Vigiar para investigar? Mandados de busca reversos e a coleta massiva de dados de localização

20/06/2026

Caso Chatrie: os fatos

Eram aproximadamente 16h50 de 20 de maio de 2019 quando um homem, vestindo um chapéu de pescador e um colete de trânsito, entrou na Call Federal Credit Union, em Midlothian, Virgínia, aparentando falar ao celular [1]. Aproximou-se do balcão e entregou à caixa um bilhete que dizia que a vigiava havia algum tempo, que mantinha sua família como refém, e que, se ela ou qualquer colega avisasse a polícia, alguém se machucaria. O bilhete acrescentava que o autor se fazia acompanhar de comparsas do lado de fora e que, se a polícia fosse avisada, pessoas iriam se ferir. Ele ordenou que a funcionária entregasse todo o dinheiro — exigindo pelo menos US$ 100 mil — com a promessa de que, se colaborassem, ninguém se machucaria e a família seria libertada [2].

A funcionária respondeu que não tinha acesso àquela quantia. O homem sacou então uma pistola prateada e preta, ordenou que todos se deitassem no chão e conduziu o gerente e outros funcionários até o cofre. Sob a mira da arma, ele forçou a gerente a abrir o cofre e colocar US$ 195 mil dentro de uma bolsa que ele havia levado e fugiu [3]. O detetive Joshua Hylton, ao chegar ao local do crime, entrevistou testemunhas e analisou as imagens das câmeras do banco. Descobriu que o assaltante havia se aproximado vindo da direção de uma igreja vizinha e, ao notar nas filmagens que ele falava ao celular ao entrar, inferiu que poderia estar "conversando com um comparsa" [4]. Em meados de junho, esgotadas as demais pistas [5] e ainda sem a identificação de um suspeito, o detetive Hylton requereu um *geofence warrant* [6].

Técnica do *geofence* em três etapas

A ordem seguiu um protocolo estruturado em *três* etapas que o próprio Google estruturou para responder a requisições de rastreamento em massa sobre seu acervo de dados de localização [7]. O pedido buscava acessar o banco de dados do *Location History* — o repositório interno conhecido como "*Sensorvault*", que armazena os registros de centenas de milhões de contas — e descobrir quais dispositivos estiveram na cena do crime no momento do assalto. A polícia delimitou a "*cerca virtual*" como um círculo de 150 metros de raio em torno de coordenadas próximas à agência, abrangendo não apenas a estrutura física, mas também a área no entorno. Para essa região, requereu os dados de *todos* os dispositivos presentes numa janela ininterrupta de uma hora — das 16h20 às 17h20, isto é, 30 minutos antes e 30 minutos depois do crime. Para cumpri-lo, o Google foi obrigado a percorrer a totalidade de seu banco de dados em busca dos aparelhos que cruzaram a cerca, e devolveu à polícia uma lista anonimizada [8] com a localização de 19 usuários, em 209 registros.

Para reconstruir as rotas de chegada e fuga e identificar o suposto autor do crime, a polícia filtrou a lista de 19 para nove dispositivos. Quanto a esses nove, porém, dois parâmetros foram alterados de maneira mais incisiva. Primeiro, a janela temporal expandiu-se para duas horas — das 15h50 às 17h50 —, ao acrescentar trinta minutos antes e trinta minutos depois do recorte original. Segundo, e mais significativo, os limites geográficos foram inteiramente removidos, ou seja, para essa janela ampliada, o Google forneceu a localização daqueles nove usuários "*sem qualquer restrição de lugar*", passando a acompanhar de maneira irrestrita o trajeto daquelas pessoas pela cidade [9].

Apenas na terceira e última etapa a polícia selecionou três dos usuários e exigiu que o Google realizasse a identificação formal ("desanonimização"), revelando nomes, números de telefone e endereços de e-mail. Um desses três aparelhos entrava na área delimitada dez minutos antes do assalto e dela se afastava em seguida, rumo a uma área residencial. O aparelho estava registrado sob o e-mail de Okello Chatrie, o que acarretou a sua identificação. O ponto a sublinhar é que a individualização do suspeito foi o último elo de uma cadeia que principiou, indistintamente, pela varredura de 19 pessoas — e que, na etapa intermediária, chegou a rastrear nove pessoas sem qualquer fronteira espacial, antes que se soubesse quem, entre elas, teria relação com o crime.

