

A REGRA DE *DISCLOSURE* NO PROCESSO PENAL E SUA RELEVÂNCIA PARA A PROVA DIGITAL

THE DISCLOSURE RULE IN CRIMINAL PROCEEDINGS AND ITS RELEVANCE TO DIGITAL EVIDENCE¹

Jamilla Monteiro Sarkis²
Nereu José Giacomolli³

Resumo:

Este artigo propõe um estudo verticalizado sobre a regra da *disclosure* no processo penal, com enfoque na sua relevância para o tratamento das provas digitais. Parte, para tanto, do conceito e das origens da *disclosure* no direito anglo-saxão. Em seguida, concentra-se na análise de sua compatibilidade com o ordenamento jurídico brasileiro, a partir de critérios de constitucionalidade, com base na garantia do contraditório, e convencionalidade, com destaque para a *par conditio*. Por fim, discute as particularidades da *disclosure* sobre a prova digital, cujo tratamento é diferenciado em razão da natureza técnica e da quantidade de dados envolvida. Ao final, espera demonstrar que a regra da *disclosure* garante à defesa a oportunidade de contraditar a hipótese acusatória e de eliminar sua dependência em relação às análises e interpretações sobre provas digitais promovidas pela Polícia e pelo Ministério Público.

Palavras-chave:

Disclosure. Defesa. Provas Digitais.

Abstract:

This article proposes a vertical study of the disclosure rule in criminal proceedings, focusing on its relevance to the treatment of digital evidence. It starts with the concept and origins of disclosure in Anglo-Saxon law. It then focuses on analyzing its compatibility with the Brazilian legal system, based on criteria of constitutionality (guarantee of contradictory), and conventionality, with emphasis on the *par conditio*. Finally, it discusses the particularities of disclosure of digital evidence, the treatment of which is different due to its technical nature and the amount of data involved. In the end, it expects to demonstrate that the disclosure rule guarantees the defense the opportunity to contradict the accusatory hypothesis and to eliminate its dependence on the analyses and interpretations of digital evidence promoted by the Police and the Public Prosecutor's Office.

Keywords:

Disclosure. Defense. Digital Evidence.

1. INTRODUÇÃO

A ideia de que a defesa deveria ter o direito de acessar todos os elementos de informação e provas produzidas pela Polícia e pelo Ministério Público durante a fase de investigação e o

¹ Artigo apresentado como requisito parcial para a conclusão do estágio de Pós-Doutoramento junto ao Programa de Pós-Graduação em Ciências Criminais da Pontifícia Universidade Católica do Rio Grande do Sul.

² Doutora em Direito pela Pontifícia Universidade Católica de Minas Gerais (PUC-MG), com bolsa CAPES. Mestra em Direito pela Faculdade de Direito da Universidade Federal de Minas Gerais (UFMG). Professora na Faculdade Anhanguera e em estágio pós-doutoral no Programa de Pós-Graduação em Ciências Criminais da Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS).

³ Doutor em Estudios de Actualidad Procesal pela Universidad Complutense de Madrid (2001), com estágio pós-doutoral na Università degli Studi di Torino (2008). Coordenador do Programa de Pós-Graduação em Ciências Criminais da PUCRS e Professor no Mestrado e Doutorado da PUCRS. Líder dos Grupos de Pesquisa Processo Penal Contemporâneo e Rede Internacional de Pesquisa em Direito Processual Penal. Professor Pesquisador na Universidade Autónoma de Lisboa e Investigador no JusGov – Universidade do Minho.

processo penal, com a intenção de conhecer eventuais evidências capazes de conduzir à absolvição ou de mitigar a responsabilidade da pessoa acusada, parece óbvia. Em um contexto de elementos e provas digitais, que além de dotadas de uma natureza particularmente técnica, abrangem uma quantidade praticamente infinita de dados que podem, eventualmente, ser úteis à defesa, a ideia parece ainda mais natural.

É disso que trata a *disclosure*⁴, regra já garantida às defesas de pessoas imputadas em alguns países e por diplomas de Direito Internacional, mas que ainda não está prevista pelo ordenamento jurídico brasileiro.

O presente artigo propõe, nesse sentido, um estudo sobre a ausência de regras sobre a *disclosure* no Brasil e os prejuízos que decorrem dessa falta, principalmente quando os elementos e provas não acessados pela defesa são digitais.

Diante desse contexto, o trabalho pretende: conceituar a regra da *disclosure* e analisar suas origens no direito anglo-saxão, com ressalvas sobre os obstáculos que as tradições jurídicas da *common law* enfrentam para garanti-la (seção 2); explicar os motivos pelos quais é incorreto afirmar que Brasil adota, hoje, uma regra de *disclosure*, esclarecendo porém que há plena compatibilidade entre a *disclosure* e o direito constitucional ao contraditório – compreendido como garantia de influência e não surpresa – no contexto do processo democrático participativo, bem como entre a *disclosure* e a *par conditio* assegurada no Estatuto de Roma às pessoas acusadas (seção 3); tratar sobre a especial relevância da *disclosure* no cenário dos elementos e provas digitais, esclarecendo porque algumas de suas particularidades, tais como sua natureza e multiplicidade, fazem com que a dependência da defesa em relação às análises da Polícia e do Ministério Público sobre evidências digitais torne-se prejudicial (seção 4).

Metodologicamente, a pesquisa foi conduzida por duas estratégias de revisão bibliográfica: uma, realizada sobre materiais jurídicos coletados no Brasil e no exterior – com destaque para textos estadunidenses e ingleses; outra, interdisciplinar (Japiassu, 1976), promovida a partir de pesquisas realizadas no âmbito das ciências da computação e da informação.

Ao final, espera-se demonstrar os motivos que tonam a *disclosure* uma necessidade, ainda mais evidente no ambiente das provas digitais, e subsidiar pesquisas futuras sobre este tema, até então inédito nas produções científicas nacionais.

⁴ O termo inglês *disclosure* costuma ser traduzido para o português como “divulgação” ou “revelação”. Os verbos “divulgar” e “revelar”, porém, não parecem os mais adequados para expressar o significado da *disclosure*, porque trazem consigo uma ideia mais ampla, como se a informação a ser divulgada e revelada pudesse ultrapassar os limites do processo e seus sujeitos, atingindo uma ideia de publicidade mais ampla – o que não é o caso. Exatamente por isso, o presente artigo adotará o estrangeirismo.

2. REGRA DE *DISCLOSURE*: CONCEITO, ORIGENS E OBSTÁCULOS

A regra de *disclosure* consiste na obrigatoriedade de que a acusação compartilhe com a defesa todos os elementos de informação e provas às quais teve acesso - sejam aquelas produzidas pelo próprio Ministério Público nas investigações por ele conduzidas, sejam aquelas produzidas pela Polícia - e, principalmente, aquelas que tenham potencial exculpatório ou de mitigação da responsabilidade criminal.

De acordo com Ellen Yaroshefsky (2011, p. 1.321), a *disclosure* figura entre as mais essenciais regras para um sistema de justiça criminal justo, na medida em que minimiza o efeito indesejável da surpresa no julgamento e contribui para uma determinação mais precisa sobre a questão da culpa ou inocência.

A regra integra o sistema adversarial que rege o processo penal em países de tradição anglo-saxã. Esse sistema se caracteriza, segundo Mirjan Damaška (1997, p. 74), como um modelo de julgamento no qual o processo é controlado pelas partes enquanto a figura do Juízo permanece, essencialmente, passiva e inerte.

No conceito adversarial, a gestão da prova é promovida exclusivamente pelas partes (Damaška, 1997, p. 75), encarregadas de buscar e encontrar material probatório (regra de *discovery*), compartilhá-lo integralmente entre si (regra de *disclosure*), apresentá-la e confrontá-la em juízo.

A associação imediata entre provas e partes, todavia, gera repercussões relacionadas à administração da justiça. A possibilidade de que os elementos factuais que subsidiam a decisão judicial sejam distorcidos ou falseados é uma das principais preocupações do direito anglo-saxão⁵ (Damaška, 1997, p. 79) e, por esse motivo, tornam-se necessárias algumas intervenções do Poder Judiciário.

A origem da regra de *disclosure* nos países da *common law* é exemplo da intervenção judicial na gestão da prova pelas partes. A seguir, a forma como essa regra surgiu, bem como os obstáculos impostos à sua consolidação serão analisadas a partir do histórico dos dois principais representantes da tradição jurídica anglo-saxã: os Estados Unidos e a Inglaterra.

2.1 A *disclosure* no direito estadunidense

⁵ Essa, obviamente, não é uma preocupação exclusiva do direito anglo-saxão, apesar de bastante acentuada no sistema jurídico adversarial. Em verdade, como bem destaca Damaška, (1997, p. 79), trata-se de um problema histórico dos julgamentos criminais, retratado até mesmo na Bíblia (aqui, o autor se refere à passagem do Livro de Daniel em que Susana, uma mulher judia casada, é acusada de adultério por dois anciões que, ao serem confrontados separadamente, confessam a mentira e assumem que se tratava de uma chantagem).

No direito estadunidense, a regra da *disclosure* nasceu a partir do precedente *Brady v. Maryland* (373, US 83), julgado pela Suprema Corte em 1963.

O caso teve início em 1958⁶, quando John Leo Brady foi acusado de matar William Brooks durante um roubo. A motivação para o crime seria o fato de que a vítima teria reconhecido Brady e seu coautor, Donald Boblit.

Em seu depoimento inicial, Boblit afirmou ter sido Brady o responsável pela execução do homicídio e disse que apenas viu o momento em que Brooks foi estrangulado por ele. Ocorre que esse depoimento foi sucedido por outras quatro declarações de Boblit e, na última delas, o homem admitiu ser ele – e não Brady – o executor do homicídio.

Essa confissão, capaz de influenciar os jurados a serem mais complacentes com Brady e deixarem de aplicar-lhe a pena capital, foi ocultada pelo Ministério Público durante o julgamento de Brady, que foi condenado pelo homicídio e sentenciado à morte pela administração de gás letal.

No corredor da morte, Brady recebeu aconselhamento religioso e foi apresentado ao advogado Clinton Bamberger. Atuante na comunidade católica, Bamberger havia deixado, há poucos anos, os quadros da Promotoria de Maryland para dedicar-se ao setor privado e aceitou representar Brady em fase recursal.

O primeiro apelo de Brady foi direcionado à Corte de Apelação de Maryland. No julgamento, apesar de reconhecer que a escolha deliberada da acusação de ocultar provas importantes violava o direito de Brady ao devido processo legal, foi negado provimento ao recurso. A decisão fundamentou-se no sentido de que a Corte não poderia presumir que o conhecimento sobre essas provas teria impactado a defesa de Brady ou interferido na decisão dos jurados.

