# PL 2630/2020

Nota sobre o relatório do Senador Angelo Coronel (de 24.06.20)

Análise feita por: **Facebook, Google, Twitter e WhatsApp**

## Resumo


- No final da tarde de 24 de junho – a menos de um dia da sessão agendada para votação –, o Senador Angelo Coronel apresentou seu relatório ao PL 2630/2020. Além do exíguo prazo, comprometendo as chances de um debate aprofundado, o relatório insiste e acentua problemas que poderão resultar em impacto desastroso e amplo sobre milhões de brasileiros e a economia do país.
- Nesta nova versão, o PL 2630/2020 tornou-se **um projeto de coleta massiva de dados das pessoas,** aprofundando a **exclusão digita**l e **pondo em risco a privacidade e segurança** de milhões de cidadãos. Além disso, **o projeto atinge em cheio a economia e a inovação**, num momento em que em que precisamos unir esforços para a recuperação econômica e social do país.
- Abaixo, listamos os principais problemas do texto. Recomendamos **que a votação do projeto seja adiada até que se construa um texto equilibrado, fruto de debate amplo**, sob pena de **ampliar a exclusão digital** e **inviabilizar o funcionamento e o acesso** a redes sociais e aplicações de mensageria privada, **impactando negativamente a economia** e **milhões de cidadãos e negócios no Brasil – agravado pelo contexto de pandemia**.


## Principais problemas

1. **Exigência de identidade e coleta massiva de dados: afronta à privacidade e à presunção de inocência, ampliação da exclusão digital (art. 7º)**

- O art. 7º exige **documento de identidade válido e número de celular** brasileiro (e, em caso de celular estrangeiro, o **passaporte**) para o uso de redes sociais e serviços de mensageria privada. E impõe também o envio de código de verificação via SMS ao celular informado.
- Essa exigência generalizada de identificação e coleta massiva de dados é **desproporcional e contrária ao direito à proteção de dados** (elevado pelo STF à categoria de direito fundamental autônomo[1]) e aos princípios de proteção

[1] ADI 6387/DF, Rel. Min. Rosa Weber, j. 07.05.2020.

de dados, como o da **necessidade** ou minimização (limitação do tratamento de dados ao mínimo necessário – art. 6º, III, LGPD).

- Além de contrariar frontalmente a Lei Geral de Proteção de Dados (LGPD), o novo texto afronta também o Marco Civil da Internet (MCI), cujo regulamento determina, em seu art. 13, §2º, a retenção da "**menor quantidade possível de dados pessoais, comunicações privadas e registros** de conexão e acesso a aplicações", que devem ser excluídos tão logo atingida a finalidade de seu uso ou encerrado prazo legal.
- Essa exigência também **afronta a garantia constitucional e cláusula pétrea da presunção de inocência** (art. 5º, LVII, Constituição Federal - CF). Com a finalidade de ampliar as possibilidades de identificação para casos de crimes, o PL converte a todos em potenciais suspeitos, até que se prove o contrário.
- Além disso, o relatório **aprofunda a exclusão digital de milhões de brasileiros**. Dados do IBGE apontam 3 milhões de pessoas sem certidão de nascimento no Brasil (ou seja, sem identidade e CPF). Some-se a isso um total de 13% de indivíduos nas áreas urbanas e 30% de indivíduos nas áreas rurais sem telefone celular, além de 47 milhões de brasileiros que não têm qualquer acesso à Internet segundo dados da pesquisa TIC 2019. Portanto, **milhões de brasileiros estariam invisibilizados e impossibilitados de usar redes sociais e aplicações de mensageria privada**.
- Tudo isso **sem a garantia de combate a abusos**, pois pessoas podem se utilizar/produzir documentos falsos ou de terceiros e ainda utilizar laranjas para criação de contas.
- Esta exigência se agrava mais quando se considera o contexto atual de pandemia, no qual milhões de jovens estudam e se comunicam através de plataformas online. Elas serão obrigadas a ter um número de telefone e apresentar documento de identidade para acessar estas plataformas?
- Além de contrária a garantias fundamentais, a exigência ampla e generalizada de identificação e de coleta e guarda massiva de dados é também **desnecessária**. O ordenamento jurídico já dispõe dos instrumentos necessários para permitir a identificação de possíveis infratores, especialmente nos termos do MCI. Além disso, as plataformas de internet vêm colaborando e dialogando com autoridades de aplicação da lei.
- De fato fica claro que o objetivo do novo texto deixa de ser criar mecanismos para combater a desinformação para transformar-se em um projeto de coleta massiva de dados dos usuários, sem que fique claro o problema que se pretende tratar e combater. Já no início, o novo texto proposto inclusive estabelece o conceito de "**conta identificada**" (art. 5º, inciso II). Essa redação vaga, abrangendo a "*conta cujo responsável está identificado nos termos desta*

*Lei*", inaugura a ideia central que permeia este texto legal: um regime de identificação geral dos usuários da Internet no Brasil baseado em um número de celular registrado.