Spacca

Um detalhe processual bastante questionado pela defesa é que a polícia exigiu essa desanonimização e obteve os nomes dos alvos diretamente com o Google, sem justificar a sua fundada suspeita ou requerer previamente ao magistrado a emissão de uma nova ordem específica para tal finalidade.

Da condenação ao Quarto Circuito: a divisão sobre a Quarta Emenda

Em setembro de 2019, um grande júri federal no Distrito Leste da Virgínia admitiu a denúncia contra Okello Chatrie por dois crimes: assalto à mão armada a um banco e uso/exibição de arma de fogo durante um crime de violência [10].

Durante o processo, a defesa de Chatrie buscou anular as provas obtidas por meio da localização do Google, argumentando violação à Quarta Emenda [11]. O tribunal distrital, no entanto, negou o pedido de exclusão, aplicando a regra de que os policiais agiram de "*boa-fé*" [12] ao cumprir o mandado, pois na época a legalidade dessa tecnologia ainda não havia sido definida pelos tribunais. Diante da derrota no tema probatório, Chatrie firmou um acordo de confissão condicional (*conditional guilty plea*), no qual se declarou culpado das acusações, mas reservou expressamente o seu direito de apelar contra a validação das provas de *geofence*. Com isso, ele foi condenado a 141 meses de prisão (quase 12 anos), seguidos por três anos de liberdade supervisionada, além de ser obrigado a pagar US$ 196.932,01 a título de restituição ao banco [13].

Chatrie recorreu da decisão que validou o mandado. O caso tramitou no Tribunal de Apelações do Quarto Circuito [14], onde inicialmente um grupo de três juízes confirmou a decisão da primeira instância. O caso foi então levado a um julgamento *en banc* (pelo plenário do tribunal, com 15 juízes), que também manteve a condenação, embora os juízes tenham ficado divididos sobre a inconstitucionalidade da medida.

A votação sobre a tese constitucional central de Chatrie, qual seja, se a coleta de dados via geofence constituiu ou não uma "busca" sob o amparo da Quarta Emenda, resultou de fato em um empate de 7 a 7, com uma abstenção. O tribunal emitiu uma decisão *per curiam* de apenas uma frase ("*The judgment of the district court is AFFIRMED*") para confirmar a condenação, acompanhada de nove opiniões separadas que ilustram a profunda divisão da corte [15].

Sete juízes (Richardson, Wilkinson, Niemeyer, King, Agee, Quattlebaum e Rushing) votaram contra a tese de Chatrie, concluindo que não houve uma busca sob o amparo da Quarta Emenda. Eles argumentaram que Chatrie não tinha uma expectativa razoável de privacidade sobre duas horas de seu histórico de localização, pois ele havia exposto esses dados voluntariamente ao Google, aplicando-se, assim, a Doutrina do Terceiro (*third-party doctrine*) [16]. Outros sete juízes (Gregory, Wynn, Thacker, Harris, Heytens, Benjamin e Berner) concordaram com a tese de Chatrie de que o uso do mandado de geofence constituiu, sim, uma busca sob a Quarta Emenda e invadiu sua expectativa razoável de privacidade. Dentre esses sete, cinco juízes (Gregory, Wynn, Thacker, Benjamin e Berner) foram além e concluíram expressamente que o mandado era inconstitucional por não ser apoiado por uma causa provável (*probable cause*) individualizada. O juiz-chefe Diaz recusou-se a decidir se a quebra de sigilo constituiu ou não uma busca. Ele preferiu pular a tese constitucional e manter a condenação fundamentando-se exclusivamente na "*exceção de boa-fé*" [17].

