



SUMÁRIO

DIREITO CONSTITUCIONAL.....	1
1. Direitos e garantias fundamentais e decisão judicial de suspensão temporária de serviços de mensagens	1
1.1. Situação FÁTICA.....	2
1.2. Análise ESTRATÉGICA.....	2
PARA TESTAR SEU CONHECIMENTO.....	10
2. QUESTÕES.....	10
2.1. Questões objetivas: CERTO ou ERRADO.	10
2.2. Gabarito.....	11

DIREITO CONSTITUCIONAL

1. Direitos e garantias fundamentais e decisão judicial de suspensão temporária de serviços de mensagens
-

AÇÃO DIRETA DE INCONSTITUCIONALIDADE e ARGUIÇÃO DE DESCUMPRIMENTO DE PRECEITO FUNDAMENTAL

Os arts. 10, § 2º, e 12, III e IV, da Lei 12.965/2014 (Marco Civil da Internet) podem ser utilizados para fundamentar justificar decisões judiciais que determinaram a suspensão temporária de serviços de mensagens entre

usuários da Internet como sanção pelo descumprimento, por parte de empresa responsável pelo aplicativo, de ordem judicial de disponibilização do conteúdo das comunicações?

ADI 5527/DF, rel. Min. Rosa Weber, julgamento em 27 e 28.5.2020 e ADPF 403/SE, rel. Min. Edson Fachin, julgamento em 27 e 28.5.2020.

1.1. Situação FÁTICA.

O Plenário **iniciou** o julgamento (**NÃO concluiu**) conjunto de arguição de descumprimento de preceito fundamental (ADPF) e de ação direta de inconstitucionalidade (ADI) ajuizadas em face dos arts. 10, § 2º, e 12, III e IV, da Lei 12.965/2014 (Marco Civil da Internet).

Esses dispositivos têm sido invocados para justificar decisões judiciais que determinaram a suspensão temporária de serviços de mensagens entre usuários da Internet como sanção pelo descumprimento, por parte de empresa responsável pelo aplicativo, de ordem judicial de disponibilização do conteúdo das comunicações. Você sabe: juiz manda bloquear WhatsApp no Brasil todo porque o Facebook (dono do aplicativo) não quebra o sigilo da comunicação via aplicativo.

1.2. Análise ESTRATÉGICA.

1.2.1. Questão JURÍDICA.

Lei 12.965/2014: "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. § 2º O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º."

*Lei 12.965/2014: "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: I – advertência, com indicação de prazo para adoção de medidas corretivas; II – multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício, excluídos os tributos, considerados a condição econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção; III – **suspensão temporária das atividades** que envolvam os atos previstos no art. 11; ou IV – proibição de exercício das atividades que envolvam os atos previstos no art. 11."*

Parágrafo único. Tratando-se de empresa estrangeira, responde solidariamente pelo pagamento da multa de que trata o caput sua filial, sucursal, escritório ou estabelecimento situado no País.”

Lei 12.965/2014: “Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: (...) II – inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei; III – inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;”

Lei 12.965/2014: “Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios: (...) II – proteção da privacidade;”

Lei 12.965/2014: “Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento. § 1º Ordem judicial poderá obrigar, por tempo certo, os provedores de aplicações de internet que não estão sujeitos ao disposto no caput a guardarem registros de acesso a aplicações de internet, desde que se trate de registros relativos a fatos específicos em período determinado. § 2º A autoridade policial ou administrativa ou o Ministério Público poderão requerer cautelarmente a qualquer provedor de aplicações de internet que os registros de acesso a aplicações de internet sejam guardados, inclusive por prazo superior ao previsto no caput, observado o disposto nos §§ 3º e 4º do art. 13. § 3º Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo. § 4º Na aplicação de sanções pelo descumprimento ao disposto neste artigo, serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência.”

1.2.2. Pode bloquear (ADI)?

R: Pode NÃO!

