorrer no marco da legalidade, em respeito aos direitos fundamentais em jogo (privacidade, intimidade, autodeterminação informativa, presunção de inocência, entre outros).

[290] SALT, Marcos. Allanamiento remoto: ¿un cambio de paradigma en el registro y secuestro de datos informáticos? In: DUPUY, Daniela (dir.); KIEFER, Mariana (coord.). Cibercrimen II. Buenos Aires-Montevideo: Editorial B de F, 2018. p. 152. Marcos Salt é diretor do programa de atualização em Cibercrimen y Evidencia Digital da pós-graduação da Facultad de Derecho da Universidad de Buenos Aires e professor adjunto de direito penal e processo penal da mesma faculdade. CURTOTTI, Donatella "Le operazioni digitali sotto copertura": l'agente provocatore e l'attività di contrasto. In: ATERNO, Stefano; CAJANI, Francesco; COSTABILE, Gerardo; CURTOTTI, Donatella (a cura di). Cyber Forensics e indagini digitali: manuale tecnico-giuridico e casi pratici. Torino: Giappichelli, 2021. p. 505. Donatella Curtotti é professora titular de direito processual penal e de criminalística e perícia digital da Università di Foggia.

As transformações sociais em um mundo híbrido, digital-analógico, alteram de maneira profunda a natureza das relações jurídicas, e essas mudanças reclamam uma nova postura de reconhecimento do poder digital, que perigosamente se acumula em mãos de determinadas agências estatais e de atores privados (corporações transnacionais), criando situações de risco a interesses vitais, a justificar, à luz de um constitucionalismo digital, que novos bens jurídicos sejam reconhecidos (domicílio digital, identidade digital, entorno digital, etc.).[291]

O ponto de equilíbrio entre esses legítimos interesses deve ser encontrado levando-se em conta a experiência concreta proporcionada pela vida digital que hoje em dia todos levamos, querendo ou não.

Este breve ensaio trata apenas de um ângulo dessa realidade: a "investigação digital intrusiva".[292]

A expressão é intencionalmente aberta, apesar de largamente empregada nos manuais estrangeiros de investigação e perícias digitais.[293]

Como consta da epígrafe, o texto se preocupa com as técnicas de "captura digital", isto é, com as provas digitais em um contexto de intervenção *online*. A expressão "captura digital" é ampla o suficiente para englobar desde as ações cautelares de apreensão e busca remotas em sistemas informáticos, como também aquelas caracteristicamente definidas como de vigilância eletrônica, quer por meio de um "agente infiltrado digital", quer por intermédio de *softwares* espiões.

---

[291] Ver: PRADO, Geraldo. Curso de Processo Penal: Tomo I - Fundamentos e Sistema. São Paulo: Marcial Pons, 2024. p. 71-73.

[292] CASEY, Eoghan; DAYWALT, Christopher; JOHNSTON, Andy. Intrusion Investigation. In: CASEY, Eoghan. (Ed.). Handbook of Digital Forensics and Investigation. Burlington: Elsevier Academic Press, 2010. p. 135-206.

[293] "A investigação de intrusão é um subconjunto especializado de investigação forense digital que é focado em determinar a natureza e a extensão total do acesso e uso não autorizados de um ou mais sistemas de computador." Tradução livre. No original: "Intrusion investigation is a specialized subset of digital forensic investigation that is focused on determining the nature and full extent of unauthorized access and usage of one or more computer systems". CASEY, Eoghan; DAYWALT, Christopher; JOHNSTON, Andy. Intrusion Investigation. In: CASEY, Eoghan. (Ed.). Handbook of Digital Forensics and Investigation. Burlington: Elsevier Academic Press, 2010. p. 135. Eoghan Casey é engenheiro pela University of California em Berkeley e mestre em Comunicação Educacional e Tecnologia pela New York University, além de professor na Johns Hopkins University Information Security Institute. Christopher Daywalt é mestre em network security pela Capitol College. Andy Johnston é desenvolvedor de software, programador e coordenador de segurança de TI na Universidade de Maryland, no condado de Baltimore.

O acesso remoto ao sistema digital visado pelos investigadores, de maneira oculta ou dissimulada e em caráter contínuo, é o elemento de base sobre o qual segue a reflexão acerca das condições de fiscalização das medidas de investigação, quer para assegurar que esse acesso contínuo não seja de índole preventiva ou prospectiva, quer para garantir a confiabilidade do material probatório que poderá ser empregado no juízo criminal pelas partes.

Essa última garantia converge com a razão de ser da cadeia de custódia das provas digitais, mas não é limitada por ela, cumprindo avaliar que papel o juiz de garantias pode vir a cumprir no mencionado contexto.

Trata-se de um esboço, pois que limitado pelas nuances do ensaio. Questões como transnacionalidade das providências cautelares ou de sua execução, aspectos relacionados à criptografia e desencriptação de dados ou mesmo problemas referentes às cautelares patrimoniais que envolvem criptomoedas não são examinados.

2. UMA TIPOLOGIA POSSÍVEL À LUZ DA NATUREZA DINÂMICA DAS PROVAS DIGITAIS

É necessário começar por uma advertência básica, levada a cabo por David Silva Ramalho, que em sua excepcional dissertação de mestrado, defendida na Universidade de Lisboa, repele a tentativa de oferecer tratamento por analogia com fundamento no binômio *prova tradicional* ⇔ *prova digital*.[294]

Afirma Ramalho:

> Para uma correta compreensão da geral inadequação das normas processuais penais tradicionais à realidade digital, é necessário compreender as especificidades da prova digital. Com efeito, ao passo que certos tipos de prova são imediatamente compreendidos como sendo dotados de características individualizadoras que os autonomizam e que reivindicam especiais meios e/ou conhecimentos técnicos para a sua recolha, a prova digital tende a ser relegada para o domínio da analogia com meios de obtenção de provas de cariz não especialmente técnicos, como as buscas e apreensões.[295]

---

[294] RAMALHO, David da Silva. Métodos Ocultos de Investigação Criminal em Ambiente Digital. Coimbra: Almedina, 2017. David da Silva Ramalho é mestre em Ciências Jurídico-Criminais pela Faculdade de Direito da Universidade de Lisboa e investigador no Centro de Investigação em Direito Penal e Ciências Criminais (CIPDCC), vinculado à Faculdade de Direito da Universidade de Lisboa.

[295] Idem, p. 102.

