

Monitoramento policial em ambiente virtual público não se confunde com infiltração, diz STJ

A atividade de rastreamento de arquivos compartilhados não implica invasão de espaço privado, nem interceptação de comunicações, e dispensa autorização judicial prévia.

Com esse entendimento, a 6ª Turma do Superior Tribunal de Justiça confirmou a legalidade da ronda virtual feita por um software da polícia que identifica imagens de pornografia infantil em redes de troca de arquivos ponto a ponto (P2P) — forma de compartilhamento que não exige um servidor central. Nesses casos, cada computador atua tanto como cliente quanto servidor, sem uma central intermediária.

O colegiado acompanhou o voto do relator, ministro Rogério Schietti Cruz. Os ministros negaram provimento ao recurso apresentado pela defesa de um dentista de Mato Grosso do Sul, denunciado por armazenar pornografia infantil em equipamentos eletrônicos.

A investigação foi conduzida pela Polícia Civil do estado, que utilizou o software **CRC (Child Rescue Coalition)**, ferramenta internacional de uso restrito a agentes públicos certificados, para rastrear IPs associados ao compartilhamento de arquivos ilícitos.

Com base nas informações do software, a polícia obteve mandado de busca e apreensão e localizou equipamentos eletrônicos com imagens pornográficas envolvendo crianças e adolescentes.

Ronda virtual não é infiltração

No STJ, a defesa do réu sustentou que as provas eram ilícitas, argumentando que o uso da ferramenta configuraria **infiltração policial** sem autorização judicial. Os advogados afirmaram ainda que houve quebra indevida de sigilo quando a operadora forneceu dados do titular do IP mediante requerimento da polícia, sem decisão judicial. O réu pediu, por conta disso, o trancamento da ação penal.

Schietti rejeitou os argumentos. Ele explicou que o monitoramento ocorre em ambiente virtualmente público, em que os próprios usuários compartilham arquivos e tornam visíveis seus endereços IP. Para o ministro, ronda virtual não se confunde com a infiltração policial prevista no artigo 190-A do Estatuto da Criança e do Adolescente, como dito pela defesa.

Na infiltração, explica, há a atuação direta de agente oculto em ambiente fechado, voltada a alvos específicos. Já na ronda virtual, o software apenas rastreia automaticamente arquivos em redes abertas, acessando dados que qualquer usuário daquelas plataformas pode visualizar, disse Schietti.

“Não se trata, portanto, de invasão a espaço privado ou interceptação de comunicações, que exigiriam prévia autorização judicial, mas de coleta de informações disponíveis em ambiente compartilhado. Trata-se de ronda contínua que não se direciona a pessoas determinadas, diferentemente do procedimento da infiltração policial”, disse.

Dados cadastrais e de conteúdo

O ministro também afirmou que a requisição de dados cadastrais simples do dono do IP (como nome, filiação e endereço) pode ser feita diretamente pela autoridade policial, conforme o artigo 10, parágrafo 3º, do **Marco Civil da Internet (Lei 12.965/2014)**. Estes dados não estão protegidos pelo sigilo das comunicações e o acesso a eles não exige ordem judicial.

Schietti também ressaltou que a legislação distingue dados cadastrais, que têm caráter objetivo e acesso mais flexível, de dados de conteúdo, que dizem respeito à vida privada e dependem de autorização judicial para acesso.

Com esse entendimento, o colegiado reconheceu a validade das provas e determinou a continuidade da ação penal contra o acusado. O processo tramita sob sigredo de Justiça. *Com informações da assessoria de imprensa do STJ.*





Fonte: <https://conjur.jumps.com.br/2025-out-31/monitoramento-policia-em-ambiente-virtual-publico-nao-se-confunde-com-infiltracao-diz-stj/>