

Sustentação do Instituto de Tecnologia e Sociedade (ITS Rio) no julgamento dos casos de bloqueio de WhatsApp no STF (27.05.2020)

Excelentíssimo Ministro Luiz Edson Fachin, relator da ADPF 403,
Excelentíssima Ministra Rosa Weber, relatora da ADI 5527,
Excelentíssimos Ministros desta Eg. Corte,
Excelentíssimos Membros da AGU, da PGR e demais colegas advogados.

Em nome do Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS Rio), gostaria de agradecer pela oportunidade de me dirigir a V.Exas. no contexto das referidas ações e na qualidade de *amicus curiae*. O presente caso é de importância ímpar para o futuro da Internet no Brasil e seus contornos são ainda mais asseverados por conta do combate à Covid-19 e à digitalização acelerada que todos vamos experimentando nas mais diversas atividades. O Judiciário não é exceção, como esse próprio julgamento atesta.

O objeto impugnado na presente ADPF é a ameaça de lesão ao preceito fundamental disposto no art. 5º, IX, da Constituição Federal de 1988, qual seja, o direito às liberdades de expressão e de comunicação, por meio de decisões judiciais proferidas com base em uma interpretação equivocada dos artigos 10, 11 e 12 da Lei 12.965/14 (Marco Civil da Internet), impondo o bloqueio de aplicativo que viabiliza a troca de mensagens e conteúdos entre diversos usuários. A ADI, por seu turno, discute a constitucionalidade do artigo 12, III e IV, do Marco Civil da Internet.

O ITS Rio gostaria de trazer como contribuição para o julgamentos dos referidos casos por essa Eg. Corte os cinco pontos a seguir, rapidamente mencionados.

1. O Marco Civil da Internet não prevê o bloqueio de aplicações. Ainda mais por descumprimento de ordem judicial.

As decisões judiciais que ordenam o bloqueio de aplicações não podem ser baseadas no Marco Civil da Internet, visto que tal medida não se encontra prevista em nenhum dos dispositivos da Lei.

O título conferido pelo legislador ao Capítulo III da Seção II do Marco Civil da Internet não poderia ser mais claro: “Da Proteção aos Registros, aos Dados Pessoais e às Comunicações Privadas”. De pronto, resta evidente que os artigos nele constantes (os artigos 10, 11 e 12) referem-se à proteção aos registros, aos dados pessoais e às comunicações privadas. As sanções para quem viola as leis brasileiras sobre privacidade e proteção de dados constam do artigo 12.

A aplicação das sanções do artigo 12, notadamente em seus incisos III (suspensão) e IV (proibição) não se destinam à suspensão e à proibição do funcionamento de um aplicativo ou de uma atividade empresarial como um todo. O seu destino é bastante específico e tanto decorre da própria redação dos incisos mencionados. Trata-se de sanções que levam à suspensão ou proibição “das atividades que envolvam os atos previstos no artigo 11”. E que atividades

são essas? “A coleta, armazenamento, guarda e tratamento de registros de dados pessoais ou de comunicações”.

São esses os atos previstos no artigo 11. Logo, a ampliação desses dispositivos para o bloqueio de aplicações como um todo representa um esgarçamento da letra legal para finalidades que com ela são claramente incompatíveis. Não se trata de suspensão de sites ou de aplicativos, mas sim das atividades de coleta e de tratamento de dados para aquele que não cumpre a legislação nacional sobre o tema.

Não apenas o Marco Civil da Internet não se dispõe a servir como fundamento para o bloqueio de aplicações, como ainda mais equivocada é a utilização dos mesmos dispositivos para o bloqueio de aplicações por conta do *não cumprimento de ordens judiciais*. Esse raciocínio está eivado de um duplo equívoco: 1) ele usa o Marco Civil da Internet para bloquear aplicativos, o que a Lei não ampara; e 2) o faz para casos de bloqueios motivados pelo descumprimento de ordem judicial, tema muito distante da proteção da privacidade e dos dados pessoais que anima as sanções previstas no artigo 12 da Lei nº 12.965/14.

2. O Marco Civil da Internet destaca a proteção da liberdade de expressão.

O descompasso entre o bloqueio de aplicações e a própria redação do Marco Civil da Internet é ainda maior quando se perceber o papel que a liberdade de expressão desempenha na Lei nº 12.965/14.