Equiparar a prova digital às provas tradicionais não é um *erro* de abordagem cometido somente em países menos avançados do ponto de vista tecnológico. Trata-se de um enviesamento causado pela tentativa que práticos e teóricos do sistema penal de qualquer lugar levaram – e levam a cabo – no sentido de enquadrar os *objetos digitais* em moldes probatórios tradicionais, *objetos digitais*, porém, insuscetíveis de serem conduzidos à «realidade analógica».[296]

Necessidades de investigação geradas pela expansão de atividades criminosas além-fronteiras ensejaram a previsão legal e a adoção prática de "medidas não convencionais" de investigação criminal, algumas das quais bastante controversas, como as chamadas "operações sob cobertura".[297]

Donatella Curtotti, a propósito dessas operações, as define como "atividade investigativa na qual uma pessoa – um oficial de polícia judiciária ou um cidadão – zelando pela própria identidade, se infiltra na organização criminal com o propósito de descobrir a estrutura, privá-la de recursos essenciais, denunciar os participantes."[298]

Sem dúvida que a inspiração para a infiltração digital foi possivelmente a infiltração de agentes, conhecida também no direito brasileiro há mais de duas décadas.[299] Creio, no entanto, que essas analogias entre *prova*

---

[296] Ver: HUI, Yuk. Sobre la existencia de los objetos digitales. Trad. de Abrahan Cordero y David Wiehls. Segovia: Materia Oscura, 2023. Yuk Hui é filósofo e professor de filosofia na Erasmus University Rotterdam.

[297] CURTOTTI, Donatella "Le operazioni digitali sotto copertura": l'agente provocatore e l'attività di contrasto. In: ATERNO, Stefano; CAJANI, Francesco; COSTABILE, Gerardo; CURTOTTI, Donatella (a cura di). Cyber Forensics e indagini digitali: manuale tecnico-giuridico e casi pratici. Torino: Giappichelli, 2021. p. 505.

[298] CURTOTTI, Donatella "Le operazioni digitali sotto copertura": l'agente provocatore e l'attività di contrasto. In: ATERNO, Stefano; CAJANI, Francesco; COSTABILE, Gerardo; CURTOTTI, Donatella (a cura di). Cyber Forensics e indagini digitali: manuale tecnico-giuridico e casi pratici. Torino: Giappichelli, 2021. p. 505-506.

[299] Na atualidade: Art. 10-A, Lei n.º 12.850, de 2 de agosto de 2013. Será admitida a ação de agentes de polícia infiltrados virtuais, obedecidos os requisitos do caput do art. 10, na internet, com o fim de investigar os crimes previstos nesta Lei e a eles conexos, praticados por organizações criminosas, desde que demonstrada sua necessidade e indicados o alcance das tarefas dos policiais, os nomes ou apelidos das pessoas investigadas e, quando possível, os dados de conexão ou cadastrais que permitam a identificação dessas pessoas. § 1º Para efeitos do disposto nesta Lei, consideram-se: I - dados de conexão: informações referentes a hora, data, início, término, duração, endereço de Protocolo de Internet (IP) utilizado e terminal de origem da conexão; II - dados cadastrais: informações referentes a nome e endereço de assinante ou de usuário registrado ou autenticado

tradicional ⇔ *prova digital* tendem a prejudicar a compreensão das nuances da prova digital, encobrindo diferenças, quer acerca do potencial de pessoas afetadas, quer das condições de manipulação e supressão de informações que, dada a volatilidade da prova digital, arriscam a configurar elemento probatório insuscetível de submissão ao contraditório.

Ademais, esse recurso teórico-prático de equiparação entre o digital e o tradicional coloca em segundo plano algo que é o "coração da prova digital", que é a sua condição de meio técnico de produção de informações.

Exemplo recente pode facilitar o entendimento acerca da impropriedade da analogia.

As polícias francesa e belga, no âmbito do caso *Encrochat*, lançaram mão de técnica opaca de monitoramento e intervenção/controle remotos nos sistemas informáticos que atingiu o expressivo número de 30 mil telefones *infectados* pelo *software* usado pelos investigadores. 30 mil dispositivos localizados em 120 países diferentes.[300]

---

para a conexão a quem endereço de IP, identificação de usuário ou código de acesso tenha sido atribuído no momento da conexão. § 2º Na hipótese de representação do delegado de polícia, o juiz competente, antes de decidir, ouvirá o Ministério Público. § 3º Será admitida a infiltração se houver indícios de infração penal de que trata o art. 1º desta Lei e se as provas não puderem ser produzidas por outros meios disponíveis. § 4º A infiltração será autorizada pelo prazo de até 6 (seis) meses, sem prejuízo de eventuais renovações, mediante ordem judicial fundamentada e desde que o total não exceda a 720 (setecentos e vinte) dias e seja comprovada sua necessidade. § 5º Findo o prazo previsto no § 4º deste artigo, o relatório circunstanciado, juntamente com todos os atos eletrônicos praticados durante a operação, deverá ser registrados, gravados, armazenados e apresentados ao juiz competente, que imediatamente cientificará o Ministério Público. § 6º No curso do inquérito policial, o delegado de polícia poderá determinar aos seus agentes, e o Ministério Público e o juiz competente poderão requisitar, a qualquer tempo, relatório da atividade de infiltração. § 7º É nula a prova obtida sem a observância do disposto neste artigo. (Incluído pela Lei nº 13.964, de 2019) BRASIL. Lei n.º 12.850, de 2 de agosto de 2013. Define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal); revoga a Lei nº 9.034, de 3 de maio de 1995; e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm. Consultado em: 14 de outubro de 2024. Na origem, a infiltração de agentes "convencional" foi introduzida no direito brasileiro pela Lei nº 10.217, de 11 de abril de 2001, que alterou a primitiva lei de repressão às ações praticadas por organizações criminosas, a Lei nº 9.034, de 3 de maio de 1995. https://www.planalto.gov.br/ccivil_03/leis/l9034.htm. Consultado em: 14 de outubro de 2024.

[300] ZARAGOZA TEJADA, Javier Ignacio. La prueba ilícita y prueba tecnológica. Reflexiones a raíz del caso Encrochat. In: ORTIZ PRADILLO, Juan Carlos; ABELLÁN ALBERTOS, Antonio (Dir.). El derecho de defensa en la justicia penal digital. Valencia: Tirant lo Blanch, 2024. p. 309. Javier Ignacio Zaragoza Tejada é promotor da Fiscalía Provincial de Gipuzkoa e especialista em cibercrime.

A operação de *hackeamento* massivo deflagrou uma grande polêmica social e jurídica, ressaltou Javier Ignacio Zaragoza Tejada, o que se entende bem, e isso não apenas porque erodiu as fronteiras sempre tênues entre *inteligência* e persecução penal.[301]

Avaliando a parte italiana do caso, a Corte de Cassação italiana se posicionou de forma contrária à legalidade do *hackeamento* massivo, em decisão de 7 de setembro de 2022, sublinhando de maneira expressa que "o princípio do contraditório implica que a dialética processual não se aplique apenas ao material obtido, mas que se estenda à forma como se obteve dito material."[302]

O caso *Encrochat* é ilustrativo de uma real e bastante visível mudança de paradigmas relacionada ao papel que cumprem sofisticadas técnicas de intromissão oculta em sistemas informáticos, deslocando essas técnicas intromissivas da periferia das preocupações jurídico-processuais para o centro do debate acerca da legalidade do emprego e execução de métodos de investigação digital.

A experiência do caso *Encrochat* na atualidade é menos uma exceção e mais um exemplo de uma das diversas maneiras pelas quais as modernas tecnologias se infiltram em sistemas informáticos, alteram dados à revelia do usuário e se protegem por trás de uma barreira de opacidade, que não é facilmente rompida devido à defesa selvagem de direitos autorais sobre softwares e de alegados interesses políticos de defesa nacional.[303]

Nesse sentido, creio que Marco Torre caminha melhor, ao propor, em primeiro lugar, e com foco nas especificidades das provas digitais, uma classificação que ao menos nesse momento pode servir como guia útil e

[301] Idem, p. 307.