2. **Rastreamento das mensagens das pessoas (art. 10): mais ameaça à privacidade e à segurança das pessoas - estado de vigilância permanente**

- O novo texto insiste na problemática proposta de rastreamento das mensagens das pessoas pelo **período** de 3 meses, nas hipóteses de encaminhamento em massa – definido como o encaminhamento por mais de 5 usuários, dentro de 15 dias, a grupos e listas de transmissão.
- Essa proposta, mirando algumas árvores, acerta toda uma diversa floresta. Ela **afronta o direito fundamental à privacidade e proteção de dados** de milhões de cidadãos, mesmo quando tenta circunscrever a intrusão ao caso definido como encaminhamento em massa. Uma tal obrigação de rastreabilidade exigiria a coleta de muito mais informações sobre os usuários do que é necessário para que os serviços funcionem normalmente, contrariando princípios e garantias da Constituição, da LGPD e do MCI – além de abrir margem a abusos.
- Todo usuário de aplicativo de mensageria privada - como Whatsapp - teria sua privacidade reduzida. **Mesmo que não cometesse um crime ou estivesse envolvido em qualquer atividade ilegal**, as mensagens que encaminhasse – ou que outros encaminhassem, sem seu controle ou ciência – seriam rastreadas e poderiam ser solicitadas perante o Poder Judiciário.
- A exigência de rastreabilidade é altamente suscetível a **abusos** e afeta também a **segurança** das pessoas, expondo-as a riscos reais. Isto porque pessoas mal-intencionadas podem usar versões não autorizadas e modificadas dos aplicativos de mensageria privada para atribuir um número de telefone diferente a uma mensagem, fazendo parecer que a mensagem veio de outra pessoa, incluindo o uso de clonagem do cartão SIM como forma de atribuir conteúdo ilegal a usuários inocentes. Também **ameaça o sigilo de fonte (art. 5º, XIV, CF)** ao permitir rastrear-se mensagem encaminhada de ou por jornalistas.
- Além disso, o novo relatório não reconhece a necessidade de se preservar o sigilo ou o uso de recursos de **criptografia** de ponta a ponta, como mecanismo de segurança e de efetivação de direitos fundamentais. A rastreabilidade permite ciência inequívoca sobre o envio de conteúdos determinados, o que por via reflexa torna inócua a proteção à privacidade garantida pela criptografia de ponta-a-ponta. Uma tentativa de desconsiderar a criptografia ou enfraquecê-la, mesmo parcialmente, fragiliza a criptografia como um todo e esbarra na legislação brasileira (que reconhece e recomenda o uso de recursos

criptográficos[2]). Com isso, ameaça a privacidade e a liberdade de expressão dos usuários, abrindo espaço para monitoramento amplo.

**3. Exigência de bancos de dados no Brasil: duro golpe na economia e na privacidade e segurança de dados (art. 31)**

- O novo texto traz ainda uma exigência muito problemática, há muito superada no Brasil: a de localização de bases de dados no país.
- Tal exigência, além de desconsiderar a natureza global e aberta da internet, tem **sérias consequências econômicas**, sendo encarada por especialistas como uma **barreira comercial** moderna**.** Argumentos contra a localização incluem **custos mais altos de negócio**s, sistemas de segurança mais frágeis, riscos de retaliação comercial e impacto adverso nos investimentos. A localização suprime a capacidade de empreendedores e pequenos negócios, em particular os que atuam no ecossistema digital, acessar e se inserir na economia digital global.
- Estudo do European Centre for International Political Economy (ECIPE) concluiu que as restrições ao fluxo de informações, por meio de exigências de localização de dados, **pode reduzir os investimentos no Brasil** em até 4,2%[3]. O mesmo estudo também demonstrou que a presença de medidas de localização de dados pode levar o Brasil a ter **perdas no PIB** de 0,7% a 1,1%. Imagine projetar esse impacto negativo em um contexto de pandemia e de sérias perdas econômicas que o país vem sofrendo.
- Mais ainda, um dever de localização de bases de dados **ameaça seriamente a privacidade e a segurança** desses dados. A localização centraliza o armazenamento de dados dos brasileiros no país, gerando maior exposição, tornando-os mais vulneráveis e impedindo melhorias de segurança[4]. Especialistas em segurança argumentam que a localização de dados degrada, ao invés de melhorar, a segurança dos dados nos países, além de facilitar a **vigilância dos cidadãos pelo Governo**.
- Não à toa, essa ideia foi superada no processo que levou ao MCI (e mesmo no âmbito das normas setoriais do Banco Central do Brasil).
- Finalmente, o texto sequer deixa claro que tipos de dados dos usuários brasileiros deveriam ser mantidos no país, demonstrando a **ausência de uma**

