Breves notas sobre o fundamento constitucional da cadeia de custódia da prova digital[1]

21 de janeiro de 2021

Por Geraldo Prado

I - A cadeia de custódia da prova consiste em método por meio do qual se pretende preservar a integridade do elemento probatório e assegurar sua autenticidade. A violação da cadeia de custódia implica a impossibilidade de valoração da prova, configurando seu exame – de verificação da cadeia de custódia – um dos objetos do juízo de admissibilidade do meio de prova ou do meio de obtenção de prova, conforme o caso. As consequências jurídicas da quebra da cadeia de custódia não se submetem a juízo de *peso probatório*, sequer de *relevância* da prova.

Não é diferente quando a análise envolve as chamadas provas digitais.[2]

---

[1] Texto correspondente à palestra proferida pelo professor Geraldo Prado intitulada "A interface entre o Direito Digital e o Processo Penal", no Ciclo Permanente de Palestras com o tema "Consequências do Uso da Inteligência Artificial no Processo Penal", oferecido pelo Núcleo de Estudo Luso-Brasileiro da Faculdade de Direito da Universidade de Lisboa (NELB), ao lado da professora Janaina Matida e do professor Alexandre Morais da Rosa, em 20 de janeiro de 2021, às 13 horas (horário de Brasília), transmitida pelo aplicativo *Zoom*. O referido evento ainda será disponibilizado no canal do NELB no site *Youtube*, acessível por meio do seguinte link: https://www.youtube.com/channel/UCisAlkBfPlphVWnZa-18WHQ. Consultado em 21 de janeiro de 2021.

[2] Sem embargo da afirmação, o trabalho pericial também poderá contribuir para a identificação de provas relevantes contidas em dispositivos informáticos, como salientam Irfan Ahmed e Vassil Roussev: "A noção de *relevância* é inerentemente específica a cada caso e uma grande parte da competência de um analista forense é a capacidade de identificar provas relevantes a um caso. Frequentemente, um componente crítico da análise forense é a *atribuição* causal de uma sequência de eventos a atores humanos específicos do sistema (tais como usuários e administradores). Quando utilizados em processos judiciais, a *proveniência*, a *confiabilidade* e a *integridade* dos dados utilizados como prova são de suma importância. Em outras palavras, consideramos todos os esforços para realizar análises de sistema ou de artefatos após o fato como uma forma de perícia forense. Isso inclui atividades comuns tais como a resposta a incidentes e investigações internas, que quase nunca resultam em quaisquer processos judiciais. Em geral, somente uma pequena fração das análises forenses chega às salas de audiência como provas formais." Tradução Livre. No original: "The notion of *relevance* is inherently case-specific, and a big part of a forensic analyst's expertise is the ability to identify case-relevant evidence. Frequently, a critical component of the forensic analysis is the causal *attribution* of an event sequence to specific human actors of the system (such as users and administrators). When used in legal proceedings, the *provenance*, *reliability*, and *integrity* of the data used as evidence are of primary importance. In other words, we view all efforts to perform system or artefact analysis after the fact as a form of forensics. This includes common activities such as incident response and internal investigations, which almost never result in any legal actions. On balance, only a tiny fraction of forensic analyses make it to the courtroom as formal evidence.". AHMED, Irfan; ROUSSEV, Vassil. Analysis of Cloud Digital Evidence. In: CHEN, Lei; TAKABI, Hassan; LE-KHAC, Nhien-An (ed.).

O tema da cadeia de custódia da prova digital, todavia, é bem ilustrativo da interseção entre conceitos consagrados há séculos no direito processual penal de matriz continental europeia e novos conceitos e noções que resultam da vida biodigital dos nosso tempo.

Didaticamente, portanto, a compreensão da matéria requisita sejam revisitados, em primeiro lugar, a noção e o papel do *corpo de delito* na apuração da responsabilidade criminal e depois disso a especificidade que caracteriza a prova digital, tecnológica ou *e-evidence*, como é conhecida.

II - O professor italiano Renzo Orlandi resgata o momento em que no século XVI, juristas italianos e alemães incorporaram as categorias da *inquisitio generalis* e *specialis*, a *veritas criminis* e o *corpus delicti*, já presentes nas obras dos glosadores e pós-glosadores "ao léxico [jurídico]... a partir dos primeiros comentários... [à] *Constitutio Criminalis Carolina*".[3]

A ideia central, reforçada desde então, era de que a primeira etapa da persecução – a *inquisitio generalis* – tinha por meta "apurar a existência do crime na sua palpável objetividade". Acentua Orlandi que se acreditava que "a primeira tarefa do inquisidor consistisse em pesquisar a *veritas criminis*, ou, segundo expressão análoga, o *corpus delicti* ou o *constare de delicto*."[4]

A precedência da verificação do corpo de delito obedecia a uma questão de ordem lógica: "do fato criminoso deriva a responsabilidade do autor", representando o *corpus delicti* "um limite e um freio aos possíveis excessos do juiz".[5]

Security, Privacy, and Digital Forensics in the Cloud. Hoboken, Singapura: John Wiley & Sons, 2019. p. 301-302.

[3] ORLANDI, Renzo. Investigações preparatórias nos procedimentos de criminalidade organizada: uma reedição da inquisitio generalis? in: Lições Contemporâneas do Direito Penal e do Processo Penal (Org. Luiza Borges Terra). 1. ed. Florianópolis, Tirant lo Blanch, 2021. No prelo.

[4] ORLANDI, Renzo. Investigações preparatórias nos procedimentos de criminalidade organizada: uma reedição da inquisitio generalis? in: Lições Contemporâneas do Direito Penal e do Processo Penal (Org. Luiza Borges Terra). 1. ed. Florianópolis, Tirant lo Blanch, 2021. No prelo.

[5] ORLANDI, Renzo. Investigações preparatórias nos procedimentos de criminalidade organizada: uma reedição da inquisitio generalis? in: Lições Contemporâneas do Direito Penal e do Processo Penal (Org. Luiza Borges Terra). 1. ed. Florianópolis, Tirant lo Blanch, 2021. No prelo.

No século XIX, Savigny, encarregado de preparar projeto de Código de Processo Penal da Prússia, irá se debruçar sobre o tema da prova, separando claramente os momentos da admissibilidade e da valoração, esta etapa sim sujeita à análise da "força probatória".[6] No texto de exposição de motivos do anteprojeto de Código o jurista tedesco distinguirá a *prova legal negativa*, portadora de uma questão de admissibilidade, da criticada *prova legal positiva*, que traduziria escala de valoração apriorística da prova incompatível com o estágio da ciência vigente. O corpo de delito era relevante.

O primeiro processualista penal brasileiro, João Mendes de Almeida Junior, forte nas lições do jurista português Pereira e Souza, não discrepará da opinião dominante a respeito da função e precedência do corpo de delito, "base de todo procedimento criminal".[7]

"O corpo de delito somente prova o delito, porém, não mostra o delinquente",[8] advertia o mestre das Arcadas que, entre outras virtudes relembrará a mesma lição, ofertada por Tobias Barreto, na valiosíssima apreciação sobre "[a] consideração dos meios [que] tem importância no processo criminal como *corpus delicti*, como sinais do fato".[9]

A ordem lógica de análise do corpo de delito é evidente, como reconheceram os práticos. Em uma investigação de homicídio trata-se de premissa verificar se a vítima não morreu de «causa natural», isto é, se a morte da vítima foi realmente provocada pela conduta de outrem.

---

[6] SAVIGNY, Friedrich Carl Von. Le questioni di principio concernenti un nuovo regolamento del processo penale. Edizione e traduzione italiana a cura di Paolo Rondini. Milano: Giuffrè, 2012. p. 73. Publicação original: 1846.

[7] ALMEIDA JUNIOR, João Mendes de. *O Processo Criminal Brazileiro*. Volume II. Rio de Janeiro: Typ. Baptista de Souza, 3ª edição, 1920. P. 17.

[8] ALMEIDA JUNIOR, João Mendes de. *O Processo Criminal Brazileiro*. Volume II. Rio de Janeiro: Typ. Baptista de Souza, 3ª edição, 1920. P. 17.

[9] BARRETO, Tobias. Comentário Teórico e Crítico ao Código Criminal Brasileiro. In: BARRETO, Tobias. BARRETO, Luiz Antonio (Org.). *Estudos de direito II*. Rio de Janeiro: J. E. Solomon; Segipe: Editora Diário Oficial, 2012. p. 203.

Por isso, o corpo de delito ao menos ao longo dos últimos séculos mereceu regramento que, na hipótese de a conduta deixar vestígios, importava realização de perícia a cargo de pessoas com amplo domínio acerca do específico campo do saber (científico, técnico ou artístico).

Neste contexto, mesmo na vigência de ditaduras (o fascismo italiano e o Estado Novo, no Brasil), os Códigos de Processo Penal (CPPs) dos anos 30/40 de Itália e Brasil reservaram a *peritos* a tarefa de constatação do corpo de delito. Hélio Tornaghi lembrava que o exame de corpo de delito "nada mais é que uma perícia, a principal, a mais importante de todas as perícias."[10]

E Manzini, por sua vez, sublinhava à luz do CPP italiano de 30, que por a perícia ter "caráter jurídico", é encargo de *experts* imparciais e não se confunde com a avaliação do elemento probatório levada a efeito por investigadores, advogados, ministério público e juízes, tendo a perícia no processo criminal seu território por excelência.[11] Não é o caráter técnico que distingue a perícia de outra prova, alertava o jurista italiano, mas a condição assumida no contexto da jurisdição, condição que por evidente considera o saber diferenciado do perito, porém, também e com ênfase, seu afastamento das hipóteses que surgem desde a notícia crime (imparcialidade).[12]

O direito brasileiro contempla a determinação do corpo de delito por meio de perícia, nos casos em que a conduta deixa vestígios. Era assim à luz das regras originais do CPP de 1941 e isso se tornou incontroverso após a minirreforma do processo penal, em 2008, por meio da edição da Lei nº 11.690.

---

[10] TORNAGHI, Hélio. *Instituições de Processo Penal*. Volume IV. Rio de Janeiro: Forense, 1959. P. 276.
[11] MANZINI, Vincenzo. *Tratado de Derecho Procesal Penal*. Tomo III – Los Actos del Proceso Penal. Tradução de Santiago Sentís Melendo e Marino Ayerra Redín. Buenos Aires: Librería El Foro, 2003. P. 379, 380, 381, 383 e 399.
[12] MANZINI, Vincenzo. *Tratado de Derecho Procesal Penal*. Tomo III – Los Actos del Proceso Penal. Tradução de Santiago Sentís Melendo e Marino Ayerra Redín. Buenos Aires: Librería El Foro, 2003. P. 378/379.