[302] ZARAGOZA TEJADA, Javier Ignacio. La prueba ilícita y prueba tecnológica. Reflexiones a raíz del caso Encrochat. In: ORTIZ PRADILLO, Juan Carlos; ABELLÁN ALBERTOS, Antonio (Dir.). El derecho de defensa en la justicia penal digital. Valencia: Tirant lo Blanch, 2024. p. 312.

[303] A propósito: QUATTROCOLO, Serena. Equità del processo penale e automated evidence alla luce della convenzione europea dei diritti dell'uomo. Revista Ítalo-Española de Derecho Procesual, v. 1, 2019. Madrid: Marcial Pons Ediciones Jurídicas y Sociales. Disponível em: http://www.rivitsproc.eu/wp-content/uploads/2018/11/quattrocolo-equita_proceso_penale_e_automated_evidence.pdf. Consultado em: 25 de junho de 2024. Serena Quattrocolo é professora de Processo Penal Italiano e Europeu na University of Eastern Piedmont.

adequado a orientar o estágio deliberativo (as decisões legislativas) e o estágio executivo (as ações dos atores do processo criminal e as decisões jurisdicionais).[304]

De acordo com Marco Torre, inicialmente é possível partir da ideia de que, à vista das múltiplas possibilidades tecnológicas de intervenção remota nos sistemas informáticos e de suas variadas finalidades, a expressão "captor informático" deve funcionar como "conceito de gênero".[305]

Sublinha o referido autor, com razão, que "um instrumento tecnológico deste tipo é consentâneo com o desenvolvimento de várias atividades", que especifica: *i)* captura do tráfego de dados na saída ou recepção dos dispositivos *infectados*; *ii)* ativação remota de microfones e câmeras de vídeo, com capacidade de gravar as atividades no ambiente circundante ao *hardware*; *iii)* de navegar internamente pelos arquivos do alvo, copiando-os total ou parcialmente; *iv)* decifrar tudo o que é digitado (*keylogger*) e visualizar o que aparece em tela (*screenshot*); *v)* de escapar de todos os antivírus disponíveis no comércio.[306]

Ao tratar do uso do *Malware* em investigação criminal, Helena Costa Rossi e Leandro Musa de Almeida também assinalam as características mais marcantes do uso de *softwares* maliciosos, incluindo "ativação de funcionalidade de *hardware* com GPS, câmera e microfone", por exemplo.[307]

Os usos práticos dessas ferramentas no contexto das investigações criminais podem ser bastante distintos em relação às suas finalidades, variando, por exemplo, do monitoramento da circulação de criptomoedas

[304] Adoto aqui o critério extraído da "Teoria das Fontes", conforme proposto por Joseph Raz. RAZ, Joseph. O conceito de sistema jurídico: uma introdução à teoria dos sistemas jurídicos. Trad. de Maria Cecília Almeida. São Paulo: WMF Martins Fontes, 2012. p. 284. Joseph Raz foi um filósofo do direito, ele lecionou na Columbia Law School e na King's College de Londres

[305] TORRE, Marco. Il captatore informatico: nuove tecnologie investigative e rispetto delle regole processuali. Milano: Giuffrè, 2017. p. 17. Marco Torre é doutor em direito penal pela Università di Firenze.

[306] Idem, p. 17-18.

[307] ROSSI, Helena Costa; ALMEIDA, Leandro Musa de. O uso do malware na investigação criminal: pontos de tensão e limites. Boletim IBCCRIM, v. 31, n. 373, dez/2023. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/693. Consultado em 14 de outubro de 2024. p. 20. Helena Costa Rossi é mestranda em Direito Processual Penal na Faculdade de Direito da USP e advogada. Leandro Musa de Almeida é mestrando em Direito Processual Penal na Faculdade de Direito da USP e Procurador da República.

ou da movimentação dos suspeitos (geolocalização) à interceptação de comunicações telemáticas e coleta continuada, em tempo real, de informações e arquivos digitais (cópia).[308]

Em razão disso, Marco Torre propõe ordenar essas atividades em dois grandes grupos: os que se referem às *buscas on line* (*on line search*) e os que compreendem a vigilância à distância (*on line surveillance*), entendendo-se, no entanto, que no curso da mesma operação, as atividades de investigação possam ter diversos escopos, atendidos simultaneamente e afetando, também ao mesmo tempo, diferentes direitos fundamentais.[309]

Vale ressaltar, por exemplo, que o emprego probatório do GPS (*Global Positioning System*) é bem ilustrativo do incremento de riscos gerado por uma multifuncionalidade potencializada por aplicações de inteligência artificial. O GPS permite localizar as pessoas em tempo real e por essa razão tem-se convertido em dispositivo preferencial das investigações criminais.

Maria Beatriz Seabra de Brito leciona que é impossível pretender uma pura e simples migração de raciocínio probatório entre métodos tradicionais de vigilância para obtenção de provas e o uso do GPS no âmbito de persecução penal.[310]

Sublinha Seabra de Brito que o recurso ao GPS para fins probatórios é causa de uma "transfiguração de intrusividade de dados em função da extensão da interferência", ultrapassando a prática da vigilância do

[308] JIMÉNEZ LÓPEZ, María de las Nieves. Las medidas tecnológicas de investigación con régimen especial, practicadas al amparo de una orden europea de investigación. In: FONTESTAD PORTALÉS, Leticia (dir.). JIMÉNEZ LÓPEZ, María de las Nieves (coord.). El uso de las TICs en la Cooperación Jurídica Penal Internacional: construyendo la sociedad digital del futuro. Corunha: Colex, 2022. p. 125-126. María de las Nieves Jiménez López é professora de Derecho Procesal na Universidad de Málaga.

[309] TORRE, Marco. Il captatore informatico: nuove tecnologie investigative e rispetto delle regole processuali. Milano: Giuffrè, 2017. p. 18-19. Fabrício Pinto Weiblen leciona que a Lei Orgânica 13/2015 espanhola optou por "tratar de forma unitária a obtenção de dados que pertencem ao 'entorno virtual' do investigado, sendo desnecessária a discussão sobre qual direito fundamental específico foi atingido." WEIBLEN, Fabrício Pinto. Abertura Tecnológica dos Meios de Obtenção de Prova e o Uso de Software Espião na Investigação Criminal. Coimbra: Almedina, 2024. p. 115.