Essa percepção pode ser retirada das cinco vezes em que o tema da liberdade de expressão aparece no texto legal. **1)** A disciplina do uso da Internet no Brasil tem a liberdade de expressão como o seu **fundamento**, conforme dispõe o artigo 2º; **2)** Logo em seguida, no artigo 3º, a sua garantia aparece como **princípio** dessa mesma disciplina; **3)** O artigo 8º, por sua vez, afirma que a proteção da liberdade de expressão é condição para o pleno exercício do direito de acesso à rede; **4)** No que diz respeito aos danos causados na Internet e a consequente **responsabilização** de seus agentes, a liberdade de expressão desempenha ainda dois relevantes papéis. O caput do artigo 19, que estabelece a regra para responsabilização dos provedores de aplicações de Internet, é iniciado com a expressão “com o intuito de assegurar a liberdade de expressão e impedir a censura.”; e **5)** Com relação aos danos causados aos **direitos autorais** na Internet, o Marco Civil, no parágrafo segundo do mesmo artigo 19, afirma ainda que a aplicação do regime de responsabilização por ele determinado depende de previsão legal específica. Embora essa redação desloque o tratamento do tema para outro processo de alteração legislativa, é importante destacar que, segundo o dispositivo mencionado, essa nova legislação específica deverá “respeitar a liberdade de expressão e demais garantias previstas no art. 5º da Constituição Federal”.

No contexto da ADPF 403, resta claro que o Marco Civil da Internet busca conferir ampla efetividade às liberdades comunicativas através dos cinco papéis que a liberdade de expressão desempenha dentro da própria lei. Sendo assim, é

notoriamente contraditório ao próprio texto do Marco Civil da Internet querer tirar dele uma medida de bloqueio que interfere sensivelmente no exercício da liberdade de expressão de milhões de brasileiros.

3. Combater os usos ilícitos de uma tecnologia não significa combater a tecnologia em si.

Chamamos ainda atenção para o fato de que os casos em tela podem levar o debate a se alargar, questionando mesmo a existência de aplicativos que permitem a criptografia ponta-a-ponta no País. Essa ampliação do escopo dos casos seria perigosa pois abre flancos para uma confusão entre o uso ilícito que se faz da tecnologia e a tecnologia em si.

É preciso separar a tecnologia da forma pela qual ela é usada. Criminosos podem usar um app de mensagens criptografadas para conversar? Claro que sim, mas isso não transforma a tecnologia em algo ilícito, assim como os golpes por telefone que fingem sequestros de parentes não fazem da telefonia uma tecnologia fora da lei.

4. A interceptação telemática é apenas uma das diversas ferramentas para o sucesso de uma investigação

Embora não seja esse o foco das presentes ações, vale destacar um ponto sobre o tema das investigações e das interceptações telemáticas, que ganhou vulto na audiência pública e em algumas manifestações nos autos.

Nesse sentido, cabe fugir da conclusão de que a interceptação das comunicações é o recurso que, por excelência, deve ser buscado em uma investigação. Os meios digitais de comunicação trazem uma enorme gama de hipóteses que podem ser exploradas para o sucesso de investigações, como 1) acesso a meta-dados que podem ser bastante reveladores, como número de telefone usado, data e hora do acesso à aplicação; 2) busca e apreensão dos aparelhos celulares e demais dispositivos usados na comunicação; 3) infiltração de agentes em grupos para a troca de mensagens; ou mesmo, 4) dentro dos estritos limites legais, a instalação de *spywares* em celulares de investigados ou outras medidas que são debatidas globalmente como *“lawful hacking”*.

5. Novos tempos não pedem menos, mas sim mais criptografia

Além disso, a criptografia que protege as comunicações no WhatsApp é a mesma técnica que garante a segurança dos serviços bancários e comerciais na rede. Quanto mais o mundo se torna digital, especialmente a partir do combate à Covid-19, mais importante é preservar a criptografia como um elemento fundamental para garantir a segurança das comunicações.

Sem ela, fragilizamos um componente fundamental desse novo mundo, cada mais digital, que estamos construindo. A recente polêmica sobre vulnerabilidades de um aplicativo que estava sendo largamente utilizado para atividades mais

distintas como *homeschooling* de colégios até importantes reuniões governamentais teve a criptografia em seu cerne.

Esperamos assim que o STF não consagre o bloqueio de aplicações como parte da cultura jurídica no Brasil, o que levaria a uma onda de decisões determinando a suspensão de aplicativos populares como forma de forçar o cumprimento de decisões que muitas vezes são tecnologicamente impossíveis ou que afetam direitos de outras tantas pessoas que nenhuma relação guardam com o processo judicial em questão.

Em síntese:

- 1. O Marco Civil da Internet não prevê o bloqueio de aplicações. Ainda mais por descumprimento de ordem judicial.*
- 2. O Marco Civil da Internet destaca a proteção da liberdade de expressão.*
- 3. Combater os usos ilícitos de uma tecnologia não significa combater a tecnologia em si.*
- 4. A interceptação telemática é apenas uma das diversas ferramentas para o sucesso de uma investigação.*
- 5. Novos tempos não pedem menos, mas sim mais criptografia.*