O ACESSO PELA POLÍCIA A CONVERSAS GRAVADAS NO WHATSAPP E AS GERAÇÕES PROBATÓRIAS DECORRENTES DAS LIMITAÇÕES À ATUAÇÃO ESTATAL

João Biffe Junior

Promotor de Justiça no Estado de Goiás.
Membro da Associação dos Promotores do Júri - Confraria do Júri
Ex-Promotor de Justiça no Estado de Mato Grosso.
Ex-Delegado de Polícia no Estado de Mato Grosso.
Ex-Advogado da Fundação Estadual "Dr. Manoel Pedro Pimentel" no Estado de São Paulo.
Pós-Graduado em Direito Civil e Processual Civil pelo Centro Universitário de Marília – UNIVEM.

Joaquim Leitão Junior

Delegado de Polícia no Estado de Mato Grosso.
Ex-assessor do Tribunal de Justiça de Mato Grosso.
Pós-graduado em Ciências Penais pela rede de ensino Luiz Flávio Gomes (LFG) em parceria com Universidade de Santa Catarina (UNISUL).
Pós-graduado em Gestão Municipal pela Universidade do Estado de Mato Grosso – UNEMAT e pela Universidade Aberta do Brasil.
Curso de Extensão pela Universidade de São Paulo (USP) de Integração de Competências no Desempenho da Atividade Judiciária com Usuários e Dependentes de Drogas.

Realizada a prisão em flagrante de uma pessoa, questiona-se a licitude do comportamento dos policiais ao realizar busca exploratória em eventual aparelho de telefonia celular apreendido, consultando imagens, registros de ligações efetuadas e recebidas, bem como o acesso a aplicativos de comunicação, tais como WhatsApp, Telegram, Kik, Skype, SnapChat, Facebook Messenger, GoSMS Pro, Im+, WeChat. BBM, Viber, dentre outros.

A questão é altamente complexa, vez que as mensagens armazenadas nestes aplicativos podem ser apagadas de maneira remota. Dessa forma, a necessidade de prévia ordem judicial para legitimar o acesso a referidos aplicativos, poderá conduzir a perda dos elementos informativos que os órgãos de persecução penal necessitavam para repressão de práticas delitivas.

Imaginemos o caso de um traficante que tem seu celular apreendido por policiais no momento de sua prisão em flagrante. As informações armazenadas em seu telefone celular poderão comprovar a prática da traficância, além de identificar fornecedores, compradores e até mesmo a localização do restante da droga.

Certamente, transcorridos poucos minutos da prisão essas mensagens serão apagadas de maneira remota, bem como cessarão todos os contatos com o interlocutor preso. Considerando que essas mensagens são criptografadas e não são armazenadas pelos servidores, não haverá meios tecnológicos para recuperá-las.

Saliente-se, novamente, que se trata de questão complexa, envolvendo a discussão quanto aos limites da atuação estatal em virtude da proteção da intimidade e do sigilo das comunicações.

O debate quanto aos limites impostos pela ordem constitucional à obtenção das provas em respeito a expectativa de privacidade, é pautado pela análise do uso da tecnologia e seu poder de penetração na intimidade do indivíduo.

Esses questionamentos estão ligados ao denominado direito probatório de terceira geração. Por essas razões, a terceira geração do direito probatório foi ventilada pelo Ministro Rogério Schietti no julgamento do HC nº 51.531, ao tratar do acesso direto por policiais aos aplicativos instalados em aparelhos de telefonia celular apreendidos.

No referido voto, o Ministro promoveu a distinção entre o caso subjacente ao *Habeas Corpus* e o precedente do STF (HC 91.867/PA de 20/09/2012) que reputara lícita a análise, logo após a prisão em flagrante, dos últimos registros telefônicos armazenados nos aparelhos de telefonia celular apreendidos, sem a necessidade de autorização judicial.

No HC 51.531 de 09/05/2016, a 6ª Turma do STJ entendeu ser **ilícita a "a devassa de dados, bem como das conversas de *whatsapp*, obtidas diretamente pela polícia em celular apreendido no flagrante, sem prévia autorização judicial"**.

O Min. Rogério Schietti apontou o *distinguishing*[1] *em relação ao HC nº 91.867*, afastando o precedente do STF.

A decisão do STF (HC 91.867/PA) versava sobre acesso ao registro de chamadas telefônicas efetuadas e recebidas. De tal forma, no precedente da Suprema Corte as autoridades policiais não tiveram acesso às conversas mantidas entre os investigados.

Eis o trecho do HC 91.867 que sintetiza o objeto do *writ*:

> "Suposta ilegalidade decorrente do fato de os policiais, após a prisão em flagrante do corréu, terem realizado a análise dos últimos registros telefônicos dos dois aparelhos celulares apreendidos. Não ocorrência. 2.2 **Não se confundem comunicação telefônica e registros telefônicos, que recebem, inclusive, proteção jurídica distinta**. Não se pode interpretar a cláusula do artigo 5º, XII, da CF, no sentido de proteção aos dados enquanto registro, depósito registral. **A proteção constitucional é da comunicação de dados e não dos dados**. 2.3 Art. 6º do CPP: dever da autoridade policial de proceder à coleta do material comprobatório da prática da infração penal. **Ao proceder à pesquisa na agenda eletrônica dos aparelhos devidamente apreendidos, meio material indireto de prova, a autoridade policial, cumprindo o seu mister, buscou, unicamente, colher elementos de informação hábeis a esclarecer a autoria e a materialidade do delito**"

Conforme esclarecem Vinícius Marçal e Cleber Masson "fixadas estas distinções, considerou-se que os atuais *smartphones* são dotados de aplicativos de comunicação em tempo real, razão pela qual a invasão direta ao aparelho de telefonia celular de pessoa presa em flagrante possibilitaria à autoridade policial o acesso a inúmeros aplicativos de comunicação *on-line*, todos com as mesmas funcionalidades de envio e recebimento de mensagens, fotos, vídeos e documentos em tempo real" (MARÇAL, 2016, p. 240).