Segundo a Relatora da ADI, Ministra Rosa Weber as penalidades de suspensão temporária e de proibição das atividades somente podem ser impostas aos provedores de conexão e de aplicativos de internet nos casos de descumprimento da legislação brasileira quanto à coleta, guarda, armazenamento ou tratamento dos dados, bem como de violação dos direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.

Desse modo, fica **AFASTADA** qualquer exegese que estenda a sua hipótese de incidência de modo a abarcar o sancionamento de inobservância de ordem judicial de disponibilização de conteúdo de comunicações passíveis de obtenção tão só mediante fragilização deliberada dos mecanismos de proteção da privacidade inscritos na arquitetura da aplicação.

Aliás, o poder estatal de determinar a disponibilização do conteúdo de mensagens no âmbito de investigação criminal ou da instrução processual penal

NÃO conduz à conclusão de ser ilegal o oferecimento de serviço que adote tecnologia que torne inacessível o conteúdo das mensagens ao próprio provedor da plataforma.

É portanto lícito o uso, nas comunicações privadas, de tecnologias de proteção do sigilo e da segurança das comunicações, notadamente das tecnologias criptográficas, ainda que **tornam materialmente inviável** o cumprimento, pela plataforma, de eventual *comando judicial de disponibilização do conteúdo de comunicações privadas*.

Isso porque, uma vez desenvolvida e adotada tecnologia voltada a garantir a segurança e a privacidade das comunicações, e oferecida essa tecnologia como valor agregado aos particulares que contratam seus serviços, **não pode o Estado compeli-lo a oferecer um serviço menos seguro e vulnerável, sob o pretexto de que pode vir, eventualmente, a utilizar essa vulnerabilidade artificial, para cumprir ordem judicial**. Isso significaria tornar ilegal a criptografia, ou pelo menos alguns de seus usos.



As ordens judiciais de bloqueio partem da **PREMISSA** de que houve o **descumprimento anterior de uma primeira ordem judicial** que determinou o *fornecimento do conteúdo das comunicações*. Acontece que, ao serem decretados, os **bloqueios comprometem o exercício, por milhões de brasileiros, das liberdades fundamentais de expressão e de comunicação asseguradas pelo texto constitucional**, causam verdadeira comoção social, e **perturbam** relações familiares, transações comerciais, reuniões de negócios e notificações de atos processuais do próprio Poder Judiciário.



O CNJ já autorizou a utilização de intimação por WhatsApp, o que vem sendo utilizado pelos juízes especialmente nos CEJUSCs e nos Juizados Especiais — vide Procedimento de Controle Administrativo (PCA) nº 0003251-94.2016.2.00.0000.

Ainda segundo a Ministra Rosa Weber, as ordens judiciais de bloqueio de aplicativos de mensagens fazem invocação indevida do Marco Civil da Internet brasileira para a prática de atos (bloqueio) que **NÃO são amparados por essa norma**. Essa interpretação equivocada da lei **não conduz à inconstitucionalidade dos referidos dispositivos, mas inquina de vício o ato assim praticado**, passível de correção pelas vias próprias do devido processo legal.



A capacidade das pessoas de escolherem livremente as informações que pretendem compartilhar, as ideias que pretendem discutir, o estilo de linguagem empregado e o meio de comunicação integram o pleno exercício das liberdades de expressão e de comunicação. O conhecimento de que a comunicação é *monitorada por terceiros* interfere em todos esses elementos componentes da liberdade de informação: os cidadãos podem mudar o modo de se expressar ou até mesmo absterem-se de falar sobre certos assuntos, no que a doutrina designa por efeito inibitório sobre a liberdade de expressão.

A Constituição Federal qualifica como invioláveis (na condição de direitos fundamentais da personalidade) a intimidade, a vida privada, a honra e a imagem das pessoas, conferindo-lhes especial proteção, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação (CF, art. 5º, X).