[310] BRITO, Maria Beatriz Seabra de. Novas Tecnologias e legalidade da prova em processo penal: natureza e enquadramento do GPS como método de obtenção de prova. Coimbra: Almedina, 2018. Maria Beatriz Seabra de Brito é investigadora no Criminalia, no Centro de Investigação da Faculdade de Direito da Universidade Nova de Lisboa (CEDIS).

modelo sensorial na direção de uma *extrassensorial surveillance*, como reconheceram a juíza Sotomayor e o juiz Alito, da Suprema Corte norte-americana, por ocasião do julgamento paradigmático sobre o tema.[311]

O caso *United States v Jones*, de janeiro de 2012, decidido pela Suprema Corte dos Estados Unidos da América, foi inovador sob os aspectos do reconhecimento da "dimensão reforçada de invasividade" de certos métodos tecnológicos, dos critérios de admissibilidade de novos métodos de obtenção de prova e da aplicação da "Teoria do Mosaico", que estabelece que, no domínio tecnológico, por causa das aplicações de inteligência artificial, "o todo *sempre* é maior que o somatório das partes".

Não custa salientar que cada vez mais nos aproximamos da capacidade de processamento dos supercomputadores, que já alcançavam, em 2020, performance de mais de 442 petaflops (quadrilhões de operações de pontos flutuantes por segundo).[312]

Ainda assim, o certo é que ambos os grupos teoricamente propostos por Marco Torre guardam em comum uma diferenciação fundamental em relação ao que se denomina "prova digital *off line*".[313]

A prova digital *off line* é aquela coletada no âmbito de buscas que apreendem *fisicamente* os dispositivos informáticos visados – *smartphones*, *desktops*, *notebooks* – viabilizando a instauração de duas cadeias de custódia: aquela que se cinge ao dispositivo de *hardware*, que deve ser coletado e preservado *no estado* até o posterior exame pericial; e a cadeia

[311] Idem, p. 63-65.

[312] Ver: FREIRE, Raquel. Computador mais poderoso do mundo: veja o que Fugaku é capaz de fazer. Supercomputador usa inteligência artificial para ajudar a prever mudanças climáticas e mapear o coronavírus, entre outros problemas atuais. Publicado em: 17 de novembro de 2021. TechTudo. Disponível em: https://www.techtudo.com.br/google/amp/noticias/2021/11/computador-mais-poderoso-do-mundo-veja-o-que-fugaku-e-capaz-de-fazer.ghtml. Consultado em 23 de agosto de 2024. Paulo Comoglio designa a atual época com "Petabyte age". COMOGLIO, Paolo. Nuove tecnologie e disponibilità della prova. L'accertamento del fatto nella diffusione delle conoscenze. Torino: Giappichelli, 2018. p. 234. Paolo Comoglio é professor associado do departamento de giurisprudenza da Università di Genova.

[313] TORRE, Marco. Il captatore informatico: nuove tecnologie investigative e rispetto delle regole processuali. Milano: Giuffrè, 2017. p. 11.

de custódia do *conteúdo digital* do dispositivo, cujo processo de coleta é necessariamente técnico e deve ser realizado, com exclusividade, por peritos informáticos.[314]

Não há dúvida de que tanto a prova digital *off line* como a *on-line* demandam intervenção pericial, haja vista a natureza técnica de sua *formação* e os altos riscos de contaminação ou perda decorrentes de sua volatilidade.

Daí que, minuciando esses cuidados em alentado estudo sobre os protocolos de preservação da prova digital, Ana Di Iorio afirma que as cautelas específicas reclamadas em âmbito internacional para este tipo de prova consideram o propósito de "evitar a contaminação da prova", em geral, resultante de atuação indevida de identificação, aquisição e preservação da prova digital, cumprindo "minimizar a manipulação da prova digital", "documentar qualquer ação que implique mudança irreversível" na mencionada prova, separar rigidamente a função pericial de quaisquer outras associadas à investigação digital ("não atuar além de suas competências e não tomar decisões sem a autorização correspondente") e, vale salientar, "aderir às regulações e leis locais".[315]

Mais do que isso, Carlos Hélder Mendes chama atenção para algo pouco advertido, relativamente à generalidade das provas digitais. Afirma este autor, corretamente, que se "a aquisição das fontes de prova digital armazenadas em dispositivos informáticos é somente possível a partir de *softwares* que permitem a exata criação de cópia forense", a cópia forense será *sempre* uma *fonte de prova derivada*, dependente de programações criadas e implementadas por terceiros, programações necessárias à conversão de *bits* nas informações possíveis de ser compreendidas e interpretadas por todas as pessoas.[316]

---

[314] Ver: PRADO, Geraldo. Parecer: Investigação criminal digital e processo penal. Revista Brasileira de Ciências Criminais, v. 199/ nov-dez/2023, p. 315-350.

[315] DI IORIO, Ana. Protocolos de preservación de evidencia digital y cuestiones forenses. In: DUPUY, Daniela (dir.); KIEFER, Mariana (coord.). Cibercrimen II. Buenos Aires-Montevideo: Editorial B de F, 2018. p. 341-343.

[316] MENDES, Carlos Hélder Carvalho Furtado. Prova penal digital: direito à não autoincriminação e contraditório na extração de dados armazenados em dispositivos informáticos. São Paulo: Tirant lo Blanch, 2024. p. 347. Carlos Hélder Carvalho Furtado Mendes é doutor e mestre em Ciências Criminais pela Pontifícia Universidade Católica do Rio Grande do Sul e professor adjunto da Universidade Estadual do Maranhão.

Ensinam corretamente Raffaella Brighi e Michele Ferrazzano que o «dado digital» consiste em representação de sequências de *bits* incompreensíveis para os humanos, a demandar uma série de operações técnicas carregadas de variáveis que os transformam em diferentes resultados possíveis, de voz, imagem, texto, etc., conforme sejam processadas essas sequências de *bits*.[317] Sem interpretação, dados não podem ter significado algum".[318]

Pois bem, se em seu aspecto *estático* (*off line*) a prova digital já demanda cuidados extremos para que seja processualmente válida, a prova digital *online* reclama um reforço de garantias. A execução quer das medidas determinadas com exclusivo propósito de busca (*on line search*) ou as que compreendem a vigilância à distância (*on line surveillance*) são passíveis de manipulação e, se não adequadamente fiscalizadas, coletadas e preservadas, tornam ineficaz qualquer esforço de submissão futura ao contraditório, inviabilizando-se como elemento probatório.

Rossi e Almeida alertam para isso. Afirmam estes autores:

> Uma vez que certas ferramentas podem garantir ao invasor privilégios administrativos do sistema, com a possibilidade de alterações das informações ali contidas, é necessário garantir que os meios de prova colhidos não tenham sido alterados.[319]

A proposta de ambos, na linha preconizada por David Silva Ramalho, consiste em fortalecer a cadeia de custódia dessas informações pela via da exigência de elaboração "de um relatório técnico de utilização desse meio de obtenção de prova".[320]

---

[317] BRIGHI, Raffaella; FERRAZZANO, Michele. Digital forensics: best practices and perspective. In: CAIANIELLO, Michele; CAMON, Alberto (ed.). Digital forensic evidence: towards common European standards in antifraud administrative and criminal investigations. Milano: CEDAM, 2021. p. 14. Raffaella Brighi é Professora associada de Informatica giuridica e Informatica forense na Università di Bologna. Michele Ferrazzano é Professor de Informatica na Università di Modena e Reggio Emilia.