O Min. Nefi Cordeiro salientou que nas "conversas mantidas pelo programa whatsapp, que é forma de comunicação escrita, imediata, entre interlocutores, tem-se efetiva interceptação inautorizada de comunicações. É situação similar às conversas mantidas por e-mail, onde para o acesso tem-se igualmente exigido a prévia ordem judicial".

[1] O *distinguishing* é a distinção do caso fático concreto, em vista do precedente fixado para a não incidência deste último, com a permissão de fixação de entendimento diverso do precedente paradigma.

Por fim, o Min. Rogério Schietti salientou que a “doutrina nomeia o chamado **direito probatório de terceira geração**, que trata de ‘provas invasivas, altamente tecnológicas, que permitem alcançar conhecimentos e resultados inatingíveis pelos sentidos e pelas técnicas tradicionais’".

Para corroborar a argumentação, o Exmo. Min. Schietti citou trecho da obra de autoria de Danilo Knijnik:

> “A menção a elementos tangíveis tendeu, por longa data, a condicionar a teoria e prática jurídicas. Contudo, a penetração do mundo virtual como nova realidade, demonstra claramente que tais elementos vinculados à propriedade longe está de abarcar todo o âmbito de incidência de buscas e apreensões, que, de ordinário, exigiriam mandado judicial, impondo reinterpretar o que são "coisas" ou "qualquer elemento de convicção", para abranger todos os elementos que hoje contém dados informacionais.
> Nesse sentido, tome-se o exemplo de um smartphone: ali, estão e-mails, mensagens, informações sobre usos e costumes do usuário, enfim, um conjunto extenso de informações que extrapolam em muito o conceito de coisa ou de telefone.
> Supondo-se que a polícia encontre incidentalmente a uma busca um smartphone, poderá apreendê-lo e acessá-lo sem ordem judicial para tanto? Suponha-se, de outra parte, que se pretenda utilizar um sistema de captação de calor de uma residência, para, assim, levantar indícios suficientes à obtenção de um mandado de busca e apreensão: se estará a restringir algum direito fundamento do interessado, a demandar a obtenção de um mandado expedido por magistrado imparcial de equidistante, sob pena de inutilizabilidade? O e-mail, incidentalmente alcançado por via da apreensão de um notebook, é uma "carta aberta ou não"? Enfim, o conceito de coisa, enquanto *res* tangível e sujeita a uma relação de pertencimento, persiste como referencial constitucionalmente ainda aplicável à tutela dos direitos fundamentais ou, caso concreto, deveria ser substituído por outro paradigma? Esse é um dos questionamentos básicos da aqui denominada de prova de terceira geração: "chega-se ao problema com o qual as Cortes interminavelmente se deparam, quando consideram os novos avanços tecnológicos: como aplicar a regra baseada em tecnologias passadas às presentes e aos futuros avanços tecnológicos"." Trata-se, pois, de um questionamento bem mais amplo, que convém, todavia, melhor examinar. [...] (KNIJNIK, Danilo. Temas de direito penal, criminologia e processo penal. *A trilogia Olmstead-Katz-Kyllo: o art. 5º da Constituição Federal do Século XXI.* Porto Alegre: Livraria do Advogado, 2014, p. 179)

Concluindo assim que, diante do direito probatório de terceira geração, “o precedente do HC n. 91.867/PA não é mais adequado para analisar a vulnerabilidade da intimidade dos cidadãos na hipótese da apreensão de um aparelho de telefonia celular em uma prisão em flagrante”.

Saliente-se ainda, como bem destacado, por Marçal e Masson:

> “Conquanto tenha sido essa a tônica da decisão, a Corte não descartou, peremptoriamente, que a depender do caso concreto, ficando evidenciado que a demora na obtenção de um mandado judicial pudesse trazer prejuízos concretos à investigação ou especialmente à vítima do delito, mostre-se possível admitir a validade da prova colhida através do acesso imediato aos dados do aparelho celular” (MARÇAL, 2016, p. 240).

No entanto, da leitura do acórdão exsurge uma pergunta inevitável: se existe um direito probatório de terceira geração, quais seriam os direitos probatórios de primeira e segunda geração?

Após análise dos precedentes Olmstead (1928), Katz (1967), Kyllo (2001) e Riley (2014), **classificamos as provas em gerações, a partir da evolução da interpretação constitucional quanto as limitações da atuação estatal em razão da proteção a intimidade.**

A divisão das gerações de direito probatório, encontra seu nascedouro nos precedentes Olmstead (1928), Katz (1967) e Kyllo (2001), nos quais a Suprema Corte Norte-Americana decidiu em quais casos incidiria a proteção conferida pela 4ª Emenda à Constituição dos Estados Unidos da América, tornando-se assim necessária a expedição prévia de ordem judicial de busca e apreensão para a obtenção lícita das provas.

Preconiza a 4ª Emenda que o "direito do povo à inviolabilidade de suas pessoas, casas, papéis e haveres contra busca e apreensão arbitrárias não poderá ser infringido; e nenhum mandado será expedido a não ser mediante indícios de culpabilidade confirmados por juramento ou declaração, e particularmente com a descrição do local da busca e a indicação das pessoas ou coisas a serem apreendidas".