[2] Apenas para citar alguns exemplos: Estratégia Nacional de Segurança da Informação (Decreto 10.222/2020), art. 46 da LGPD; decreto regulamentador do Marco Civil (art. 13, IV).
[3] ECIPE, http://ecipe.org/publications/dataloc.
[4] Por exemplo, "sharding", processo no qual as linhas de uma tabela de bancos de dados são mantidas separadamente em servidores ao redor do mundo de modo que os fragmentos ("shards") fornecem dados suficientes para operações, mas separadamente não permitem a re-identificação de um indivíduo.

**análise de impacto** ou que relacione a classificação de risco destes dados com a necessidade de sua manutenção em território nacional.

4. **Mudança expressa do Marco Civil para exigir guarda de dados que permitam "indivualização inequívoca" (arts. 34-35)**

- Via de regra, os dados já disponibilizados pelas aplicações de internet às autoridades de investigação (registros de acesso previstos no MCI combinados com dados cadastrais, como endereços de email, números de telefone e números de cartão de crédito quando existentes), aliados aos dados fornecidos pela telcos, **já são suficientes para identificação de indivíduos por trás de condutas ilegais nas plataformas.**
- Esta é, ainda, uma obrigação que deverá **tornar-se totalmente obsoleta** tão logo concluídos os investimentos das telcos sobre o protocolo IPV6 no Brasil.

5. **"Indevido" processo: excessiva procedimentalização que coloca em risco o combate a violações, inclusive as mais graves (art. 12)**

- O art. 12 do novo texto busca refletir nas redes sociais e serviços de comunicação uma lógica de processo civil ou penal, mas além de criar excessiva procedimentalização, tem sérias consequências sobre a segurança no ambiente online, contribuindo para mantê-los nas redes.
- Essa tentativa, embora mirando maior transparência, acaba produzindo outros efeitos - possivelmente não previstos, mas desastrosos. Além de criar excessiva burocratização, a exigência do art. 12 na prática **inviabiliza ou prejudica seriamente o combate a abusos e conteúdos nocivos online**, na aplicação, pelos provedores de aplicações de internet, de seus termos e políticas.
- Por exemplo, pelo texto do novo relatório, **antes de remover um conteúdo de terrorismo ou pornografia infantil, seria preciso notificar previamente o autor do conteúdo e dar-lhe prazo** para exercer "o contraditório e o direito de defesa". Mesmo conteúdos graves como **discurso de ódio** ou, mains **incitação à violência contra pessoa ou grupo em razão de características protegidas** como raça e gênero deverão, antes, contar com esse "indevido processo" que na prática perpetua ou prolonga nas redes a existência de abusos (art. 12, §4º).
- Plataformas são e devem ser livres para estabelecer suas políticas e termos e condições de uso, isto é, as "regras de convivência" desses ambientes online - informando-os de maneira clara. Essa é uma garantia prevista não apenas no MCI (art. 2º, VIII), como reforçada pela Lei nº 13.874/2019 (Lei da Liberdade Econômica) e pela garantia constitucional da livre iniciativa (art. 170, CF).

