A doutrina da plain view e a apreensão de vestígios cibernéticos

21/06/2025

A Quarta Emenda à Constituição dos Estados Unidos consagra o direito à proteção contra buscas e apreensões arbitrárias, estabelecendo parâmetros para a atuação das autoridades estatais. Ela disciplina:

> *"O direito do povo de estar seguro em suas pessoas, casas, papéis e efeitos, contra buscas e apreensões não razoáveis, não será violado, e nenhum mandado será emitido senão por justa causa, apoiada por juramento ou afirmação, e particularmente descrevendo o lugar a ser revistado e as pessoas ou coisas a serem apreendidas."*

Este dispositivo constitucional constitui uma das mais importantes garantias individuais no ordenamento jurídico dos EUA, representando um freio ao arbítrio estatal e um sustentáculo da proteção da privacidade e segurança dos indivíduos. Tal garantia nasce como resposta às práticas abusivas da Coroa britânica, notadamente os chamados *general warrants* e *writs of assistance*, utilizados para realizar buscas e apreensões amplas, sem delimitação específica de pessoas, locais ou objetos. Esses instrumentos permitiam verdadeiras averiguações investigativas arbitrárias, incompatíveis com a proteção à esfera privada do indivíduo [1].

Por esse motivo, a Quarta Emenda estabeleceu a exigência de que os mandados judiciais sejam expedidos por uma autoridade independente e imparcial e que estejam baseados em "*probable cause*" (causa provável), contendo "*a particular description of the place to be searched, and the persons or things to be seized*". Trata-se da chamada cláusula da particularidade (*particularity clause*), que, juntamente com a exigência de supervisão judicial imparcial, constitui núcleo irrestrito da proteção contra abusos estatais.

Entretanto, ao longo do tempo, a Suprema Corte desenvolveu exceções à exigência de mandado, entre as quais destaca-se a doutrina da *plain view* ("visão à plena vista"). O presente artigo analisará, de maneira sucinta, a evolução jurisprudencial da doutrina da *plain view* e, num segundo momento, abordará os seus desdobramentos no contexto das provas digitais.

O tema guarda importância ímpar diante da imersão social a uma lógica digital que permeia todas as nossas atividades, sendo correto afirmar que na atual quadra, "quase nenhuma atividade analógica pode prescindir de sua extensão digital, seja offline ou online" [2].

Contextualizando com dados atuais, De Vita esclarece que em 2025 a população atingiu mais de 8,2 bilhões de pessoas, das quais 5,56 bilhões têm acesso à internet (67,9%). Para além do crescimento dos usuários, houve igualmente um crescimento inimaginável dos dados. "De fato, estima-se que, atualmente, são produzidos diariamente 328,77 milhões de terabytes, o que levou, em 2025, ao total de mais de 200 zettabytes (ou seja, bilhões de terabytes)" [3].

Vivemos num ecossistema digital onde a interconexão dos mais diversos dispositivos e dados implica a necessidade de uma nova regulação de gestão e controle da informação e, acima de tudo, de proteção de direitos. "No mundo, existem mais dispositivos com conexão móvel do que pessoas: 8,78 bilhões, dos quais 8,31 bilhões têm conexão banda larga. E isso sem contar os dispositivos IoT (Internet das Coisas) conectados à rede" [4].

Para tanto, partiremos da premissa de que a Quarta Emenda possui dupla função: impedir buscas e apreensões sem *justa causa* e garantir que o Poder Judiciário controle *previamente* os atos invasivos por meio do mandado judicial. Os requisitos centrais para sua aplicação são: (i) a existência de *probable cause*, (ii) a necessidade de autorização judicial, e (iii) a delimitação específica do objeto da busca.

A doutrina da *plain view*, por sua vez, permite que objetos visivelmente incriminadores, descobertos durante uma busca legal, sejam apreendidos sem necessidade de mandado específico. Seu fundamento repousa na razoabilidade e no fato de que o objeto já se encontra *à vista plena* do agente legalmente autorizado a adentrar ao local.

Originada no caso *Coolidge v. New Hampshire* [5] (1971), a doutrina estabeleceu inicialmente quatro requisitos para sua aplicação: (1) uma admissão previamente justificada; (2) o objeto estar à plena vista; (3) ser imediatamente aparente sua

natureza incriminatória; e (4) a descoberta ser não intencional (*inadvertent*).

Admissão

O requisito da *admissão previamente justificada* é elemento fundante da doutrina da *plain view*, pois ela não legitima, por si só, o ingresso em área protegida pela Quarta Emenda. Ou seja, a doutrina da *plain view* não autoriza o agente estatal a fazer a apreensão de objetos que estejam à vista. Antes, ela é uma permissão de apreender algo *desde que* o seu ingresso ao local tenha sido previamente justificado.