[318] Tradução livre. No original: "Without interpretation, data cannot have any meaning." BRIGHI, Raffaella; FERRAZZANO, Michele. Digital forensics: best practices and perspective. In: CAIANIELLO, Michele; CAMON, Alberto (ed.). Digital forensic evidence: towards common European standards in antifraud administrative and criminal investigations. Milano: CEDAM, 2021. p. 14.

[319] ROSSI, Helena Costa; ALMEIDA, Leandro Musa de. O uso do malware na investigação criminal: pontos de tensão e limites. Boletim IBCCRIM, v. 31, n. 373, dez/2023. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/693. Consultado em 14 de outubro de 2024. p. 22.

[320] Ibidem.

Não custa recordar, segundo a Diretora do InfoLab do Ministério Público da Província de Buenos Aires, que o "controle da cadeia de custódia" configura uma "série de cuidados destinados a traçar a origem, identidade e integridade da prova para que esta não se perca, seja destruída ou alterada".[321]

Sou da opinião, no entanto, de que para as provas digitais *online* a exigência da instauração e preservação da cadeia de custódia não é suficiente.

Muito embora em muitos pontos não essenciais divirja da tese que, em 2023, Fabrício Pinto Weiblen apresentou na Universidade de Lisboa com a seguinte designação: "Abertura tecnológica dos meios de obtenção de prova e o uso de *software* espião na investigação criminal",[322] cuja leitura recomendo, fato é que o autor tem razão quando afirma que o *monitoramento online* tem acentuado grau de intrusividade na vida privada, "seja pela quantidade e qualidade dos dados, seja pela possibilidade de continuação no tempo."[323]

Quer as buscas *online*, quer a vigilância *online* são dispositivos de controle altamente invasivos que contendem com as liberdades básicas das pessoas visadas e daquelas que, colateralmente, são atingidas pelas mesmas medidas sem terem qualquer relação com as investigações criminais em curso.

Além da exigência constitucional de que essas providências se submetam à reserva de lei parlamentar, sendo inválidas quando amparadas em atos normativos que não se revestem dessa qualidade, a lei parlamentar em questão deve ser *adequada* e *proporcional*. Proporcional no sentido

---

[321] Tradução libre de DI IORIO, Ana. Protocolos de preservación de evidencia digital y cuestiones forenses. In: DUPUY, Daniela (dir.); KIEFER, Mariana (coord.). Cibercrimen II. Buenos Aires-Montevideo: Editorial B de F, 2018. p. 344. Ana Haydeé Di Iorio é professora e pesquisadora, especializada em Ciência da Computação e Direito, Defesa do Consumidor, Ontologias, Sistemas Operacionais e Computação Forense, dirige o InFo-Lab, Laboratório de Pesquisa e Desenvolvimento de Tecnologia em Computação Forense, organização vinculada à Universidade FASTA, em Buenos Aires.

[322] WEIBLEN, Fabrício Pinto. Abertura Tecnológica dos Meios de Obtenção de Prova e o Uso de Software Espião na Investigação Criminal. Coimbra: Almedina, 2024.

[323] Idem, p. 105.

de prever as hipóteses excepcionais de breve incidência das infiltrações digitais – quer as buscas *online*, quer a vigilância *online* – e adequada no tocante à previsão de rigorosos métodos de supervisão continuada de sua execução.

Ao tratar da legislação processual penal espanhola posterior à alteração de 2015, envolvendo medidas tecnológicas para investigar crimes cibernéticos, Eltjon Mirashi afirma que "diligências de busca remota sobre equipamentos informáticos que se realizem sem autorização do juiz geram nulidade das provas obtidas."[324]

Não se trata, apenas, de autorização judicial. Tanto o princípio de reserva de lei como o princípio de reserva de jurisdição, relativamente à compressão do exercício de direitos fundamentais, estão assegurados por nossa Constituição.

O que, em geral, é indevidamente desprezado na prática é o controle técnico e pessoal *sobre a execução* das providências cautelares digitais, normalmente delegado aos próprios executores das medidas, o que é um contrassenso.

Como frisou a Corte Constitucional italiana, no caso *Encrochat*, "o princípio do contraditório implica que a dialética processual não se aplique apenas ao material obtido, mas que se estenda à forma como se obteve dito material."[325]

Temos aqui questões técnicas que devem ser enfrentadas, tais como a indicação precisa dos *softwares* empregados nas diligências, seus requisitos técnicos, a indicação de como e por quem foram usados, por quanto tempo e sob fiscalização de quem.

Trata-se de métodos ocultos de obtenção de informações. Por isso, o contraditório é diferido. Em sendo diferido e, pois, não estando submetido ao exame da parte contrária em tempo real, é essencial que um terceiro desinteressado no resultado das diligências funcione como *supervisor*

[324] MIRASHI, Eltjon. Tratamiento procesal del cibercrimen y diligencias de investigación: casuística y problemática. Pamplona: Aranzadi, 2023. p. 187. Eltjon Mirashi é doutor em direito pela Universidade de Salamanca.

[325] ZARAGOZA TEJADA, Javier Ignacio. La prueba ilícita y prueba tecnológica. Reflexiones a raíz del caso Encrochat. In: ORTIZ PRADILLO, Juan Carlos; ABELLÁN ALBERTOS, Antonio (Dir.). El derecho de defensa en la justicia penal digital. Valencia: Tirant lo Blanch, 2024. p. 312.

das medidas, atuando efetivamente neste sentido enquanto durar a autorização judicial.

A previsão de um procedimento cautelar probatório em apartado deve contemplar os relatórios diários de execução das providências probatórias *online* e os registros de sua fiscalização.

A evolução das investigações criminais para o patamar das investigações digitais realça o papel do juiz de garantias que é, na minha opinião, a autoridade responsável por essa supervisão.[326]