Sendo o direito ao devido processo legal garantido pela 14ª Emenda à Constituição dos Estados Unidos, Bamberger submeteu o caso à Suprema Corte. Sob relatoria do Justice William O. Douglas, a Suprema Corte manteve a decisão da Justiça primeva naquilo que se referia à condenação de Brady pelo homicídio, mas anulou a sentença em relação à pena de morte.

Em seu voto, Justice Douglas reconheceu que o Ministério Público de Maryland violou o direito de Brady ao devido processo legal e promoveu uma virada revolucionária (Bibas, 2005, p. 129) ao estabelecer a Regra Brady (*Brady Rule*), segundo a qual a acusação deve compartilhar (*to disclose*) com a defesa qualquer prova favorável à pessoa imputada, seja ela

⁶ Todas as informações fáticas sobre o caso foram extraídas da obra de Thomas L. Dybdahl (2023).

absolutória ou com potencial de reduzir a pena. Em um dos trechos mais conhecidos de seu voto, Justice Douglas afirmou:

Society wins not only when the guilty are convicted, but when criminal trials are fair; our system of the administration of justice suffers when any accused is treated unfairly. An inscription on the walls of the Department of Justice states the proposition candidly for the federal domain: "The United States wins its point whenever justice is done its citizens in the courts." A prosecution that withholds evidence on demand of an accused which, if made available, would tend to exculpate him or reduce the penalty helps shape a trial that bears heavily on the defendant⁷.

Desde o julgamento pela Suprema Corte, porém, o dever de *disclosure* tem recebido uma aplicação descontínua, circunstância bastante recorrente na *common law* (Catalano; Gloeckner; Dalmagro Junior, 2025, p. 156).

A aplicação da Regra de Brady varia entre as jurisdições federais e estaduais. No âmbito federal, a *disclosure* é regulada pela *Regra 16* do Código de Processo Criminal Federal, que determina ser um dever da acusação facultar à defesa o acesso a: (a) qualquer declaração oral que tenha sido tomada da pessoa acusada; (b) qualquer registro em áudio ou vídeo de depoimento tomado da pessoa acusada; (c) folha de antecedentes da pessoa acusada; (d) qualquer documento ou objeto – tangível ou intangível – que esteja sob custódia do Estado; (e) relatórios de exames ou testes científicos que tenham sido realizados; (f) em relação aos peritos e assistentes técnicos do Estado, todos os pontos que serão objeto de seu depoimento, além de uma lista de publicações de autoria da pessoa *expert* nos últimos dez anos e uma lista de todos os casos nos quais a pessoa *expert* testemunhou nos últimos quatro anos.

Nos âmbitos estaduais, por sua vez, a *disclosure* nem sempre é prevista ou o é com tanta exatidão. A falta de clareza sobre seus limites e exigências acaba transformando a expectativa de civilizar a justiça criminal estadunidense em uma promessa não cumprida (Yaroshefsky, 2011, p. 1.325-1.326):

Federal and state court rules and statutes supplement prosecutors' constitutional obligations. For example, Federal Rule of Criminal Procedure 16 compels prosecutors to produce "[u]pon a defendant's request" information "material to preparing the defense.". The Jencks Act requires, inter alia, prosecutors to produce prior statements of a government witness after that witness testifies State court rules and statutes also

⁷ Em tradução livre: “A sociedade ganha não apenas quando os culpados são condenados, mas também quando os julgamentos criminais são justos; nosso sistema de administração da justiça sofre quando qualquer acusado é tratado injustamente. Uma inscrição nas paredes do Departamento de Justiça afirma abertamente a proposição para o domínio federal: “Os Estados Unidos ganham sempre que a justiça é feita aos seus cidadãos nos tribunais”. Uma acusação que retém provas solicitadas por um acusado que, se disponibilizadas, tenderiam a exculpá-lo ou reduzir a pena, contribui para moldar um julgamento que pesa fortemente sobre o réu”. A íntegra dos registros do julgamento *Brady v. Maryland* está disponível em: <https://supreme.justia.com/cases/federal/us/373/83/>. Acesso em: 14 jul. 2025.

impose disclosure obligations. These varying rules call for disclosure of specified documents, physical items, and other information. These may include: written and recorded statements of the defendant, reports of the defendant's prior criminal convictions, physical evidence that the prosecution plans to use at trial, expert reports, witnesses' criminal records, and prosecution witnesses' relevant written and recorded statements. Unlike in the federal system, where prosecutors need not list their witnesses prior to trial, prompt and full disclosure of witness statements is the rule in many states.⁸ Many states specify time limits within which disclosures must be produced⁸.

Mas a falta de uniformização na aplicação do precedente de Brady não é o único problema enfrentado pela *disclosure* no direito estadunidense. Apesar da intensa publicidade⁹ no que se refere aos casos de reversão de condenações injustas pelo descumprimento da *Brady Rule* – das 2.400 revisões de casos penais documentadas entre os anos de 1989 e 2019, as violações à *disclosure* corresponderam a 44% (Gross; Possley; Roll; Stephens, 2020) - os obstáculos à sua aplicação são culturais e envolvem, principalmente, a negligência, os erros e os vieses de confirmação.

É o que conclui a pesquisa conduzida com por Ellen Yaroshefsky (2013) com Promotores de Justiça estaduais lotados nas regiões nordeste, sudeste e centro-oeste dos Estados Unidos. Em relação à negligência e aos erros, a autora pontua que o grande volume de casos e a falta de recursos, principalmente nos grandes centros urbanos, criam um ambiente repleto de documentações insuficientes, falhas no acompanhamento das provas policiais e falta de atenção a itens de valor probatório.

Já naquilo que se refere aos vieses de confirmação, a autora sugere a tendência natural dos Promotores de revisar os relatórios não em busca de provas exculpatórias que possam refutar a hipótese testada, mas sim em busca de provas incriminatórias que a confirmem. Ainda, pondera a hipótese de que os Promotores, convencidos de sua teoria de culpa, sequer

⁸ Em tradução livre: “As regras e estatutos dos tribunais federais e estaduais complementam as obrigações constitucionais dos promotores. Por exemplo, a Regra Federal de Processo Penal 16 obriga os promotores a apresentar, “mediante solicitação do réu”, informações “relevantes para a preparação da defesa”. A Lei Jencks exige, entre outras coisas, que os promotores apresentem declarações anteriores de uma testemunha do governo após o depoimento dessa testemunha. As regras e estatutos dos tribunais estaduais também impõem obrigações de divulgação. Essas regras variadas exigem a divulgação de documentos específicos, itens físicos e outras informações. Estas podem incluir: declarações escritas e gravadas do réu, relatórios de condenações criminais anteriores do réu, provas físicas que a acusação planeja utilizar no julgamento, relatórios de peritos, registros criminais das testemunhas e declarações escritas e gravadas relevantes das testemunhas da acusação. Ao contrário do sistema federal, em que os promotores não precisam de listar as suas testemunhas antes do julgamento, a divulgação rápida e completa das declarações das testemunhas é a regra em muitos estados. Muitos estados especificam prazos dentro dos quais as divulgações devem ser apresentadas.”

⁹ Como exemplo, cita-se o premiado documentário “Marking a Murderer” (Netflix, 2015), que narra a história de Steven Avery, exonerado após cumprir 18 anos de pena. Testes de DNA revelaram que o crime havia sido praticado por outra pessoa, que era conhecida pela acusação à época das investigações. As informações sobre essa pessoa, bem como provas relevantes sobre o álibi de Avery foram, comprovadamente, ocultadas da defesa.

conseguem perceber uma teoria alternativa de como as informações poderiam ser usadas pela defesa (Burke, 2006, p. 1.590).

Um outro fator - subjacente, mas de grande relevância - constatado por Yaroshefsky (2013) e que dificulta o acatamento da acusação às regras de *disclosure* é a cultura local de cada Promotoria. Enquanto, em alguns órgãos, a regra é manter as provas à disposição das defesas – com a cautela necessária em casos que envolvem a segurança de vítimas e testemunhas, como a omissão de seus endereços, em outros a orientação era diametralmente oposta: não fornecer à parte contrária (defesa) nenhum material que pudesse contribuir para suas teses ou atrasar esse fornecimento ao máximo.

Por fim, como pondera Yaroshefsky (2013), não se pode ignorar o fato de que o descumprimento da Regra de Brady não costuma gerar nenhuma repercussão aos Promotores de Justiça. Há uma imunidade sobre eventuais responsabilizações nos âmbitos administrativo, cível e penal e, em contrapartida, inexistente qualquer vantagem ou bônus a quem cumpre a *disclosure* – na verdade, se o cumprimento da regra implicar em uma absolvição, as consequências pessoais e profissionais podem ser negativas.

2.2 A *disclosure* no direito inglês

No ordenamento jurídico inglês, o precedente considerado como marco da regra de *disclosure* (Johnston, 2021, p. 4) é *Rex v. Bryant and Dickson*, de 1946¹⁰. O caso tem origem a partir de uma fraude envolvendo a empresa de manutenção de ambulâncias que era de Dickson e na qual Bryant trabalhava.

A fraude, de acordo com a acusação, envolvia a execução de serviços diversos dos contratados, sempre sob a supervisão de outro funcionário da empresa, de nome Campbell. Esse supervisor, responsável por facilitar as fraudes, prestou depoimento extrajudicial para a acusação, mas suas declarações nunca foram apresentadas à defesa. Além disso, a acusação não arrolou Campbell como testemunha, impossibilitando a oportunidade da defesa de confrontá-lo em juízo.

Para a Suprema Corte do Reino Unido, não haveria qualquer falha na conduta da acusação porque as declarações extrajudiciais prestadas por Campbell não poderiam ser

¹⁰ Todas as informações fáticas sobre o caso foram extraídas de: <https://swarb.co.uk/rex-v-bryant-and-dickson-cca-1946/> e <https://publications.parliament.uk/pa/ld199798/ldjudgmt/jd970724/mills02.htm>. Acesso em: 15 jul. 2025.

utilizadas como prova no processo judicial e porque, apesar de não o arrolar como testemunha, o Ministério Público deu à defesa a oportunidade de fazê-lo.

O Relator do processo, Lord William Edgar Rayner Goddard, entendeu que o dever da acusação seria possibilitar à defesa (*to disclose*) a identificação de uma testemunha capaz de contribuir para sua tese e que esse dever, no caso concreto, foi cumprido.

A ideia da *disclosure* como regra que impunha à acusação o dever de compartilhar com a defesa informações que lhe pudessem ser relevantes – ainda que não fosse obrigação do Ministério Público produzir, em juízo, as provas absolutórias – foi reforçada pela Suprema Corte em 1964, durante o julgamento do caso *Dallison v. Caffery*¹¹.

