2020 | JUNHO

PAULO HENRIQUE ATTA
THIAGO MORAES

RELATÓRIO RESUMIDO SOBRE O JULGAMENTO DA ADPF Nº 403 E DA ADI Nº 5.527

O CASO WHATSAPP

Em 26 e 27 de maio de 2020, o Supremo Tribunal Federal (STF) iniciou o julgamento dos seguintes processos constitucionais: Ação Direta de Inconstitucionalidade - **ADI nº 5.527,** e Arguição de Descumprimento de Preceito Fundamental - **ADPF nº 403**. Embora com solicitações relativamente diferentes, ambas as ações visavam discutir a interpretação dos **artigos 10 e 12 do Marco Civil da Internet - MCI**, à luz dos direitos fundamentais de comunicação e liberdade de expressão, garantidos pela Constituição Federal (CF), artigo 5º, número IX [1]

Esses casos foram motivados por sucessivos eventos de suspensão do serviço do aplicativo de mensagens instantâneas Whatsapp, conforme determinado por diferentes juízes estaduais. Em um dos casos mais notórios, em 2016, um juiz do estado de Sergipe ordenou que a empresa divulgasse os registros de conversas trocadas entre réus de investigação criminal, quebrando o sigilo de suas comunicações. A empresa negou a solicitação e, com base no MCI, Artigo 12, Inciso III [2], o juízo local decidiu suspender as atividades do serviço no Brasil por 72 horas.

Durante o julgamento atual, a empresa Whatsapp Inc. alegou que o bloqueio do aplicativo móvel em todo o território brasileiro prejudicaria os direitos de liberdade de comunicação e de expressão de cidadãos. Além disso, alegou não poder acessar os dados das mensagens trocadas entre seus usuários, devido à implementação da criptografia de ponta a ponta em seus serviços de comunicação. Assim, não foi possível cumprir a ordem judicial.

Assistido pelo Laboratório de Políticas Públicas e Internet - LAPIN, o Instituto Beta para Internet e Democracia - IBIDEM, figurou como *amicus curiae* no presente caso. Durante o julgamento, enfatizou que as sanções estabelecidas no MCI deveriam ser aplicadas apenas se a empresa demandada agisse contra os direitos de seus usuários à privacidade e à proteção de dados. Portanto, punir uma empresa por não colaborar em uma investigação criminal estava além do escopo da norma discutida.

A **Ministra Rosa Weber**, relatora da **ADI nº 5527**, elogiou o MCI por seus mecanismos de proteção aos direitos fundamentais de privacidade e proteção de dados. Ela destacou o papel central das comunicações em rede e smartphones na vida contemporânea e a relevância da proteção da privacidade nesse contexto. Assim, uma tentativa de violar a privacidade dos usuários sem salvaguardas legais (por exemplo, enviando esses dados a funcionários públicos sem o devido processo legal) pode prejudicar a segurança de suas informações pessoais, expondo-os a usuários mal-intencionados.

Avançando, a Ministra explicou que o **direito à privacidade,** protegido pela Constituição Brasileira, **não deve ser interpretado apenas como o direito de ser deixado em paz** (*right to be left alone*), um aspecto negativo desse direito, o qual permite que um indivíduo proteja sua vida pessoal de olhos alheios. Mais que isso,

a proteção da privacidade é um fator essencial da sociedade contemporânea e qualquer invasão injustificada deve ser evitada e punida, mesmo que essa invasão se origine do Estado.

Além disso, **o sigilo da comunicação privada está estritamente conectado ao direito à privacidade.** Este direito ao sigilo é apenas temporariamente diminuído por uma ordem judicial que esteja de acordo com o devido processo legal. E mesmo assim, os direitos fundamentais e limitações técnicas da empresa que processa dados pessoais do réu devem ser respeitados ao processar a ordem judicial.

De acordo com a Ministra Weber, o artigo 10 do MCI [3] concede uma estrutura normativa apta a garantir o direito fundamental à privacidade de acordo com a Constituição. No entanto, se a empresa que fornece o serviço de mensagens instantâneas não puder acessar os dados do conteúdo devido às técnicas adotadas para fornecer segurança e privacidade ao usuário, como criptografia de ponta a ponta, a impossibilidade de cumprir uma ordem judicial não significa agir contra a lei. Além disso, exigir que essas empresas implementem ***backdoors*** para permitir o cumprimento da ordem judicial significa expor esses dados a **riscos desnecessários de violação de dados**.

Por fim, a Ministra Weber decidiu que, de acordo com o MCI, as sanções de suspensão e proibição de serviço devem ser aplicadas apenas se a empresa agir contra os direitos à privacidade e à proteção de dados e não ao desobedecer uma ordem judicial de uma investigação criminal, desde que haja uma razão justificada para a não conformidade.

Por sua vez, o **Ministro Edson Fachin**, relator da **ADPF nº 403**, estruturou seu voto com base na seguinte pergunta: o risco público relacionado à implementação da criptografia justifica sua proibição ou, ainda, a criação de meios excepcionais para acessar os dados dos usuários (ou seja, backdoor), reduzindo assim o nível de proteção nos serviços de comunicação?

Em um elaborado voto de 76 páginas, o Ministro declarou que todos os direitos concedidos aos cidadãos offline devem ser igualmente protegidos online. Em outras palavras, os **direitos digitais também são direitos fundamentais.** Na Internet, a privacidade não é apenas uma questão de intimidade, mas também uma ferramenta de salvaguarda da liberdade de expressão. Portanto, qualquer tentativa de reduzir esse direito à privacidade, mesmo que momentaneamente, deve ser fundamentada e seguir o devido processo legal. Qualquer invasão que não siga essas etapas é, portanto, ilegal. Referindo-se ao LAPIN e ao Instituto de Tecnologia e Sociedade - ITS-Rio (outro *amicus curiae* do caso), ele destacou que o **MCI visa fazer valer os direitos de proteção de dados**.

A tecnologia de criptografia surgiu como uma resposta dos cidadãos para proteger sua privacidade contra invasões. É verdade que a implementação dessa tecnologia cria alguns riscos, como custos extras de investigações criminais. Isso

ocorre porque a criptografia reduz a capacidade de monitoramento e interceptação, medidas amplamente aplicadas durante esses inquéritos..

No entanto, o Ministro Fachin alertou que qualquer tentativa de contornar essa tecnologia implementando *backdoors* ou ataques do tipo "*man-in-the-middle*" cria violações de segurança em massa. Portanto, os riscos relacionados ao uso da criptografia são superados pelos riscos relacionados à implementação da interceptação em massa. Qualquer **proibição de criptografia de ponta a ponta é inconstitucional,** porque essa ordem prejudicaria desproporcionalmente os cidadãos mais vulneráveis.

O julgamento, apesar de não ter encerrado, já representa um marco significativo na história da Privacidade e Proteção de Dados no Brasil. Uma declaração fundamental já foi pronunciada: **a criptografia é um aliado fundamental na proteção dos direitos digitais** e, portanto, qualquer tentativa de reduzi-la seria contra a democracia e instituiria um estado de vigilância.

---

[1] *Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:*

IX - é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença;

[2] *Art. 12. Sem prejuízo das demais sanções cíveis, criminais ou administrativas, as infrações às normas previstas nos arts. 10 e 11 ficam sujeitas, conforme o caso, às seguintes sanções, aplicadas de forma isolada ou cumulativa:*

III - suspensão temporária das atividades que envolvam os atos previstos no art. 11; (grifo nosso).

[3] *Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.*

§ 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do

usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º . (grifo nosso).