[326] Art. 3º-B, CPP. O juiz das garantias é responsável pelo controle da legalidade da investigação criminal e pela salvaguarda dos direitos individuais cuja franquia tenha sido reservada à autorização prévia do Poder Judiciário, competindo-lhe especialmente: (Incluído pela Lei nº 13.964, de 2019) (Vigência) (Vide ADI 6.298) (Vide ADI 6.300) (Vide ADI 6.305) I - receber a comunicação imediata da prisão, nos termos do inciso LXII do caput do art. 5º da Constituição Federal; (Incluído pela Lei nº 13.964, de 2019) II - receber o auto da prisão em flagrante para o controle da legalidade da prisão, observado o disposto no art. 310 deste Código; III - zelar pela observância dos direitos do preso, podendo determinar que este seja conduzido à sua presença, a qualquer tempo; IV - ser informado sobre a instauração de qualquer investigação criminal; V - decidir sobre o requerimento de prisão provisória ou outra medida cautelar, observado o disposto no § 1º deste artigo; VI - prorrogar a prisão provisória ou outra medida cautelar, bem como substituí-las ou revogá-las, assegurado, no primeiro caso, o exercício do contraditório em audiência pública e oral, na forma do disposto neste Código ou em legislação especial pertinente; VII - decidir sobre o requerimento de produção antecipada de provas consideradas urgentes e não repetíveis, assegurados o contraditório e a ampla defesa em audiência pública e oral; VIII - prorrogar o prazo de duração do inquérito, estando o investigado preso, em vista das razões apresentadas pela autoridade policial e observado o disposto no § 2º deste artigo; IX - determinar o trancamento do inquérito policial quando não houver fundamento razoável para sua instauração ou prosseguimento; X - requisitar documentos, laudos e informações ao delegado de polícia sobre o andamento da investigação; XI - decidir sobre os requerimentos de: a) interceptação telefônica, do fluxo de comunicações em sistemas de informática e telemática ou de outras formas de comunicação; b) afastamento dos sigilos fiscal, bancário, de dados e telefônico; c) busca e apreensão domiciliar; d) acesso a informações sigilosas; e) outros meios de obtenção da prova que restrinjam direitos fundamentais do investigado; XII - julgar o habeas corpus impetrado antes do oferecimento da denúncia; XIII - determinar a instauração de incidente de insanidade mental; XIV - decidir sobre o recebimento da denúncia ou queixa, nos termos do art. 399 deste Código; XV - assegurar prontamente, quando se fizer necessário, o direito outorgado ao investigado e ao seu defensor de acesso a todos os elementos informativos e provas produzidos no âmbito da investigação criminal, salvo no que concerne, estritamente, às diligências em andamento; XVI - deferir pedido de admissão de assistente técnico para acompanhar a produção da perícia; XVII - decidir sobre a homologação de acordo de não persecução penal ou os de colaboração premiada, quando formalizados durante a investigação; XVIII - outras matérias inerentes às atribuições definidas no caput deste artigo. § 1º O preso em flagrante ou por força de mandado de prisão provisória será encaminhado à presença do juiz de garantias no prazo de 24 (vinte e quatro) horas, momento em que se realizará audiência com a presença do Ministério Público e da Defensoria Pública ou de advogado constituído, vedado o emprego de videoconferência. § 2º Se o investigado estiver preso, o juiz das garantias poderá, mediante representação da autoridade policial e ouvido o Ministério Público, prorrogar, uma única vez, a duração do inquérito por até 15 (quinze) dias, após o que, se ainda assim a investigação não for concluída, a prisão será imediatamente relaxada.

Vale salientar que o dever de proteção dos sistemas informáticos também decorre dos compromissos internacionais assumidos pelo Brasil, como é o caso da Convenção de Budapeste.[327]

O Supremo Tribunal Federal (STF), no entanto, desconfigurou o juiz de garantias ao privá-lo de sua competência quanto ao ato de recebimento da denúncia ou queixa.[328]

A *legalidade interpretada* pelo STF alterou a estrutura planejada para o sistema de justiça criminal, modificando a relação jurídica entre os sujeitos do sistema, em prejuízo da constituição de um ambiente institucional de valorização da imparcialidade.

O acórdão do STF, ao negar os efeitos pesquisados cientificamente acerca do «viés de confirmação», transformou-se na *voz* desse viés, que

[327] Artigo 19, Decreto nº 11.491, de 12 de abril de 2023 - Busca e apreensão de dados de computador. 1. Cada Parte adotará medidas legislativas e outras providências necessárias para dar poderes a suas autoridades competentes para busca ou investigação, em seu território: a. de qualquer sistema de computador ou de parte dele e dos dados nele armazenados; e b. de qualquer meio de armazenamento de dados de computador no qual possam estar armazenados os dados procurados em seu território. 2. Cada Parte adotará medidas legislativas e outras providências necessárias para assegurar que, quando a autoridade competente proceder a busca em um determinado sistema de computador ou em parte dele, de acordo com o parágrafo 1. a, e tiver fundadas razões para supor que os dados procurados estão armazenados em outro sistema de computador ou em parte dele, situado em seu território, e que tais dados são legalmente acessíveis a partir do sistema inicial, ou disponíveis a esse sistema, tal autoridade poderá estender prontamente a busca ou o acesso ao outro sistema. 3. Cada Parte adotará medidas legislativas e outras providências necessárias para dar poderes às suas autoridades competentes para apreender ou proteger dados de computador acessados de acordo com os parágrafos 1 ou 2. Estas medidas incluirão o poder de: a. apreender ou proteger um sistema de computador ou parte dele ou um meio de armazenamento de dados; b. fazer e guardar uma cópia desses dados de computador; c. manter a integridade dos dados de computador relevantes; d. tornar inacessíveis esses dados no sistema de computador acessado ou dele removê-los. 4. Cada Parte adotará medidas legislativas e outras providências necessárias para dar poderes a sua autoridade competente para determinar que qualquer pessoa que conheça o funcionamento do sistema de computador ou as medidas empregadas para proteger os dados nele armazenados que forneça, tanto quanto seja razoável, as informações necessárias para permitir as providências referidas nos parágrafos 1 e 2. 5. Os poderes e procedimentos referidos neste artigo estarão sujeitos aos dispositivos dos Artigos 14 e 15. BRASIL. Decreto nº 11.491, de 12 de abril de 2023. Promulga a Convenção sobre o Crime Cibernético, firmada pela República Federativa do Brasil, em Budapeste, em 23 de novembro de 2001. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11491.htm. Consultado em: 14 de outubro de 2024.

[328] Ver: PRADO, Geraldo. Curso de Processo Penal: Tomo I - Fundamentos e Sistema. São Paulo: Marcial Pons, 2024. p. 314-316.

encarnou, ainda que *inconscientemente*, em defesa de uma espécie de superioridade moral dos juízes e juízas.[329]

O STF subordinou a *imparcialidade* a algum inexplicável e insustentável juízo de conveniência ao antecipar a competência do juiz ou juíza da etapa final da persecução penal para o momento do recebimento da denúncia ou queixa, de sorte a lhe permitir o acesso a elementos informativos que tendem a ensejar o «viés confirmatório», contra o texto legal que argumenta que está *corrigindo*.

Mantida a lógica do raciocínio que inspira a decisão do STF a propósito da instituição do «juiz das garantias», também não há explicação plausível para a decisão ter excluído de sua incidência o procedimento "das infrações penais de menor potencial ofensivo, de competência dos juizados especiais", bem como afirmado uma hipotética incompatibilidade sistêmica com "o procedimento especial previsto na Lei 8.038/1990, que trata dos processos de competência originária dos tribunais... o rito do tribunal do júri... [e] os casos de violência doméstica e familiar."