No julgamento, o Relator Lord Tom Denning consignou ser um dever da acusação possibilitar à defesa o acesso a elementos relevantes capazes de provar a inocência da pessoa acusada. Lord Denning salientou, ainda, que independentemente de a acusação estar ou não convencida sobre a credibilidade dos elementos ou sobre seu potencial exculpatório, estes devem ser compartilhados com a defesa, dando-lhe a oportunidade de valer-se ou não dessas informações em juízo¹².

Atualmente, o dever de *disclosure* da acusação na Inglaterra está previsto na terceira seção da Lei de Processo Penal e Investigações (CPIA). A norma dispõe que é direito da pessoa acusada ter acesso a qualquer material que possa ser considerado capaz de prejudicar a acusação ou auxiliar a defesa. A legislação ressalva, todavia, que a pedido da Promotoria de Justiça, o material poderá ser mantido em sigilo no caso de proteção do “interesse público”, conceito que carece de definição mais precisa.

No cenário inglês, contudo, a regra de *disclosure* apresenta um ponto de inflexão relevante (Johnston, 2021, p. 5) desde a vigência da Lei de Justiça Criminal de 1967, que impôs também à defesa o dever de compartilhar com a acusação detalhes de quaisquer testemunhas cujo depoimento tivesse teor exculpatório. Em 1987, os deveres de *disclosure* da defesa foram estendidos e passaram a abranger o compartilhamento de provas periciais com a acusação antes dos julgamentos¹³. O rigor sobre as obrigações da defesa tornou-se ainda maior em 1996,

¹¹ Todas as informações fáticas sobre o caso foram extraídas de: <https://vlex.co.uk/vid/dallison-v-caffery-803896285>. Acesso em: 15 jul. 2025.

¹² Eis o trecho do voto de Lord Denning: "The duty of a prosecuting counsel or solicitor, as I have always understood it, is this: if he knows of a credible witness who can speak to material facts which tend to show the prisoner to be innocent, he must either call that witness himself or make his statement available to the defence. It would be highly reprehensible to conceal from the court the evidence which such a witness can give. If the prosecuting counsel or solicitor knows, not of a credible witness, but a witness whom he does not accept as credible, he should tell the defence about him so that they can call him if they wish". Disponível em: <https://lite.judicial.org.uk/cases/dallison-v-caffery>. Acesso em: 15 jul. 2025.

¹³ Em 1987, foi criado o chamado Comitê Roskill para examinar processos relacionados a fraudes ocorridas na Inglaterra e no País de Gales. O relatório final do comitê recomendou uma extensão do regime de *disclosure* da

quando promulgada CPIA, com o objetivo de “restaurar a imagem abalada do governo em relação à lei e à ordem” (Johnston, 2021, p. 6). Em relação à *disclosure*, a Lei exigia que a defesa, antes do julgamento, apresentasse: (a) os termos gerais e a natureza da defesa a ser desenvolvida; (b) a indicação dos objetos de discordância em relação à acusação; (c) os fundamentos sobre cada objeto de discordância em relação à acusação.

Em 2003, uma nova Lei de Justiça Criminal alterou algumas disposições da CPIA de 1996 e aumentou, significativamente os deveres de *disclosure* da defesa, que permanecem – até os dias de hoje – sendo os seguintes: (a) estabelecer a natureza da defesa, incluindo qualquer tese específica sobre a qual pretenda se basear; (b) indicar as questões de fato que são objeto de discordância em relação à acusação; (c) expor os fundamentos sobre cada objeto de discordância em relação à acusação; (d) indicar qualquer questão de direito (incluindo questões relativas à admissibilidade de provas ou excessos da acusação) que pretenda suscitar.

Impor à defesa tantas regras de *disclosure*, de acordo com Ed Johnston (2021, p. 8) implica em um grande obstáculo ao modelo adversarial de processo penal. Ao obrigar a defesa a contribuir, de forma significativa, com a acusação, há uma evidente inversão no papel defensivo, que passa a somar-se ao discurso acusatório na busca pela condenação. Essa inversão, para o autor, viola os direitos fundamentais da pessoa acusada ao devido processo legal, à não autoincriminação, à presunção de inocência e ao ônus da prova.

Para além das atribuições de *disclosure* à defesa, outro obstáculo enfrentado pelo instituto no direito inglês – e comum ao sistema estadunidense – é o cultural. Há uma grande resistência às regras da *disclosure* que impliquem no compartilhamento de provas com a defesa, em especial por parte da Polícia. Segundo Tom Smith (2021, p. 34), apesar de ser um órgão independente do Ministério Público, a Polícia inglesa também é influenciada pela cultura de partes (ou “lados”) e de perda-ganho próprias da tradição adversarial. Com isso, acaba por tender a investigar fatos e provas incriminadores ao invés de buscar evidências exculpatórias.

O autor chama a atenção para o fato de que a noção de partes (ou “lados”) incentiva uma espécie de lealdade que, na perspectiva das Polícia, seria devida aos interesses da vítima defendidos pela acusação, e não aos direitos da pessoa acusada e seus defensores. Ressalta, ainda, que nessa circunstância os conceitos de “lados”, “ganhar” ou “perder” prevalecem sobre a lealdade ao processo e aos fatos.

Ao concluir pela necessidade de mudanças paradigmáticas na cultura policial, Smith (2021, p. 43) destaca que a *disclosure* é um mecanismo investigativo importante para o trabalho

defesa, afirmando que o público acreditava que o processo, da forma como estava, era “um convite aberto a atrasos e abusos flagrantes” e deu origem à nova regra, estabelecida pelo Tribunal da Coroa (Smith, 2021).

policiais de qualidade, que se concentra nos fatos ao invés de preocupar-se com resultados ou vitórias. Reconhece o autor, todavia, que tais mudanças estruturais devem ter início desde o treinamento dos recrutas e estarem baseadas em aprendizagem proativa e práticas engajadas por parte dos policiais.

Os relatórios anuais da Comissão de Revisão de Casos Criminais (CCRC) reforçam os argumentos de Smith (2021) sobre as dificuldades de cumprimento, pelas Autoridades, das regras da *disclosure*. Um estudo realizado sobre os casos submetidos à CCRC entre 1997 e 2007 (Elks, 2008) revelou que 15% dos casos encaminhados pela Comissão à Corte de Apelação para novo julgamento se fundamentavam no descumprimento da *disclosure* pela acusação.

Dados da Comissão nos anos posteriores (Quirk, 2021, p. 92) passaram a registrar as falhas de *disclosure* como principal motivo para condenações injustas (2010-2011), um tema recorrente (2012-2014) e a causa mais frequente para revisões (2015-2016). No ano de 2018, a CCRC divulgou a estimativa de que, nos últimos 10 anos (ou seja, entre 2008 e 2018), cerca de um em cada cinco casos nos quais as condenações foram anuladas foram baseados na falta de *disclosure* da acusação em relação à defesa.

2.3 Conclusão (parcial) sobre a *disclosure* no direito anglo-saxão

A *disclosure*, em ordenamentos jurídicos da tradição *common law*, deriva de precedentes das décadas de 1940 a 1960 que evoluíram – positiva ou negativamente – no decorrer do tempo.

As indefinições legislativas sobre a *Brady Rule* nos Estados Unidos e os robustos deveres de *disclosure* incumbidos à defesa na Inglaterra são, certamente, obstáculos à consagração dos direitos das pessoas acusadas.

Em comum, os sistemas de ambos os países demonstram uma resistência por parte das Autoridades em relação à *disclosure*. Essa resistência pode ser compreendida pela própria lógica do modelo adversarial de processo penal e a ideia de confronto entre partes (acusação *v.* defesa).

Obstáculos e resistências, porém, não diminuem a importância da *disclosure* como regra capaz de garantir um julgamento mais equânime pela perspectiva da defesa e de diminuir os riscos de condenações injustas. Exatamente por isso, passar-se-á a analisar a aderência da *disclosure* ao direito brasileiro, tanto no âmbito da constitucionalidade quanto na perspectiva da convencionalidade.

3. CONSTITUCIONALIDADE E CONVENCIONALIDADE DA REGRA DE DISCLOSURE E SUA ADERÊNCIA AO PROCESSO PENAL BRASILEIRO

Na legislação brasileira, não existe nenhuma previsão que garanta à defesa o direito de receber, por parte da acusação, todos os elementos de informação ou provas que tenham sido produzidos durante as investigações ou que serão utilizados durante o processo, com foco nas evidências que tenham potencial exculpatório ou de redução da responsabilidade criminal.

É preciso, desde já, esclarecer que a previsão do artigo 7º, inciso XIV da Lei 8.9606/1994 (Estatuto da Advocacia e a Ordem dos Advogados do Brasil) e o teor da Súmula Vinculante nº 14 do Supremo Tribunal Federal (STF) não se confundem com a regra de *disclosure*.

Enquanto o direito assegurado pelo Estatuto da Advocacia se limita a autorizar o acesso, por parte de profissional inscrito na Ordem dos Advogados do Brasil, dos autos de flagrante e de investigações de qualquer natureza, a Súmula Vinculante nº 14 garante à defesa o acesso a elementos de prova que já estejam documentados em procedimento investigatório.

Veja-se que, em ambas as hipóteses, o compartilhamento de elementos de informação entre acusação e defesa não é espontâneo – como ocorre na regra de *disclosure*, dependendo sempre de requerimento por parte de advogados e advogadas.

Além disso, nenhum dos dispositivos impõe às autoridades públicas (Polícia ou Ministério Público) o dever de registro, documentação e compartilhamento de todos os elementos porventura obtidos durante a investigação ou no curso dos processos.

Nem mesmo a Lei de Acesso à Informação (Lei nº 12.527/2011) prevê essa obrigatoriedade, limitando-se a incumbir aos órgãos públicos que observem as normas e procedimentos específicos para uma gestão transparente da informação, garantindo sua disponibilidade, autenticidade e integridade. Tais “normas e procedimentos específicos”, porém, não existem de forma uniformizada no caso das Polícias e do Ministério Público.

Como exemplo de “norma e procedimento específico”, a Resolução nº 2010/2020 do Conselho Nacional do Ministério Público Federal, que dispõe sobre os procedimentos investigatórios realizados por aquele órgão, apenas prevê o direito da pessoa investigada de ter acesso aos autos (artigo 22) – sem atribuir às Autoridades o dever de registrar e documentar nesses autos todos os elementos de informação e provas coletadas no decorrer da investigação.

Por fim, necessário destacar que, tanto o Estatuto da Advocacia, quanto a Súmula Vinculante nº 14 e a Lei de Acesso à Informação comportam – ainda que a título de exceção – hipóteses de manutenção do sigilo em relação ao teor das investigações.