A trilogia dos precedentes *Olmstead (1928), Katz (1967) e Kyllo (2001),* representa a mutação constitucional quanto aos objetos que poderiam ser objetos de apreensão pelos agentes do Estado, sem ordem judicial previamente expedida.

Passemos a análise de cada geração do direito probatório à luz dos referidos precedentes.

Direito probatório de 1ª Geração:*teoria proprietária ou trespasstheory.*

O precedente *Olmstead*é apontado como o precursor da teoria que ainda hoje condiciona, em grande parte, a teoria e prática do direito brasileiro. No caso levado a

julgamento em 1928 perante a Suprema Corte, a polícia instalara um equipamento para interceptar as conversas telefônicas, fazendo-o diretamente na fiação da empresa telefônica, em via pública (KNIJNIK, p. 85)[2].

Ocorre que a polícia descobrira a existência de uma conspiração para violar a Lei de Proibição, visando importar, possuir e vender bebidas alcoólicas ilegalmente. Olmstead era o líder da conspiração e gerente geral do negócio utilizado para viabilizar a prática ilícita.

Os investigados foram condenados no Tribunal Distrital por conspiração para violar a proibição estabelecida pela Lei Nacional que proibia a posse, transporte e importação de bebidas intoxicantes. Além de Olmstead, setenta e dois outros investigados foram indiciados[3].

No entanto, a informação que levou à descoberta da conspiração, sua natureza e extensão, foi obtida através da interceptação de mensagens nos telefones dos conspiradores por quatro oficiais de proibição federais.

A interceptação foi realizada por pequenos fios de telefone instalados nas residências dos investigados, sem que houvesse qualquer violação às propriedades, uma vez que foram realizadas no porão de um prédio e nas ruas perto das casas[4].

---

2 KNIJNIK, Danilo. A trilogia Olmstead-Katz-Kyllo: o art. 5º daConstituição Federal do século XXI. Revista da Escola da Magistratura do TRF da 4ª Região,ano 2, número 4. Porto Alegre/RS, 2016.

[3]The petitioners were convicted in the District Court for the Western District of Washington of a conspiracy to violate the National Prohibition Act by unlawfully possessing, transporting and importing intoxicating liquors and maintaining nuisances, and by selling intoxicating liquors. Seventy-two others in addition to the petitioners were indicted. Some were not apprehended, some were acquitted, and others pleaded guilty (precedente*Olmstead v. United States*. Disponívelem: https://www.law.cornell.edu/supremecourt/text/277/438).

[4]The information which led to the discovery of the conspiracy and its nature and extent was largely obtained by intercepting messages on the telephones of the conspirators by four federal prohibition officers. Small **[p457]** wires were inserted along the ordinary telephone wires from the residences of four of the petitioners and those leading from the chief office. The insertions were made without trespass upon any property of the defendants. They were made in the basement of the large office building. The taps from house lines were made in the streets near the houses (precedente*Olmstead v. United States*. Disponívelem: https://www.law.cornell.edu/supremecourt/text/277/438).

Os investigadores não invadiram a casa de Olmstead, nem tampouco apreenderam objetos. Ademais, o sinal acústico (voz) que era transmitido pelos fios da companhia telefônica não poderia ser tido como uma coisa.

A interpretação constitucional foi no sentido de que a Emenda determina que seja descrito no mandado o local a ser pesquisado e a pessoa ou coisas a serem apreendidas[5].

Como no caso em vertente não houve busca ou apreensão no interior de casas ou escritórios, a Suprema Corte decidiu que não houve violação a quarta Emenda[6].

No histórico julgamento, a Suprema Corte "concluiu que a ação policial não havia 'penetrado em qualquer propriedade do acusado', e que a correta interpretação da 4ª Emenda não poderia dar-se de forma a 'alargá-la para além do conceito prático de pessoas, casas, papéis e pertences" ou "para aplicar buscas e apreensões de forma a proibir escutar ou observar'" (KNIJNIK, p. 85).

Nesta primeira etapa de evolução da interpretação constitucional, entendia-se que **a proteção conferida pela 4ª emenda destinava-se apenas a coisas, objetos e lugares**.

> "Esse precedente consagrou o que a doutrina convencionou chamar de ***'trespasstheory'* ou 'teoria proprietária'**: a proteção constitucional estender-se-ia apenas para áreas tangíveis e demarcáveis, exigindo a entrada, o ingresso e a violação de um espaço privado ou particular, o que, na espécie, efetivamente não havia ocorrido, dado que nenhuma propriedade de Olmstead fora devassada pela autoridade" (KNIJNIK, p. 85).

[5]The Amendment itself shows that the search is to be of material things -- the person, the house, his papers, or his effects. The description of the warrant necessary to make the proceeding lawful is that it must specify the place to be searched and the person or *things* to be seized (precedente*Olmstead v. United States*. Disponívelem: https://www.law.cornell.edu/supremecourt/text/277/438).

[6]The United States takes no such care of telegraph or telephone messages as of mailed sealed letters. The Amendment does not forbid what was done here. There was no searching. There was no seizure. The evidence was secured by the use of the sense of hearing, and that only. There was no entry of the houses or offices of the defendants (precedente Katz v. United States. Disponível em: https://www.law.cornell.edu/supremecourt/text/389/347).

.

Em suma, a proteção constitucional aplicava-se apenas a áreas tangíveis e demarcáveis, exigindo a entrada, o ingresso e a violação de um espaço privado ou particular, ou seja, a proteção constitucional abrangia apenas coisas, objetos e lugares (Precedente *Olmstead v. United States de 1928*).