Entre as alternativas possíveis – sistema de perícia de partes e sistema oficial de perícias – o processo penal brasileiro optou pelo segundo e o aperfeiçoou facultando aos interessados (durante a investigação criminal) e às partes (ao longo do processo) a constituição de assistentes técnicos.

Será visto que o modelo de perícia oficial cumprirá função de garantia fundamental no contexto da prova digital, mas é imprescindível rematar aqui que a cadeia de custódia dos elementos probatórios é uma consequência inevitável e obrigatória do modelo escolhido, porque a etapa prévia de acertamento do fato é dependente da segurança na preservação dos vestígios.

Retornando ao exemplo do homicídio, se é imprescindível verificar a causa da morte da vítima, antes mesmo é ainda mais relevante saber se o cadáver examinado é o da vítima do caso investigado.

É óbvio que se João está sendo investigado sob suspeita de matar José e o cadáver examinado não é de José, mas de alguém completamente diferente (uma mulher, uma criança, um idoso), o laudo de exame de corpo de delito é inadmissível como prova, não deve ingressar nos autos e se inadvertidamente o fizer deve ser excluído, sendo proibida a sua valoração.

Violada a cadeia de custódia do elemento probatório, não é mais possível assegurar a autenticidade da prova e sua integridade, sendo a prova inadmissível e, pois, insuscetível de exame de peso ou força probatória.

Isso é assim no exemplo supra, e o é igualmente na hipótese de violação da cadeia de custódia de armas, drogas ou quaisquer outros vestígios, incluindo os elementos digitais, elementos probatórios insuscetíveis de valoração ainda que a título de corroboração por outras provas. Trata-se de atividades probatórias funcionalmente distintas e inconfundíveis.

Retomar às lições de João Mendes de Almeida Junior sobre a amplitude do objeto que caracteriza o *corpo de delito* por certo favorecerá o entendimento do tema.[13]

Não há dúvida de que a cadeia de custódia é condição de procedibilidade do exame de corpo de delito. Por isso no Brasil o instituto mereceu ser regulado pela Lei nº 13.964/2019 no artigo 158-A-F do CPP.

III - O valor da cadeia de custódia é sensivelmente incrementado quando o elemento probatório é de natureza digital. Releva notar que se manuais, guias de procedimento, atos normativos de toda espécie, estatais e supra estatais, enfatizam em geral o papel que a cadeia de custódia desempenha para assegurar integridade e autenticidade à prova digital, fato é que a jurisprudência firmada por cortes constitucionais e tribunais de direitos humanos assinala à cadeia de custódia da prova digital funções ainda mais relevantes.

Com efeito, referindo-se a duas decisões paradigmáticas do Tribunal Constitucional Federal alemão, de 27 de fevereiro de 2008[14] e de 20 de abril de 2016,[15] Wolfgang Hoffmann-Riem chama atenção para o reconhecimento de que a tutela da autodeterminação informativa foi ultrapassada na direção da proteção constitucional especial dos sistemas de tecnologia de informação e comunicação.[16]

---

[13] ALMEIDA JUNIOR, João Mendes de. *O Processo Criminal Brazileiro*. Volume II. Rio de Janeiro: Typ. Baptista de Souza, 3ª edição, 1920. P. 9-11 e 16, com menção, para a ação penal, à imprescindibilidade do exame de corpo de delito nos crimes que deixam vestígios.

[14] ALEMANHA. Bundesverfassungsgericht (Tribunal Constitucional Federal da Alemanha). BVerfGE 120, 274. 1 BvR 370/07; 1 BvR 595/07. Decisão. Data: 27 de fevereiro de 2008. Versão em inglês disponível em: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2008/02/rs20080227_1bvr037007en.html. Consultado em 14 de janeiro de 2021.

[15] ALEMANHA. Bundesverfassungsgericht (Tribunal Constitucional Federal da Alemanha). BVerfGE 141, 220. 1 BvR 966/09; 1 BvR 1140/09. Decisão. Data: 20 de abril de 2016. Versão em inglês disponível em: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2016/04/rs20160420_1bvr096609en.html. Consultado em 19 de janeiro de 2021.

[16] HOFFMANN-RIEM, Wolfgang. *Teoria geral do direito digital*. Transformação digital. Desafios para o direito. Trad. de Italo Fuhrmann. Rio de Janeiro: Forense, 2021. p. 49.

Wolfgang Hoffmann-Riem alude ao direito fundamental independente orientado a assegurar a confidencialidade e a integridade dos sistemas de tecnologia da informação.

Assim é que a decisão de fevereiro de 2008, do Tribunal Constitucional Federal alemão, reconheceu, de forma expressa: "1. O direito geral da personalidade (artigo 2.1 em conjunto com o artigo 1.1 da Lei Fundamental (*Grundgesetz - GG*)) abrange o direito fundamental à garantia da confidencialidade e integridade dos sistemas de tecnologia da informação."[17]

Tutela da confidencialidade e garantia da integridade dos sistemas de tecnologia da informação também são funções destacadas que a cadeia de custódia da prova digital irá cumprir, **ao lado da verificação da autenticidade e integridade da informação (dado digital)** que se pretende que sirva de elemento probatório. Isso sem perder de vista o direito à proteção do entorno digital, da identidade digital, do domicílio digital e, por óbvio, da privacidade associada ao direito de decidir o que tornar público ou não relativamente à esfera da vida da pessoa.[18]

Neste sentido, compreende-se a imensa preocupação de legislação e doutrina, em nível internacional, com a preservação da cadeia de custódia da prova digital, inadmitindo-se a prova à vista da demonstração de sua violação.

Aqui também convém ser didático. Com efeito, é indispensável saber que a *e-evidence*, prova eletrônica ou prova digital se caracteriza por ser "qualquer

[17] Tradução livre da versão em inglês. No original (inglês): "1. The general right of personality (Article 2.1 in conjunction with Article 1.1 of the Basic Law (*Grundgesetz – GG*)) encompasses the fundamental right to the guarantee of the confidentiality and integrity of information technology systems. (…) ALEMANHA. Bundesverfassungsgericht (Tribunal Constitucional Federal da Alemanha). BVerfGE 120, 274. 1 BvR 370/07; 1 BvR 595/07. Decisão. Data: 27 de fevereiro de 2008. Ementa. Versão em inglês disponível em: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2008/02/rs20080227_1bvr037007en.html. Consultado em 14 de janeiro de 2021.

[18] PRADO, Geraldo. Notas sobre proteção de dados, prova digital e o devido processo penal. *Site Geraldo Prado*, 18 de agosto de 2020. Disponível em: https://geraldoprado.com.br/artigos/notas-sobre-protecao-de-dados-prova-digital-e-o-devido-processo-penal/. Consultado em: 19 de janeiro de 2021.

classe de informação (dados) que tenha sido produzida, armazenada ou transmitida por meios eletrônicos".[19]

O surgimento quase cotidiano de novas tecnologias do gênero desanima a elaboração de uma taxonomia das «provas digitais», como, por exemplo, aparece sob a denominação de «ativos de Tecnologia de Informação e Comunicação (TIC)» nos artigos 3º e 4º da Portaria nº 242 de 10 de novembro de 2020 do Conselho Nacional de Justiça (CNJ), que cria o Comitê de Segurança Cibernética do Poder Judiciário brasileiro.

De toda maneira, dada a digitalização da vida, que afeta todas as suas dimensões, é possível buscar alguma sistematização a partir das fontes da prova digital, revelando-se, pela mera exposição, o grau de dificuldade da tarefa de preservar a integridade do elemento probatório digital e verificar sua autenticidade, além de determinar o cuidado extremado que se deve ter, haja vista os riscos concretos de manipulação e alteração dos dados.[20]

Assim, temos, conforme Joaquín Delgado Martín, a informação digital disponível: a) nas redes sociais e páginas da Web; b) em dispositivos eletrônicos; c) armazenados em provedores de serviços.[21]

---

[19] DELGADO MARTÍN, Joaquín. *Judicial-Tech, el proceso digital y la transformación tecnológica de la justicia*: Obtención, tratamiento y protección de datos en la justicia. Madrid: Wolters Kluwer, 2020. P. 55.

[20] Para ilustrar, mais uma vez, Ahmed e Roussev destacam as dificuldades inerentes à perícia em face de novas tecnologias: **"A perícia forense digital é fundamentalmente reativa por natureza – não podemos investigar sistemas e artefatos que não existem; não podemos ter *melhores práticas* antes de um período experimental durante o qual diferentes abordagens técnicas são experimentadas, testadas (perante os tribunais) e validadas. Isso significa que sempre há um atraso entre a introdução de um objeto de tecnologia da informação e o tempo em que uma capacidade forense correspondente adequada é implementada. A evolução da infraestrutura das tecnologias da informação é impulsionada pela economia e pela tecnologia; a perícia forense apenas identifica e segue as migalhas digitais deixadas para trás."** Tradução Livre. No original: "Digital forensics is fundamentally reactive in nature – we cannot investigate systems and artifacts that do not exist; we cannot have *best practices* before an experimental period during which different technical approaches are tried, (court-) tested, and validated. This means there is always a lag between the introduction of a piece of information technology and the time an adequate corresponding forensic capability is in place. The evolution of the IT infrastructure is driven by economics and technology; forensics merely identifies and follows the digital breadcrumbs left behind.". AHMED, Irfan; ROUSSEV, Vassil. Analysis of Cloud Digital Evidence. In: CHEN, Lei; TAKABI, Hassan; LE-KHAC, Nhien-An (ed.). *Security, Privacy, and Digital Forensics in the Cloud*. Hoboken, Singapura: John Wiley & Sons, 2019. p. 302.

[21] DELGADO MARTÍN, Joaquín. *Judicial-Tech, el proceso digital y la transformación tecnológica de la justicia*: Obtención, tratamiento y protección de datos en la justicia. Madrid: Wolters Kluwer, 2020. P. 55/56.

Os dados podem ainda estar *nas nuvens* (*in the cloud*) em sistemas privados, públicos, híbridos, móveis e comunitários,[22] alimentados em redes abertas ou fechadas que cada dia com maior frequência se caracterizam pela ubiquidade.

Com isso, por exemplo, a apreensão de computadores por si só não garante integridade da informação e autenticidade da fonte de prova, estas sujeitas a adoção de métodos que consideram algoritmos criptografados destinados a reter e preservar os dados (cópias espelho e lógica e cálculo da função HASH).[23] Adiante estas técnicas serão mencionadas.