É o que diz o § 11 do artigo 7º do Estatuto da Advocacia, quando prevê a hipótese de que as autoridades impeçam o acesso do advogado aos elementos de prova relacionados a diligências em andamento ou ainda não documentados nos autos; o Precedente Representativo da Súmula Vinculante nº 14¹⁴, que admite hipóteses em que as diligências devem ser mantidas em sigilo para preservar a investigação; e o artigo 23, inciso VIII da Lei de Acesso à Informação, que classifica como sigilosos os dados que possam comprometer atividades de investigação relacionadas com a prevenção ou repressão de infrações.

O sigilo das investigações, conforme ensinam Aury Lopes Jr. e Ricardo Gloeckner (2014, p. 200), tem o fundamento básico e utilitário de garantir a eficácia da investigação sem a presença ou intervenção da pessoa investigada. Parte, também, da ideia de que a atuação dos órgãos públicos durante a investigação será sempre pautada por diretrizes de integridade e imparcialidade.

Os autores pontuam ser o sigilo, nesses moldes, uma tradição do sistema inquisitório que reforça a desigualdade entre os sujeitos da investigação, com reflexos negativos sobre a fase processual.

O argumento utilitário da busca pela maior eficácia da investigação é insustentável (Lopes Jr; Gloeckner, 2014, p. 201) quando levando em consideração que a ausência de intervenção da defesa impossibilita o controle das evidências e causa erros de interpretação ou omissões que poderiam ser evitados pelo compartilhamento de provas e elementos de informação.

A imparcialidade, por outro lado, não passa de uma ilusão: nas investigações conduzidas pelo Ministério Público, porque as figuras de investigador e acusador se concentram sobre uma mesma autoridade; nas investigações conduzidas pelas Polícias, pelo baixo grau cultural e pela fragilidade a pressões externas (Lopes Jr; Gloeckner, 2014, p. 203).

Mas, se a *disclosure* não foi – até o momento – incorporada no ordenamento jurídico pátrio, quais seriam os fundamentos para sua aderência ao processo penal brasileiro? A resposta parece estar na Constituição da República de 1988 e no Estatuto de Roma, promulgado pelo Brasil por meio do Decreto nº 4.388/2002.

3.1 Aderência constitucional da *disclosure*: um necessário reforço ao contraditório

¹⁴ HC 88.190/RJ. Relator: Ministro Cezar Peluso. Supremo Tribunal Federal: Segunda Turma. Data de julgamento: 29 de ago. de 2006. Diário da Justiça: 6 de out. de 2006.

Mesmo diante dos direitos fundamentais previstos pela Constituição de 1988 e assegurados por tratados e convenções internacionais de direitos humanos que integram o bloco de constitucionalidade brasileiro, o processo penal sempre sofreu com a dificuldade de se adaptar às mudanças proporcionadas pelas garantias asseguradas às pessoas acusadas.

Essa crise desafia os direitos fundamentais, ainda que dotados de *status* constitucional e convencional, a deixarem de ser normas meramente enunciadoras de uma intenção e passarem a se adaptar e equilibrar à coerência do sistema.

Apesar dos desafios enfrentados pela processualidade penal, a Constituição de 1988 parece ter feito a sua parte: previu que seu rol de direitos fundamentais tivesse, de acordo com o próprio texto legal, aplicação imediata (artigo 5º, § 1º) e se alinhou às tendências de internacionalização dos direitos fundamentais (artigo 5º, § 2º), cristalizando as bases de um devido processo democrático.

Todas as importantes ferramentas concedidas pela Constituição ao processo penal para sua democratização, porém, dependem da mudança na compreensão dos institutos processuais. Essa mudança somente se perfaz quando o movimento de constitucionalização do processo passa a “assegurar, para as partes, igual oportunidade, de intervenção influente, na atividade preparatória da decisão” (Marinho Marques, 2016, p. 45).

A noção de que todas as pessoas afetadas pelo provimento judicial devem ter o direito de participar, plenamente, do espaço procedimentalizado no qual se desenvolve sua construção é o que caracteriza, de acordo com Aroldo Plínio Gonçalves (1992, p. 127) e com amparo no pensamento de Elio Fazzalari (1989), o direito ao contraditório.

Concebido a partir do princípio da influência, segundo o qual as partes têm idêntico direito de influir, argumentativamente, no desenvolvimento e no resultado do processo (Nunes, 2006), o direito ao contraditório assume contornos dinâmicos que vão muito além de elementos como a necessidade de informação e a possibilidade de reação.

É da influência, concretamente, que surge a garantia da não surpresa, que assegura às partes o direito de não serem afetadas por uma decisão sem participarem de sua construção. Desde a vigência do Código de Processo Civil de 2015, o contraditório passou a ser definido por sua face dinâmica - como influência e não surpresa – nos termos do artigo 9º.

Não basta, todavia, ressignificar o contraditório sem viabilizá-lo. Afinal, há significativa diferença entre garantir às partes o direito de influenciar a decisão e de não ser surpreendida pelos provimentos judiciais e possibilitar, efetivamente, o exercício dessa influência e não surpresa.

Surge, nessa perspectiva, a ideia de um sistema participativo de processo (Nunes; Bahia; Pedron, 2020, p. 298). Longe do ideal romântico de que as partes precisam contribuir, solidariamente, para que o processo possa atingir um resultado melhor ou mais “justo”, a participação deve ser tida como um ambiente processual em que uma das partes possa agir na defesa estratégica de seus interesses sem, contudo, limitar o direito da outra parte de fazer o mesmo.

Obviamente, não se trata de esperar que as partes ajam de maneira imparcial ou contrária às pretensões. Muito menos, de enfraquecer o desempenho das partes e reforçar o papel judicial – pensamento típico do já superado movimento de socialização processual.

No conceito de sistema participativo, a intenção é retirar o protagonismo de uma outra parte para tornar o processo policêntrico (Picardi, 2006, p. 208), envolvendo sujeitos diversos – cada um com sua função, estratégia e interesses – mas se desenvolvendo de forma dialética e pautada pela boa-fé processual.

Transpor as ideias de contraditório dinâmico e sistema participativo ao processo penal não é nada fácil. Não se pode ignorar que o contexto brasileiro está imerso na tradição inquisitória (Coutinho, 2024) e enfrenta, há décadas, uma realidade de intenso autoritarismo e contaminação pelo pensamento tecnicista (Gloeckner, 2018). Também não se pode esquecer que, mesmo na perspectiva democrática da Constituição da República de 1988, o processo penal brasileiro não foi capaz de concretizar direitos e garantias fundamentais, inclusive o contraditório (Barros; Marinho Marques, 2017, p. 350).

No caso do contraditório, especificamente, o processo penal passa por uma constante “erosão silenciosa” que, segundo Paolo Ferrua (2017, p. 4), é vislumbrada à medida em que se trata de garantia cujo valor é sempre reafirmado – nunca repudiado ou afastado – mas que, sutil e constantemente, acaba enfraquecida pelos mais diversos expedientes legislativos e judiciais.

Mas, é importante reconhecer a adequação desses fundamentos teóricos à regra de *disclosure*. Para que a defesa tenha a oportunidade de influenciar e de não ser surpreendida pelo provimento judicial, é preciso que conheça e tenha acesso a todos os elementos de informação e provas que tenham o potencial de absolver a pessoa imputada ou proporcionar-lhe qualquer mitigação de culpa.

E, para garantir o direito da defesa de conhecer e ter acesso a informações e provas, é necessário que as autoridades responsáveis por sua obtenção – Polícia e Ministério Público – revelem sua existência.

A *disclosure*, com base nessas premissas, se compatibiliza com o processo constitucional e atribui aos direitos fundamentais – entre eles, o contraditório – a função de orientar a atuação estatal pela via da fiscalidade, participação, controle.

3.2 Aderência convencional da *disclosure*

Sob a ótica da convencionalidade, definida como a aderência a tratados de direitos humanos ratificados pelo Brasil (Mazzuoli, 2009, p. 114) a regra da *disclosure* está prevista de forma expressa no artigo 67, item 2 do Estatuto de Roma (Decreto nº 4.388/2002), considerado um marco na defesa dos direitos humanos e um guia para as modificações legislativas dos Estados signatários (Giacomolli, 2015, p. 6).

De acordo com o dispositivo internacional, cabe à acusação informar à defesa, logo que possível, as provas que tenha em seu poder ou sob o seu controle com o potencial de revelar a inocência da pessoa acusada, atenuar sua culpa ou impactar a credibilidade das provas acusatórias.

Esse direito decorre da exigibilidade de *par conditio*, que objetiva afastar o domínio de uma das partes sobre o direito da outra de participar – mediante influência e sem surpresas - da construção da decisão judicial. Nereu Giacomolli (2015, p. 135) ressalta que no processo penal, em regra, a acusação dispõe de um nível superior de possibilidades de atuação quando comparada à defesa, em especial porque conta com a organização de toda a estrutura do Estado a seu favor e serviço.

Veja-se que a ideia de *par conditio* não se confunde com o conceito de paridade de armas, decorrente do princípio da igualdade (Vieira, 2014, p. 206). Essa diferença é de especial relevo para o processo penal, marcado pelo que Glauco Giostra (2021, p. 75) define como uma inevitável assimetria estrutural congênita, ainda mais acentuada na “fase das investigações, na qual é quase impossível prefigurar uma especularidade de deveres e direitos entre o investigador público e a defesa privada”.

Ainda que eliminar, por completo, a assimetria entre acusação e defesa seja difícil, considerando que o modelo de processo penal brasileiro se estrutura na supremacia da acusação oficial sobre defesa, existem medidas que podem mitigá-la:

Por isso, a defesa há de ser dotada da mesma capacidade e dos mesmos poderes que a acusação, admitindo-se o contraditório em todo momento e em todas as etapas do processo, em face de qualquer ato probatório. Essa função verifica-se no processo, mas vai além e alcança o conteúdo da decisão e os efeitos dela irradiantes às demais partes, em idêntica situação fática e jurídica (Giacomolli, 2015, p. 407).

Deve-se, nesse sentido, “limitar ao máximo o inevitável desequilíbrio de poderes e de prerrogativas a favor do acusador público, garantindo ao acusado direitos que não tornem irreversível a desvantagem no momento da formação da prova” (Giostra, 2021, p. 77).

A *disclosure*, nesse contexto, se mostra como uma alternativa para a *par conditio*, a ser estabelecida pela Lei e capaz de reduzir os níveis de arbitrariedade já constantemente desequilibrados no processo penal.

3.3 Conclusão (parcial) sobre a *disclosure* no direito brasileiro

As possibilidades que a legislação brasileira garante à defesa de acessar elementos de informação e provas produzidas no âmbito de investigações e processos criminais são singelas e não se confundem com a regra da *disclosure*.