Em resumo, o fator decisivo que selou a derrota de Chatrie na corte foi a "*exceção de boa-fé*". Dos sete juízes que concordaram que houve uma busca, seis deles decidiram que, mesmo com a violação à Quarta Emenda e a falta de causa provável, as provas não deveriam ser anuladas porque o detetive responsável agiu de boa-fé ao confiar em um mandado assinado por um magistrado, em um momento em que a tecnologia era nova e a lei ainda era incerta [18]. Somando esses seis juízes, o juiz-chefe Diaz e os sete juízes que acharam que sequer houve uma busca, formou-se uma significativa maioria de 14 votos. O único juiz a acolher integralmente a tese de Chatrie foi o Juiz Gregory, que discordou da aplicação da exceção de boa-fé e argumentou que a condenação deveria ser revertida e as provas suprimidas.

O certiorari e o que está em jogo

Contudo, a condenação que se confirmou não encerrou a questão. A Suprema Corte dos Estados Unidos concedeu *certiorari* em 16 de janeiro de 2026, deixando claro que o tema em discussão em *Chatrie* ultrapassa o interesse individual de *um* acusado. A mais alta corte do país irá decidir se uma técnica que inverte a lógica da suspeita — que parte da prova para então buscar a pessoa — pode conviver com uma Constituição que foi escrita, em boa parte, justamente para impedir buscas exploratórias. Assim, a pergunta que estrutura o artigo subsequente é se há, e em que condições, um ponto de equilíbrio entre a eficiência de uma investigação que se vale dos rastros digitais e os limites que o devido processo, a privacidade e o sigilo de dados impõem ao Estado.

---

[1] ESTADOS UNIDOS (2026a): ESTADOS UNIDOS. Brief for the United States. Supreme Court of the United States. Caso nº 25-112 (Okello T. Chatrie, Petitioner, v. United States of America, Respondent). Representante: D. John Sauer (Solicitor General). Washington, DC, mar. 2026.

[2] Id.

[3] Id.

[4] Id.

[5] No curso da investigação, duas diligências investigativas não produziram efeito. Na primeira, uma mulher que se apresentou como ex-companheira de um possível suspeito comunicou à polícia que ele seria o autor do roubo, razão pela qual os investigadores o localizaram, colheram sua versão, examinaram seu telefone celular e, ao final, afastaram sua participação no crime. Na segunda, um funcionário de outra agência bancária informou a existência de um homem que conduzia um veículo Buick Lacrosse azul e utilizava colete de trânsito, vestimenta semelhante à usada pelo assaltante, mas a posterior verificação dessa informação levou o detetive a concluir que também não se tratava do autor do delito.

[6] ESTADOS UNIDOS (2026a): ESTADOS UNIDOS. Brief for the United States. Op. cit.

[7] CHATRIE, Okello T. Brief for Petitioner. Supreme Court of the United States. Caso nº 25-112 (Okello T. Chatrie, Petitioner, v. United States of America, Respondent). Representante: Adam G. Unikowsky. Washington, DC

[8] Esta lista não continha nomes ou e-mails, mas apenas números pseudônimos de identificação dos aparelhos (*Device IDs*), acompanhados de suas respectivas coordenadas de latitude e longitude, os dados de data/hora, o nível de precisão (intervalo de confiança/raio do mapa) e a fonte do dado (ex: GPS, redes Wi-Fi ou Bluetooth). CHATRIE, Okello T. Petition for a Writ of Certiorari. Supreme Court of the United States. Caso nº 25-112 (Okello T. Chatrie, Petitioner, v. United States of America, Respondent). Representante: Adam G. Unikowsky. Washington, DC, 28 jul. 2025

[9] Parecer do Google (Amicus Curiae) GOOGLE LLC. Brief for Amicus Curiae Google LLC in Support of Neither Party. Supreme Court of the United States. Caso nº 25-112 (Okello T. Chatrie, Petitioner, v. United States, Respondent). Representante: Scott A. Keller. Washington, DC, mar. 2026.