Acrescentem-se ao arsenal investigativo as tecnologias de acesso remoto e o domínio ou não, pelas autoridades de investigação, das chaves de acesso aos repositórios de dados e se compreenderá a imperatividade atribuída à adoção de métodos de preservação da cadeia de custódia da prova digital em guias e roteiros de investigação digital.

Como sublinhado no *Mobile Forensic Investigations*, quando a prova está armazenada em dispositivos móveis incidem duas diferentes cadeias de custódia: uma sobre o equipamento; e outra acerca dos dados coletados no próprio equipamento.[24]

O guia de apreensão, análise e apresentação da prova eletrônica obtida em dispositivo móvel acentua o caráter de extraordinária importância que a cadeia de custódia assume.[25]

---

[22] DELGADO MARTÍN, Joaquín. *Judicial-Tech, el proceso digital y la transformación tecnológica de la justicia*: Obtención, tratamiento y protección de datos en la justicia. Madrid: Wolters Kluwer, 2020. P. 55.

[23] FÉRNANDEZ MARTÍNEZ, Juan Carlos. Especialidades de la prueba cuando, esta, es tecnológica. In: ORTEGA BURGOS, Enrique. *Actualidad: Nuevas Tecnologías*. Valencia: Tirant lo Blanch, 2020. P. 336/337.

[24] "A perícia forense digital é o processo de reconstrução da sequência relevante de eventos que levaram ao estado atualmente observável de um sistema de tecnologia da informação ou artefatos (digitais) em específico." (Tradução livre). No original: "When it comes to electronic evidence from a mobile device, there are two different chains of custody: one for the physical device and another for the data collected from the device.". REIBER, Lee. *Mobile forensic investigations*: A Guide to Evidence Collection, Analysis, and Presentation. Nova Iorque: McGraw-Hill Education, 2ª edição, 2018. p. 84.

[25] "Nota: O estabelecimento de uma cadeia de custódia é um dos detalhes mais importantes em relação às provas coletadas no local. Isso é extremamente importante nos casos em que a prova é encontrada no local por uma pessoa, que entrega essa prova a outra pessoa, que então leva esse dispositivo à pessoa que irá realizar a extração do dispositivo. Como descrito, a cadeia de custódia seria extremamente difícil de ser

Reitere-se que há dificuldades práticas geradas pelo incremento veloz dos dispositivos e programas empregados no âmbito das TICs, o que leva a que a perícia hoje seja basicamente reativa, como salientaram Ahmed e Roussev,[26] o que, todavia, não impede que se apliquem metodologias internacionalmente consagradas, dirigidas à preservação da prova eletrônica.[27]

Importa aqui entender, neste momento, principalmente, que a cadeia de custódia das provas digitais é uma **garantia de natureza constitucional** e não mera consequência lógica do sistema de preservação do *corpo de delito digital*.

IV – Por meio da cadeia de custódia das provas digitais são tutelados os **direitos fundamentais à confidencialidade e garantia da integridade dos sistemas de tecnologia da informação**, à proteção do entorno digital, da identidade digital, do domicílio digital e, por óbvio, da privacidade associada ao direito de decidir o que tornar público ou não relativamente a essa esfera da vida.

---

mantida sem documentação. Se a documentação não for registrada corretamente, todo o processo e a admissibilidade das provas serão, sem dúvida, questionados." (Tradução livre). No original: "Note: Establishing a chain of custody is one of the most important details regarding evidence collected at a scene. This is extremely important in cases when the evidence is located at the scene by one person, who hands that evidence to another, who then takes that device to the person who will conduct the device extraction. As described, the chain of custody would be extremely difficult to maintain without documentation. If documentation is not captured correctly, the entire process and the admissibly of the evidence will undoubtedly be questioned.". REIBER, Lee. *Mobile forensic investigations*: A Guide to Evidence Collection, Analysis, and Presentation. Nova Iorque: McGraw-Hill Education, 2ª edição, 2018. p. 101.

[26] No original: "Digital Forensics is the process of reconstructing the relevant sequence of events that have led to the currently observable state of a target IT system or (digital) artifacts.". AHMED, Irfan; ROUSSEV, Vassil. Analysis of Cloud Digital Evidence. In CHEN, Lei; TAKABI, Hassan; LE-KHAC, Nhien-An (ed.). *Security, Privacy, and Digital Forensics in the Cloud*. Hoboken, Singapura: John Wiley & Sons, 2019. p. 301.

[27] International Organization for Standardization. ISO/IEC 27037:2012. Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence. Norma técnica. Publicada em outubro de 2012. Revisada e confirmada em 2018. Versão vigente. Disponível para aquisição em: https://www.iso.org/standard/44381.html. Consultado em: 20 de janeiro de 2021; Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC 27037:2013. Tecnologia da informação — Técnicas de segurança — Diretrizes para identificação, coleta, aquisição e preservação de evidência digital. Identifica a: ISO/IEC 27037:2012. Norma técnica. Publicada em 09 de dezembro de 2013. Confirmada em 26 de novembro de 2018. Versão vigente. Disponível para aquisição em: https://www.abntcatalogo.com.br/norma.aspx?ID=307273. Consultado em: 20 de janeiro de 2021.

Justamente porque se trata de tutela de informações sensíveis é que a proteção da integridade dos sistemas de tecnologia da informação, pelo CNJ, na proposta de criação do Comitê de Segurança Cibernética do Poder Judiciário, confere evidência a que idêntica proteção seja assegurada a todas as pessoas. A «segurança cibernética» é igualmente um novo direito fundamental, oponível verticalmente ao Estado e horizontalmente às pessoas de direito privado.

O caráter sensível do dado que pode servir de elemento probatório eletrônico e a multifuncionalidade dos dados e dispositivos digitais que, em virtude da convergência de tecnologias, podem levar a que dispositivos digitais contenham ao mesmo tempo informações de interesse da investigação criminal e outras, da esfera privada constitucionalmente protegida do investigado, impõem providências adicionais de preservação da cadeia de custódia da prova digital que a diferenciam em grau de complexidade e relevância normativa da tutela da cadeia de custódia ordinária.

Não por outra razão, a decisão de 20 de abril de 2016, do Tribunal Constitucional Federal alemão, deliberou pela adoção de salvaguardas ao nível da coleta e seleção dos dados, afastando da tarefa quer entes privados, quer mesmo o investigador.

Vale aqui reproduzir a interessante passagem da decisão que a rigor reconhece o caráter manipulável da informação digital e seu possível emprego enviesado na investigação criminal, tolhendo esse desvio por meio da participação de um órgão público que teria a responsabilidade pela triagem dos dados. Segue a passagem:

> "Se, entretanto, dados relevantes para a área central não puderem ser filtrados antes ou no momento da coleta de dados, o acesso ao sistema de tecnologia da informação é, no entanto, permitido, mesmo que seja provável que dados altamente pessoais também

> possam ser coletados incidentalmente. **A este respeito, o legislador deve levar em conta a necessidade de proteção da pessoa em questão, colocando em vigor salvaguardas nos níveis de análise e uso, e minimizando os efeitos de tal acesso. É atribuída importância decisiva à triagem por um órgão independente que filtra as informações relevantes à área central antes da sua disponibilidade e uso pelo Departamento de Polícia Criminal Federal** (cf. BVerfGE 120, 274 <338 e 339>).”[28] (Grifo nosso).

Derivam, pois, do caráter constitucional que assume a proteção da cadeia de custódia da prova digital, não somente a imperatividade da perícia oficial, independente e imparcial também em relação à própria investigação criminal, à acusação e à defesa, como a proibição absoluta de delegar a entes privados a tarefa de exame do corpo de delito. A atuação de partes e interessados deverá ser necessariamente supletiva, em reforço ao contraditório.

A proteção da informação digital é de tal ordem tutela reforçada do Estado de Direito, por conta da multifuncionalidade dos dados e dispositivos digitais em um contexto *on life*, tal seja, de vida digital, que a Constituição dirige ao legislador ordinário um mandado de regulação que especificamente diz com os temas da segurança pública e da responsabilização criminal.

---

[28] Tradução livre da versão em inglês. No original (inglês): “If, however, data relevant to the core area cannot be filtered out before or at the time of the data collection, access to the information technology system is nevertheless permissible even if it is probable that highly personal data too might incidentally be collected. In this respect, the legislature must take into account the need for protection of the person concerned by putting in place safeguards at the levels of analysis and use, and by minimising the effects of such access. Decisive significance attaches to the screening by an independent body that filters out information relevant to the core area prior to its availability to and use by the Federal Criminal Police Office (cf. BVerfGE 120, 274 <338 and 339>).”. ALEMANHA. Bundesverfassungsgericht (Tribunal Constitucional Federal da Alemanha). BVerfGE 141, 220. 1 BvR 966/09; 1 BvR 1140/09. Decisão. Data: 20 de abril de 2016. Parágrafo nº. 220. Versão em inglês disponível em: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2016/04/rs20160420_1bvr096609en.html. Consultado em 19 de janeiro de 2021.

Este é o contexto que permeia a Lei nº. 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados - LGPD).[29]

Neste sentido, os artigos 3º e 4º da LGPD vedam o tratamento dos dados sobre segurança pública, defesa nacional, segurança do Estado ou **atividades de investigação e repressão de infrações penais por pessoa de direito privado**, exceto em procedimentos sob tutela de pessoa jurídica de direito público.[30]

---

[29] BRASIL. Lei nº. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD).

[30] Art. 3º, LGPD. Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que: I - a operação de tratamento seja realizada no território nacional; ~~II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou (Redação dada pela Medida Provisória nº 869, de 2018)~~ II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou (Redação dada pela Lei nº 13.853, de 2019) Vigência III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional. § 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta. § 2º Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do caput do art. 4º desta Lei.