Em *Washington v. Chrisman* [6] (1982), um estudante detido por posse de álcool foi escoltado até seu dormitório. O policial, da soleira da porta, viu um cachimbo e sementes de maconha. A Corte entendeu que, como o agente já possuía direito de ingressar no local para acompanhar o detido e garantir o êxito da detenção, a apreensão foi válida sob a *plain view*. Em contrapartida, em *State v. Lewis* [7] (1989), a Corte decidiu que a visualização de entorpecentes feita de um corredor público não autorizava a entrada e apreensão, pois não havia admissão prévia justificada. Esse caso é exemplo de *open view* — observações feitas a partir de local público, que podem fundamentar pedido de mandado, mas não autorizam ingresso ou apreensão.

Spacca

Daniel Avelar
juiz de Direito

O requisito de que o *objeto esteja à plena vista* implica que ele seja imediatamente visível, sem necessidade de manipulação ou busca adicional. Este elemento assegura que a apreensão não envolva invasão adicional de privacidade. Em *Coolidge*, a Suprema Corte destacou que o objeto deve estar claramente visível durante a intrusão justificada, como armas ou drogas expostas em um local acessível. A doutrina não autoriza manipulações que impliquem nova busca, como mover objetos para revelar números de série.

No caso *Arizona v. Hicks* [8] (1987), a Suprema Corte estabeleceu, de forma categórica, que o padrão da "imediatidade aparente da sua natureza incriminatória" equivale ao critério de *probable cause*, eliminando interpretações anteriores que sugeriam a necessidade de algum elemento adicional de certeza. Em *Hicks*, policiais adentraram legitimamente em um apartamento em resposta a um tiroteio, onde encontraram e apreenderam diversas armas. Um dos agentes, observando equipamentos de som de alto valor que pareciam incompatíveis com o ambiente precário, suspeitou tratar-se de itens furtados.

Na sequência, o policial movimentou os equipamentos para ler os números de série, sendo posteriormente informado pela central que vários daqueles itens haviam sido efetivamente subtraídos. A Corte decidiu unanimemente que o simples registro dos números de série não configurava busca ou apreensão sob a Quarta Emenda. Contudo, a maioria entendeu que mover o aparelho para examinar seu número de série constituía uma busca, requerendo justificação sob alguma exceção ao mandado. Rejeitou-se a aplicação da doutrina da *plain view*, pois o Estado não demonstrou que a natureza incriminatória do aparelho fosse imediatamente aparente, já que o policial admitidamente não possuía causa provável antes de sua ação.

O requisito da inadvertência (*inadvertent*), inicialmente estabelecido em *Coolidge*, exigia que a descoberta do objeto fosse acidental, sem antecipação pelo agente. Este elemento foi eliminado em *Horton v. California* (1990)[9].

Em *Coolidge*, a inadvertência era vista como uma salvaguarda contra apreensões planejadas que contornassem a exigência de mandado. Mas, em *Horton*, a Suprema Corte eliminou a inadvertência como requisito, considerando-a supérflua. No caso, a apreensão de armas e itens furtados, não listados no mandado, foi validada, pois estavam à vista durante a busca autorizada. A Corte argumentou que a especificidade do mandado e a legitimidade da admissão já protegem contra abusos, tornando a inadvertência desnecessária.

Assim, a evolução jurisprudencial da doutrina da *plain view* demonstra significativo esclarecimento de incertezas iniciais, particularmente através das decisões em *Hicks* (definindo "imediata aparência" como causa provável) e *Horton* (eliminando o requisito da inadvertência).

Porém, a doutrina da *plain view*, desenvolvida para o contexto físico, tem provocado amplas controvérsias ao ser aplicada a buscas de vestígios cibernéticos. Conforme a praxe, um mandado de busca deve detalhar previamente o objeto da apreensão (como documentos, armas ou drogas) e o local onde será conduzida. Investigações exploratórias que ultrapassem esse escopo são flagrantemente ilícitas e podem configurar uma *fishing expedition*. Ademais, buscas de objetos físicos são limitadas no tempo, pois seria inadmissível estender indefinidamente uma busca domiciliar para além de um prazo razoável.

Nas buscas por evidências cibernéticas, porém, é praticamente inviável que o magistrado determine *ex ante* quais dispositivos, como computadores, celulares, redes, e-mails ou arquivos, devem ser inspecionados, devido ao vasto volume de dados armazenáveis em equipamentos eletrônicos. Após a apreensão do dispositivo ou a realização do espelhamento de informações, os peritos dispõem de um prazo praticamente ilimitado para conduzir buscas exploratórias, utilizando as técnicas mais avançadas disponíveis. Nesse sentido, Kerr destaca que a "fisicalidade da evidência" deixa de limitar o alcance da busca, uma vez que dados digitais podem estar em qualquer lugar. Ele conclui, portanto, que as justificativas para a exceção da *plain view* no âmbito físico não encontram correspondência no ambiente digital [10].