[10] Forced Accompaniment During Armed Bank Robbery, 18 U.S.C. § 2113(a), (d), and (e), and Using, Carrying, or Brandishing a Firearm During and in Relation to a Crime of Violence. 18 U.S.C. § 924(c)(1)(A).

[11] A Quarta Emenda da Constituição dos Estados Unidos estabelece a proteção fundamental dos cidadãos contra buscas e apreensões arbitrárias pelo Estado. Em sua tradução para o português, a emenda consagra o seguinte texto: “O direito do povo de estar seguro em suas pessoas, casas, papéis e bens [efeitos], contra buscas e apreensões irrazoáveis, não será violado, e nenhum mandado será expedido, senão mediante causa provável, apoiado por juramento ou afirmação, e descrevendo com particularidade o local a ser revistado e as pessoas ou coisas a serem apreendidas.”

[12] A exceção de boa-fé (*good-faith exception*) é uma doutrina consagrada pela Suprema Corte dos Estados Unidos no precedente *United States v. Leon* (1984), que estabelece que as provas obtidas por meio de um mandado de busca não devem ser excluídas se os policiais atuaram de forma objetivamente razoável e de boa-fé ao confiar na autorização expedida por um juiz ou magistrado neutro. ESTADOS UNIDOS. Brief for the United States in Opposition. Supreme Court of the United States. Caso nº 25-112 (Okello T. Chatrie, Petitioner, v. United States of America, Respondent). Representante: D. John Sauer (Solicitor General). Washington, DC, nov. 2025.

[13] ESTADOS UNIDOS. United States District Court for the Eastern District of Virginia. United States v. Okello T. Chatrie. Caso nº 3:19-cr-00130-MHL. Decisão proferida em: 3 mar. 2022. 590 F. Supp. 3d 901.

[14] ESTADOS UNIDOS. United States Court of Appeals for the Fourth Circuit. United States v. Okello T. Chatrie. Julgamento *En Banc*. Caso nº 22-4489. Decisão proferida em: 30 abr. 2025. 136 F.4th 100.

[15] CHATRIE, Okello T. Petition for a Writ of Certiorari. Supreme Court of the United States. Caso nº 25-112 (Okello T. Chatrie, Petitioner, v. United States of America, Respondent). Representante: Adam G. Unikowsky. Washington, DC, 28 jul. 2025.

[16] A Doutrina do Terceiro (*Third-Party Doctrine*) estabelece que uma pessoa não possui uma expectativa legítima de privacidade em relação às informações que ela entrega ou revela voluntariamente a terceiros (como bancos, empresas de telefonia ou provedores de tecnologia e internet). A principal consequência prática é que, como não há expectativa razoável de privacidade sobre os dados compartilhados, a obtenção dessas informações pelo governo junto a esses terceiros não é considerada uma "busca" protegida pela Constituição. Por não ser uma busca no sentido técnico-jurídico, a polícia fica dispensada da exigência de obter um mandado judicial fundamentado em causa provável para acessá-los. GOOGLE LLC. Brief for Amicus Curiae Google LLC in Support of Neither Party. Supreme Court of the United States. Caso nº 25-112 (Okello T. Chatrie, Petitioner, v. United States, Respondent). Representante: Scott A. Keller. Washington, DC, mar. 2026.

[17] KERR, Orin S. Brief of Professor Orin S. Kerr as Amicus Curiae in Support of Respondent. Supreme Court of the United States. Caso nº 25-112 (Okello T. Chatrie, Petitioner, v. United States, Respondent). Stanford, CA, 1 abr. 2026.

[18] CHATRIE, Okello T. Brief for Petitioner. Supreme Court of the United States. Caso nº 25-112 (Okello T. Chatrie, Petitioner, v. United States of America, Respondent). Representante: Adam G. Unikowsky. Washington, DC.

Fonte: https://conjur.jumps.com.br/2026-jun-20/vigiar-para-investigar-mandados-de-busca-reversos-e-a-coleta-massiva-de-dados-de-localizacao-2/