



# Autorizações judiciais para fazer grampo caem 30%

14/10/2008

Desde que o ministro Gilmar Mendes resolveu enfrentar os abusos cometidos contra a privacidade das comunicações, o volume de ordens judiciais determinando às operadoras a interceptação de comunicações telefônicas caiu 30%. A informação é de uma das maiores operadoras brasileiras.

Até dois anos atrás, havia ordem judicial para grampear não só o telefone do investigado mas, em cascata, todos os demais que entrassem em contato com ele. Hoje os juízes pararam com isso.

Ele autoriza de acordo com o pedido. Há quem peça pelo número da linha (IMSI — Internal Mobile Subscriber Identifier), mas há quem peça pelo número de série (IMEI — Internal Mobile Equipment Identifier). A esperteza de pedir o número de série é que o usuário pode trocar de chip quantas vezes quiser que o grampo continua.

Há juizados especiais cíveis, varas de execuções criminais (a quem cabe cuidar de progressão de regime e condições de encarceramento), varas da infância e juventude e mesmo varas do trabalho autorizando grampos. Já houve prisão de advogados de operadoras que se negaram a cumprir ordens que consideraram ilegais.

A senha autorizada pelo juiz, agora, só permite acompanhar o histórico de gravações do telefone do investigado. A quebra de sigilo não alcança, como se noticiou, toda a rede de assinantes. Mas ainda há quem não saiba que a quebra de sigilo, assim como a interceptação, tem reserva de jurisdição — ou seja, dependem de ordem judicial específica e própria.

Outra forma de cobrir a área é pedir o grampo nas ERBs (Estações de Rádio Base), mais usadas em casos de seqüestro. Estações Rádio Base ou ERBs são equipamentos (antenas) que fazem a conexão entre os telefones celulares e a companhia telefônica, ou mais precisamente a Central de Comutação e Controle (CCC). A ERB ou cell site é a denominação dada em um sistema de telefonia celular para a estação fixa com que os terminais móveis se comunicam. A interconexão que a ERB tem com a CCC ou com outras ERBs é que permite a realização das chamadas entre os terminais celulares e deles com os telefones fixos comuns, e vice-versa.

Não existe no Brasil a facilidade do Echelon — o grampo automático, de acordo com a pronúncia de certas palavras ou nomes. Contudo, o software Guardiã, fabricado pela Dígitro, de Santa Catarina, oferece essa facilidade. O Guardiã, em posse de órgãos policiais, secretarias de segurança e do Ministério Público, funciona como um clone da central telefônica, para onde são desviadas as ligações dos números monitorados. O desvio, em pelo menos quatro operadoras, é feito pelo sistema Vigia (fabricado por uma empresa também de Santa Catarina, a Suntech). Uma vez armazenadas no Guardiã, as gravações podem ser verificadas com um sistema de busca. Pode-se localizar pessoas pela sua voz (frequência), independentemente do



telefone que utilizem, ou por palavras pronunciadas.

As operadoras e os serviços policiais asseguram: tanto o Vigia quanto o Guardião só podem ser acionados depois que for preenchido formulário indicando os dados do processo, o número da ordem judicial e demais elementos que respaldem a interceptação. Ou seja, não haveria, tecnicamente, a possibilidade de se trabalhar com grampos clandestinos com o uso dos equipamentos. Esse temor foi levantado quando se levantou a hipótese de donos de operadoras, ou mesmo seus empregados, passarem a fazer seus próprios grampos.

Mas as operadoras estão preocupadas com a instrução do CNJ de que o empregado da operadora que cuidar do grampo deve ser identificado. Elas comparam com o carrasco da idade média, que tinha o rosto encoberto para que ele ou sua família não fossem alvo de vingança dos punidos. Discute-se se a informação da senha do usuário não seria igualmente eficiente e menos prejudicial.

Um caso paradigmático que expõe as divergências dentro do próprio judiciário para a liberação de senhas de acesso ao tráfego de ligações telefônicas é o Habeas Corpus 0468639-9, de março de 2008, concedido pelo Tribunal de Justiça do Paraná atendendo a pedido da gerente da Brasil Telecom em Curitiba. O caso é didático sobre como as concessionárias têm lutado contra o acesso irrestrito a senhas de clientes oficialmente investigados. [Clique aqui para ler o acórdão](#)

No caso, o juiz da Vara de Inquéritos Policiais de Curitiba deu ordem para que a Brasil Telecom franqueasse senha a um delegado de polícia e a um auditor judicial para que os mesmos passem “a ter acesso 24 horas, durante o prazo de seis meses, aos dados cadastrais, localização de ERBs e bilhetagens de telefones que estejam sendo utilizados para a prática de crimes investigados pelo Núcleo de Repressão a Crimes Econômicos, lembrando que a senha deverá ser de âmbito nacional (...).

A defesa alegou que o pedido era genérico e que a ordem concedida pela Justiça não apresentava uma justa causa específica e individual para a concessão da senha. Alega também que não foi demonstrada a individualização dos destinatários da ordem de quebra e que o prazo para cumprimento da ordem é exorbitante.

O Ministério Público também deu parecer contra a liberação das senhas pro entender que “a decisão da autoridade impetrada viola o direito de privacidade e intimidade dos usuários das empresas de telefonia, porque genérica e abrangente, sem delimitar a investigação e os investigados, devendo por isso ser cassada”.

Para a relatora do HC na Segunda Câmara Criminal do TJ do Paraná, juíza convocada Lílian Romero, o acesso ao posicionamento das ERBs permite ao detentor da identificar a localização aproximada do usuário do telefone celular, no momento em que está procedendo a ligação. Para ela

“é indubitável que tal informação pode mostrar-se útil na localização de bandidos em rota de fuga ou em seus esconderijos. Mas também permite que se identifique a localização aproximada de um usuário comum: se está no local de trabalho ou fora dele e onde, na escola, em trânsito, no shopping, etc”.



A juíza faz a distinção da bilhetagem, que “consiste na emissão de um relatório ou listagem contendo todas as ligações feitas pelo usuário num determinado período de tempo, contendo: os números dos terminais para os quais foram feitas e dos quais foram recebidas ligações, a data, o horário e duração da chamada”.

Para a relatora, o acesso irrestrito burla a liberdade de ir e vir. “As mesmas informações, por outro lado, possibilitam também a identificação de todo o círculo de relações de qualquer cidadão, inclusive, por exemplo, de um homem casado com mulheres solteiras, sujeitando-o a chantagens e extorsão em caso de vazamento da informação. Ao contrário do que sustenta o Juiz impetrado, o direito de sigilo não se restringe ao teor das conversas telefônicas mas também aos números para os quais o usuário ligou, os horários e duração das chamadas”.

Ela acrescenta ainda que o sigilo das comunicações não é absoluto, e não pode servir para acobertar a prática de crimes. Mas a quebra do sigilo só pode ser feita se devidamente fundamentada. E no caso, a ordem do juiz de primeiro grau, não é apenas exorbitante, como mal fundamentada.

Acompanharam a relatora, o desembargador José Maurício Pinto de Almeida e o juiz convocado Carlos Augusto Altheia de Mello, em sessão presidida pelo desembargador Noeval de Quadros.

Fonte: [https://conjur.jumps.com.br/2008-out-14/autorizacoes\\_judiciais\\_grampo\\_caem\\_30/](https://conjur.jumps.com.br/2008-out-14/autorizacoes_judiciais_grampo_caem_30/)