Apesar disso, a *disclosure* teria espaço o ordenamento jurídico, ainda que diante de múltiplos desafios. Seus obstáculos, principalmente aqueles de matriz autoritária e cultural, são próximos daqueles enfrentados pelos países da tradição *common law* e descritos no item 2.

Já os fundamentos teóricos que a sustentam são a garantia do contraditório, compreendida na perspectiva dinâmica (como influência e não surpresa) de um espaço processual compartilhado, e a noção da *par conditio*, concentrada na possibilidade de diminuir a assimetria das partes, natural ao processo penal.

Como reforço da importância que a regra de *disclosure* tem para a processualidade penal, aderente à constitucionalidade e à convencionalidade, o tópico seguinte analisa a relevância do compartilhamento – por parte da acusação – de todos os elementos de informação e provas digitais que tenham ou possam ter potencial exculpatório ou de mitigação da responsabilidade penal da pessoa acusada.

4. RELEVÂNCIA DA *DISCLOSURE* À PROVA DIGITAL

Significativa parcela das evidências capazes de relacionar pessoas a fatos penais consistem em elementos probatórios digitais, armazenados em mídias como *smartphones*, *smartwatches*, *pendrives* e *notebooks*.

O crescente protagonismo dessas evidências eletrônicas, permeado pela interdisciplinaridade própria ao tema, suscita “problemas relacionados a tutelas constitucionais clássicas – privacidade, proteção das comunicações e devido processo legal” (Prado, 2024, p.

48) e impacta, de forma direta, todos os atos que integram o procedimento de gestão da prova penal.

Em razão disso, os métodos de obtenção (*discovery*) da prova digital e a higidez de sua cadeia de custódia (*chain of custody*) têm sido objeto de análises acadêmicas (no Brasil, ver: Prado, 2021; Mendes, 2024; Parodi, 2024; Lopes, 2025) da criação de procedimentos operacionais padronizados¹⁵ e da elaboração de propostas normativas¹⁶.

O tema da *disclosure*, compreendido como o acesso - por parte da defesa - à íntegra de elementos de informação e provas digitais colhidas durante a fase de investigação e utilizadas ou não pelo órgão acusatório no decorrer do processo judicial, porém, não costuma ser problematizado.

Essa lacuna somente passou a ser percebida e enfrentada no âmbito do processo penal a partir de casos específicos. Na Inglaterra – país que adota regras de *disclosure* (conforme elaborado no item 2.2), por exemplo, o tema passou a ser discutido em 2017 após a ampla repercussão dada pela imprensa ao caso *Liam Allan*¹⁷ (Johnston; Smith, 2021), preso por dois anos em decorrência do descumprimento da *disclosure* de provas digitais. Allan, um estudante universitário, foi acusado em 2015 de ter praticado, por doze vezes, o crime de estupro contra uma mesma vítima.

Por diversas vezes, a defesa solicitou, com base nas regras de *disclosure* estabelecidas pela Lei de Processo Penal e Investigações do país, o acesso aos documentos relacionados à quebra de sigilo telemático da vítima. De acordo com a Polícia, entre as mais de 57.000 mensagens localizadas no celular da jovem, nenhuma informação era relevante para a acusação ou para a defesa.

Em juízo, durante a fase de instrução iniciada em 2017, a defesa insistiu em acessar o material, com o objetivo de poder analisá-lo e tirar suas próprias conclusões sobre sua relevância ou não para o caso.

Com a garantia de acesso às provas digitais pela defesa, revelaram-se circunstâncias que culminaram na imediata retirada de todas as acusações: nas mensagens, a suposta vítima

¹⁵ É o caso dos Procedimentos Operacionais Padrão estabelecidos pelo Ministério da Justiça e Segurança Pública para perícias de informática forense <https://www.gov.br/mj/pt-br/assuntos/sua-seguranca/seguranca-publica/analise-e-pesquisa/pop/pop-pericia-criminal-2024-informatica-forense-vol-5-pdf.pdf/view>. Acesso em: 22 jul. 2025.

¹⁶ A título de exemplo, menciona-se a iniciativa do Conselho Nacional de Justiça (CNJ) de reunir especialistas no tema para subsidiarem a elaboração de uma proposta normativa sobre a cadeia de custódia de vestígios digitais em investigações e processos criminais. Nesse sentido: <https://www.cnj.jus.br/agendas/seminario-sobre-provas-digitais/>. Acesso em: 22 jul. 2025.

¹⁷ Um resumo sobre os fatos está disponível em: <https://www.bbc.com/news/uk-england-42873618>. Acesso em: 22 jul. 2025.

manifestava seu interesse por manter relações sexuais casuais com Allan e compartilhava com ele algumas fantasias sexuais que envolviam a simulação de estupro. Em outras conversas, a jovem comentava com terceira pessoa que Allan sempre a tratou muito bem e que as acusações que havia feito em seu desfavor eram falsas.

Nos Estados Unidos, outro país que adota a *disclosure* (conforme elaborado no item 2.1), as discussões envolvendo o compartilhamento com a defesa de elementos de informação e provas digitais colhidos pela acusação têm se concentrado na natureza técnica dessas evidências.

O volume de dados que costumam ser extraídos de dispositivos eletrônicos gerou controvérsias nas Cortes daquele país sobre a forma como eventuais informações exculpatórias ou com contexto favorável à mitigação da responsabilidade poderiam ser encontrados pela defesa.

Alguns julgados proferidos por Cortes Estaduais (Turner, 2019, p. 257) sugerem que a acusação deve disponibilizar à defesa arquivos em formatos pesquisáveis e sem uma sobrecarga por volume inútil de dados (por exemplo, no caso *United States v. Quinones*). Outros, minoritários, vão além e impõe à acusação o dever de localizar, entre todos os elementos de informação ou provas digitais obtidas, aqueles que têm o potencial exculpatório ou de diminuição da responsabilidade da pessoa acusada (por exemplo, no caso *United States v. Blankenship*).

De fato, a *disclosure* da prova digital é relevante porque telefones e outros dispositivos eletrônicos são verdadeiros repositórios de informações sobre as pessoas usuárias que neles depositam seus cotidianos, hábitos, gostos, desejos, paixões e ódios. Essa *disclosure*, todavia, precisa considerar as particularidades de tal modalidade probatória, que enfrenta desafios próprios – alguns, inclusive, de ordem técnica e que dependem do suporte, ao Direito, de áreas diversas do conhecimento.

4.1 Particularidades da prova digital que influenciam na *disclosure*

As evidências digitais são dotadas de características específicas que acabam por demandar uma disciplina jurídica própria (Saad; Rossi; Partata, 2024).

A primeira dessas características está relacionada à sua natureza. Na definição de Burkhard Schafer e Stephen Mason (2017, p. 19), são elementos de informação ou provas digitais quaisquer dados – sejam eles originalmente digitais ou analógicos – que possam ser

manipulados, armazenados ou comunicados por qualquer dispositivo fabricado, computador ou sistema de computador ou transmitidos por um sistema de comunicação.

Esses dados, por sua vez, são intangíveis e compostos, exclusivamente, por *bits* - dígitos binários (sequências dos números 0 e 1). Tal circunstância atribui a essas evidências um caráter de volatilidade e maleabilidade (Mason; Sheldon; Dries, 2017, p. 331), de modo que se tornam facilmente dispersas, podendo ser perdidas; corruptíveis, o que significa que podem ser modificadas de forma anônima ou involuntária; e reproduzíveis, sem qualquer limite sobre o número de cópias que podem ser potencialmente feitas a partir deles (Brighi; Ferrazzano, 2021, p. 14).

Por natureza, portanto, elementos de informação e provas digitais exigem maiores cautelas nos momentos de sua obtenção (*discovery*) e gestão (*chain of custody*). A obtenção, em regra, é feita pela apreensão dos suportes físicos que abrigam as evidências digitais (tais como *smartphones*, *pendrives* ou *notebooks*), sucedida da cópia (espelhamento) de seu conteúdo, ou pelo acesso remoto aos servidores as armazenam (Saad; Rossi; Partata, 2024, p. 16), com a posterior cópia (espelhamento) dos dados.

Já a cadeia de custódia é regida pelos termos do artigo 158-A e seguintes do Código de Processo Penal, os quais envolvem a manutenção e a documentação da história cronológica dos vestígios (físicos ou digitais) e permitem o rastreamento de sua posse e manuseio desde a coleta até o descarte. Mas não são apenas as fases da *discovery* e da *chain of custody* que sofrem com a influência da natureza das provas digitais, que também repercute sobre a *disclosure*.

Concretamente, a *disclosure* desses elementos e provas digitais somente é realizada sobre cópias (espelhamentos), sejam aquelas realizadas em relação à apreensão dos suportes físicos, sejam aquela relacionada ao acesso remoto. A defesa, em última instância, nunca tem acesso aos materiais originais.

Ao comentar essa particularidade da prova digital, Lorenzo Parodi (2024, p. 51) ressalta que o procedimento de cópias (espelhamento) pode ser realizado em duas modalidades: a cópia em sentido estrito ou a imagem. Enquanto na cópia em sentido estrito uma mídia física é copiada para outra mídia física similar, que passará a ter o exato e idêntico conteúdo da original (com o mesmo código *hash*¹⁸, inclusive); na imagem, o conteúdo integral de uma mídia é

¹⁸ “O *hash* é uma função que atende às demandas criptografadas necessárias para resolver uma computação blockchain. Os *hashes* têm um comprimento fixo, pois torna quase impossível adivinhar o comprimento do *hash* se alguém estiver tentando quebrar a blockchain. Os mesmos dados sempre produzirão o mesmo valor de *hash*. Uma função *hash* é um algoritmo matemático que pode usar qualquer tipo de entrada, como uma *string*, um arquivo de texto, ou um arquivo de imagem, e traduzi-lo para uma *string* de saída de tamanho fixo chamado *hash*. É uma função unidirecional, o que significa que a única maneira de recriar os dados de entrada originais (mensagem) do

transferido para um arquivo (ou um conjunto de arquivos) em formatos específicos que possibilitam a análise e as pesquisas.

O autor (Parodi, 2024, p. 52) dispõe que, em ambos os casos – de cópia em sentido estrito ou imagem – é fundamental que sejam adotadas ferramentas (*softwares* ou *hardwares*¹⁹), como os bloqueadores de escrita ou duplicadores forenses, capazes de impedir ou mitigar o risco de alterações (escritas) no conteúdo original. Essa cautela é necessária porque a capacidade de alterar ou atualizar arquivos é praticamente orgânica e decorre, muitas vezes, dos próprios sistemas operacionais, como o *Windows*.