Direito probatório de 2ª Geração:*teoria da proteção constitucional integral (estendeu a proteção de coisas, lugares e pertences para pessoas e suas expectativas de privacidade)*

Após quase quarenta anos do precedente *Olmstead*, a Suprema Corte alterou sua posição e passou a entender que a 4ª Emenda regulava não apenas a busca de itens tangíveis, mas estendia-se também a gravação de declarações orais (caso *Katz v. United States, em **1967**)*.

No caso *Katz v. United State*so investigado foi condenado por Tribunal da Califórnia por transmitir informações de apostas por telefone, de Los Angeles para Miami e Boston, conduta esta proibida por lei federal.

A prova da prática delitiva foi obtida pelos agentes do FBI através da instalação de um dispositivo de gravação externamente a uma cabine de telefone público, utilizada pelo investigado.Como a cabine telefônica era pública, não haveria invasão ou ingresso em propriedade privada e, tampouco, apreensão de coisas, portanto, aplicável o precedente *Olmstead v. United States*, o que tornava a prova lícita.

A Corte de Apelação rejeitou a alegação de que as gravações foram obtidas em violação da Quarta Emenda, pois não houve entrada física em área ocupada pelo requerente, aplicando a teoria proprietária, sedimentada no precedente Olmstead.

No entanto, a Suprema Corte firmou o entendimento que o meio pelo qual o Governo obteve a prova violou a privacidade do investigado, no momento em que ele utilizou a cabine de telefone, pois ainda que o investigado pudesse ser visto pelos agentes (cabine de vidro), ao fechar a porta atrás de si e pagar o valor que lhe permitia realizar a chamada, tinha o direito de supor que as palavras que pronunciaria ao telefone

não seriam transmitidas para o mundo[7], tratando-se assim de uma busca e apreensão, na acepção da Quarta Emenda.

Ou seja, a Quarta Emenda regula não só a apreensão de itens tangíveis, mas estende-se também ao registo de declarações orais.

Considerando que a Quarta Emenda protege as pessoas, ao invés de lugares, o seu alcance não pode girar sobre a presença ou ausência de uma intrusão física em um determinado lugar, assim o objetivo da norma constitucional não pode ser frustrado pela presença ou ausência de intrusão física em qualquer compartimento fechado.

Salientou-se ainda que, embora a vigilância pudesse ter sido constitucionalmente previamente autorizada, não havia a possibilidade de se excepcionar a regra da necessidade de autorização prévia por um juiz, uma vez que o mandado judicial era uma pré-condição constitucional para a realização da vigilância eletrônica[8].

Em síntese, a Suprema Corte entendeu que a prova era nula, pois, neste caso, seria necessária ordem judicial para a realização da diligência policial, sedimentando o entendimento de que a 4ª Emenda estende sua proteção a gravação de declarações orais[9].

---

[7] One who occupies it, shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world. To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication (precedente Katz v. United States. Disponívelem: https://www.law.cornell.edu/supremecourt/text/389/347).

[8]Although the surveillance in this case may have been so narrowly circumscribed that it could constitutionally have been authorized in advance, it was not in fact conducted pursuant to the warrant procedure which is a constitutional precondition of such electronic surveillance (precedente Katz v. United States. Disponívelem: https://www.law.cornell.edu/supremecourt/text/389/347).

[9] 1. The Government's eavesdropping activities violated the privacy upon which petitioner justifiably relied while using the telephone booth, and thus constituted a "search and seizure" within the meaning of the Fourth Amendment (precedente Katz v. United States. Disponívelem: https://www.law.cornell.edu/supremecourt/text/389/347).
(a) The Fourth Amendment governs not only the seizure of tangible items, but extends as well to the recording of oral statements. *Silverman v. United States* (precedente Katz v. United States. Disponívelem: https://www.law.cornell.edu/supremecourt/text/389/347).
(b) Because the Fourth Amendment protects people, rather than places, its reach cannot turn on the presence or absence of a physical intrusion into any given enclosure. The "trespass" doctrine of *Olmstead v. United States,* 277 U.S. 438, and *Goldman v. United States,* 316 U.S.

A teoria proprietária, estabelecida no precedente *Olmstead v. United States*,**foi superada, ampliando-se o âmbito de proteção constitucional de coisas, lugares e pertences para pessoas e suas expectativas de privacidade**, conforme consta do julgado: “The "trespass" doctrineof *Olmstead v. United States*, 277 U.S. 438, and *Goldman v. United States*, 316 U.S. 129, is no longercontrolling”.

A evolução introduzida pelo precedente *Katz v. United States*ocasionou a migração da teoria proprietária para a teoria da proteção constitucional integral, com a introdução de duas premissaspara a aplicação da proteção conferida pela 4ª Emenda:

a) A existência de uma expectativa real e efetiva de privacidade;

b) E se a sociedade reconhece esta expectativa como razoável (se está disposta a confirmar a pretensão do sujeito).

Direito probatório de 3ª Geração:*provas tecnológicas invasivas.*

A Suprema Corte dos Estados Unidos, em 2001, fixou o entendimento de que o avanço da tecnologia sobre a materialidade das coisas “não pode limitar o escopo e a abrangência da proteção constitucional outorgada às pessoas”. Assim, a interpretação da 4ª Emenda, ao aludir a coisas, pertences, papéis e lugares, deveria sofrer uma atualização interpretativa, para além da doutrina Katz (KNIJNIK, p. 89).

O caso subjacente ao precedente remonta a 1991, período em que o agente de polícia, Willian Elliot, desconfiava que Danny Kyllo, morador de um tríplex situado no Rhododendron Drive, em Florença, Oregon, cultivava maconha no interior de sua

---

129, is no longer controlling. (precedente Katz v. United States. Disponível em: https://www.law.cornell.edu/supremecourt/text/389/347).