Foi pensando o sistema de justiça criminal como um sistema social que deve prezar pela harmonia que a minirreforma processual penal brasileira de 2008 instituiu o princípio *da reserva de código*, por meio do qual, na conformação de um procedimento penal *sempre trifásico* – com as etapas, escrupulosamente separadas, da **(a)** investigação criminal, **(b)** admissibilidade da acusação e **(c)** instrução probatória e decisão (sentença) de mérito – se deu o primeiro passo na direção de um ambiente processual penal amigável à *imparcialidade*.[330]

---

[329] Ações Diretas de Inconstitucionalidade n.º 6.298, 6.299, 6.300 e 6.305/DF. Plenário do Supremo Tribunal Federal. Rel.: Min. Luiz Fux. Julgamento em 24 de agosto de 2023. No item III da Ementa, ao tratar da regra do art. 3º-C, caput, do CPP (que diz: "a competência do juiz das garantias abrange todas as infrações penais, exceto as de menor potencial ofensivo, e cessa com o recebimento da denúncia ou queixa na forma do art. 399 deste Código"), consta o seguinte entendimento: "(c) Ademais, além das infrações penais de menor potencial ofensivo, de competência dos juizados especiais, a nova sistemática do juiz das garantias não se compatibiliza com o procedimento especial previsto na Lei 8.038/1990, que trata dos processos de competência originária dos tribunais; com o rito do tribunal do júri; com os casos de violência doméstica e familiar. (d) Por tais motivos, deve ser atribuída interpretação conforme à primeira parte do caput do art. 3º-C do CPP, incluído pela Lei nº 13.964/2019, para esclarecer que as normas relativas ao juiz das garantias não se aplicam às seguintes situações: (1) processos de competência originária dos tribunais, os quais são regidos pela Lei nº 8.038/1990; (2) processos de competência do tribunal do júri; (3) casos de violência doméstica e familiar; e (4) infrações penais de menor potencial ofensivo".

[330] Princípio da reserva de código: Art. 397, §4º, CPP. O procedimento será comum ou especial. [...] § 4º As disposições dos arts. 395 a 398 deste Código aplicam-se a todos os procedimentos penais de primeiro grau, ainda que não regulados neste Código. (Incluído pela Lei nº 11.719, de 2008).

Neste tipo de situação, o choque entre *legalidade* e *imparcialidade* causa danos ao «estado de direito», à «dignidade da pessoa humana» e à função jurisdicional penal de contenção do abuso de poder.

Naquilo em que reescreve a lei, a decisão do STF sobre a competência do «juiz das garantias» extrapola os limites do legítimo controle de constitucionalidade pelo tribunal e é causa da instauração de um ambiente institucional desfavorável à *imparcialidade* no processo penal. Deve ser revertida pelo próprio STF para que seja restabelecida a regra legal, corrigindo-se o erro judicial.

E a oportunidade se oferece no contexto da sugerida elaboração de projeto de lei que regule a prova digital *online* em todas as suas modalidades que não contendam com o estado de direito, o fazendo sob os princípios da legalidade estrita, reserva de jurisdição, proporcionalidade e adequação.

A função do juiz de garantias, como efetivo supervisor da legalidade jurídica e adequação técnica das medidas, é compatível com o exercício do juízo de admissibilidade da acusação, evitando que o futuro juiz da causa seja afetado pelo viés de confirmação.

Por derradeiro, embora não seja objeto do artigo, faço questão de registrar que em minha opinião o uso de *software* espião para vigilância – e não para a coleta de arquivos digitais – é inconstitucional a qualquer título, na medida em que, potencializado pelos recursos da inteligência artificial, produz aquele tipo de concentração de poder informacional verificado pela Teoria do Mosaico.

O emprego de "programas maliciosos" por criminosos que se dedicam a "atacar a infraestrutura informática"[331] é uma realidade infelizmente bastante comum e conhecida, causadora de danos às vezes irreparáveis. As diversas espécies de programas maliciosos: vírus clássicos, troianos, *riskware*, *ransomware*, *spyware*, *pharming, backdoors* e outros,[332] que, inoculados no sistema informático da pessoa visada, acabam por interferir e mesmo dominar por completo o sistema informático alvejado, proporcionam condições de manipulação maliciosa de arquivos digitais.

[331] ABOSO, Gustavo E. Evidencia Digital en el Proceso Penal: La investigación forense en el entorno digital y la validez de las garantías judiciales. Buenos Aires: B de F, 2023. p. 333. Gustavo Eduardo Aboso é doutor em direito pela Universidad Nacional de Educación a Distancia (UNED-Madrid).

[332] Ibidem.

Ofertar aos governos que, conjunturalmente, podem estar inclinados ao exercício arbitrário e abusivo do poder político uma ferramenta tão potente é um risco injustificável à democracia e à separação dos poderes.

O "agente infiltrado digital", funcionário da polícia que se vale de falsa identidade para estabelecer contato digital com criminosos, é ainda, com todas as ressalvas, uma pessoa cuja atuação digital deixa traços. Se devidamente fiscalizado, pode alcançar resultados aceitáveis à luz de nosso ordenamento jurídico.[333]

A vigilância eletrônica automatizada por meio de *software* espião, contudo, avança de forma grave na direção do domínio das informações vitais das pessoas, instalando autênticas "portas de trás" (*backdoors*) não apenas nos sistemas informáticos visados, mas na própria condição existencial das pessoas investigadas, seus familiares, amigos e até estranhos que eventualmente convivam com elas.

Nem toda aplicação digital inovadora é necessariamente boa. Nesse ponto, é a ética a ditar o que pode ou não pode ser realizado e referendado.

[333] Ver: Art. 190-A, ECA. A infiltração de agentes de polícia na internet com o fim de investigar os crimes previstos nos arts. 240, 241, 241-A, 241-B, 241-C e 241-D desta Lei e nos arts. 154-A , 217-A , 218 , 218-A e 218-B do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) , obedecerá às seguintes regras: (Incluído pela Lei nº 13.441, de 2017) I – será precedida de autorização judicial devidamente circunstanciada e fundamentada, que estabelecerá os limites da infiltração para obtenção de prova, ouvido o Ministério Público; (Incluído pela Lei nº 13.441, de 2017) II – dar-se-á mediante requerimento do Ministério Público ou representação de delegado de polícia e conterá a demonstração de sua necessidade, o alcance das tarefas dos policiais, os nomes ou apelidos das pessoas investigadas e, quando possível, os dados de conexão ou cadastrais que permitam a identificação dessas pessoas; (Incluído pela Lei nº 13.441, de 2017) III – não poderá exceder o prazo de 90 (noventa) dias, sem prejuízo de eventuais renovações, desde que o total não exceda a 720 (setecentos e vinte) dias e seja demonstrada sua efetiva necessidade, a critério da autoridade judicial. (Incluído pela Lei nº 13.441, de 2017) § 1 º A autoridade judicial e o Ministério Público poderão requisitar relatórios parciais da operação de infiltração antes do término do prazo de que trata o inciso II do § 1 º deste artigo. (Incluído pela Lei nº 13.441, de 2017) § 2 º Para efeitos do disposto no inciso I do § 1 º deste artigo, consideram-se: (Incluído pela Lei nº 13.441, de 2017) I – dados de conexão: informações referentes a hora, data, início, término, duração, endereço de Protocolo de Internet (IP) utilizado e terminal de origem da conexão; (Incluído pela Lei nº 13.441, de 2017) II – dados cadastrais: informações referentes a nome e endereço de assinante ou de usuário registrado ou autenticado para a conexão a quem endereço de IP, identificação de usuário ou código de acesso tenha sido atribuído no momento da conexão. § 3 º A infiltração de agentes de polícia na internet não será admitida se a prova puder ser obtida por outros meios. (Incluído pela Lei nº 13.441, de 2017)

3. PALAVRAS FINAIS

A prova digital tem aspectos dinâmicos e práticos.