## 6. Exigências desproporcionais de transparência (art. 14-18)

- O novo texto impõe, de maneira excessiva e desconsiderando a diversidade de aplicações e a necessária neutralidade tecnológica, um dever amplo de transparência, mais uma vez sem que fique claro que problemas públicos se busca resolver.
- Para além da quase dezena de tipos de informação exigidos em relatórios com periodicidade reduzida (apenas três meses), o art. 14 abre ainda uma porta ampla e perigosa, conferindo ao Conselho de Transparência e Responsabilidade na Internet o poder de solicitar "outras informações" (§2º) – sobre as quais não se tem qualquer clareza, pois serão definidas por um órgão a ser criado, sem critérios definidos para guiar essa exigência adicional e indeterminada de "outras informações".
- É elevada a insegurança a jurídica e sérios os impactos sobre os provedores de aplicações objeto do PL – especialmente quando se considera a complexidade envolvida na elaboração de relatórios de transparência, bem como a necessidade de se observar o princípio da qualidade de dados (refletido, no ordenamento brasileiro, no art. 6, V, da LGPD).
- As exigências do §1º, combinadas com a amplitude do §2º, criam não apenas barreiras práticas possivelmente insuperáveis, mas ameaçam criar a insólita situação de relatórios de transparência que não informam ou mesmo desinformam, a depender da qualidade de dados e métricas disponíveis (em período tão curto como 3 meses). Mais ainda, diversos itens exigidos neste §1ºsuscitam preocupações adicionais quanto à privacidade e proteção de dados pessoais (por exemplo, quando exige dados de "engajamento", sem sequer definir o que seja isso - inciso IX).
- Transparência é preocupação central para as plataformas que subscrevem esta nota. Mas não é possível, menos ainda em meros 90 dias, passar a produzir detalhadíssimos relatórios em períodos curtos (mais curtos do que o exigido no mundo), no nível específico de país e com a excessiva granularidade exigida (granularidade que corre ainda o risco de se tornar ultrapassada ou inútil aos fins a que se destina, dado o caráter altamente dinâmico da tecnologia e da economia digital).
- Além disso, entende-se que um alto grau de transparência, inclusive a título de valores aproximados gastos e público alcançado pelas campanhas, deve existir no contexto eleitoral, com foco em propaganda eleitoral e política. Por exemplo, é excessivo exigir confirmação de identidade de todo e qualquer anunciante, que contrata todo e qualquer tipo de anúncio junto a provedores de aplicação de

internet (art. 18). Essa exigência reforça a abordagem de identificação e coleta massiva de dados do PL, além de colocar em questão a necessidade da coleta e divulgação desse tipo de informação (questões acentuadas com a recente decisão do STF na ADI 6387).

## 7. Outros problemas

- O texto do relatório atribui a empresas privadas a tarefa pública, vagamente prevista, de detectar "o uso de contas em desacordo com a legislação", transferindo ônus excessivo de monitoramento aos provedores de aplicações na internet (art. 7º, §3º).
- A proposta busca ainda regular condutas ao nível de produto, impondo limitações para o uso de grupos em aplicativos de mensageria privada (art. 9º). Essas são medidas que podem rapidamente cair em obsolescência, além de deixar empresas que se caracterizam pela inovação "engessadas" em termos do que podem ou não ofertar a seus usuários.
- Cria obrigações desproporcionais sobre usuários que fazem usos legítimos de automação, como aplicativos que facilitam o gerenciamento de conteúdo em múltiplas redes simultaneamente.
- O período para a entrada em vigor de tão profundas transformações (período de *vacatio legis*) é ainda muito breve, tornando impraticável a realização das adequações necessárias ao cumprimento – meros 90 dias.
- Ainda, a criação do Conselho de Transparência e Responsabilidade na Internet no formato proposto gera risco evidente de indevida interferência do Poder Legislativo na livre iniciativa e liberdade econômica por meio do Conselho. Eventual organismo para essa finalidade deveria ser independente de quaisquer poderes, ter caráter de autorregulação e de adesão voluntária. (art. 24).
- E o novo relatório também tem repercussões diretas sobre o exercício da liberdade de expressão – em um momento em que esse exercício deveria ser ainda mais protegido, o período eleitoral (art. 12, §5º e art. 36). Para além da vagueza (imagem ou voz manipuladas para imitar a realidade) e da falta de neutralidade tecnológica (possivelmente até a próxima eleição a sociedade estará enfrentando outros e novos desafios), estes dispositivos afetam diretamente a expressão da opinião e a expressão artística e humorística. Eles se assemelham aos dispositivos que, em junho de 2018, o STF declarou inconstitucionais – os quais impediam a veiculação de programas de humor envolvendo candidatos, partidos e coligações nos três meses anteriores ao pleito, como forma de evitar que sejam ridicularizados ou satirizados.

## Conclusões

- Como se vê, o texto do novo relatório insiste em concepções equivocadas e aprofunda muitos problemas, trazendo ainda desafios adicionais, como a **exclusão digital**, exigência de localização de dados, abrindo espaço para um duro **golpe na privacidade e segurança** dos cidadãos, e na **economia do país**. Tudo isso agravado pelo contexto atual de pandemia, em que as pessoas cada vez mais dependem da internet e do uso de plataformas digitais, como redes sociais e mensageria, para se manterem conectadas com família e amigos, para se informar, trabalhar e empreender.
- Diante disso, solicitamos que a votação seja adiada e o diálogo permaneça em busca de um texto equilibrado. É importante haver mais debate e amadurecimento de tão complexo tema – para diagnosticar com clareza que problemas se quer resolver, e construir um texto de consenso, pautado principalmente por premissas como: abordagem principiológica, um núcleo de transparência, exploração do caminho de co- ou auto-regulação (para permitir flexibilidade e evolução em transparência) e responsabilização dos atores maliciosos.