

Justiça Comentada: Constituição protege inviolabilidade de celulares

Spacca

A proteção aos direitos fundamentais não pode ser utilizada como instrumento para a prática de atividades ilícitas, ou seja, como um verdadeiro escudo protetivo para a criminalidade, mas, igualmente, não pode ser enfraquecida com a genérica alegação de necessidade de garantia da segurança pública, sob pena de eficácia zero da Constituição Federal, com a transformação de seu texto em letra morta.

A interpretação para solucionar essa conflituosa relação deve se utilizar do princípio da concordância prática ou da harmonização, de forma a coordenar e combinar os bens jurídicos em conflito, evitando o sacrifício total de uns em relação aos outros, realizando uma redução proporcional do âmbito de alcance de cada qual (contradição dos princípios), sempre em busca do verdadeiro significado da norma e da harmonia do texto constitucional com suas finalidades precípuas.

No último 25 de junho, a Suprema Corte dos Estados Unidos solucionou na prática, em relação a dados existentes em celulares, essa importante discussão teórica, pois, em decisão unânime, entendeu que a Polícia e os órgãos de segurança nacional devem obter mandados judiciais para a realização de buscas em telefones celulares de pessoas presas, independentemente do motivo.

O *Chief Justice*, John Robert, relator do voto em nome da corte, afirmou que não é possível sacrificar os direitos individuais dos cidadãos em nome da garantia genérica de segurança pública, lembrando que um dos grandes motivos da Independência Americana foi a revolta popular contra a existência de mandados genéricos de busca e apreensão, que permitiam as forças inglesas o ingresso em residências em busca desenfreada de quaisquer provas para comprovação de qualquer ilícito.

Especificamente, em relação à telefonia celular, o Presidente da Suprema Corte Americana relatou que aproximadamente 90% dos norte-americanos possuem aparelhos e que 75% dos usuários de *smartphones* declararam que deles não se separam, pois, em média, possuem 33 aplicativos em seu dispositivo, de maneira que “cada usuário cria uma grande fonte de informações sobre a própria vida, desde assuntos médicos, lugares onde vai, pessoas com as quais contata por voz ou por texto e intimidades”, concluindo que “o fato de que a tecnologia permite a uma pessoa carregar tantas informações em suas mãos, não torna os dados no celular menos dignos de proteção do que os fatos pelos quais os Fundadores da Nação lutaram”.



Essa importante discussão tem lugar no ordenamento jurídico brasileiro, em especial na proteção constitucional à inviolabilidade à honra, intimidade e vida privada (CF, artigo 5º, X) e nas inviolabilidades as correspondências, comunicações telegráficas, de dados e telefônicas (CF, artigo 5º, XI), bem como nos dispositivos da Lei 9.296/96, que introduziu a proteção aos dados telemáticos, hoje tão comuns nos celulares e *smartphones*, e seus diversos aplicativos, inclusive o armazenamento de dados de mensagens eletrônicas, como bem observado pela Suprema Corte Americana.

A Constituição Federal determina ser inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas. No caso, porém, da inviolabilidade das interceptações telefônicas, a própria Constituição Federal, no inciso XII, do artigo 5º, abriu uma exceção expressa, exigindo para sua aplicação a presença de três requisitos: ordem judicial, finalidade de investigação criminal ou instrução processual penal e hipóteses e forma estabelecidas na lei.

A ausência da edição da necessária lei estabelecendo as hipóteses e formas permissivas para as interceptações telefônicas fez com que o STF reiteradas vezes julgasse a utilização desse meio de prova como ilícito, tornando-o, bem como todas as provas dela derivadas, inadmissíveis no processo. O Congresso Nacional para resolver essa questão editou a Lei 9.296, de 24 de julho de 1996, aproveitando para regulamentar a possibilidade de interceptação do fluxo de comunicações em sistemas de informática e telemática, mediante os requisitos previstos nessa mesma lei, ou seja, mediante os mesmos requisitos exigidos para a interceptação telefônica.

Note-se, portanto, que o legislador condicionou a quebra do sigilo de dados telemáticos, hoje comumente presentes em computadores e nos telefones celulares e *smartphones*, com seus diversos aplicativos, aos mesmos requisitos constitucionalmente exigidos para o afastamento do sigilo telefônico, sob pena da imprestabilidade da prova obtida em face de sua ilicitude.

Em virtude dessa equiparação protetiva, passou-se, então, à discussão da possibilidade da referida lei regulamentar a interceptação do fluxo de comunicações em sistemas de informática e telemática, uma vez que sua ementa diz: “Regulamenta o Inciso XII, Parte Final, do artigo 5º da Constituição Federal”, e os requisitos constitucionais mais rígidos foram expressa e diretamente direcionados para as interceptações telefônicas. Alguns doutrinadores entenderam possível essa ampliação, como por exemplo, Luiz Flávio e Raúl Cervini, na obra *Interceptação telefônica*, e Lenio Streck em *As interceptações telefônicas e os direitos fundamentais*, enquanto Vicente Greco Filho, em sua obra *Interceptação telefônica*, entendeu ser inconstitucional essa extensão. O Supremo Tribunal Federal posicionou-se pela validade da norma (STF, ADI 1.488/9/DF).