Além da natureza das evidências eletrônicas, outra particularidade é a vasta quantidade e espécie de informações envolvidas: e-mails, mensagens de texto, conversas em aplicativos, fotografias, áudios, arquivos de texto, planilhas. Em cada um desses arquivos, além de seu conteúdo primário - em um arquivo de foto, a imagem; em um arquivo de áudio, o som; em um arquivo de texto, as palavras – estão inseridos outros dados que podem ter relevância para o processo penal, tais como atributos e metadados (Parodi, 2024, p. 42).

Os atributos consistem em informações sobre os arquivos - nome, tamanho, proprietário, direitos de acesso e datas de criação ou modificação. Por outro lado, os metadados são “blocos de informações estruturadas presentes em diversos tipos de arquivo e normalmente embutidos em sua estrutura interna” (Parodi, 2024, p. 43) – datas efetivas da criação de última modificação do arquivo, registros da origem do arquivo (equipamento ou *software* utilizado para gerá-lo), identificação da pessoa que o criou etc.

Tanto os metadados, quanto os atributos também podem sofrer alterações – situação de diminui seu potencial de confiabilidade -, mas são relevantes na medida em que contribuem para a detecção dos rastros deixados por eventuais alterações. Isto porque, como explica Parodi (2024, p. 46), “uma vez realizada uma apreensão (ou obtenção de arquivos de outra forma) e estando sob custódia, não deveria – em tese – ser mais possível a ocorrência de qualquer tipo de edição ou alteração” dos atributos e dos metadados.

Na *disclosure*, essa particularidade se projeta sobre os limites técnicos de defensores e defensoras. Para se extrair qualquer potencial exculpatório ou de mitigação da pena de um elemento de informação ou de uma prova digital, é necessário avaliar uma quantidade praticamente infinita de dados.

hash é tentar todas as variações possíveis para ver se elas produzem uma correspondência. O que só é possível utilizando-se os dados originais (Pastore; Fonseca, 2022, p. 105).

¹⁹ Segundo Irv Englander (2014, p. 2), o *software* consiste no sistema e nos programas de aplicativos que definem as instruções que são executadas pelo *hardware*, cuja função é determinar o trabalho a ser realizado e controlar a operação do sistema.

Da mesma forma, é preciso o acesso a uma série de ferramentas técnicas que dependem da aquisição de licenças para operação, cujo custo é extremamente alto. Algumas dessas ferramentas – talvez as mais conhecidas no Brasil – são aquelas desenvolvidas pela empresa israelense *Cellebrite*.

O discurso empresarial da *Cellebrite*, na compreensão de David Leal e Yuri Felix (2020, p. 14), se alinha às fórmulas econômicas efficientistas, regidas pela redução de custos e economia de tempo. Diante de uma quantidade e variedade cada vez maior de dispositivos digitais, a empresa oferece às agências de segurança pública soluções avançadas para a extração e análise das informações contidas nesses aparelhos: “Se os celulares registram todos os hábitos do usuário, cabe ao investigador se servir desse banquete de dados e, ao aprimorar sua performance pelo uso [dessas ferramentas] oferece respostas rápidas sobre o caso” (Leal; Felix, 2020, p. 14).

De acordo com o *website* oficial da empresa²⁰, um de seus produtos – o *UFED* - é capaz de contornar bloqueios, realizar desbloqueios avançados, realizar extrações lógicas/completas do sistema de arquivos/físicos, realizar extração seletiva de dados de aplicativos e tokens de nuvem, entre outras atividades. De acordo com a *Cellebrite*, existem mais de 60.000 licenças do *UFED* em operação ao redor de 150 países.

Uma noção de custo pode ser obtida em consulta aos arquivos da Secretaria Nacional de Segurança Pública (SENASP). Em proposta direcionada à Secretaria²¹, a empresa Techbiz Forense Digital Ltda., especializada na distribuição de soluções tecnológicas para as forças de segurança pública²², propõe a aquisição de 27 unidades – uma para cada Estado da Federação e Distrito Federal - das ferramentas abaixo, com um custo total de R\$ 64.908.955,80:

Solução para desbloqueio, extração avançada com capacidade de enriquecimento de dados de nuvem, geração e compartilhamento de relatórios – com suporte técnico e atualização tecnológica por 12 (doze) meses
Marca: Cellebrite - Modelo: Inseyets Collaborate Volume License Pack - Part Number: B- CNR-05-BRA

Hardware acessório para solução de desbloqueio, extração avançada com capacidade de enriquecimento de dados de nuvem, geração e compartilhamento de relatórios – Com suporte técnico e atualização tecnológico por 12 (doze) meses.
Marca: Cellebrite - Modelo: Inseyets Kit - Part Number: F-KAS-05-000

Renovação de Licença - Solução para desbloqueio, extração avançada com capacidade de enriquecimento de dados de nuvem, geração e compartilhamento de

²⁰ Disponível em: <https://cellebrite.com/en/ufed/>. Acesso em: 24 jul. 2025.

²¹ Disponível em: https://www.gov.br/mj/pt-br/aceso-a-informacao/licitacoes-e-contratosv1/licitacoes-e-contratos-senasp/cglic/contratos_senasp/contratos/copy_of_2024/copy88_of_contrato-no-01-2024/proposta-comercial.pdf. Acesso em: 24 jul. 2025.

²² Informações disponíveis em: <https://www.techbiz.com.br/>. Acesso em: 24 jul. 2025.

relatórios – com suporte técnico e atualização tecnológica por 12 (doze) meses.
Marca: Cellebrite - Modelo: Inseyets Collaborate Volume License Park - Part number:
B- CNR-05-BRA

Esses números revelam que a *disclosure* da prova digital, definitivamente, não é acessível para as defesas de expressiva maioria das pessoas acusadas. Ainda que profissionais da tecnologia possam adquirir essas ferramentas e oferecer seus serviços como assistentes técnicos, na forma prevista pelo artigo 159, 3º do Código de Processo Penal, o custo da contratação ainda precisaria ser arcado pela pessoa acusada – afinal, não existe previsão para a nomeação de peritos para auxiliar a defesa às custas do Estado.

Com uma justiça penal notadamente concentrada em réus e réis hipossuficientes (por todos: Zaffaroni, 2014), a contratação de assistentes técnicos *experts* para a análise de evidências eletrônicas não faz parte da realidade forense brasileira.

Sendo assim, mesmo que a defesa recebesse todos os elementos de informação e provas digitais coletados durante as investigações, buscar evidências exculpatórias ou mitigatórias em meio a uma infinidade de dados e sem apoio das ferramentas técnicas adequadas é missão impossível – ou, no ditado popular, é como “procurar agulha no palheiro”.

É por isso que, no atual estágio – sem regras de *disclosure* definidas e em meio às particularidades técnicas da prova digital – a defesa se coloca em posição de dependência absoluta dos trabalhos desenvolvidos durante a investigação e o processo pela Polícia e pelo Ministério Público.

4.2 O problema da *disclosure* para a prova digital: dependência das defesas em relação aos materiais produzidos pela Polícia e Ministério Público

Hoje, o exercício da defesa em processos que envolvem evidências digitais está sujeito aos materiais que são compartilhadas pela Polícia e pelo Ministério Público.

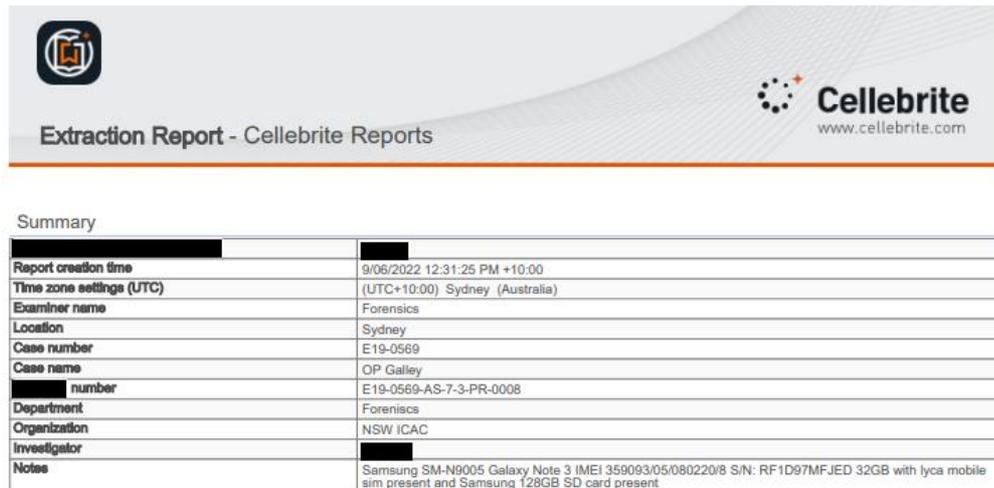
Além de não terem o dever de possibilitar à defesa o acesso à íntegra do conteúdo que foi objeto de *discovery* em aparelhos e dispositivos eletrônicos (conforme debatido no item 3 deste artigo), esses órgãos incluem nos autos de inquéritos policiais e ações penais tão-somente: (a) os Relatórios de Extração e (b) as análises realizadas por seus profissionais sobre alguns dos dados coletados.

Os Relatórios de Extração (*Extraction Reports*) contêm informações relacionadas ao procedimento técnico promovido pela ferramenta forense adotada. No caso da *UFED*,

desenvolvida pela *Cellebrite*, o relatório é dividido em alguns itens: Sumário, Fonte de Extração, Conteúdos Extraídos e Dados dos Arquivos.

No Sumário (*Summary*), o relatório especifica questões como a sua data de criação, o horário local, nome da pessoa responsável, localização, número do processo, departamento, e órgão responsável. Veja-se um exemplo:

Figura 1 – Item “Sumário” (*Summary*) no Relatório de Extração:



The screenshot shows the header of a Cellebrite report with the title 'Extraction Report - Cellebrite Reports' and the Cellebrite logo. Below the header is a table titled 'Summary' with the following data:

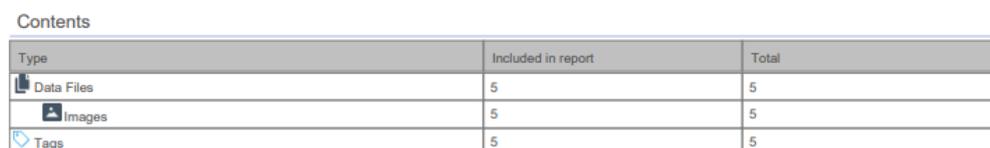
| Summary | |
|--------------------------|--|
| Report creation time | 9/06/2022 12:31:25 PM +10:00 |
| Time zone settings (UTC) | (UTC+10:00) Sydney (Australia) |
| Examiner name | Forensics |
| Location | Sydney |
| Case number | E19-0569 |
| Case name | OP Galley |
| number | E19-0569-AS-7-3-PR-0008 |
| Department | Forensics |
| Organization | NSW ICAC |
| Investigator | |
| Notes | Samsung SM-N9005 Galaxy Note 3 IMEI 359093/05/080220/8 S/N: RF1D97MFJED 32GB with lycra mobile sim present and Samsung 128GB SD card present |

Fonte: NSW Independent Commission Against Corruption²³

No item Fonte de Extração (*Source Extraction*), o relatório apresenta os dados do objeto da extração (por exemplo, um aparelho celular) como marca, modelo, sistema operacional, integridade da fonte e tipo de conexão.