Tal como a liberdade de manifestação do pensamento (e seus desdobramentos como a liberdade de expressão intelectual, artística e científica e a liberdade de imprensa), o assim chamado **direito à privacidade** (e os seus consectários: direito à intimidade, à honra e à imagem) também emana do reconhecimento de que *a personalidade individual merece ser protegida em todas as suas manifestações*.

A privacidade, isto é, o “direito a ser deixado em paz”, merece proteção adequada e efetiva do ordenamento jurídico.

A proteção da privacidade também é uma característica ESTRUTURAL indispensável das sociedades democráticas.

Tanto o reconhecimento de uma (1) esfera de privacidade imune à ingerência quanto a (2) garantia de salvo-conduto à palavra proferida

surgiram, na história do constitucionalismo moderno, como **fatores de limitação do poder das autoridades** constituídas sobre os cidadãos.

Ora, qual é a utilidade da liberdade de expressão, se aos cidadãos não for assegurada uma esfera de intimidade privada, livre de ingerência externa, um lugar onde o pensamento independente e novo possa ser gestado com segurança?

Lembrando que o escopo dessa proteção são os *assuntos pessoais*, em relação aos quais **não se vislumbra interesse público legítimo na sua revelação**, e que o indivíduo prefere manter privados. A invasão injustificada da privacidade individual é que deve ser repreendida e, tanto quanto possível, prevenida.

Portanto, NÃO podem a **hermenêutica constitucional** e o **desenvolvimento legislativo** ficar **alheios às mudanças no tempo**, tendo em vista a manutenção do **equilíbrio entre proteção da privacidade e os limites da atuação do Estado**. É que a **Constituição, assim como o estado da técnica, institui um conjunto de restrições à atuação estatal**. É a combinação de *constrangimentos tecnológicos* e *constrangimentos legais* que define, em um dado momento, as restrições efetivamente enfrentadas pelo Estado, caso este deseje intervir em determinado aspecto do domínio privado de um cidadão.



A **Constituição escrita no mundo analógico** deve ser traduzida para o **mundo digital**, resguardando os interesses, os direitos e as liberdades previstos originalmente. Desse modo, o **sentido das palavras da Constituição**, o alcance da proteção constitucional, é preservado em face da mudança do contexto.

A cada estágio do desenvolvimento tecnológico, em que se torna materialmente possível a imposição de níveis de controle cada vez maiores sobre diferentes aspectos das vidas das pessoas, renova-se a questão a ser respondida pelas Cortes quanto a **permitir que esses espaços sejam preenchidos com incremento do poder estatal**, ou com o incremento das proteções à privacidade individual.

1.2.3. E quanto à ADPF?

R: Foi no mesmo sentido...

Ao apreciar a ADPF, o ministro Edson Fachin (relator) votou por afastar qualquer interpretação do dispositivo que autorize ordem judicial que exija acesso excepcional a conteúdo de mensagem criptografada ponta-a-ponta ou que, por qualquer outro meio, enfraqueça a proteção criptográfica de aplicações da internet. Ora, a criptografia é especialmente derivada da proteção que se espera ter da liberdade de expressão em uma sociedade democrática.

A criptografia é, portanto, meio de se assegurar a proteção de direitos que, em uma sociedade democrática, são essenciais para a vida pública.



A criptografia é um meio de proteger a privacidade das pessoas no ambiente digital. A criptografia nada mais é do que um **processo matemático de conversão de mensagens, informações ou dados que os torna ilegíveis por qualquer pessoa a não ser o destinatário da mensagem.** A criptografia serve, assim, para proteger o conteúdo da mensagem.

Não sem razão todos os órgãos estatais, assim como a sociedade civil, reconhecem que a criptografia protege os direitos dos usuários da internet, garantindo a privacidade de suas comunicações, e que, portanto, é do interesse do Estado brasileiro encorajar as empresas e as pessoas a utilizarem a criptografia a fim de manter o ambiente digital com a maior segurança possível para os usuários.