Art. 4º, LGPD. Esta Lei não se aplica ao tratamento de dados pessoais: I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos; II - realizado para fins exclusivamente: a) jornalístico e artísticos; ou ~~b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei; b) acadêmicos; (Redação dada pela Medida Provisória nº 869, de 2018)~~ b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei; III - realizado para fins exclusivos de: a) segurança pública; b) defesa nacional; c) segurança do Estado; ou d) atividades de investigação e repressão de infrações penais; ou IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei. § 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei. ~~§ 2º É vedado o tratamento dos dados a que se refere o inciso III do caput deste artigo por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico à autoridade nacional e que deverão observar a limitação imposta no § 4º deste artigo. § 2º O tratamento dos dados a que se refere o inciso III do caput por pessoa jurídica de direito privado só será admitido em procedimentos sob a tutela de pessoa jurídica de direito público, hipótese na qual será observada a limitação de que trata o § 3º. (Redação dada pela Medida Provisória nº 869, de 2018)~~ § 2º É vedado o tratamento dos dados a que se refere o inciso III do caput deste artigo por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico à autoridade nacional e que deverão observar a limitação imposta no § 4º deste artigo. ~~§ 3º A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais. § 3º Os dados pessoais constantes de bancos de dados constituídos para os fins de que trata o inciso III do caput não poderão ser tratados em sua totalidade por pessoas jurídicas de direito privado, não incluídas as controladas pelo Poder Público. (Redação dada pela Medida Provisória nº 869, de 2018)~~ § 3º A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais. ~~§ 4º Em nenhum caso a totalidade dos dados pessoais de banco de dados de que trata o inciso III do caput deste artigo poderá ser tratada por pessoa de direito~~

O Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal, elaborado por Grupo de Trabalho criado pela Câmara dos Deputados igualmente reproduz a interdição:[31]

> Art. 10. É vedado o tratamento de dados pessoais para atividades de segurança pública e de persecução penal por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico ao Conselho Nacional de Justiça, sem prejuízo de outras exigências legais.
>
> [...]
>
> Art. 14. O tratamento de dados pessoais sigilosos por autoridades competentes somente poderá ser realizado se estiver previsto em lei e para atividades de persecução penal.
>
> §1º O acesso a dados pessoais sigilosos por meio de ferramentas de investigação e medidas cautelares de obtenção de prova deve observar a legislação especial aplicável.
>
> 2º O acesso a dados pessoais sigilosos controlados por pessoas jurídicas de direito privado será específico a pessoas investigadas e dependerá de ordem judicial prévia baseada em indícios de envolvimento dos

~~privado. (Revogado pela Medida Provisória nº 869, de 2018)~~ § 4º Em nenhum caso a totalidade dos dados pessoais de banco de dados de que trata o inciso III do caput deste artigo poderá ser tratada por pessoa de direito privado, salvo por aquela que possua capital integralmente constituído pelo poder público. (Redação dada pela Lei nº 13.853, de 2019) Vigência.

[31] Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal, elaborado por Grupo de Trabalho criado pela Câmara dos Deputados para sua formulação. Texto integral disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissao-de-juristas-dados-pessoais-seguranca-publica/documentos/outros-documentos/DADOSAnteprojetocomissaoprotecaodadossegurancapersecucaoFINAL.pdf. Consultado em 11 de novembro de 2020.

> titulares de dados afetados em infração penal e na demonstração de necessidade dos dados à investigação, na forma da lei, sem prejuízo da comunicação de operações suspeitas, nos termos do art. 11 da Lei nº 9.613.

A realidade é que a prova digital demanda princípios cujo caráter cogente é imprescindível para a defesa da dignidade da pessoa humana. A prova digital é central, decisiva para o esclarecimento das infrações penais, indispensável para a defesa da democracia contra ataques do poder econômico e do poder político.

Para que cumpra satisfatoriamente estas tarefas, a prova digital também deve assegurar transparência, controle, proporcionalidade e condições concretas de efetivação de um contraditório digital.

Com este propósito, um grupo de juristas sugeriu à Comissão Especial da Câmara dos Deputados para a elaboração do novo Código de Processo Penal brasileiro a adoção de dispositivo que contemple alguns destes princípios:

> "Princípios para o uso da tecnologia na persecução penal
>
> Art. 8º - Na persecução penal admite-se o uso de quaisquer meios tecnológicos, dentre eles a inteligência artificial, desde que não ofensivos à Dignidade da Pessoa Humana e outros Direitos Fundamentais, respeitados o Devido Processo Legal, o Contraditório e a Ampla Defesa, no ambiente digital, atentando-se em particular para:
>
> I – a proibição de tratamento de dados sensíveis sem relação com o processo, tais como raça, gênero,

situação socioeconômica, orientação sexual, ou qualquer outro dado que possa gerar discriminação.

II – a qualidade e a segurança dos dados obtidos, de modo a assegurar a confiabilidade das fontes e a cadeia de custódia, garantindo a rastreabilidade e a confiabilidade dos resultados obtidos.

III – a transparência técnica e a auditabilidade externa das tecnologias e das ferramentas de inteligência artificial, vedando-se, no caso das ferramentas de inteligência artificial, o segredo das variáveis utilizadas, dos objetivos pretendidos pela otimização dos algoritmos, os desvios encontrados, devendo ser regularmente corrigidos para o alcance de maior equidade em seu uso.

IV – a vedação do uso de ferramentas preditivas, sendo proibidas decisões judiciais não humanas, quaisquer que sejam seu objeto, para fins do processo penal.

V – a vedação do uso indiscriminado e ininterrupto de meios de geolocalização dirigidos a pessoas ou grupos ou ambientes nos quais são realizados atos predominantemente privados.

VI – a duração estritamente necessária do emprego dos meios tecnológicos para os fins legítimos da persecução.

VII – a subsidiariedade do emprego dos meios tecnológicos, que somente serão utilizados quando fundamentadamente comprovado que os demais não se

> mostram suficientes ou adequados para fins da obtenção de meios de prova."[32]

V - Relativamente aos dados digitais, a preservação da cadeia de custódia da prova é uma entre as diversas técnicas de certificação dos elementos apresentados, de modo que deverá responder aos questionamentos sobre a «integralidade» (o documento/objeto apresentado como prova se encontra da mesma forma em que foi originalmente adquirido?), a «espoliação» (houve alterações intencionais no documento/objeto durante o manuseio ou análise, ou a evidência em potencial foi destruída em antecipação a uma investigação?) e a «volatilidade» (o documento/objeto é suscetível de mudança devido a fatores mecânicos, ambientais ou de passagem de tempo?).[33]

Ao cuidar especificamente da cadeia de custódia de dados digitais, Jacob Heilik destaca a necessidade de autenticação e da demonstração da proveniência desses dados. Pela clareza e importância das observações, reproduz-se o trecho da obra do autor canadense:

> "A proveniência é importante porque fornece uma ligação clara entre a informação apresentada e a fonte legalmente adquirida da qual provém. A autenticação é importante para estabelecer que a informação apresentada não foi alterada desde o momento em que foi coletada – ou seja, não é nem mais nem menos do que os dados da fonte original."[34]

---

[32] MORAIS, Flaviane de Magalhães Barros Bolzan de; *et al*. *Novo Código Processual Penal*: sugestões do Grupo de Trabalho de apoio à Comissão Especial do Código. Brasília, 2020. p. 8-9.

[33] HEILIK, Jacob. *Chain of Custody for Digital Data*: A Practitioner's Guide. Canadá: Independently published, 2019. p. 15-16.

[34] Tradução livre. No original: "Provenance is important because it provides a clear link between the introduced information and the lawfully acquired source from which it comes. Authentication is important to establish that the introduced information has not been altered since the time it was collected – that is, it is no more and no less than the original source data." (HEILIK, Jacob. *Chain of Custody for Digital Data:* A Practitioner's Guide. Canadá: Independently published, 2019. p. 16-17).

A propósito também leciona Michele Taruffo, no que concerne ao processo civil, no qual não está em jogo a liberdade do acusado:

> "68. *Os computadores como fontes de prova.* Os avanços da informática e da telemática, bem como o uso cotidiano dos computadores em um número crescente de domínios, têm extensos efeitos na experiência jurídica e na sua prática. Alguns desses efeitos relacionam-se às provas no processo civil: cada vez com mais frequência negócios são realizados ou documentados por computadores, e os registros informáticos e as cópias impressas são comumente usados como meios de prova. Assim, dada a natureza singular dos dados armazenados nos computadores e as importantes diferenças existentes entre tais dados e documentos escritos, a questão é definir se esse tipo peculiar de dados e documentos pode ser admitido como prova judicial, assim como a definição da forma de coleta e apresentação e a determinação do seu valor probatório.
>
> [...]Portanto, o perigo de falsificação, erros e uso indevido ou abuso são especialmente frequentes e relevantes e, em certa medida, ainda desconhecidos. Os vários sistemas jurídicos empenham-se em reagir a essa situação na tentativa de oferecer uma regulação adequada do novo domínio das 'provas informáticas'."[35]

A importância do tema não é pequena. Para constatar isso, basta observar o que afirma o Procurador da República Antonio do Passo Cabral. Em

[35] TARUFFO, Michele. *A prova*. São Paulo: Marcial Pons, 2014. p. 83-84.

interessante texto, ao tratar do tema da metaprova (*meta-evidence*), o primeiro observará:

> «Cresce em importância, de um lado, analisar o procedimento de produção da prova, especialmente quando produzida por entes privados. E, de outro lado, indagar a respeito da integridade dos elementos de prova colhidos, cuidando para que os registros não sejam adulterados (com inserção de dados falsos, do rosto de pessoas que nunca estiveram naquele local etc.). Fala-se, na práxis, em investigar a cadeia de custódia da prova, perquirindo o caminho da produção à juntada da prova em juízo.»[36]

A título de exemplo, o «*Eletronic Evidence Guide – A basic guide for police officers, prosecutors and judges*» editado pelo Conselho da Europa prevê a documentação de toda a fase de coleta das provas eletrônicas, incluindo, por exemplo, a documentação da cena do local onde se realiza a coleta, todo o equipamento encontrado (marca, modelo e número de série), da condição e localização de cada sistema contendo provas eletrônicas, incluindo seu estado (ligado, desligado ou em hibernação), sobre as pessoas encontradas no local, todas as pessoas que usaram o sistema informático relevante e todas a ações realizadas no local, com o registro da ação realizada e a hora exata.[37] A exigência de documentação detalhada, precisa e rigorosa de toda a fase de coleta da prova eletrônica é exigida por outros órgãos internacionais, como a *Association of Chief Police Officers* (ACPO), o *National Institute of*

[36] CABRAL, Antonio do Passo. Processo e tecnologia: novas tendências. In: LUCON, Paulo Henrique dos Santos *et al.* (coord.). *Direito, processo e tecnologia*. São Paulo: RT, 2020. p. 94.
[37] CONSELHO DA EUROPA. Eletronic Evidence Guide – A basic guide for police officers, prosecutors and judges. Cybercrime Division. Directorate General of Human Rights and Rule of Law. Strasbourg, France. Data: 06 de março de 2020. Disponível em: https://rm.coe.int/c-proc-electronic-evidence-guide-2-1-en-june-2020-web2/16809ed4b4. Consultado em 20 de agosto de 2020. p. 41-44.