O presente ensaio preocupa-se com os aspectos dinâmicos que caracterizam a chamada prova digital *online*.

Essa prova pode ser classificada em dois grupos: a) busca *online*; b) vigilância *online*.

O estatuto jurídico da prova *online* submete-se ao princípio da estrita legalidade, da reserva de jurisdição, da proporcionalidade e adequação das medidas.

Por sua vez, o componente técnico (lógico) das medidas probatórias digitais deve estar em condições de ser submetido ao contraditório digital, que se estende à forma de obtenção do material digital.

É necessário assegurar a cadeia de custódia de todas as informações obtidas por intermédio desses métodos ocultos.

De lege ferenda deve ser estabelecido um procedimento probatório digital autônomo em relação à investigação criminal, que preserve as condições de êxito das atividades realizadas em sigilo, sob permanente e escrupulosa supervisão do juiz de garantias.

A vigilância *online* implementada e executada de forma automática, por meio de *software* espião, é inconstitucional por violar as regras fundamentais de liberdade que caracterizam o estado de direito.

4. REFERÊNCIAS

ABOSO, Gustavo E. **Evidencia Digital en el Proceso Penal:** La investigación forense en el entorno digital y la validez de las garantías judiciales. Buenos Aires: B de F, 2023.

BRIGHI, Raffaella; FERRAZZANO, Michele. Digital forensics: best practices and perspective. In: CAIANIELLO, Michele; CAMON, Alberto (ed.). **Digital forensic evidence**: towards common European standards in antifraud administrative and criminal investigations. Milano: CEDAM, 2021. p. 13-48.

BRITO, Maria Beatriz Seabra de. **Novas Tecnologias e legalidade da prova em processo penal:** natureza e enquadramento do GPS como método de obtenção de prova. Coimbra: Almedina, 2018.

CASEY, Eoghan; DAYWALT, Christopher; JOHNSTON, Andy. Intrusion Investigation. In: CASEY, Eoghan. (Ed.). **Handbook of Digital Forensics and Investigation.** Burlington: Elsevier Academic Press, 2010. p. 135-206.

COMOGLIO, Paolo. **Nuove tecnologie e disponibilità della prova**. L'accertamento del fatto nella diffusione delle conoscenze. Torino: Giappichelli, 2018.

CURTOTTI, Donatella "Le operazioni digitali sotto copertura": l'agente provocatore e l'attività di contrasto. In: ATERNO, Stefano; CAJANI, Francesco; COSTABILE, Gerardo; CURTOTTI, Donatella (a cura di). **Cyber Forensics e indagini digitali:** manuale tecnico-giuridico e casi pratici. Torino: Giappichelli, 2021. p. 505-518.

DI IORIO, Ana. Protocolos de preservación de evidencia digital y cuestiones forenses. In: DUPUY, Daniela (dir.); KIEFER, Mariana (coord.). **Cibercrimen II.** Buenos Aires-Montevideo: Editorial B de F, 2018. p. 335-356.

FREIRE, Raquel. Computador mais poderoso do mundo: veja o que Fugaku é capaz de fazer. Supercomputador usa inteligência artificial para ajudar a prever mudanças climáticas e mapear o coronavírus, entre outros problemas atuais. Publicado em: 17 de novembro de 2021. **TechTudo.** Disponível em: https://www.techtudo.com.br/google/amp/noticias/2021/11/computador-mais-poderoso-do-mundo-veja-o-que-fugaku-e-capaz-de-fazer.ghtml. Consultado em 23 de agosto de 2024. Paulo Comoglio designa a atual época com "Petabyte age".

HUI, Yuk. **Sobre la existencia de los objetos digitales.** Trad. de Abrahan Cordero y David Wiehls. Segovia: Materia Oscura, 2023.

JIMÉNEZ LÓPEZ, María de las Nieves. Las medidas tecnológicas de investigación con régimen especial, practicadas al amparo de una orden europea de investigación. In: FONTESTAD PORTALÉS, Leticia (dir.). JIMÉNEZ LÓPEZ, María de las Nieves (coord.). **El uso de las TICs en la Cooperación Jurídica Penal Internacional:** construyendo la sociedad digital del futuro. Corunha: Colex, 2022. p. 187-224.

MENDES, Carlos Hélder Carvalho Furtado. **Prova penal digital:** direito à não autoincriminação e contraditório na extração de dados armazenados em dispositivos informáticos. São Paulo: Tirant lo Blanch, 2024.

MIRASHI, Eltjon. **Tratamiento procesal del cibercrimen y diligencias de investigación:** casuística y problemática. Pamplona: Aranzadi, 2023.

PRADO, Geraldo. **Curso de Processo Penal:** Tomo I - Fundamentos e Sistema. São Paulo: Marcial Pons, 2024.

PRADO, Geraldo. Parecer: Investigação criminal digital e processo penal. **Revista Brasileira de Ciências Criminais**, v. 199/ nov-dez/2023, p. 315-350.

QUATTROCOLO, Serena. Equità del processo penale e automated evidence alla luce della convenzione europea dei diritti dell'uomo. **Revista Ítalo-Española de Derecho Procesal**, v. 1, 2019, p. 107-123. Madrid: Marcial Pons Ediciones Jurídicas y Sociales. Disponível em: http://www.rivitsproc.eu/wp-content/uploads/2018/11/quattrocolo-equita_proceso_penale_e_automated_evidence.pdf. Consultado em: 25 de junho de 2024.

RAMALHO, David da Silva. **Métodos Ocultos de Investigação Criminal em Ambiente Digital.** Coimbra: Almedina, 2017.

RAZ, Joseph. **O conceito de sistema jurídico**: uma introdução à teoria dos sistemas jurídicos. Trad. de Maria Cecília Almeida. São Paulo: WMF Martins Fontes, 2012.

ROSSI, Helena Costa; ALMEIDA, Leandro Musa de. O uso do malware na investigação criminal: pontos de tensão e limites. **Boletim IBCCRIM**, v. 31, n. 373, dez/2023, p. 20–23. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/693. Consultado em: 14 de outubro de 2024.

SALT, Marcos. Allanamiento remoto: ¿un cambio de paradigma en el registro y secuestro de datos informáticos? In: DUPUY, Daniela (dir.); KIEFER, Mariana (coord.). **Cibercrimen II**. Buenos Aires-Montevideo: Editorial B de F, 2018. p. 151-181.

TORRE, Marco. **Il captatore informatico**: nuove tecnologie investigative e rispetto delle regole processuali. Milano: Giuffrè, 2017.

WEIBLEN, Fabrício Pinto. **Abertura Tecnológica dos Meios de Obtenção de Prova e o Uso de Software Espião na Investigação Criminal**. Coimbra: Almedina, 2024.

ZARAGOZA TEJADA, Javier Ignacio. La prueba ilícita y prueba tecnológica. Reflexiones a raíz del caso Encrochat. In: ORTIZ PRADILLO, Juan Carlos; ABELLÁN ALBERTOS, Antonio (Dir.). **El derecho de defensa en la justicia penal digital.** Valencia: Tirant lo Blanch, 2024. p. 281-348.