2. Although the surveillance in this case may have been so narrowly circumscribed that it could constitutionally have been authorized in advance, it was not in fact conducted pursuant to the warrant procedure which is a constitutional precondition of such electronic surveillance. (precedente Katz v. United States. Disponível em: https://www.law.cornell.edu/supremecourt/text/389/347).

residência, no entanto, não possuía elementos para pleitear a expedição de um mandado de busca.

Sabendo que para o cultivo da maconha são utilizadas lâmpadas de alta intensidade, os agentes Elliot e Dan Haas utilizaram o equipamento "AgemaThermovision 210", promovendo uma captação térmica da residência (thermalimaging).

No dia 16 de janeiro de 1992, os agentes pararam um veículo em via pública e em poucos minutos constataram que o telhado em cima da garagem e uma parede lateral da casa de Kyllo eram mais quentes em comparação com o resto da casa e, substancialmente, mais quentes do que os tríplex vizinhos.

Com base nisso, a polícia conseguiu o elemento que faltava para o mandado de busca.

Durante a busca realizada na casa do investigado, os agentes encontraram mais de cem plantas de *cannabis sativa* sendo cultivadas, sendo então Kyllo acusado de fabricação de drogas.

Em juízo, Kyllo tentou o reconhecimento da nulidade da prova sob a alegação de que esta era invasiva, pois o equipamento utilizado era ofensivo a sua privacidade e que, portanto, sua utilização dependeria de uma prévia autorização judicial.

O Tribunal de Apelações não acolheu a tese da defesa, pois, de acordo com o precedente *Katz*, não ocorreu uma busca e, tampouco, violação de expectativa de privacidade, vez que não houve por parte do acusado nenhuma tentativa de conter o calor que emanava de sua residência. Além disso, não havia nenhuma expectativa razoável de privacidade, pois o equipamento utilizado não poderia expor detalhes íntimos de sua vida, captando apenas o calor proveniente da residência.

No entanto, a Suprema Corte acolheu o argumento defensivo, promovendo um avanço em relação ao precedente *Katz*, estabelecendo mecanismos de proteção contra o poder penetrante dos novos aparatos tecnológicos.

> "A ideia fundamental que preside essa importante decisão é a de que '**retirar da proteção sua mínima expectativa garantida seria permitir à tecnologia policial erodir a privacidade garantida pela 4ª Emenda**', o que poderia ser feito, obviamente, sem nenhum tipo de intrusão física. Porém, nem todo uso de tecnologia para além dos olhos nus converteria uma diligência policial em uma busca a reclamar autorização judicial, mas '**somente quando a tecnologia não está no uso geral do público. Isto assegura a preservação daquele grau mínimo de privacidade que já existia quando a 4ª Emenda foi adotada'**" (KNIJNIK, p. 92).

Segundo a decisão da Suprema Corte, se o Governo utiliza um dispositivo que não é de uso público geral, para explorar os detalhes de umacasa que antes seriam desconhecidos sem intrusão física, tal atividade constituirianuma busca desarrazoada se não fosse precedida por um mandado judicial.

Neste contexto, se uma autoridade policial almeja utilizar determinada tecnologia que ainda não está disseminada no uso geral do público, segundo o precedente *Kyllo*, deverá obter autorização judicial.

Dessa forma, concluiu-se que as informações captadas pela câmara termográfica são resultado de uma busca e que a Quarta Emenda não poderia ser interpretada de forma restritiva, deixando o cidadão à mercê doavanço da tecnologia.

O precedente*Kyllo*revela que devido ao avanço tecnológico, com suas imprevisíveis e incontroláveis aplicações, capazes de penetrar e devassar a intimidade de qualquer pessoa, é necessário que haja uma análise prévia por uma autoridade imparcial (Juiz)[10].

No HC nº. 51.531, o Min. Schietti citou ainda o precedente Riley v. California, no qual a Suprema Corte norte-americana concluiu ser necessário um mandado judicial para permitir o acesso ao telefone celular de um cidadão durante uma prisão em flagrante, haja vista que "telefones celulares modernos não são apenas mais conveniência tecnológica, porque o seu conteúdo revela a intimidade da vida. O fato de

[10]**"**O uso de recursos e artefatos tecnológicos, para além dos sentidos ou do emprego de técnicas de domínio público, permite ver o que àqueles seria inviável, representando, assim, ao contrário das aparências, um fenômeno de "intrusão virtual" na vida das pessoas e, como tal, uma restrição de seu direito fundamental, que somente a um juiz é dado autorizar, sob pena de ilicitude"(ob. cit., p. 93).

a tecnologia agora permitir que um indivíduo transporte essas informações em sua mão não torna a informação menos digna de proteção".

No caso que deu origem ao precedente, David Leon Riley foi abordado pela polícia em San Diego no dia 22 de agosto de 2009, constatando-se que estava com sua carteira de motorista vencida. Ao proceder a busca veicular,foram localizadas duas pistolas sob o capô do automóvel. Em seguida, a polícia acessou o telefone celular de Riley e descobriu que ele era membro de uma gangue envolvida em diversos assassinatos.

Riley foi condenado e recorreu a Corte de Apelação, tendo o Tribunal entendido que a Quarta Emenda permitiria à polícia a realização da busca exploratória no aparelho celular, sempre que localizado perto do suspeito no momento da prisão.

Três precedentes foram utilizados para amparar referido entendimento Chimel v. California, United States v. Robinson e Arizona v. Gant.