Note-se que a simples existência de lei não se afigura suficiente para legitimar a intervenção no âmbito dos direitos e liberdades individuais, pois absolutamente necessário que as restrições impostas sejam proporcionais, isto é, que sejam adequadas e justificadas pelo interesse público e atendam ao critério da razoabilidade, de maneira a observar também a legitimidade dos objetivos perseguidos pelo legislador e a necessidade de sua utilização, para que sempre haja verdadeira ponderação entre a restrição a ser imposta aos indivíduos e os objetivos pretendidos pelo Estado.

Na presente hipótese, desde a edição da lei, sempre nos posicionamos pela plena validade da extensão

legal, uma vez que garantiu maior proteção às comunicações telemáticas, e conseqüentemente, maior respeito à intimidade e vida privada, direitos fundamentais amplamente tutelados, não somente por nosso ordenamento jurídico, mas também pela Convenção Europeia de Direitos Humanos, que em seu artigo 8.1 tutela a vida privada do indivíduo, assegurando que “toda pessoa tem direito ao respeito de sua vida familiar, do seu domicílio e da sua correspondência”, interpretado o termo “correspondência”, à partir do caso *Klass vs. Alemanha*, em sentença de 6 de agosto de 1978 da Corte Europeia de Direitos Humanos, de maneira extensiva a todas as formas de comunicação privada — inclusive as correspondências eletrônicas — e não somente a correspondência epistolar, objeto principal do referido dispositivo legal da Convenção, editada em 1950, quando ainda não existiam as comunicações telemáticas.

E assim nos posicionamos, em primeiro lugar, porque a interpretação do texto da Constituição Federal exige que a uma norma constitucional seja atribuído o sentido que maior eficácia lhe conceda, sendo vedada a interpretação que lhe suprima ou diminua a finalidade, na hipótese, a proteção das inviolabilidades públicas, sem que com isso fosse possível sua utilização para a prática de atividades criminosas.

Portanto, apesar de a exceção constitucional (CF, artigo 5º, XI, *in fine*) expressamente referir-se somente à interceptação telefônica, nada impede que nas outras espécies de inviolabilidades haja possibilidade de relativização da norma constitucional, por exemplo, na permissão da gravação clandestina com autorização judicial, nas possibilidades de interceptação de correspondência, entre outras hipóteses, pois não há dúvidas de que nenhuma liberdade individual é absoluta, sendo possível, respeitados certos parâmetros, a interceptação das correspondências, das comunicações e de dados, sempre que essas liberdades públicas estiverem sendo utilizadas como instrumento de salvaguarda de práticas ilícitas, pois, “afirmar que um direito é absoluto significa que ele é inviolável pelos limites que lhe são assinalados pelos motivos que o justificam” (TJ-SP, MS 13.176/02/SP). Portanto, a regra permanece a inviolabilidade, sendo excepcional a possibilidade de quebra dos sigilos tutelados pela Carta Magna, observados estritos requisitos.

Em segundo lugar, porque o fato de a ementa da lei afirmar somente que “regulamenta o Inciso XII, Parte Final, do artigo 5º da Constituição Federal”, de forma alguma impede que o texto legal discipline outros assuntos — inclusive a proteção às comunicações telemáticas — uma vez que a lei que veicula matéria estranha ao enunciado constante de sua ementa, por só esse motivo, não ofende nenhum postulado constitucional, não vulnerando tampouco as regras de processo legislativo constitucional, pelo que excluída da possibilidade de declaração de inconstitucionalidade (STF, ADI 1.096/4), pois inexistente no vigente sistema de direito constitucional brasileiro regra idêntica à prevista pelo artigo 49 da Constituição Federal de 1934: “Os projectos de lei serão apresentados com a respectiva ementa, enunciando, de fôrma succinta, o seu objectivo, e não poderão conter matéria estranha ao seu enunciado”.

A proteção à inviolabilidade de dados telemáticos existentes em computadores e aparelhos celulares e *smartphones*, portanto, segue a proteção prevista na parte final do inciso XI, do artigo 5º, pois inexistente qualquer inconstitucionalidade da norma de extensão prevista no parágrafo único do artigo 1º da Lei 9.296, de 24 de julho de 1996, que expressamente determina “o disposto nesta Lei aplica-se à interceptação do fluxo de comunicação em sistemas de informática e telemática”, devendo, portanto, existir rigorosa e estrita observância de todos os requisitos constitucionais e legais para o afastamento do sigilo constitucional e legalmente protegido nessas hipóteses, sob pena de ilicitude da prova obtida e seu

expurgo imediato do processo, com a responsabilização daqueles que a obtiveram irregularmente.

Date Created

27/06/2014