

Permissão ao bloqueio de celulares nos Jogos Olímpicos 2016 evidencia crescimento do vigilantismo no Estado brasileiro.

---

As Forças Armadas estão autorizadas a usar bloqueadores de sinais de radiocomunicação (BSR's) durante a realização dos Jogos Olímpicos e Paralímpicos Rio 2016. A medida, aprovada pela Agência Nacional de Telecomunicações (Anatel), ainda se estende às chamadas Operações de Garantia de Lei e da Ordem (referente a manifestações e revoltas populares).

A permissão ao bloqueio de celulares não se limitará à data da realização dos Jogos e já estaria em voga. De acordo com a portaria aprovada pela Anatel, “a utilização dos BSR's deve restringir-se a operações específicas, episódicas, urgentes e temporárias relacionadas à segurança dos eventos esportivos referidos no caput, ou a eventuais operações de Garantia da Lei e da Ordem, em que se identifiquem evidências concretas de risco potencial ou iminente de ações necessária”.

Além de se caracterizar como um ataque à Constituição, convenções e tratados internacionais relacionados ao direito de comunicação e de livre expressão, uma abordagem tão ampla e vaga concedendo às Forças Armadas tamanho poder desvela a intrínseca relação entre o Estado brasileiro e a indústria internacional de vigilância.

Para Camila Marques, advogada do Centro de Referência Legal em Liberdade de Expressão e Acesso à Informação da Artigo 19, as definições são vagas o suficiente para colocar qualquer manifestação de rua sob suspeita de intenções criminosas, “possibilitando um nível impensável de repressão”. Para ela, antes de fazer esse tipo de concessão, seria preciso perguntar: “o que

é considerado urgente? O que é temporário? Alguns dias? Horas?”

A advogada questiona ainda a atribuição da Anatel de permitir o bloqueio de celulares. “Não deveria ser essa agência a conceder uma permissão tão genérica e ampla; e que não pode ser usada de maneira indiscriminada pelas Forças Armadas. É necessário que se analise os fatos concretos e as razões que justificariam um bloqueio geral; ou pelo menos deveriam ter delimitado muito melhor quais as ações a serem permitidas às Forças Armadas”, explica a advogada.

O histórico de ataque aos direitos humanos por parte de agentes do Estado, somados a possíveis cortes na comunicação em tempo real executados pelas Forças Armadas tendem a expor ainda mais os indivíduos aos abusos dos agentes de segurança do Estado. “A transmissão ao vivo constrange minimamente os atos dos agentes policiais. Já é preocupante como está; ficará muito menor o constrangimento de agentes”, analisa a advogada da Artigo 19.

Somada aos ataques a direitos relacionados à comunicação, à livre expressão e ao livre acesso à informações relacionadas a protestos, a permissão ao bloqueio de celulares concedida às Forças Armadas pela Anatel revela a escalada da parceria entre a indústria de segurança e vigilância e Estados nacionais, principalmente o Brasil.

“Após junho de 2013, o Estado brasileiro buscou inúmeros dispositivos legais para legitimar a vigilância e criminalizar ativistas e movimentos sociais. A [possível aprovação da] Lei Antiterrorismo entra nessa mesma lógica”, lembra Camila Marques.

Junto com as manifestações de rua, a realização de grandes eventos como a Copa do Mundo e as Olimpíadas transformaram o Brasil em “mercado prioritário da vigilância”, segundo Lucas Texeira, da Oficina Antivigilância. Para ilustrar isso, Lucas lembra, como foi noticiado em 2013,

que “gigantes do setor obtiveram contratos em diversas cidades para monitorar brasileiros durante a Copa de 2014”.

O membro da Oficina Antivigilância reforça que uma das várias gigantes do ramo que financiam o ISS World (Feira empresarial do setor), a empresa italiana Hacking Team, teve recentemente uma grande quantidade de e-mails exposta .