A Suprema Corte da Califórnia ratificou o entendimento dasinstâncias inferiores, aplicando precedentes da Suprema Corte norte-americana que permitiam aos funcionários aproveitar objetos sob o controle de um detido e realizar buscas sem mandadopara fins de preservação de provas(People v. Diaz).

Entretanto, a Suprema Corte norte-americana concluiu que o mandado era necessário para acessar o telefone celular.

Neste cenário, a citação pelo Ministro Rogério Schietti do **direito probatório de terceira geração,** ao apreciar o HC nº 51.531 de 09/05/2016, é extremamente oportuna, pois o caso subjacente aos autos versava justamente acerca da discussão dos limites da atuação estatal no que tange as provas obtidas por mecanismos tecnológicos que transcendem os resultados que seriam alcançados pelos meios tradicionais.

Segundo a doutrina, as provas de terceira geração abrangem os seguintes meios probatórios: testes genéticos (DNA), exames biológicos, químicos e toxicológicos, exames psicológicos com fulcro em estudos epidemiológicos e de experimentação,

reconstrução dos fatos através de dinâmicas realizadas por avançados software; reconhecimento vocal *(voice-print)*, cálculos estatísticos, estilometria (individualização de estilos literários de uma pessoa), reconhecimento por GPS da localização de alguém, leitura labial, *thermalimaging* (análise térmica de um ambiente), sobrevoo com câmeras de alta precisão, utilização de cães farejadores, utilização de equipamentos de raios-x para leitura de ambientes ou localização de objetos inseridos no corpo humano, interceptação de sinais ambientais, infiltração de agentes, *keylogger* (programa espião que registra tudo o que é digitado no computador – *registrador do teclado*), dentre diversas outras possibilidades de obtenção de provas através do uso da tecnologia (KNIJNIK, p. 81).

Cumpre ressaltar que, de acordo com a doutrina e a jurisprudência nacional, nem todas as hipóteses acima descritas necessitam de autorização judicial. De acordo com as peculiaridades do caso concreto, deverá ser ponderado o poder de penetração dos aparatos tecnológicos e a expectativa de intimidade dos indivíduos, impondo-se aos agentes estatais o dever de obtenção de prévia ordem judicial quando o recurso utilizado violar a expectativa de intimidade do indivíduo.

Por fim, ressalte-se que Gabriella Di Paolo[11] classifica os novos instrumentos de investigação em três categorias:

a) **Buscas superintrusivas**(*hyper-intrusivesearches*);
b) **Observações virtuais**(*virtual surveillance)*;
c) **Organização de grandes volumes de informações**, que se encontram no nível mais alto da escala de mitigação dos direitos fundamentais (*high volume collection).*

As **buscas superintrusivas**(hyper-intrusivesearches) compreendem os meios de investigação que dão acesso a informações extremamente confidenciais, permitindo adentrar naquele mínimo espaço de sigilo que deve ser garantido a toda pessoa, para que possa existir e se desenvolver em harmonia com o postulado da dignidade humana. Em razão dessa aptidão intrusiva na esfera privada, tais instrumentos investigativos

11DI PAOLO, Gabriella. Tecnologiedelcontrollo e prova penale: l'esperienzastatunitense espunti per lacomparazione. Padova: Cedam, 2008.

permitem controlar os aspectos mais íntimos da vida das pessoas. Cite-se como exemplo as interceptação telefônicas, e o sistema *Key Logger*(programa espião que registra tudo o que é digitado no computador – *registrador do teclado*) (DI PAOLO, 2008)[12].

As **observações virtuais**(*virtual surveillance*) compreendem as tecnologias que são dotadas de uma menor capacidade de intrusão da categoria anterior, devido à natureza diferente dos dados captados, pois apesar de permitir que os órgãos de investigação adquiram informações nãoacessíveis sem a ajuda tecnológica, tais dispositivos permitem apreender informações menos sensíveis das anteriores. Os exemplos citados são o *thermalimagers*(mapeamento de calor emanado de prédios, veículos ou objetos), *pen registers&trapand trace devices*(armadilha e dispositivo de rastreamento: dispositivo que identifica o número de origem, discagem, roteamento, endereçamento e outras informações, identificando a origem de um terminal de comunicação telefônico,sem incluir informações quanto ao conteúdo de qualquer comunicação)e *see-throughdevices*(tecnologia que permite enxergar através de barreiras físicas)(DI PAOLO, 2008)[13].

[12]Al livello più alto di questa scala ideale si collocano le c.d. *hyper-intrusive searches*, categoria da intendersi come compreensiva di tutti quei mezzi di indagine che danno acesso a informazioni estremamante riservate, poiché permettono di insinuarsi in quello spazio mínimo di segretezza che deve essere garantito attorno alle persone affinché possano esistere e svilupparsi in armonia con i postulati della dignitá umana, nel rispetto dela libertá d'autodeterminazione. Per tale spiccata attitudine intrusiva all'interno della esfera privata, gli strumenti in esame consentono di controllare gli aspetti più intimi della vita delle persone, per di più all'insaputa degli interessati e in tempo reale. Il caso paradigmatico di impiego di *hyper intrusive technologies* è rappresentato dalle intercettazioni di comunicazioni, da tempo ricondotte tra le attività qualificabili come *search* ai sensi del IV Emendamento, e oggetto anche di specifica disciplina legislativa, che le ha circondate di um aparato di garanzie che va ben oltre quello desumibile dal precetto costituzionale. Ma negli ultimi anni sono venute alla ribalta anche le c.d. video-intercettazioni e congegni come la Lanterna Magica e i *Key Logger Systems.* In mancanza di una specifica disciplina legislativa, rispetto a tali inediti mezzi di indagine ci si chiede se il loro impiego sia legitimo, se e da quali garanzie debba essere assistito. In sostanza, la questione che si pone è se sia sufficiente applicare il sistema di garanzie desumibile dal IV Emendamento o se viceversa occorra assicurare uno *standard* di tutela più elevato, como quello previsto dal Titolo III per l'esecuzione di intercettazioni (DI PAOLO, Gabriella, 2008).