Standards and Technology (NIST) e o *Internet Engineering Task Force* (IETF).[38]

Fernanda Teixeira Souza Domingos, Procuradora da República, sublinha que:

> «A **completude** ou a **integridade** da prova digital é o terceiro requisito de validade das evidências digitais. [...] Técnicas especiais periciais são aptas a identificar a assinatura digital do arquivo ou *hash* de forma a verificar a integralidade da prova. Caso algum bit tenha sido alterado, é como o DNA do arquivo, sua integralidade terá sido violada ou corrompida, não se prestando a ser avaliada em juízo.
>
> A fim de não comprometer a integralidade da prova digital, seu conteúdo original juntamente com seus *hashes* (assinatura digital) devem ser preservados e efetuada a análise na cópia».[39] (negrito no original, sublinhado nosso).

Juan Carlos Férnandez Martínez, por sua vez, esclarece que a obtenção do cálculo do código Hash implica emprego de programas como FktImager,

---

[38] ACPO. *Good Practice Guide for Digital Evidence*. Association of Chief Police Officers of England, Wales & Nothern Ireland. Data: março de 2012. Disponível em: http://library.college.police.uk/docs/acpo/digital-evidence-2012.pdf. Consultado em 20 de agosto de 2020. p. 6-7; NIST. *Guide to Integrating Forensic Techniques into Incident Response*. Karen Kent, Suzanne Chevalier, Tim Grance e Hung Dang. Special Publication 900-86. Data: agosto de 2006. Disponível em: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf. Consultado em 20 de agosto de 2020. p. 3-4/3-5; IETF. *Guidelines for Evidence Collection and Archiving* (RFC 3227). Data: fevereiro de 2002. Disponível em: https://tools.ietf.org/html/rfc3227. Consultado em 20 de agosto de 2020. p. 5.

[39] DOMINGOS, Fernanda Teixeira Souza. As provas digitais nos delitos de pornografia infantil na internet. In: SALGADO, Daniel de Resende; QUEIROZ, Ronaldo Pinheiro (orgs.). *A prova no enfrentamento à macrocriminalidade*. 3ª ed. rev., atual. e ampl. Salvador: Juspodvim, p. 197.

Encase e outros, copiando-se a informação *bit* a *bit* ou mediante cópia seletiva, denominada cópia lógica.[40]

Em outra oportunidade busquei descrever os cuidados necessários à preservação da cadeia de custódia das provas digitais e mesmo as cautelas pertinentes à denominada busca *on line*.[41]

A rigor seria desnecessário sublinhar que a natureza constitucional dos interesses protegidos configura limite *a priori* para a busca e apreensão de dispositivos digitais e de arquivos e programas digitais de qualquer formato, ainda quando se trate de busca *on line*.

À vista de muitos casos no Brasil em que este cuidado na prática não é respeitado, vale reproduzir as ponderações de Barbara A. Frederiksen e Susan Brenner relativamente aos requisitos de validade jurídica quer da decisão de busca e apreensão de computadores, quer de sua execução:

> "Além disso, não deve ser emitido qualquer mandado autorizando a apreensão de um hardware de computador, em vez de ser feita uma "cópia de segurança" forense dos dados, a menos que o pedido pelo mandado forneça uma explicação específica das razões técnicas pelas quais a busca não pode ser realizada no local ou conduzida fora do local utilizando "cópias de segurança" forenses dos dados.
>
> [...]
>
> **Quando um tribunal emite uma autorização de apreensão e de busca fora do local, deveria exigir que os agentes criem pelo menos uma "cópia de segurança" das informações sobre o equipamento**

[40] FÉRNANDEZ MARTÍNEZ, Juan Carlos. Especialidades de la prueba cuando, esta, es tecnológica. In: ORTEGA BURGOS, Enrique (dir.). *Actualidad:* Nuevas Tecnologías. Valencia: Tirant lo Blanch, 2020. p. 336.

[41] PRADO, Geraldo. *A Cadeia de Custódia da Prova no Processo Penal*. São Paulo: Marcial Pons, 2019. P. 109-114.

> **apreendido e deem essa cópia de segurança ao dono desse equipamento.** Se o conteúdo do disco for tal que o material não possa ser deixado na posse do proprietário, por exemplo, os agentes apreendem pornografia infantil, então uma segunda "cópia de segurança" selada deve ser produzida e retida para uso do advogado e de peritos do acusado. A cópia selada pode ser utilizada para demonstrar se a prova foi contaminada ou adulterada após a perda da sua posse pelo suspeito."[42] (grifo nosso)

A banalização da apreensão de computadores, como em passado próximo se deu com a interceptação das comunicações telefônicas, tem proporcionado verdadeiro festival de ilegalidades rudimentares e elementares, e de práticas inconstitucionais, inadmissíveis no contexto de um conhecimento jurídico básico.

Estas ações ilegais variam da apreensão desnecessária do *hardware*, quando o juridicamente válido seria o perito executor da medida examinar o dispositivo no local e proceder à cópia adequada (lógica ou espelho) apenas dos arquivos de interesse para a investigação, até a indevida entrega dos dispositivos a pessoas naturais ou jurídicas de direito privado. O não emprego imediato das técnicas certificadas para o cálculo *hash*, conforme

[42] Tradução livre. No original: "Also, no warrant should be issued authorizing the seizure of computer hardware, instead of making a forensic back-up copy of the data, unless the warrant affidavit provides a specific explanation of the technical reasons why the search cannot be conducted on-site or conducted off-site using forensic back-up copies of data. […]When a court issues a seizure and an off-site search authorization, it should require that the officers create at least one back-up copy of the information on the seized equipment and give this back-up copy to the owner of that equipment. If the contents of the disk are such that the materials cannot reasonably be left in possession of the owner, for example, agents seize child pornography, then a second sealed backup copy should be produced, and retained for use by defendant's counsel and experts. The sealed copy can be used to demonstrate whether the evidence was contaminated or tampered with after leaving the suspect's possession.". BRENNER, Susan W.; FREDERIKSEN, Barbara A.. Computer Searches and Seizures: Some Unresolved Issues. In: *Michigan Telecommunications and Technology Law Review*, vol. 8, i. 1, p. 39-114, 2002. p. 75-79. Disponível em: https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1186&context=mttlr. Consultado em: 06 de novembro de 2020.

mencionado,[43] a não identificação da existência de rede aberta ou fechada a evitar manipulação à distância, e a manipulação de dispositivos, *softwares* e arquivos, quer diretamente do computador ou disco rígido apreendido, quer em cópias não lacradas eletronicamente (*hash*) vulnera o objeto (material ou eletrônico) apreendido e o sujeita a manipulações, supressão, acréscimo ou alterações de conteúdo que dadas as características próprias dos elementos digitais tornam imprestável o elemento probatório.

Igualmente não tem sido excepcional o acesso direto aos arquivos digitais pelas autoridades policiais, seus agentes e membros do Ministério Público sem que antes tenha havido a necessária filtragem, por órgão público independente, daquilo que interessa efetivamente à acusação e o que, sob proteção constitucional, não deve ser compartilhado.

Em analogia com o exemplo do homicídio, depois dessas práticas não há mais como determinar com segurança se o objeto da prova está íntegro e é autêntico, isto é, se é corpo de delito ou outra coisa qualquer, que simulando o corpo de delito falseia *a priori* o juízo prévio sobre a existência do fato em tese demonstrável pela prova digital.

Não custa levar em conta a advertência de Fernández Martínez, de que o primeiro passo para que se possa dispor processualmente de uma prova digital é assegurar que não se questione sua integridade e autenticidade, "ya que todos sabemos de la facilidad de su manipulación, así como de su volatilidad".[44]

---

[43] International Organization for Standardization. ISO/IEC 27037:2012. Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence. Norma técnica. Publicada em outubro de 2012. Revisada e confirmada em 2018. Versão vigente. Disponível para aquisição em: https://www.iso.org/standard/44381.html. Consultado em: 20 de janeiro de 2021; Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC 27037:2013. Tecnologia da informação — Técnicas de segurança — Diretrizes para identificação, coleta, aquisição e preservação de evidência digital. Identifica a: ISO/IEC 27037:2012. Norma técnica. Publicada em 09 de dezembro de 2013. Confirmada em 26 de novembro de 2018. Versão vigente. Disponível para aquisição em: https://www.abntcatalogo.com.br/norma.aspx?ID=307273. Consultado em: 20 de janeiro de 2021.

[44] FÉRNANDEZ MARTÍNEZ, Juan Carlos. Especialidades de la prueba cuando, esta, es tecnológica. In: ORTEGA BURGOS, Enrique. *Actualidad: Nuevas Tecnologías*. Valencia: Tirant lo Blanch, 2020. P. 333.

VI - Como afirmado no início, violada a cadeia de custódia da prova digital incide imperiosa proibição de valoração da prova assim obtida. É o corpo de delito que se converte em algo juridicamente imprestável à luz do direito fundamental à integridade dos sistemas informáticos e o igualmente fundamental direito à confidencialidade, princípios constitucionais implícitos assim como o é o direito fundamental à autodeterminação informativa.

Reitere-se: a cadeia de custódia da prova digital é condição de procedibilidade do exame de corpo de delito.

Dois problemas especiais merecem atenção. Ambos, em alguma medida suscitados pelo doutorando de Coimbra Tulio Felippe X. Januário, na palestra na qual este artigo foi apresentado.

A Constituição brasileira considera inadmissíveis as provas obtidas por meios ilícitos.[45]

O acesso criminoso a *hardwares*, *softwares* e arquivos digitais a rigor gera a inadmissibilidade de seu uso em processo.

A disposição constitucional é original do texto de 1988, não havendo precedentes nas Constituições brasileiras anteriores. Até 1988 o tema da ilicitude da prova era tratado ao nível infraconstitucional e debatia-se a respeito da incidência das causas de justificação a neutralizar a antijuridicidade da conduta típica de obtenção da prova.

Com a constitucionalização da proibição da prova ilícita, em grau superior ao do paradigma português que a trata como causa de nulidade, o direito brasileiro adotou o modelo da *inadmissibilidade* e com isso monopolizou o regime de antijuridicidade da prova.

[45] Art. 5º, CR. Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: [...] LVI - são inadmissíveis, no processo, as provas obtidas por meios ilícitos;

No caso brasileiro não cabem quer a regra de exceção, que tornaria admissível toda prova originalmente ilícita desde que obtida em determinadas condições (em favor do acusado, por exemplo), quer juízo de proporcionalidade que autorize o emprego de prova ilícita em desfavor de alguém.

No entanto, é necessário compreender que a metódica constitucional que rege o conflito entre interesses constitucionalmente protegidos, se na hipótese proíbe a regra de exceção do tipo «toda prova ilícita pro reo é admissível», não exclui um regime próprio de controle da antijuridicidade constitucional quando conflitam estes interesses.