Outrossim, no contexto digital, a depender do local onde as buscas são realizadas (computador, celular, servidor de e-mail, nuvens etc.), a ação invasiva pode atingir informações de terceiros e dados protegidos por sigilo (bancário, fiscal, médico, profissional etc.) que dependeriam de fundamentação específica e detalhada para ser alcançado. De outro giro, os arquivos localizados num computador são praticamente idênticos externamente e, num primeiro momento, são apenas identificáveis pelo nome atribuído a eles. Contudo, "[e]xtensões como 'jpg' ou '.mov' podem ser manipuladas, criptografadas ou ocultadas de analistas, de modo que pouco se sabe sobre o conteúdo do arquivo até que ele seja aberto" [11]. E, embora as buscas por palavras-chave sejam úteis para identificar documentos incriminadores, elas se mostram ineficazes na localização de evidências fotográficas ou em vídeo armazenadas em discos rígidos [12].

Portanto, quando um mandado judicial autoriza a investigação de informações particulares em um dispositivo eletrônico, isso efetivamente expõe todo o conteúdo digital armazenado. Uma vez que os agentes precisam examinar individualmente cada arquivo para determinar sua natureza, sujeitam-se à observação todas as informações contidas no dispositivo durante o iter investigativo. Dessa forma, qualquer material probatório incriminatório descoberto, mesmo que não tenha correlação com o objeto original da ordem judicial, poderia ser apreendido pelas autoridades.

A preocupação com o acesso massivo a dados de terceiros por ocasião da apreensão de elementos probatórios digitais é tema que não passa despercebido aos grandes pensadores da matéria. Em recente palestra proferida no Conselho Nacional de Justiça, Geraldo Prado deixou claro o alerta:

> *"Quando uma operação policial é realizada e leva à apreensão de dispositivos eletrônicos ou ao acesso a canais ou plataformas digitais (nas nuvens), os dados coletados não dizem respeito somente às pessoas suspeitas, investigadas ou mesmo às vítimas. Na imensa maioria dos casos, são colhidos dados de um sem-número de pessoas sem qualquer relação com as investigações.*
>
> *Um regime constitucional que preze a autodeterminação informativa, como ocorre no Brasil, deve estar atento à possibilidade de manipulação desses dados e à necessidade de sua proteção contra uso indevido." [13]*

A análise da doutrina da *plain view* revela sua evolução jurisprudencial e os desafios de sua aplicação no contexto digital, onde a natureza intangível e o volume massivo de dados cibernéticos dificultam a delimitação de buscas e amplificam os riscos de invasão à privacidade. Na segunda parte deste artigo, serão examinadas as decisões proferidas pelos Quarto, Décimo, Sétimo e Nono Circuitos, que abordam a adaptação da doutrina às buscas de vestígios cibernéticos, destacando as tensões entre a proteção constitucional e as necessidades investigativas. Além disso, será discutida a "Teoria do Uso" proposta por Orin Kerr, uma moldura teórica inovadora para distinguir entre o acesso legítimo e a exploração indevida de informações digitais durante buscas autorizadas, propondo parâmetros mais ajustados à proteção da privacidade informacional e à efetividade das garantias constitucionais no cenário digital contemporâneo.

---

[1] Mannheimer, Michael J. Z.. **The Fourth Amendment: Original Understandings and Modern Policing**. University of Michigan Press. Edição do Kindle, 2023, pp. 22-23

[2] DE VITA, Roberto. **La Prova Digitale nel Processo Penale**. Devitalaw (Autopubblicato), 2025.

[3] Id.

[4] Id.

[5] 403 U.S. 443, (1971).

[6] 455 U.S. 1, (1982).

[7] 561 A.2d 1153 (N.J. 1989).

[8] 480 U.S. 321 (1987).

[9] 496 U.S. 128 (1990).

[10] The physicality of the evidence no longer limits the scope of the search because digital evidence can be located anywhere. The justifications for why the plain view exception exists for physical evidence don't fit the digital world. (KERR, Orin. **The Digital Fourth Amendment: Privacy and Policing in Our Online World** (p. 104). Oxford University Press. Edição do Kindle, p. 104).

[11] WEIR, Bryan K. **It's (Not So) Plain to See: The Circuit Split on the Plain View Doctrine in Digital Searches**, 21 Geo. Mason University Civil Rights Law Journal, 21(1), 83-122, 2010: "File extensions such as **".jpg"** or ".mov" can be manipulated, encrypted, or hidden from analysts so that little is known of a file's contents until the file is opened".

[12] Ibid., p. 109.

[13] PRADO, Geraldo. Palestra "**Fundamentos Teóricos e Normativos das Provas Digitais**", proferida em Brasília, no dia 28 de maio de 2025, no âmbito do "Seminário sobre Provas Digitais", promovido pelo Conselho Nacional de Justiça (CNJ).

Fonte: https://conjur.jumps.com.br/2025-jun-21/a-doutrina-da-plain-view-e-a-apreensao-de-vestigios-ciberneticos/