[13]La seconda categoria (*virtual survellance)* compreende quelle tecnologie che sono dotade di una minore capacità intrusiva rispetto a quelle poc'anzi considerate in ragione della diversa natura del dato captato: benché permettano agli organi investigativi di acquisire conoscenze non accessibili senza l'ausilio tecnologico, simili dispositivi consentono infatti di apprendere informazioni meno sensibili delle precedenti. È il caso dei *pen registers & trap and trace devices*, che rivelano non il contenuto della comunicazione telefonica o telematica, ma solo i dati esterni della medesima. Si potrebbe anche pensare ai *thermal imagers*, che si limitano ad una sorta di mappatura del calore emanato dall'edificio, per evidenziare la differenza di temperature tra le varie zone del medesimo, senza svelare alcunché su ciò che vi accade. Un ulteriore esempio potrebbe essere costituito dai c.d. *see-through devices*, tecnologie binarie che

Por fim, a **organização de grandes volumes de informações** se encontra no nível mais alto da escala de mitigação dos direitos fundamentais (*high volume collection)*compreende a coleta de informação em massa, provenientes de diversas fontes. Abrange os programas de reconhecimento facial instalados em áreas públicas que permitem controlar o movimento das pessoas, bem como identificar pessoas procuradas ou que adotem comportamento suspeito. A referida autora cita também o *software* do FBI que controla a comunicação via Internet (*Carnivore System*)(DI PAOLO, 2008)[14].

Em apertada síntese, quanto às limitações da atuação estatal em razão da proteção à intimidade,as gerações probatórias, à luz dos precedentes da Suprema Corte dosEstados Unidos, estabelecemos a seguinte classificação:

Direito probatório de 1ª Geração:a proteção constitucional aplicava-se apenas a áreas tangíveis e demarcáveis, exigindo a entrada, o ingresso e a violação de um espaço privado ou particular, com abrangência apenas de coisas, objetos e lugares. Segundo a Suprema Corte dos EUA,a correta interpretação constitucional não permitiria alargá-la além do conceito de pessoas, casas, papéis e pertences, para proibir escutar ou

---

pur essendo in grado di scrutare attraverso barriere come indumenti o borse, possono rivelare soltanto la presenza o l'assenza dell'oggetto ricercato (armi o sostanze stupefacenti), senza dire nulla circa gli altri effetti personali contenuti sotto o all'interno di tali involucri. In assenza di una specifica disciplina legislativa, anche per questi strumenti investigativi il nodo problematico da sciogliere è se il loro impiego possa essere qualificato come *search,* vale a dire se possa essere riconosciuta in capo ai soggetti monitorati una legittima aspettativa alla *privacy*. La questione non è di poco momento, perché a seconda del responso muta sensibilmente il regime giuridico di riferimento. In caso di risposta affermativa l'attivittà degli inquirenti dovrebbe espletarsi quantomeno nel rispetto delle garanzie disegnate dal IV Emendamento, che notoriamente sancisce una vera e propria *exclusionary rule* nei confronti delle prove illegittimamente ottenute. Nell'ipotesi contraria si dovrebbe invece ritenere che gli inquirenti non siano soggetti a particolari restrizioni, se non a quelle eventualmente imposte dalla *statute law*, che peraltro non sempre presidia l'osservanza dei propri precetti mediante *suppression remedies (*DI PAOLO, Gabriella, 2008).

[14]La terza e ultima categoria (*high volume collection technologies)* compreende quei ritrovati che procedono alla raccolta di massa di informazioni provienienti da varie fonti, e successivamente passano al setaccio i dai coi raccolti per individuare quell'esigua percentuale che potrebbe essere rilevante per la indagini. Simili dispositivi vengono impiegati per lo più in aree pubbliche o aperte al pubblico, dove transitano o stazionano una gran quantità di soggetti al fine di controllarne gli spostamenti oppure per identificare persone ricercate o sospettate. Un recente esempio di *high volume collection technologies* è il sistema de identificazione biometrico noto come *facial recognition technology*, che si basa sull'intreccio delle immagini raccolte dagli inquirenti con i dati biometrici della persona ricercata. Presenta caratteristiche omologhe anche il c.d. *Carnivore System* utilizzato dall' FBI per il controllo delle comunicazioni via *internet (*DI PAOLO, Gabriella, 2008).

observar.Na primeira geração a captação da imagem e da voz, incluindo-se a realizada através da interceptação telefônica, não eram protegidas constitucionalmente - ***teoria proprietária ou trespasstheory***(Precedente *Olmstead v. United States de 1928*).

Direito probatório de 2ª Geração:o âmbito de proteção constitucional foi ampliado de coisas, lugares e pertences para pessoas e suas expectativas de privacidade. A teoria proprietária, estabelecida no precedente *Olmstead v. United States* foi superada, tendo o âmbito de proteção constitucional migrado de coisas, lugares e pertences para pessoas e suas expectativas de privacidade, sedimentando o entendimento de que a 4ª Emenda estende sua proteção a gravação de declarações orais. *Teoria da proteção constitucional integral* (Precedente *Katz v. United States de 1967*).