O processo penal constitucional é garantia do imputado contra o arbítrio estatal. Por essa razão o imputado não está em posição simétrica equivalente ao do Estado investigador e acusador. A revisão criminal e o *habeas corpus*, por exemplo, são remédios de estrita defesa do imputado e da liberdade de locomoção. Não há revisão criminal em favor da acusação ou condenação.

Assim, constatado o conflito entre interesses constitucionalmente tutelados em cada caso concreto, é imprescindível a intervenção jurisdicional (reserva jurisdicional de função) para aquilatar se *no caso* será excepcionalmente admissível a prova.

Não se pode torturar ou matar para obter a prova da inocência. Outras infrações, no entanto, podem levar a violação de bem jurídico que deve ser moderadamente suportado pela vítima em favor da comprovação da inocência e da garantia da liberdade de outrem.

Este é sem dúvida o tema do momento à luz da atuação de *hackers* que tem divulgado ilegalidade de governos, governantes, agentes públicos, corporações privadas e empresários.[46]

[46] Aliás, assunto da conferência "«Wikidenunciantes»: Piratas ou Heróis?" proferida pelo professor Mário Ferreira Monte, com a participação da professora Rachel Herdy como debatedora e com a coordenação do professor Geraldo Prado. Evento promovido pelo Programa de Pós-Graduação em Direito da Universidade Federal do Rio de Janeiro (UFRJ) e o Grupo de Pesquisa Matrizes do Processo Penal Brasileiro, também

A propósito vale a leitura da Diretiva nº 2019/1.937 do Parlamento Europeu, de cujo teor é extraída pequena, mas iluminada passagem:

> "Os denunciantes constituem fontes importantes, em particular para os jornalistas de investigação. Uma proteção eficaz dos denunciantes contra atos de retaliação aumenta a segurança jurídica dos potenciais denunciantes e, deste modo, encoraja a denúncia também através dos meios de comunicação social. Neste contexto, a proteção dos denunciantes enquanto fontes jornalísticas é crucial para salvaguardar o papel de «vigilante» do jornalismo de investigação nas sociedades democráticas.[47]

Em se tratando da obtenção criminosa de prova digital e desde que não tenha havido tortura ou morte, o peso constitucional de valoração da antijuridicidade pende em favor da defesa da liberdade e da inocência do indivíduo.

Opera-se aqui ao nível da excepcionalidade em que a proibição de ingresso da prova no processo não corresponde uma proibição de valoração. A prova digital a princípio poderá ser valorada, mas seu emprego estará limitado à defesa da liberdade e inocência. Em hipótese alguma esta prova poderá ser usada em desfavor de quem quer que seja.

Vencida esta etapa é que se coloca o problema da cadeia de custódia, que também aqui necessariamente da admissibilidade.

---

da Universidade Federal do Rio de Janeiro (UFRJ) em 21 de maio de 2019 às 19 horas no Auditório Alfredo Valladão da Faculdade Nacional de Direito da Universidade Federal do Rio de Janeiro.

[47] PARLAMENTO EUROPEU E CONSELHO. *Diretiva 2019/1937 do Parlamento Europeu e do Conselho de 23 de outubro de 2019 relativa à proteção das pessoas que denunciam violações do direito da União*. Estrasburgo: Jornal Oficial da União Europeia, L 305, 26 de novembro de 2019, preâmbulo, parágrafo 46, p. 25. Disponível em https://eur-lex.europa.eu/legal-content/pt/TXT/?uri=CELEX:32019L1937. Consultado em: 03 de fevereiro de 2020.

A cadeia de custódia configura método de preservação da integridade e autenticidade do elemento probatório. A cadeia de custódia, por evidente, é uma imposição ao Estado investigador, acusador ou juiz, conforme o caso.

A prova trazida por terceiros estará sujeita ao exame de fiabilidade que, em um sistema de controles epistêmicos, abarca a cadeia de custódia (uma das formas pelas quais funciona), mas não se limita a esta.

Assim, será imprescindível que se preserve a cadeia de custódia da prova digital (como de qualquer outra) a partir do momento em que é apreendida ou apresentada por terceiro a órgão oficial, quer o terceiro tenha sido o autor do ato ilícito de obtenção do elemento probatório, quer seja seu mero detentor, sem prejuízo da valoração mais abrangente de sua fiabilidade.

O exame de fiabilidade configura análise ao estilo de «prova sobre a prova».

VII – A Lei nº 13.964/2019 formalmente instituiu a cadeia de custódia das provas como condição de procedibilidade do exame de corpo de delito no direito brasileiro.

A sua importância pode ser medida pela quantidade e qualidade de atos normativos nacionais e internacionais que procuram detalhar sua prática e orientar os agentes estatais.

Temos desde Portarias emitidas pela Secretaria Nacional de Segurança Pública do Ministério da Justiça,[48] a Provimentos e projetos editados nos seguintes Estados da Federação e pelo Distrito Federal: Acre[49]; Rondônia[50];

[48] Portaria n. 82, de 16 de julho de 2014, da Secretaria Nacional de Segurança Pública do Ministério da Justiça. Publicação em: 18 de julho de 2014. Disponível em: http://www.lex.com.br/legis_25740023_PORTARIA_N_82_DE_16_DE_JULHO_DE_2014. Consultado em: 11 de janeiro de 2021.

[49] Provimento Conjunto n. 001, de 22 de março de 2019, da Secretaria de Estado da Polícia Civil do Estado do Acre. DOEAC n. 12.518, pp. 23-24. Publicação em: 26 de março de 2019. Disponível em: http://diario.ac.gov.br/download.php?arquivo=KEQxQHI3IyEpRE8xNTUzNTY1NTk5NzczOC5wZGY. Consultado em: 12 de janeiro de 2021.

[50] Resolução n. 002, de 2020, da Polícia Técnico-Científica do Estado de Rondônia. DOERO ed. 185, pp. 112-113. Publicação em: 22 de setembro de 2020. Disponível em: http://www.diof.ro.gov.br/data/uploads/2020/09/DOE-22.09.2020.pdf. Consultado em: 12 de janeiro de 2021.

Pará[51]; Piauí[52]; Bahia[53]; Ceará[54]; Alagoas[55]; Mato Grosso[56]; Goiás[57]; Mato Grosso do Sul[58]; Distrito Federal[59]; Rio de Janeiro[60]; Minas Gerais[61]; Espírito Santo[62]; São Paulo[63]; Paraná[64]; e Rio Grande do Sul.[65]

---

[51] Portaria n. 12, de 29 de novembro de 2016, da Secretaria de Estado de Segurança Pública e Defesa Social do Pará. DOEPA n. 33262, p. 25. Publicação em: 01 de dezembro de 2016. Disponível em: http://www.ioepa.com.br/diarios/2016/12/01/2016.12.01.DOE_25.pdf. Consultado em: 12 de janeiro de 2021.

[52] Portaria n. 12.000-108, de 14 de outubro de 2014, da Secretaria de Estado da Segurança Pública do Piauí. Disponível em: http://www.pc.pi.gov.br/download/201410/PC23_96f4e2e54e.pdf. Consultado em: 12 de janeiro de 2021.

[53] Portaria n. 0074, de 2020, do Departamento de Polícia Técnica do Estado da Bahia. Publicação em: 16 de julho de 2020. DOEBA n. 22.944, p. 40. Disponível em: http://dool.egba.ba.gov.br/portal/visualizacoes/pdf/10351#/p:40/e:10351?find=cadeia. Consultado em: 13 de janeiro de 2021.

[54] Portaria Normativa n. 2195, de 23 de dezembro de 2020, da Secretaria de Segurança Pública e Defesa Social do Estado do Ceará. DOECE n. 290, pp. 76-78. Publicação em: 30 de dezembro de 2020. Disponível em: http://imagens.seplag.ce.gov.br/PDF/20201230/do20201230p02.pdf. Consultado em: 13 de janeiro de 2021.

[55] Recomendação n. 012, de 13 de agosto de 2020, da 62ª Procuradoria de Justiça da Capital do Estado de Alagoas. DOEAL n. 249, pp. 8-10. Publicação em: 18 de agosto de 2020. Disponível em: https://sistemas.mpal.mp.br/DiarioOficialEletronico/download/diario/1761. Consultado em: 11 de janeiro de 2021.

[56] Portaria n. 005, de 18 de novembro de 2020, da Perícia Oficial e Identificação Técnica do Estado do Mato Grosso. DOEMT n. 27.881, p. 33. Publicação em: 19 de novembro de 2020. Disponível em: https://www.iomat.mt.gov.br/portal/visualizacoes/pdf/16109/#/p:33/e:16109?find=cadeia%20de%20cust%C3%B3dia. Consultado em: 13 de janeiro de 2021.

[57] Portaria n. 0135, de 11 de fevereiro de 2020, da Secretaria de Estado da Segurança Pública de Goiás. Disponível em: https://www.seguranca.go.gov.br/editais-e-licitacoes/portarias/portaria-n-0135-20-designacao-da-comissao-de-trabalho-cadeia-de-custodia.html. Consultado em: 13 de janeiro de 2021.

[58] Portaria "N" n. 007, de 23 de abril de 2020, Coordenadoria-Geral de Perícias do Estado de Mato Grosso do Sul. DOEMS n. 10.154, pp. 15-17. Publicação em: 24 de abril de 2020. Disponível em: https://www.spdo.ms.gov.br/diariodoe/Index/Download/DO10154_24_04_2020. Consultado em: 14 de janeiro de 2021.

[59] Portaria n. 97, de 10 de novembro de 2020, da Polícia Civil do Distrito Federal. DODF n. 221, pp. 11-12. Publicação em: 24 de novembro de 2020. Disponível em: https://dodf.df.gov.br/index/visualizar-arquivo/?pasta=2020|11_Novembro|DODF%20221%2024-11-2020|&arquivo=DODF%20221%2024-11-2020%20INTEGRA.pdf. Consultado em: 14 de janeiro de 2021.

[60] Resolução n. 755, 17 de setembro de 2020, da Secretaria de Estado da Polícia Militar do Estado do Rio de Janeiro. DOERJ n. 187, pp. 6-8. Publicação em: 08 de outubro de 2020. Disponível em: http://www.ioerj.com.br/portal/modules/conteudoonline/mostra_edicao.php?session=VGxWU1IxRlZWVE5OYWxsMFRucFdSRTVwTURCT1ZFRTFURlJuTTFGVlNYUlBWRTE0VW1wWk1WSnJSVEpPZWtreVRWUlpkMDFxUlRKTlZHTXhUbmM5UFE9PQ. Consultado em: 11 de janeiro de 2021.