De acordo com o relatório Vigilância das Comunicações pelo Estado Brasileiro, elaborado pelo InternetLab em parceria com a Electronic Frontier Foundation, há negociações com vários setores do governo como a Agência Brasileira de Inteligência(Abin); a Polícia Civil e Militar do Rio, São Paulo e Distrito Federal; o Centro de Inteligência do Exército; e o Ministério Público. A Polícia Federal, como nos aponta Lucas, parece ter obtido um projeto-piloto, de acordo com o relatório:

“O arquivo é vasto e exige uma análise cuidadosa, inclusive de veracidade de cada documento, não sendo possível afirmar, até o momento, se as agências citadas chegaram de fato a adquirir as “soluções” da empresa italiana.

A única exceção parece ser, no entanto, a Polícia Federal, uma vez que a pesquisa nos arquivos, ainda que superficial, revela trocas de e-mails entre agentes e funcionários daHacking Team, relatos sobre treinamentos em Brasília, e diversos documentos, como um certificado de entrega de produto, que confirmam a negociação e aquisição da ‘solução’ RCS (Remote Control System) da Hacking Team para um projeto-piloto de três meses de duração”.

Lucas destaca que a data da entrega, 21 de maio de 2015, coincide com a notícia da Folha de S. Paulo, veiculada pouco mais de um mês antes, de que a Polícia Federal “quer instalar vírus em telefone grampeado para copiar informações”. No certificado de entrega da licença do malware, constam os itens Remote Mobile Installer, e Android e BlackBerrycomo plataformas

suportadas.

Outra empresa notável na indústria da vigilância e que tem ganhado espaço no Brasil, de acordo com Lucas Texeira, é a Harris Corporation, empresa estadunidense que produz o Stingray. Este aparelho é um exemplo de IMSI Catcher, dispositivo que se passa por torre de telefone celular, o que permite obter números identificadores dos dispositivos que ligam ao aparato espião.

De acordo com um documento descrevendo o KingFish, uma versão portátil do aparelho (que cabe numa mala), o sistema “age como uma torre de telefonia móvel e tem a capacidade de encontrar, rastrear e/ou negar serviço de telefonia móvel”, o que torna possível que um aparelho com tamanho potencial intrusivo seja portado pelas Forças Armadas – que já têm firmes relações comerciais com a Harris, que produz “equipamentos e serviços de transmissão via rádio para as forças armadas e polícias de diversos estados”, e tem sedes no Rio de Janeiro (RJ), em São Paulo (SP) e Macaé (RJ).

O membro da Oficina Antivigilância destaca que a utilização de IMSI catchers foi detectada, por exemplo, na Ucrânia, onde os participantes de uma grande manifestação nesse país foram identificados por meio do uso de um desses aparelhos, tendo muitos deles recebido uma mensagem de texto contendo o seguinte: “Caro assinante, você foi cadastrado como participante em um motim em massa”.

Do mesmo modo, surgiram evidências do uso de IMSI catchers para monitorar manifestações nos Estados Unidos. A polícia da cidade de Baltimore, no estado de Maryland (epicentro de grandes manifestações contra a violência policial, desde a morte de Freddie Gray em abril de 2015) recentemente admitiu ter usado mais de 4.300 vezes desde 2007 o Stingray, um IMSI catcher produzido pela Harris Corporation.

Lucas pondera que é difícil estabelecer exatamente em quais situações o dispositivo foi usado, pois seu uso costuma ser mantido sob sigilo – a Harris exigia um acordo de sigilo proibindo os departamentos de mencionarem os Stingrays em seus relatórios e pedidos judiciais.

Dessa forma, o Brasil abre precedentes a uma escalada no aparelhamento estatal por setores ligados ao vigilantismo e mesmo à perseguição de indivíduos ligados a movimentos sociais no Brasil.

“O uso de bloqueadores de celular compartilha com ferramentas de vigilância o fato de ser um equipamento relativamente pequeno e barato, adquirido em tempos de emergência e posteriormente usado em situações onde não são necessários ou proporcionais, ou não seguem o devido processo legal ao ser utilizado sem um mandato judicial ou fora de seu escopo”, conclui o membro da Oficina Antivigilância.

[Fonte: Diário Liberdade, 15 de fevereiro de 2016](#)