Direito probatório de 3ª Geração: abrange as provas tecnológicas, altamente invasivas, que permitem ao Governo alcançar conhecimentos e resultados que transcendem àqueles que seriam obtidos pelos sentidos e técnicas tradicionais. A partir do precedente *Kyllov. United States,* fixou-se o entendimento de que o avanço da tecnologia sobre a materialidade das coisas não pode limitar o escopo e a abrangência da proteção constitucional outorgada às pessoas. Assim, a interpretação da 4ª Emenda, ao aludir a coisas, pertences, papéis e lugares, deveria sofrer uma atualização interpretativa, para além da doutrina *Katz.* O precedente Kyllo alerta que devido ao poder devassador, imprevisível e penetrante da tecnologia, sua utilização, se ainda não pertencer ao uso geral do público, dependerá da análise de uma autoridade judiciária(Precedente *Kyllo v. United States de 2001*).

Conclusão

Após a análise da evolução da matéria perante a Suprema Corte norte-americana e à luz das decisões do Supremo Tribunal Federal (HC 91.867/PA de 20/09/2012) e do Superior Tribunal de Justiça (HC 51.531 de 09/05/2016), apresentamos a seguinte solução quanto à realização da busca exploratória no aparelho celular apreendido pela polícia.

Em regra, os policiais não poderão, sem prévia autorização judicial, realizar a busca exploratória no telefone celular apreendido, em virtude da expectativa de privacidade quanto aos arquivos armazenados.

Em situações excepcionais, nas quais as peculiaridades do caso concreto demonstrem, de forma inequívoca, a urgência na obtenção das informações e/ou o risco concreto de perecimento dessas,justificada a excepcionalidade por escrito, sob pena de responsabilidade disciplinar, civil e penal do agente ou autoridade policial, **poderão os policiais proceder ao acesso dos arquivos e registros existentes no referido aparelho, inclusive com a consulta a aplicativos de comunicação,** vez que a expectativa de privacidade não pode servir para amparar crimes que estão em plena consumação (ex.: extorsão mediante sequestro e tráfico de drogas) e, tampouco, ser utilizada para salvaguardar associações e organizações criminosas, legitimando a impunidade.

Nestes casos excepcionais, **ressalve-se que deverá a polícia desabilitar a conexão do celular à rede mundial de computadores, limitando-se assim a consulta a troca de mensagens pretéritas e demais dados armazenados no aparelho**[15], o que

[15] No que concerne a eventual proteção aos dados cadastrais ou dados contidos no artigo 5º, XII da Constituição (*art. 5º, XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das* ***comunicações telefônicas****, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;*), que traria a obrigatoriedade de ordem judicial para seu acesso, o STF já se posicionou sobre o assunto, no sentido da proteção do mencionado dispositivo ser referente à comunicação de dados e não aos dados em si, conforme extensa ementa abaixo parcialmente transcrita. Além disso, o conceito de "dados" contido no preceito constitucional é diverso do conceito de dados cadastrais. Parece um jogo de palavras, mas não é. Nesse sentido, veja o aresto do Supremo Tribunal Federal sobre os dados e sua possibilidade de acesso: EMENTA: (...) IV - **Proteção constitucional ao sigilo das comunicações de dados - art. 5º, XVII, da CF: ausência de violação, no caso.** 1. Impertinência à hipótese da invocação da AP 307 (Pleno, 13.12.94, Galvão, DJU 13.10.95), **em que a tese da inviolabilidade absoluta de dados de computador não pode ser tomada como consagrada pelo Colegiado, dada a interferência, naquele caso, de outra razão suficiente para a exclusão da prova questionada - o ter sido o microcomputador apreendido sem ordem judicial** e a conseqüente ofensa da garantia da inviolabilidade do domicílio da empresa - este segundo fundamento bastante, sim, aceito por votação unânime, à luz do art. 5º, XI, da Lei Fundamental. 2. Na espécie, ao contrário, não se questiona que a apreensão dos computadores da empresa do recorrente se fez regularmente, na conformidade e em cumprimento de mandado judicial. 3. Não há violação do art. 5º. XII, da Constituição que, conforme se acentuou na sentença, não se aplica ao caso, pois não houve "quebra de sigilo das comunicações de dados (interceptação das comunicações), mas sim apreensão de base física na qual se encontravam os dados, mediante prévia e fundamentada decisão judicial". 4. **A proteção a que se refere o art. 5º, XII, da Constituição, é da comunicação "de dados" e não dos "dados em si mesmos", ainda quando armazenados em computador.** (cf. voto no MS 21.729, Pleno, 5.10.95, red. Néri da Silveira - RTJ 179/225, 270). V - Prescrição pela pena concretizada: declaração, de ofício, da

evitará a interceptação da comunicação em tempo real com a consequente nulidade das provas obtidas em virtude da cláusula de reserva de jurisdição, imposta pela ordem constitucional no caso de interceptação de dados ou comunicações.

Por fim, saliente-se que, havendo autorização, expressa e inequívoca, do usuário do celular (proprietário ou possuidor), não será necessária ordem judicial, haja vista que àquele que abdica da sua intimidade, não poderá, posteriormente, pleitear a nulidade da prova[16].

prescrição da pretensão punitiva do fato quanto ao delito de frustração de direito assegurado por lei trabalhista (C. Penal, arts. 203; 107, IV; 109, VI; 110, § 2º e 114, II; e Súmula 497 do Supremo Tribunal). (STF. Pleno. Relator: Min. Sepúlveda Pertence. DJ 19-12-2006 PP-00037).

[16]Não se pode presumir, que as autorizações dadas na esfera policial, sejam obtidas por meios escusos como se propalam em defesas a todo e qualquer preço, já que isto é inverter a presunção da legitimidade e veracidade dos atos policiais (atos administrativos) imantados com tais efeitos de lícitos.