[61] Resolução n. 8.144, de 9 de julho de 2020, da Polícia Civil do Estado de Minas Gerais. DOEMG n. 140, p.3. Publicação em: 10 de julho de 2020. Disponível em: https://www.jornalminasgerais.mg.gov.br/?dataJornal=2020-07-10#caderno-jornal. Consultado em: 14 de janeiro de 2021.

[62] Portaria Conjunta n. 001-R, de 29 de outubro de 2020, da Secretaria de Estado e da Segurança Pública e Defesa Social, junto com a Polícia Militar e a Polícia Civil do Estado do Espírito Santo. DOEES ed. 25.353, pp. 20-21. Publicação em: 03 de novembro de 2020. Disponível em: https://ioes.dio.es.gov.br/ver-flip/5196/#/p:20/e:5196. Consultado em: 14 de janeiro de 2021.

[63] Portaria n. 6.449, de 18 de junho de 2020, da Procuradoria Geral de Justiça do Estado de São Paulo. DOSP n. 119, p.40. Publicação em: 19 de junho de 2020. Disponível em: https://www.imprensaoficial.com.br/DO/BuscaDO2001Documento_11_4.aspx?link=%2f2020%2fexecutivo%2520secao%2520i%2fjunho%2f19%2fpag_0041_e6d1b71a19339bfe8449b9310dc1d9b6.pdf&pagina=41&data=19/06/2020&caderno=Executivo%20I&paginaordenacao=100041. Consultado em: 14 de janeiro de 2021.

[64] Manifestação n. 032, de 11 de março de 2020, do Grupo de Atuação Especializada em Segurança Pública (GAESP) do Ministério Público do Estado do Paraná. Disponível em: https://criminal.mppr.mp.br/arquivos/File/Manif_032-2020_-_PA_20033098-6_-_cadeia_de_custodia.pdf. Consultado em: 11 de janeiro de 2021.

[65] Instrução Normativa Conjunta n. 001, de 2020, da Secretaria da Segurança Pública do Estado do Rio Grande do Sul. DOERS. Publicação em: 12 de novembro de 2020. Disponível em: https://www.diariooficial.rs.gov.br/materia?id=483750. Consultado em: 14 de janeiro de 2021.

Os Códigos de Processo Penal da Espanha[66], Itália[67], Colômbia[68], Federal do México[69], Chile[70] e Uruguai[71] cuidam especificamente da matéria.

[66] Art. 338, CPP Espanhol. Sin perjuicio de lo establecido en el Capítulo II bis del presente título, los instrumentos, armas y efectos a que se refiere el artículo 334 se recogerán de tal forma que se garantice su integridad y el Juez acordará su retención, conservación o envío al organismo adecuado para su depósito. (Se modifica por el art. 2.40 de la Ley 13/2009, de 3 de noviembre)

[67] Art. 254-bis, CPP Italiano. Sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni. (Articolo inserito dall'art. 8, comma 5, della L 18 marzo 2008, n. 48)

1. L'autorità giudiziaria, quando dispone il sequestro, presso i fornitori di servizi informatici, telematici o di telecomunicazioni, dei dati da questi detenuti, compresi quelli di traffico o di ubicazione, può stabilire, per esigenze legate alla regolare fornitura dei medesimi servizi, che la loro acquisizione avvenga mediante copia di essi su adeguato supporto, con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità. In questo caso è, comunque, ordinato al fornitore dei servizi di conservare e proteggere adeguatamente i dati originali.

[68] Art. 254, CPP Colombiano. Aplicación

Con el fin de demostrar la autenticidad de los elementos materiales probatorios y evidencia física, la cadena de custodia se aplicará teniendo en cuenta los siguientes factores: identidad, estado original, condiciones de recolección, preservación, embalaje y envío; lugares y fechas de permanencia y los cambios que cada custodio haya realizado. Igualmente se registrará el nombre y la identificación de todas las personas que hayan estado en contacto con esos elementos.

La cadena de custodia se iniciará en el lugar donde se descubran, recauden o encuentren los elementos materiales probatorios y evidencia física, y finaliza por orden de autoridad competente.

PARÁGRAFO. El Fiscal General de la Nación reglamentará lo relacionado con el diseño, aplicación y control del sistema de cadena de custodia, de acuerdo con los avances científicos, técnicos y artísticos.

[69] Art. 123-Bis, CPP Mexicano. La preservación de los indicios, huellas o vestigios del hecho delictuoso, así como los instrumentos, objetos o productos del delito es responsabilidad directa de los servidores públicos que entren en contacto con ellos.

En la averiguación previa deberá constar un registro que contenga la identificación de las personas que intervengan en la cadena de custodia y de quienes estén autorizadas para reconocer y manejar los indicios, huellas o vestigios del hecho delictuoso, así como los instrumentos, objetos o productos del delito.

Los lineamientos para la preservación de indicios, huellas o vestigios del hecho delictuoso, así como de los instrumentos, objetos o productos del delito, que por acuerdo general emita la Procuraduría General de la República, detallarán los datos e información necesaria para asegurar la integridad de los mismos.

La cadena de custodia iniciará donde se descubra, encuentre o levante la evidencia física y finalizará por orden de autoridad competente.

[70] Art. 181, CPP Chileno. Actividades de la investigación. Para los fines previstos en el artículo anterior, la investigación se llevará a cabo de modo de consignar y asegurar todo cuanto condujere a la comprobación del hecho y a la identificación de los partícipes en el mismo. Así, se hará constar el estado de las personas, cosas o lugares, se identificará a los testigos del hecho investigado y se consignarán sus declaraciones. Del mismo modo, si el hecho hubiere dejado huellas, rastros o señales, se tomará nota de ellos y se los especificará detalladamente, se dejará constancia de la descripción del lugar en que aquél se hubiere cometido, del estado de los objetos que en él se encontraren y de todo otro dato pertinente.

Para el cumplimiento de los fines de la investigación se podrá disponer la práctica de operaciones científicas, la toma de fotografías, filmación o grabación y, en general, la reproducción de imágenes, voces o sonidos por los medios técnicos que resultaren más adecuados, requiriendo la intervención de los organismos especializados. En estos casos, una vez verificada la operación se certificará el día, hora y lugar en que ella se hubiere realizado, el nombre, la dirección y la profesión u oficio de quienes hubieren intervenido en ella, así como la individualización de la persona sometida a examen y la descripción de la cosa, suceso o fenómeno que se reprodujere o explicare. En todo caso se adoptarán las medidas necesarias para evitar la alteración de los originales objeto de la operación.

[71] Art. 53, CPP Uruguaio. (Actuaciones de la autoridad administrativa sin orden previa).- Corresponderá a los funcionarios con funciones de policía realizar las siguientes actuaciones, sin necesidad de recibir previamente instrucciones particulares de los fiscales:

d) Resguardar el lugar donde se cometió el hecho. Para ello, impedirán el acceso a toda persona ajena a la investigación y procederán a la clausura si se trata de local cerrado, o a su aislamiento si se trata de lugar abierto. Asimismo, evitarán que se alteren o borren de cualquier forma los rastros o vestigios del hecho o se remuevan los instrumentos usados para llevarlo a cabo, mientras no intervenga personal experto de la

Sem pretensão de exaurir os documentos existentes, releva destacar os diversos protocolos ainda na Argentina[72], México[73], Colômbia[74], Uruguai[75], Costa Rica[76], Venezuela[77], Panamá[78] e Peru[79].

São igualmente relevantes, como mencionado ao longo do texto:

Nos Estados Unidos da América: "Guide to Integrating Forensic Techniques into Incident Response (ago. 2006) – U.S. Department of Commerce, Technology Administration, National Institute of Standards and

autoridad con funciones de policía que el Ministerio Público designe. Deberá también recoger, identificar y conservar bajo sello los objetos, documentos o instrumentos de cualquier clase que se presuma hayan servido para la comisión del hecho investigado, sus efectos o los que pudieren ser utilizados como medios de prueba, para ser remitidos a quien corresponda, dejando constancia de la individualización completa de los funcionários intervinientes.

[72] MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS. *Protocolo unificado de los ministerios públicos de la República Argentina*: Guía para el levantamiento y conservación de la evidencia. Ciudad Autónoma de Buenos Aires: Ediciones SAIJ, 2017. Disponível em: http://www.bibliotecadigital.gob.ar/files/original/20/1724/protocolo-unificado-ministerios-publicos-republica-argentina.2.pdf. Consultado em: 15 de janeiro de 2021.

[73] AGENCIA DE INVESTIGACIÓN CRIMINAL; PROCURADORIA GENERAL DA REPÚBLICA. *Guia Técnica de Cadena de Custodia de Evidencia Digital*. México: AIN, PGR, EUM, jun. 2018. Disponível em: http://www.coahuilatransparente.gob.mx/disp/documentos_disp/GU%C3%8DA%20T%C3%89CNICA%20DE%20CADENA%20DE%20CUSTODIA%20DE%20EVIDENCIA%20DIGITAL.pdf. Consultado em: 15 de janeiro de 2021.

[74] FISCALÍA GENERAL DE LA NACIÓN. *Manual del Sistema de Cadena de Custodia*. 4ª versão. Colômbia: Fiscalía General de la Nación, 2018. Disponível em: https://www.fiscalia.gov.co/colombia/wp-content/uploads/MANUAL-DEL-SISTEMA-DE-CADENA-DE-CUSTODIA.pdf. Consultado em: 15 de janeiro de 2021.

[75] MINISTERIO DEL INTERIOR; FISCALÍA GENERAL DE LA NACIÓN. *Protocolos de actuación conjunta del Ministerio Público y de la Policía Nacional en materia de procedimiento penal*. Uruguai: Ministerio del Interior, Fiscalía General de la Nación, 2017. Disponível em: http://www.fiscalia.gub.uy/innovaportal/file/4673/1/res.-753_2017_instruccion-7-y-anexos.pdf. Consultado em: 15 de janeiro de 2021.

[76] MINISTERIO PÚBLICO; ORGANISMO DE INVESTIGACIÓN JUDICIAL. *Protocolo Cadena de Custodia*. 2ª versão. Costa Rica: Poder Judicial, fev. 2020. Disponível em: https://ministeriopublico.poder-judicial.go.cr/images/phocadownload/CircularesAdministrativas/2020/Anexos2020/protocoloCadenaCustodia.pdf. Consultado em: 15 de janeiro de 2021.