Na seção dedicada aos Conteúdos extraídos (*Contents*), o relatório especifica a quantidade e o tipo de arquivos extraídos, conforme Figura abaixo:

Figura 2 – Item “Conteúdos Extraídos” (*Contents*) no Relatório de Extração:



The screenshot shows a table titled 'Contents' with the following data:

| Type | Included in report | Total |
|------------|--------------------|-------|
| Data Files | 5 | 5 |
| Images | 5 | 5 |
| Tags | 5 | 5 |

Fonte: NSW Independent Commission Against Corruption

Por fim, no último item do relatório, são descritos os Dados dos Arquivos (*Data Files*) extraídos. Na Figura a seguir, os arquivos correspondiam a imagens, motivo pelo qual são detalhados dados como o tamanho, a data de criação, a resolução e a orientação:

²³

Figura 3 – Item “Dados do Arquivo” (Data Files) no Relatório de Extração:

| Data Files (5) | | | | | |
|----------------|---|---|--|---------|---|
| Images (5) | | | | | |
| # | File Info | Additional file info | Thumbnail | Deleted | * |
| 1 | Name: sns_tmpt_11948070911428141152 Path: Image18 (ExD)\Root\media\0\tencent\MicroMsg\046e85de777abaa82ddb61d1aeef2831\sns\fb\sns_tmpt_11948070911428141192 MD5: 64772ff4c45ab66d12865ba5539edc7 | Size (bytes): 50568 Created: 19/02/2015 4:38:13 PM(UTC+11) Modified: 19/02/2015 4:38:13 PM(UTC+11) Accessed: 19/02/2015 4:38:13 PM(UTC+11) Source Extraction: Physical (1) Meta Data: Pixel resolution: 596x800 Orientation: Horizontal (normal) |  | |  |
| 2 | Name: sns1_11948070911428141192 Path: Image18 (ExD)\Root\media\0\tencent\MicroMsg\046e85de777abaa82ddb61d1aeef2831\sns\fb\sns1_11948070911428141192 MD5: 62b6fb68b12fe8b3e35fe3e3fd2677b0 | Size (bytes): 44386 Created: 19/02/2015 4:38:13 PM(UTC+11) Modified: 19/02/2015 4:38:13 PM(UTC+11) Accessed: 19/02/2015 4:38:13 PM(UTC+11) Source Extraction: Physical (1) |  | |  |
| 3 | Name: th_919a9d14837d882b62022767f88f725.jpg Path: Image18 (ExD)\Root\media\0\tencent\MicroMsg\046e85de777abaa82ddb61d1aeef2831\image2\91\9a\th_919a9d14837d882b62022767f88f725 MD5: 3fba7a384c7e60c905260c2d01296314 | Size (bytes): 5198 Created: 19/02/2015 5:00:10 PM(UTC+11) Modified: 19/02/2015 5:00:10 PM(UTC+11) Accessed: 19/02/2015 5:00:10 PM(UTC+11) Source Extraction: Physical (1) |  | |  |
| 4 | Name: 919a9d14837d882b62022767f88f725.jpg Path: Image18 (ExD)\Root\media\0\tencent\MicroMsg\046e85de777abaa82ddb61d1aeef2831\image2\91\9a\919a9d14837d882b62022767f88f725.jpg MD5: 24dd864cac681f5c72a637d481a3a21a | Size (bytes): 65302 Created: 19/02/2015 5:00:10 PM(UTC+11) Modified: 19/02/2015 5:00:10 PM(UTC+11) Accessed: 19/02/2015 5:00:10 PM(UTC+11) Source Extraction: Physical (1) |  | |  |
| 5 | Name: th_919a9d14837d882b62022767f88f725hd Path: Image18 (ExD)\Root\media\0\tencent\MicroMsg\046e85de777abaa82ddb61d1aeef2831\image2\91\9a\th_919a9d14837d882b62022767f88f725hd MD5: 521544b43301a821e621ef89b2d2bc5b | Size (bytes): 29611 Created: 19/02/2015 5:00:11 PM(UTC+11) Modified: 19/02/2015 5:00:11 PM(UTC+11) Accessed: 19/02/2015 5:00:11 PM(UTC+11) Source Extraction: Physical (1) |  | |  |

Fonte: NSW Independent Commission Against Corruption

As informações constantes do Relatório de Extração, portanto, são bastante limitadas. Além disso, são submetidas a filtros e seleções por parte dos seus operadores, cujos critérios não são revelados pelo documento.

No caso retratado nas Figuras 1, 2 e 3, o fato de somente terem sido extraídas do dispositivo eletrônico (telefone celular) cinco arquivos de imagem não significa que esses eram os únicos dados disponíveis no dispositivo. Pelo contrário, significa apenas que essas cinco imagens foram os únicos elementos considerados relevantes pela pessoa que procedeu à extração.

Ainda, com base exclusivamente no Relatório, é impossível conhecer os critérios adotados pela pessoa que operou a ferramenta para filtrar e selecionar os arquivos extraídos. No exemplo ilustrado pelas Figuras 1, 2 e 3, essas imagens podem ter sido o único objeto de interesse para a investigação por vários motivos – como a natureza do crime apurado, o objeto material do delito etc. – que são desconhecidos por quem acessa o relatório.

Válido esclarecer que esse obstáculo na identificação dos critérios não é suprido pela disponibilização, em conjunto com o Relatório, do *software* de extração na versão de leitura (*reader*). O referido *software*, que costuma ser disponibilizado pelas autoridades às defesas que

solicitam acesso às provas digitais, limita o acesso de seus usuários e usuárias aos dados que foram previamente selecionados - conforme informa o próprio *website* da *Cellebrite*²⁴.

No campo da *disclosure*, a importância de se conhecer os critérios para filtros e seleções de informações adotados por quem opera as ferramentas tecnológicas de extração de provas digitais já foi reconhecida, por exemplo, na Alemanha. Naquele país, segundo Sabine Whal (2021, p. 71), a *disclosure* das provas digitais compreende o direito da defesa de acessar todos os documentos e registros de natureza técnica, o que inclui dados computacionais, arquivos de dados criados durante as fases de investigação e impressões de dados em formato digital. Além disso, se as autoridades responsáveis pela investigação filtraram e selecionaram os dados, o direito de acesso abrange os critérios sobre os quais o relatório foi baseado.

Se os Relatórios de Extração apresentam informações filtradas e selecionadas, as análises realizadas pelas pessoas encarregadas da investigação sobre alguns dos dados coletados constituem elemento com a confiabilidade ainda mais reduzida.

Essas análises nada mais são que a interpretação – em regra, de agentes da Polícia ou do Ministério Público – sobre as provas digitais coletadas pela extração de dados de dispositivos apreendidos. Tal interpretação, pessoal e subjetiva, costuma ser amparada, de acordo com Parodi (2024, p. 73) pelo argumento da “fé pública”: afinal, por qual motivo uma pessoa investida em cargo público, cujos atos praticados são presumidamente legítimos e verdadeiros, teria sua análise sobre provas digitais contestada?

Esse argumento, quando seguido com tamanho fideísmo e cegueira seletiva (Parodi, 2024, p. 75) ignora a possibilidade de que as análises realizadas pelos agentes públicos sejam influenciadas por fatores como negligência, erros e vieses de confirmação – estes, definidos por Yaroshefsky (2013) como principais obstáculos à regra da *disclosure*, conforme visto no item 2.1 deste trabalho.

Além disso, o argumento da “fé pública” ignora o fato de que, no Brasil, a extração de dados e sua posterior análise pode ser realizada por qualquer agente público, independentemente de ter ou não recebido formação específica em tecnologia ou treinamento especializado para a utilização de ferramentas forenses (Dalmagro; Gloeckner, 2025)²⁵.

Finalmente, a “fé pública” corresponde a um argumento cuja fiscalidade é diminuída. Em especial, pela impossibilidade de a defesa submetê-lo ao contraditório, porquanto subordinada ao conteúdo produzido oficialmente.

²⁴ Informações disponíveis em: <https://cellebrite.com/pt/cellebrite-reader-pt/>. Acesso em: 25 jul. 2025.

²⁵ Os autores fazem referência ao seguinte julgado: AgRg no RHC nº 195.921/MG, rel. min. Rogerio Schietti Cruz, 6ª Turma, julgado em 27-5-2024, *DJe* de 3-6-2024.

Nesse aspecto, o risco é de que as análises realizadas por agentes públicos sobre alguns dos dados coletados a partir de dispositivos eletrônicos se converta em prova científica. Como adverte Elena Catalano (2017, p. 148), essa prova científica expropria da prova oral em julgamento o papel de prova soberana e marca a afirmação da prova *lato sensu* documental, de formação extrajudicial, como a nova “rainha das provas”.

4.3 Conclusão (parcial) sobre a relevância da *disclosure* para as provas digitais

As dificuldades para lidar com a prova digital, decorrentes de sua natureza e da vastidão de dados envolvidos, não obstaculizam as atividades do Estado de investigação e processamento de crimes, que seguem cada vez mais sofisticadas e com suporte tecnológico da melhor qualidade. A recíproca para a defesa, porém, não é verdadeira.

Sem ter os meios adequados (técnicos) para buscar, por si, evidências que possam absolver ou mitigar a responsabilidade da pessoa acusada ou para contraditar os documentos gerados, não é possível desenvolver uma atividade defensiva satisfatória.

Enquanto a defesa estiver submetida às informações que são descobertas (*discovery*), custodiadas (*chain of custody*), extraídas e analisadas pelas agências de investigação – Polícias e Ministério Público, não haverá que se falar em *disclosure* para a prova digital.

5. CONSIDERAÇÕES FINAIS

Este trabalho buscou explicar a importância da regra da *disclosure* ao exercício da defesa. Para tanto, cuidou de conceituar a *disclosure* e de explicar suas origens do direito anglo-saxão, sem deixar de lado as fragilidades enfrentadas pelos países da tradição *common law* para a sua verdadeira aplicação.