O DESAFIO a esse modelo de proteção da privacidade emerge basicamente de casos em que o acesso a mensagens protegidas por criptografia depende da *autorização exclusiva do próprio usuário do serviço.* O desafio também se faz presente na proteção da criptografia disponível para equipamento específicos, como *telefones celulares smartphones, ou computadores portáteis.*

Em ambos os casos, a preocupação é justificada pelas dificuldades técnicas na apuração de crimes que gravemente violam direitos fundamentais, como, por exemplo, os casos de pornografia infantil e de condutas antidemocráticas, como manifestações xenófobas, racistas e intolerantes, que ameaçam o Estado de Direito.



Os órgãos de segurança ficam, pois, **privados** de instrumento tido por indispensável (e que é reconhecido como plenamente **legítimo** em relação às chamadas telefônicas) na solução dessas violações.

A partir dessas premissas, é possível localizar a questão que se afigura chave para enfrentar o mérito da ação, qual seja, **saber se o risco público representado pelo uso da criptografia justifica a restrição desse direito** por meio da imposição de soluções de software, como, por exemplo, a *proibição da criptografia ou a criação de canais excepcionais* de acesso ou pela diminuição do nível de proteção.



A resposta a essa questão depende de um **rigoroso exame de proporcionalidade**, isto é, de uma avaliação cuidadosa para saber se o que se ganha com a promoção de um interesse público é ou não compensado com a restrição de direitos.

Além disso, é preciso que a Corte leve em devida conta a certeza científica que se tem sobre essas informações, assim como o grau de institucionalização promovido pelo Estado. Afinal, *"quanto mais grave for o peso de uma interferência em um direito constitucional, maior deve ser a certeza sobre as premissas que a fundamentam"*.

O Marco Civil da Internet ainda prevê, em seu art. 8º, que "a garantia do direito à **privacidade e à liberdade de expressão** nas comunicações é **condição para o pleno exercício do direito de acesso à internet**". A proteção constitucionalmente assegurada ao direito à privacidade é, portanto, elevada, digna dos direitos que detêm a mais ampla primazia no ordenamento nacional.

De fato, a legislação brasileira prevê salvaguardas à proteção da privacidade nos casos de interceptação de comunicações, como a excepcionalidade da medida, a restrição apenas para casos mais graves e, finalmente, a reserva de jurisdição.

O próprio Marco Civil da Internet, no art. 7º, II, indica a possibilidade de restrição da privacidade. A dúvida, portanto, não recai sobre a relevância do direito que fundamenta a restrição, em alguns casos, certamente elevada, mas a de saber se o que se ganha com o acesso excepcional é modico o suficiente para justificá-la (se a proteção criptográfica aos direitos à privacidade, à liberdade de opinião e à liberdade de expressão pode ser afastada).

É inegável que a garantia de proteção à privacidade e à liberdade de expressão por meio da criptografia traz riscos à segurança pública. Esse risco é medido pelos aumentos de custos para a realização de investigações criminais, porquanto a *capacidade de monitoramento e de interceptação de mensagens é tida como uma das principais formas — e para alguns crimes até a única — de se apurar ilícitos*. Por outro lado, a concessão de privilégios especiais a agentes do governo para o acesso à criptografia apresenta **riscos graves à segurança de todos**.

Além dos riscos de tornar a vulnerabilidade do sistema explorável por outras pessoas, eventual acesso excepcional de um aplicativo faria com que os usuários migrassem em direção a outros, mais seguros. No caso de criminosos, a consequência provável, como se teve oportunidade de debater na audiência pública, é de optarem por sistemas ainda mais restritos, *ainda mais difíceis de serem rastreados*.



É contraditório, portanto, que, em nome da segurança pública, se deixe de promover e buscar uma internet mais segura. Uma internet mais segura é direito de todos e dever do Estado. Medidas que, à luz da melhor evidência científica, trazem insegurança aos usuários somente se justificam se houver certeza comparável aos ganhos obtidos em outras áreas. *Não é isso, porém, o que ocorre*. O risco causado pelo uso da criptografia ainda não justifica a imposição de soluções que envolvam acesso excepcional.