[77] REPÚBLICA BOLIVARIANA DE VENEZUELA. *Manual Único de Cadena de Custodia de Evidencias Físicas*. Caracas (Venezuela): RBV, ago. 2017. Disponível em: http://www.mpprijp.gob.ve/wp-content/uploads/2018/05/ManualDeCustodia.pdf. Consultado em: 15 de janeiro de 2021.

[78] INSTITUTO DE MEDICINA LEGAL Y CIENCIAS FORENSES; REPUBLICA DE PANAMA, MINISTERIO PUBLICO. *Manual de Procedimiento del Sistema de Cadena de Custodia*. 2ª versão. Panamá: Instituto de Medicina Legal y Ciencias Forenses, 2015. Disponível em: http://www.imelcf.gob.pa/wp-content/uploads/2020/01/manual-de-cadena-de-custodia.pdf. Consultado em: 15 de janeiro de 2021.

[79] MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS. *Protocolo de actuación interinstitucional para la aplicación de la incautación, comiso, hallazgo y cadena de custodia*. Peru: Ministerio de Justicia y Derecho Humanos, 2018. Disponível em: https://static.legis.pe/wp-content/uploads/2018/09/Protocolo-12-Incautaci%C3%B3n-comiso-hallazgo-cadena-de-custodia-Legis.pe_.pdf. Consultado em: 15 de janeiro de 2021.

Technology";[80] "Best Practices for Seizing Electronic Evidence v.3: A Pocket Guide for First Responders. (2007) – U.S. Department of Homeland Security; United States Secret Service";[81] "Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition (abr. 2008) – U.S. Department of Justice, Office of Justice Programs, National Institute of Justice";[82] "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations. Third Edition. (2009) – U.S. Department of Justice, Computer Crime and Intellectual Property Section, Criminal Division"[8384]; "Justice Manual. Title 9: Criminal. 9-13.000 – Obtaining Evidence. 9-13.420 - Searches of Premises of Subject Attorneys. – U.S. Department of Justice"[85],[86] [United States Attorney's Manual –

[80] KENT, Karen; *et al*. *Guide to Integrating Forensic Techniques into Incident Response*. U.S. Department of Commerce – Technology Administration – National Institute of Standards and Technology, Special Publication 800-86. Data: agosto de 2006. Disponível em: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf. Consultado em: 29 de dezembro de 2020.

[81] U.S. DEPARTMENT OF HOMELAND SECURITY; UNITED STATES SECRET SERVICE. *Best Practices for Seizing Electronic Evidence v.3*: A Pocket Guide for First Responders. Data: 2007. 24 p. Disponível em: https://www.crime-scene-investigator.net/SeizingElectronicEvidence.pdf. Consultado em: 04 de janeiro de 2021.

[82] U.S. DEPARTMENT OF JUSTICE. Office of Justice Programs, National Institute of Justice. *Electronic Crime Scene Investigation*: A Guide for First Responders, Second Edition. Data: abril de 2008. Disponível em: https://www.ncjrs.gov/pdffiles1/nij/219941.pdf. Consultado em: 15 de janeiro de 2021.

[83] U.S. DEPARTMENT OF JUSTICE. Computer Crime and Intellectual Property Section, Criminal Division. *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*. Third Edition. Office of Legal Education Executive Office for United States Attorneys, OLE Litigation Series, 2009. Disponível em: https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf. Consultado em: 06 de novembro de 2020.

[84] O referido manual [Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations Manual (2009)] é a terceira e atual edição do documento que sucedeu o "Federal Guidelines For Searching and Seizing Computers", originalmente publicado em 1994 [disponível em: https://epic.org/security/computer_search_guidelines.txt, consultado em 06 de novembro de 2020], com complementações publicadas em 1997 e 1999. Fonte: https://www.govcon.com/doc/justice-department-releases-guide-to-searchin-0001. Consultado em 06 de novembro de 2020. A normativa mencionada no livro Cadeia de Custódia da Prova, por sua vez, é a "Electronic Crime Scene Investigation - A Guide for First Responders, Second Edition" (2008), edição atual. Ambos são do Departamento de Justiça Norte-Americano, embora o "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations Manual" (2009) seja do Computer Crime & Intellectual Property Section, da Criminal Division, e o "Electronic Crime Scene Investigation - A Guide for First Responders, Second Edition" (2008) seja do National Institute of Justice (NIJ), uma das divisões do "Office of Justice Programs". Ambos parecem complementares e não vinculantes, em uma primeira análise.

[85] U.S. DEPARTMENT OF JUSTICE. 9-13.420 - Searches of Premises of Subject Attorneys. In: 9-13.000 – Obtaining Evidence. Title 9: Criminal. *Justice Manual*. Disponível em: https://www.justice.gov/jm/jm-9-13000-obtaining-evidence. Consultado em: 06 de novembro de 2020.

[86] **Cumpre destacar que as normativas dessa seção são específicas para buscas realizadas nas premissas de advogados "suspeitos", advogados relacionados a "suspeitos" ou advogados sob os quais recai a suspeita de terem posse de meios ou produtos de crime ou contrabando, conforme nota**

USAM, agora "Justice Manual – JM, section 9-13.420"]; e as Federal Rules of Evidence (2020)[87].

No Reino Unido temos o "ACPO Good Practice Guide for Digital Evidence (mar. 2012) – Association of Chief Police Officers of England, Wales and Northern Ireland",[88] na Austrália o "Collecting Electronic Evidence After a System Compromise (2017) – Matthew Braid, Australian Computer Emergency Response Team (AusCERT)",[89] na Índia "A Forensic Guide for Crime Investigators: Standard Operating Procedures (2017) – LNJN National Institute of Criminology and Forensic Science (Ministry of Home Affairs)"[90] e em âmbito europeu o referido "Electronic evidence – a basic guide for First Responders: Good practice material for CERT first responders (2014) – European Union Agency for Network and Information Security (ENISA)".[91]

Sem dúvida que o extenso rol é indicativo de que o cuidado para com a cadeia de custódia das provas é demonstração de reverência para com o devido

introdutória desta seção. Veja-se: "NOTE: For purposes of this policy only, "subject" includes an attorney who is a "suspect, subject or target," or an attorney who is related by blood or marriage to a suspect, or who is believed to be in possession of contraband or the fruits or instrumentalities of a crime. This policy also applies to searches of business organizations where such searches involve materials in the possession of individuals serving in the capacity of legal advisor to the organization. Search warrants for "documentary materials" held by an attorney who is a "disinterested third party" (that is, any attorney who is not a subject) are governed by 28 C.F.R. 59.4 and JM 9-19.221 et seq. See also 42 U.S.C. Section 2000aa-11(a)(3)." U.S. DEPARTMENT OF JUSTICE. 9-13.420 - Searches of Premises of Subject Attorneys. In: 9-13.000 – Obtaining Evidence. Title 9: Criminal. *Justice Manual*. Disponível em: https://www.justice.gov/jm/jm-9-13000-obtaining-evidence. Consultado em: 06 de novembro de 2020.

[87] ESTADOS UNIDOS. *Federal Rules of Evidence*. Data da última alteração até o momento: 1º de dezembro de 2020. Disponível em: https://www.law.cornell.edu/rules/fre. Consultado em: 15 de janeiro de 2021.

[88] Association of Chief Police Officers of England, Wales and Northern Ireland. *ACPO Good Practice Guide for Digital Evidence*. Versão 5. Data: março de 2012. Disponível em: http://library.college.police.uk/docs/acpo/digital-evidence-2012.pdf. Consultado em: 29 de dezembro de 2020.

[89] BRAID, Matthew. *Collecting Electronic Evidence After a System Compromise*. Australian Computer Emergency Response Team (AusCERT). Primeiro publicado em: 2 de agosto de 2001. Última versão: 11 de setembro de 2017. Disponível em: https://www.auscert.org.au/publications/2017-09-11-collecting-electronic-evidence-after-sy. Consultado em: 15 de janeiro de 2021.

[90] LNJN National Institute of Criminology and Forensic Science (Ministry of Home Affairs*). A Forensic Guide for Crime Investigators:* Standard Operating Procedures. Data: 2017. Disponível em: http://nicfs.gov.in/wp-content/uploads/2017/01/Introduction.pdf. Consultado em: 15 de janeiro de 2021.

[91] European Union Agency for Network and Information Security (ENISA). *Electronic evidence* - a basic guide for First Responders: Good practice material for CERT first responders. Data: 2014.

processo legal. O amplo acesso aos documentos, além disso, indica respeito para com a transparência que é princípio orientador de toda a atividade pública.

A lamentar, todavia, o fato de que se documentos dos mais diversos países e agências estejam disponíveis para consulta, favorecendo a troca de ideias e o aperfeiçoamento das práticas, em benefício do saber jurídico, da verdade e da melhor aplicação da Justiça, a 2ª Câmara de Coordenação e Revisão do Ministério Público Federal, responsável pela publicação da 3ª edição do Roteiro de Atuação sobre Crimes Cibernéticos, respondeu que o citado roteiro era de uso exclusivo para autoridades: polícia civil e federal, promotores e procuradores da república e juízes.[92]

À luz da Constituição não há espaço para roteiro de uso exclusivo da polícia civil e federal, promotores e procuradores da república e juízes. Publicidade e transparência ainda são princípios do Estado de Direito.

Também releva notar que se o Brasil está avançado em termos de doutrina acerca do assunto e começa a dar os passos no que concerne à legislação, o assunto da cadeia de custódia das provas ainda é tratado como filigrana jurídica, obstáculo à atuação das autoridades ou, o que talvez seja ainda pior, a depender do ângulo de observação, com profunda ignorância em alguns juízos e tribunais, reservando ao país uma incômoda posição típica do desapreço ao direito como prática civilizatória.

[92] Em 24 de agosto de 2020, requereu-se, em e-mail enviado à 2ª Câmara de Coordenação e Revisão do Ministério Público Federal (responsável pela publicação), o acesso à cópia eletrônica ou física da 3ª edição do Roteiro de Atuação sobre Crimes Cibernéticos, publicado em 2016. No entanto, ainda no dia 24, a 2ª Câmara de Coordenação e Revisão respondeu ao e-mail informando que o «referido roteiro é de uso exclusivo para autoridades: polícia civil e federal, promotores e procuradores da república e juízes». O documento, ao qual não foi possível obter acesso, é mencionado no site do Ministério Público Federal, no item «Roteiros de Atuação» da página da 2ª Câmara de Coordenação e Revisão: http://www.mpf.mp.br/atuacao-tematica/ccr2/publicacoes/roteiro-atuacoes. Consultado em 21 de janeiro de 2021.

A expectativa é de que este artigo em alguma medida possa contribuir para modificar este cenário.