Igualmente, preocupou-se em explicar os motivos pelos quais não se pode dizer que, no ordenamento jurídico brasileiro, existem regras de *disclosure* vigentes, apesar de encontrarem uma fundamentação concreta e teórica a partir da Constituição da República de 1988 e do Estatuto de Roma.

Por fim, em uma proposta de estudo verticalizado, dedicou-se a aprofundar a relevância da *disclosure* em relação a uma modalidade probatória específica: as evidências eletrônicas. Em razão de suas particularidades, as provas digitais demandam uma disciplina jurídica própria, situação que repercute, imediatamente, sobre as possibilidades de *disclosure*.

Espera-se, a partir desta pesquisa, contribuir com os debates acadêmicos sobre os temas da prova e das evidências digitais, com enfoque nos direitos da defesa e nas possibilidades de atuação na busca de elementos exculpatórios ou capazes de mitigar a responsabilidade criminal da pessoa acusada.

Por suas limitações, o trabalho não esgota o tema, sendo necessários maiores aprofundamentos sobre a viabilização da *disclosure* no Brasil, inclusive com estímulos de *lege ferenda*, bem como sobre métodos que possam proporcionar o exercício de defesa técnica em favor de pessoas hipossuficientes nos assuntos que envolvem tecnologia.

REFERÊNCIAS

BARROS, Flaviane de Magalhães; MARQUES, Leonardo Augusto Marinho. A atuação do juiz no contraditório dinâmico: uma análise comparativa entre o sistema processual penal adversarial chileno e o modelo constitucional de processo brasileiro. *In*: POSTIGO, Leonel González (Dir.); BALLESTEROS, Paula R. (Coord.). **Desafiando a Inquisição: ideias e propostas para a reforma processual penal no Brasil**. Santiago: Centro de Estudios de Justicia de las Américas, 2017.

BIBAS, Stephanos. The Story of Brady v. Maryland: From Adversarial Gamesmanship Toward The Search for Innocence?. **Penn Carey Law**, v. 77, jul. 2005.

BRIGHI, Raffaella; FERRAZZANO, Michele. Digital forensics: best practices and perspective. *In*: CAIANIELLO, Michele; CAMON, Alberto (Edts.). **Digital forensic evidence: towards common European standards in antrifraud administrative and criminal investigations**. Milão: CEDAM, 2021.

BURKE, Alafair S. Improving Prosecutorial Decision Making: Some Lessons of Cognitive Science. **William & Mary Law Review**, v. 47, 2006.

CATALANO, Elena Maria. Il metodo del controesame sul letto di procuste: le insidie e le sfide della prova scientifica. *In*: NEGRI, Daniele; ORLANDI, Renzo. **Le erosioni silenziose del contraddittorio**. Torino: G. Giappichelli Editore, 2017.

CATALANO, Elena Maria; GLOECKNER, Ricardo Jacobsen (Trad.); DALMAGRO JUNIOR, João Carlos (Trad.). Jurisprudência criativa no processo penal italiano e na *common law*: *abnormalità, inexistência e plain error rule*. **Revista de Estudos Criminais**, n. 96, 2025.

COUTINHO, Jacinto Nelson de Miranda. Uma breve síntese histórica-filosófica-jurídica-processual sobre os sistemas processuais penais. **Revista Brasileira de Ciências Criminais**, São Paulo, v. 185, n. 185, 2024.

DAMAŠKA, Mirjan R. **Evidence Law Adrift**. New Haven: Yale University Press, 1997.

DYBDAHL, Thomas L. **When innocence is not enough: Hidden evidence and the failed promise of the Brady Rule**. Nova Iorque: The New Press, 2023.

ELKS, Laurie. **Righting Miscarriages of Justice?** Ten Years of the Criminal Cases Review Commission. Londres: Justice, 2008.

ENGLANDER, Irv. **The architecture of computer hardware, systems software & networking:** an information technology approach. Hoboken: John Wiley & Sons, 2014.

FAZZALARI, Elio. **Istituzioni di diritto processuale.** Padova: Cedam, 1989.

FERRUA, Paulo. Il contraddittorio tra declino della legge e tirannia del diritto vivente. *In:* NEGRI, Daniele; ORLANDI, Renzo. **Le erosioni silenziose del contraddittorio.** Torino: G. Giappichelli Editore, 2017.

GIACOMOLLI, Nereu José. **O devido processo penal:** abordagem conforme a Constituição Federal e o pacto de São José da Costa Rica. São Paulo: Atlas, 2015.

GIOSTRA, Glauco. **Primeira lição sobre a justiça penal.** São Paulo: Tirant lo Blanch, 2021.

GLOECKNER, Ricardo Jacobsen. **Autoritarismo e processo penal:** uma genealogia das ideias autoritárias no processo penal brasileiro. Florianópolis: Tirant Lo Blanch, 2018.

GLOECKNER, Ricardo Jacobsen; DALMAGRO JUNIOR, João Carlos. Prova digital como prova científica: limites e perspectivas à extração de dados de dispositivos eletrônicos via Cellebrite. **ConJur**, 7 jul. 2025.

GONÇALVES, Aroldo Plínio. **Técnica Processual e Teoria do Processo.** Rio de Janeiro: Aide Editora, 1992.

GROSS, Samuel R.; POSSLEY, Maurice J.; ROLL, Kaitlin Jackson; STEPHENS, Klara Huber. Government misconduct and convicting the innocent: the role of prosecutors, police and other law enforcement. Report. National Registry of Exonerations, 1 set. 2020. Disponível em: https://www.law.umich.edu/special/exoneration/Documents/Government_Misconduct.pdf. Acesso em: 15 jul. 2025.

JAPIASSU, Hilton. **Interdisciplinaridade e patologia do saber.** Rio de Janeiro: Imago, 1976.

JOHNSTON, Ed. The rise of managerialism: the impact of swift and (un)sure justice on disclosure in criminal proceedings. *In:* JOHNSTON, Ed; SMITH, Tom (Eds.). **The law of disclosure:** a perennial problem in criminal justice. Londres: Routledge, 2021.

LEAL, David; FELIX, Yuri. O mercado de dados: o caso Cellebrite e a investigação digital no Brasil. **Boletim IBCCRIM**, v. 28, n. 328, p. 13-15, 2020.

LOPES JR., Aury; GLOECKNER, Ricardo Jacobsen. **Investigação preliminar no processo penal.** São Paulo: Saraiva, 2014.

MARQUES, Leonardo Augusto Marinho. O modelo constitucional de processo e o eixo estrutural da processualidade democrática. **Revista Brasileira de Direito Processual Penal**, v. 2, n. 1, 2016.

MASON, Stephen; SHELDON, Andrew; DRIES, Hein. Proof: the technical collection and examination of electronic evidence. *In*: MASON, Stephen; SENG, Daniel (ed.). **Electronic Evidence**. 4. ed. London: Institute of Advanced Legal Studies, 2017.

MAZZUOLI, Valério de Oliveira. O controle jurisdicional de convencionalidade das leis no Brasil. **Revista de Informação Legislativa**, Brasília, v. 46, n. 181, jan./mar. 2009.

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

NUNES, Dierle José Coelho. **Direito Constitucional ao Recurso: da teoria geral dos recursos, das reformas processuais e da comparticipação das decisões: comentários à Lei nº 11.187, de 19/10/2005, que alterou a sistemática do recurso de agravo**. Rio de Janeiro: Lumen Juris, 2006.

NUNES, Dierle; BAHIA, Alexandre; PEDRON, Flávio Quinaud. **Teoria Geral do Processo**. Salvador: JusPodivm, 2020.

PARODI, Lorenzo. **Perícia defensiva em provas digitais no Processo Penal: Origem, Custódia, Integralidade e Integridade**. São Paulo: Revista dos Tribunais.

PASTORE, Alexandre Mariano; FONSECA, Manoel Augusto Cardoso da. Cadeia de Custódia de Provas Digitais nos Processos do Direito Administrativo Sancionador com a adoção da tecnologia Blockchain. **Cadernos Técnicos da CGU**, Brasília, v. 3, p. 97-109, nov. 2022.

PICARDI, Nicola. **Manuale del processo civile**. Milão: Giuffrè, 2006.

PIMENTA, Marcus Vinícius. Busca e apreensão de elementos digitais. São Paulo: **Revista dos Tribunais**, 2025.

PRADO, Geraldo. **A cadeia de custódia da prova no processo penal**. São Paulo: Marcial Pons, 2021.

PRADO, Geraldo. Investigação criminal digital e processo penal. *In*: ABELLÁN, Marina Gascón; MATIDA, Janaina (Coords.). **Melhorar a prova**. São Paulo: Marcial Pons, 2024.

QUIRK, Hannah. Uncovering disclosure errors: appeals, innocence projects and the Criminal Cases Review Commission. *In*: JOHNSTON, Ed; SMITH, Tom (Eds.). **The law of disclosure: a perennial problem in criminal justice**. Londres: Routledge, 2021.

SAAD, Marta; ROSSI, Helena Costa; PARTATA, Pedro Henrique. A obtenção das provas digitais no processo penal demanda uma disciplina jurídica própria? Uma análise do conceito, das características e das peculiaridades das provas digitais. **Revista Brasileira de Direito Processual Penal**, v. 10, n. 3, 2024.

SCHAFER, Burkhard; MASON, Stephen. The characteristics of electronic evidence. *In*: MASON, Stephen; SENG, Daniel (ed.). **Electronic Evidence**. 4th ed. London: University of London Press, Institute of Advanced Legal Studies, 2017.

SMITH, Tom. Changing culture? Thinking differently about police and prosecution disclosure. *In*: JOHNSTON, Ed; SMITH, Tom (Edts.). **The law of disclosure: a perennial problem in criminal justice**. Londres: Routledge, 2021.

TUNER, Jenia I. Managing Digital Discovery in Criminal Cases. **Journal of Criminal Law and Criminology**, v. 109, n. 2, maio de 2019.

VIEIRA, Renato Stanzola. **Paridade de Armas no Processo Penal**. Brasília: Gazeta Jurídica, 2014.

WHAL, Sabine Gless-Thomas. The handling of digital evidence in Germany. *In*: CAIANIELLO, Michele; CAMON, Alberto (Edts.). **Digital forensic evidence: towards common European standards in antifraud administrative and criminal investigations**. Milão: CEDAM, 2021.

YAROSHEVSKY, Ellen. Prosecutorial Disclosure Obligations. **Hastings Law Journal**, v. 62, n. 5, maio de 2011.

YAROSHEFSKY, Ellen. Why Do Brady Violations Happen? Cognitive Bias and Beyond. **Hofstra Law Faculty Scholarship**, maio de 2013.

ZAFFARONI, Eugenio Raúl. **O inimigo no direito penal**. Rio de Janeiro: Revan, 2014.