Christina Milles: É preciso enfrentar limites de investigação em celular

Recentemente, a Suprema Corte dos Estados Unidos analisou a validade jurídica de uma busca e apreensão de um dispositivo móvel sem mandado específico para tanto. A situação envolveu dois casos: o primeiro, foi "o Governo dos EUA contra Wurie (13-212)" e; o segundo, "Riley contra a Califórnia (13-132)".

Embora os juízes tivessem inúmeras questões a decidir, no centro de tudo estava o direito à privacidade contra a intrusão do governo e, ao mesmo tempo, a necessidade de acesso pelo governo a informações privadas para proteger a segurança pública.

Mais especificamente: Se o acesso da polícia a uma fonte de dados pessoais, sem um mandado específico, pode incluir todo e qualquer dado privado, ou se deve haver exceções; Que tipos de dados de dispositivos móveis podem ser investigados sem mais amarras; Se todos os tipos de crimes em investigação, desde contravenções até crimes graves, deixariam os dispositivos móveis dos cidadãos expostos a buscas sem a exigência de um mandado; Qual a diferença entre buscas em um dispositivo móvel e buscas em outros recipientes particulares, como carteiras ou bolsas; e como a polícia pode equilibrar os direitos à privacidade e a necessidade de preservar evidências que, inclusive, poderiam ser criptografadas ou apagadas remotamente.

Mesmo antes de a Suprema Corte ouvir os argumentos, porém, o jornal *Washington Post* publicou um artigo sobre a preocupação de alguns juízes federais de que as buscas do governo pudessem ultrapassar os limites e obter dados não relevantes para o caso em investigação e, então, reter estes dados "para uso futuro não específico".

O Juiz Antonin Scalia também levantou essa questão, segundo o *National Public Radio* (NPR), ao sugerir uma regra pudesse limitar a busca a material efetivamente relevante para a investigação do crime pelo qual a pessoa foi detida.

Como os limites de busca poderiam impactar a elucidação de casos?
O problema, claro, é que nem sempre você sabe exatamente o que você "não sabe" — ou seja, o que pode ou não ser relevante numa determinada investigação. Embora a boa investigação deva ser capaz de restringir seu campo de observação para um certo intervalo de datas; ou um certo conjunto de comunicações entre suspeito(s) e/ou vítima(s), o surgimento de informações conflitantes e indivíduos não cooperativos podem tornar esses tipos de filtros difíceis de serem assimilados.

Ademais, as evidências digitais nem sempre são óbvias. É possível, por exemplo, descobrir novas vítimas de sedução infantil, antes desconhecidas, nos registros de bate-papo de um suspeito não relacionados com o caso em enfoque. Ou encontrar evidências reais ocultas em nomes de arquivos aparentemente inócuos; ou ainda, detectar evidências de que a atividade ilegal do suspeito vinha acontecendo há muito mais tempo do que se pensava inicialmente (e, portanto, fora de eventuais prazos limites).

Além disso, os padrões de vida de um indivíduo — sua movimentação física, suas comunicações,

vínculos sociais e assim por diante — podem ajudar a estabelecer os meios, o motivo ou a oportunidade de um crime em fase de elucidação, podendo também ajudar no trabalho de inteligência em investigações longas ou na evidenciação de um planejamento operacional relacionado ao caso.

Além disso, conteúdos que não implicam em evidências também podem ser importantes para autenticar evidências. Eles podem, por exemplo, mostrar o estado de espirito de um indivíduo antes, durante e depois de um incidente. Os padrões de linguagem que se encaixam às evidências podem indicar que a mesma pessoa foi a autora das mensagens. Localizações e carimbos de data e hora podem mostrar que o suspeito usava o dispositivo, seja para atividades "normais" como criminosas, no mesmo horário que a conduta criminosa se consumou, demonstrando que ninguém mais poderia ter postado o conteúdo ilegal a partir daquele dispositivo e naquele horário.

Finalmente, como demonstram os fatos nos casos de Riley e Wurie, analisados pelo Supremo dos EUA, os confrontos com de fatos com versões de suspeitos em campo não ajudam a decidir, de imediato, qual a melhor maneira de lidar com seus dispositivos móveis. A verdadeira análise forense não condiz com esse tipo de rápida tomada de decisão que geralmente é necessária para preservar e coletar diferentes formas de evidências e manter o controle da situação em que o incidente de insere.

De volta ao debate na Suprema Corte

No caso de Riley, segundo o NPR, o Procurador Geral da Califórnia, Edward DuMont, "disse que nenhum mandado deve ser exigido para qualquer informação que seja 'do mesmo tipo' que a polícia tem sido tradicionalmente capaz de apreender sem um mandado (tais como diários, cartas, fotografias) quando em posse de um indivíduo".