Portanto, é INCONSTITUCIONAL proibir as pessoas de utilizarem a “criptografia ponta-a-ponta”, pois uma ordem como essa impacta **desproporcionalmente** as pessoas mais vulneráveis.

Claro que o reconhecimento de um direito constitucional à criptografia forte NÃO isenta as empresas que produzem os aplicativos de se conformarem com a legislação brasileira e de cumprirem as ordens judiciais que, na medida da *estrita proporcionalidade*, exijam a entrega de dados que não dependam da quebra de criptografia.

Seja como for, a suspensão das atividades do aplicativo ou mesmo sua proibição não caberá para o caso de descumprimento de decisão judicial de quebra de criptografia, mas para um quadro de violação grave do dever de obediência à legislação.

Não é preciso minudenciar, mas é evidente que mesmo aqui a sanção deverá observar a **proporcionalidade**, tendo sempre em conta o **direito do usuário de não ter suspenso seu acesso à internet**. É certo, pois, que NÃO cabe aos juízes que ordinariamente autorizam as interceptações telemáticas aplicarem a sanção prevista no art. 12, III, do Marco Civil da Internet.

1.2.4. Para TUDO

Em seguida, pediu **VISTA** dos dois feitos, o ministro Alexandre de Moraes.

AGUARDEMOS o desfecho da questão...

PARA TESTAR SEU CONHECIMENTO

2. QUESTÕES

2.1. Questões objetivas: CERTO ou ERRADO.



Q1°. Estratégia Carreiras Jurídicas. Diante da ausência de segurança e certeza, é inviável a comunicação de atos processuais via aplicativos como o WhatsApp.

Q2°. Estratégia Carreiras Jurídicas. O monitoramento de comunicações pode gerar o chamado efeito inibitório sobre a liberdade de expressão, o que possui desdobramento constitucional.

Q3°. Estratégia Carreiras Jurídicas. A privacidade pode ser entendida como o "direito a ser deixado em paz.

Q4°. Estratégia Carreiras Jurídicas. O reconhecimento de uma esfera de privacidade imune à ingerência atua como fator de limitação do poder das autoridades constituídas sobre os cidadãos.

Q5°. Estratégia Carreiras Jurídicas. A utilidade da liberdade de expressão prescinde de ser assegurada aos cidadãos um lugar de pensamento independente.

2.2. Gabarito.

Q1°. ERRADO: O CNJ já autorizou a utilização de intimação por WhatsApp, o que vem sendo utilizado pelos juízes especialmente nos CEJUSCs e nos Juizados Especiais (PCA nº 0003251-94.2016.2.00.0000).

Q2°. CORRETO: O conhecimento de que a comunicação é monitorada por terceiros interfere em todos esses elementos componentes da liberdade de informação: os cidadãos podem mudar o modo de se expressar ou até mesmo absterem-se de falar sobre certos assuntos, no que a doutrina designa por efeito inibitório sobre a liberdade de expressão (CF, art. 5º, X).

Q3°. CORRETO: Expressão utilizada pela Ministra Rosa Weber: a privacidade, isto é, o “direito a ser deixado em paz”, merece proteção adequada e efetiva do ordenamento jurídico.

Q4°. CORRETO: Tanto o reconhecimento de uma (1) esfera de privacidade imune à ingerência quanto a (2) garantia de salvo-conduto à palavra proferida surgiram, na história do constitucionalismo moderno, como fatores de limitação do poder das autoridades constituídas sobre os cidadãos.

Q5°. ERRADO: A utilidade da liberdade de expressão depende de ser assegurada aos cidadãos uma esfera de intimidade privada, livre de ingerência externa, um lugar onde o pensamento independente e novo possa ser gestado com segurança.