No entanto, os juízes tiveram o cuidado de considerar que a quantidade de dados que pode ser carregada em um smartphone é muito maior do que aqueles em diários, cartas ou fotografias físicass ou, bem como em bolsas, pastas ou porta-luvas, nos quais a polícia pode fazer buscas em prol de sua própria segurança ou para preservar provas.

Em paralelo, uma breve análise realizada pelo professor de direito Orin Kerr concluiu que parecia que os juízes não apoiaram uma regra para os dispositivos digitais poderem "ser sempre investigados em sua totalidade no ato da apreensão", nem uma regra clara para exigir um mandado a cada situação. Ao invés disso, Kerr acredita que a Corte estabelecerá uma "regra intermediária" que, em última análise, exigirá que a polícia limite suas buscas na maioria dos casos.

Limites para a busca como a melhor prática

A Corte não deve anunciar sua decisão até junho deste ano. Portanto, nesse meio tempo, pense como você pode restringir a linguagem do mandado de busca em um dispositivo móvel em vez de usar texto padrão. Tenha em mente que o limite de busca em dados digitais não é coisa nova: tanto operadoras de dados sem fio como provedores de serviços de internet, como o Facebook, exigem intervalos de data e/ou hora específicos para solicitações de registros e conteúdo.

Em geral, ser específico é uma boa prática. Fora as questões de privacidade, um jornalista norte-americano observou que a simples solicitação "dê-me tudo o que há no seu telefone" tornou-se um pedido não razoável, uma vez que a capacidade de armazenamento dos dispositivos móveis e a

quantidade de dados armazenados aumentam cada vez mais. Para enfrentar juízes em sua jurisdição, aqui vão algumas dicas para ajudá-lo.

(Nota: este não é um aconselhamento legal. Não deixe de trabalhar com promotores em sua própria jurisdição para determinar quais as políticas e procedimentos operacionais devem ser estabelecidos)

Para preservar as provas (e evitar que sejam apagadas remotamente ou alguma submetidas a outra ação do suspeito para ocultá-las ou destruí-las), isole o dispositivo de qualquer rede sem fio, colocando-o em Modo Avião. Certifique-se de que esta ação esteja em seu termo de consentimento, se estiver buscando autorização para a busca.

É possível coletar dados, através de perícia, sem "fazer uma busca"? Talvez, mas lembre-se: parte do debate envolve a retenção — ou por quanto tempo guardar os dados depois de coletados. Se achar que sua investigação vai demorar, mas você precisa liberar o dispositivo para o indivíduo, obtenha um mandado para coletar os dados que você quer investigar.

A causa apontada em um mandado de busca não pode ser exageradamente genérica. Você deve apontar razoavelmente que um crime foi ou está prestes a ser cometido e que podem existir provas no dispositivo que você quer investigar.

As exigências para um mandado de especificidade (o dispositivo a ser investigado, os dados a serem apreendidos) impõem que o seu pedido deve incluir dados específicos: bate-papos, mensagens instantâneas, imagens, e-mails e intervalos de data/hora quando aplicável. Seu mandado deve conter esses detalhes para aumentar sua base para a busca de provas.

Mas também não seja específico demais. Fazer uma busca em um dispositivo móvel pode ser como fazer uma busca em uma casa, mas dar nomes a bancos de dados específicos não é tão simples quanto dar nomes aos cômodos de uma casa. Mesmo quando a distribuição das casas difere, os nomes dos diferentes cômodos (sala de estar, quarto, porão) continuam consistentes.

Os nomes do banco de dados de um dispositivo móvel não são. Pode-se armazenar dados relevantes em vários bancos de dados diferentes e, portanto, em diferentes locais da memória de um dispositivo. Isso depende da marca, modelo, sistema operacional, versão do firmware do dispositivo, além de outras variáveis.

Imagens, por exemplo, podem estar em seu próprio diretório, ou armazenadas no diretório para os aplicativos com os quais estão associadas,ou ainda, apagadas e fragmentadas em um espaço não localizável na memória do dispositivo. Em suma, ao dar nomes a bancos de dados específicos a serem investigados, corre-se o risco de perder evidências importantes.

Se encontrar evidências de outro crime que não seja aquele que está investigando, pare sua busca imediatamente e vá atrás de um novo mandado. A doutrina da primeira vista protegerá sua descoberta inicial, mas não as evidências subsequentes se você continuar sua busca sem obter outro mandado.

Finalmente, lembre-se que as exigências legais ajudam-no a ser melhor em seu trabalho: mais minucioso, mais crível e mais profissional. Em um momento em que as agências do governo estão sob

maior escrutínio público do que jamais esteve, use para sua vantagem profissional, seja qual for a decisão promulgada em junho, e aproveite a oportunidade para aprender o máximo possível sobre os dispositivos que esteja investigando.

Date Created
03/06/2014