OS IMPACTOS DA TECNOLOGIA 5G AO DIREITO À PRIVACIDADE NO BRASIL

THE IMPACTS OF 5G TECHNOLOGY ON PRIVACY RIGHTS IN BRAZIL

Lucas Enriquez Rocha[*]

Resumo:
O presente artigo tem como principal meta delinear os possíveis impactos ao direito à privacidade trazidos pelo advento da tecnologia 5G no Brasil. Com tal objetivo em vista, utilizou-se o método de análise comparativa, traçando paralelos com a União Europeia, onde o 5G já está mais presente, para, em seguida, com base em tal análise, estudar a forma como certos institutos do ordenamento jurídico brasileiro (Marco Civil da Internet, Lei Geral de Proteção de Dados, Código de Defesa do Consumidor) lidarão com tal tecnologia. Ademais, no âmbito do setor regulatório, também foi estudada a capacidade da Anatel, órgão responsável por lidar com tal setor, de tratar dos impactos em tela. Conclui-se que o 5G trará novas características, como a alta velocidade de transmissão de dados, os quais podem representar grandes desafios para o ordenamento jurídico pátrio no âmbito da privacidade, os quais devem ser observados no futuro.

Palavras-chave: Direito de privacidade. Impactos. Ordenamento jurídico brasileiro. Tecnologia 5G.

Abstract:
The present paper has as its main objective to delineate the possible impacts to privacy rights brought upon by the arrival of 5G technology in Brazil. With such goal in mind, the method of comparative analysis was used, drawing parallels with the European Union, where the 5G is more available. As a following step, with such analysis as an underlying base, the way how certain institutes of the Brazilian law order (the Civilian Framework of the Internet, the General Data Protection Law, the Consumer Protection Code) will deal with aforementioned technology, was studied. Furthermore, in the sphere of the regulatory sector, the capacity of Anatel (a government agency which is responsible for dealing with such area) managing such impacts was also analysed. The conclusion of this paper is that 5G will bring new characteristics, such as the high speed of data transmission, which may represent big challenges to the national law order, that must be observed in the future.

Keywords: Privacy rights. Impacts. Brazilian law order. 5G technology.

[*] Bacharel em Direito pela Universidade de São Paulo. Lattes: http://lattes.cnpq.br/2497877100117640. *E-mail*: lucaserinrocha@gmail.com.

1. Introdução

A história do Direito sempre foi marcada por mudanças tecnológicas as quais forçaram a alteração e, não raramente, a completa revisão dos institutos jurídicos em voga. Pode-se pensar, por exemplo, na maneira como o advento das invenções da Segunda Revolução Industrial, como os trens a carvão, levaram ao surgimento da responsabilidade objetiva, a fim de se buscar a indenização, pelas poderosas companhias de trem, às vítimas de acidentes nas linhas férreas.

Entretanto, nunca se presenciou tantas mudanças no setor da tecnologia como no século XX e no começo do século XXI, com o advento da Internet, do rádio, da televisão, dentre outros, os quais, inevitavelmente, alteraram, alteram e alterarão o Direito como um todo. Nesse sentido, o mundo se depara hoje com o começo da Quarta Revolução Industrial, marcada pela nanorrobótica, pelos avanços na seara da inteligência artificial, engenharia genética e, principalmente, pela tecnologia 5G.

A importância do 5G será extrema e o seu impacto nos ordenamentos jurídicos do mundo inteiro, tremendo. Por sua velocidade de fluxo de informação sem precedentes, a quinta geração de telecomunicações irá permitir ampla gama de aplicações nos mais diversos setores: automatização total de fábricas, aplicativos de realidade virtual, cidades interligadas entre si e autômatas, redes de distribuição de energia elétrica e água inteligentes, veículos autônomos (isto é, sem motoristas), cirurgias a distância, dentre outras.

Porém, como toda tecnologia ainda nova, a totalidade dos efeitos é desconhecida. Afinal, como provado pelos escândalos recentes envolvendo as grandes empresas da Internet, como os casos da Cambridge Analytica e do Facebook, no qual vários dados de usuários foram roubados e usados sem o consentimento destes para influenciar em campanhas políticas, como nas eleições presidenciais nos Estados Unidos da América e no *Brexit* no Reino Unido, ambas em 2016. Invenções promissoras, tais quais as redes sociais, podem parecer integralmente benéficas à primeira vista, escondendo seus traços deletérios.

É por tal razão, somada à importância central da privacidade na economia contemporânea, no chamado capitalismo de vigilância, ou *surveillance capitalism*, como cunhado pela autora Shoshana Zuboff (2019) que o autor propõe, com o presente artigo, mapear os impactos à tecnologia 5G ao direito à privacidade. Adicionalmente, o autor optou por estudar tais impactos no contexto brasileiro, por ser este o seu local de pesquisa e de vivência.

Para se realizar tal objetivo, o autor pesquisou as características tecnológicas do 5G, que a tornam disruptiva, analisou como a legislação de proteção de dados referência no mundo – qual seja, o Regulamento Geral de Proteção de Dados europeu – absorveu tais

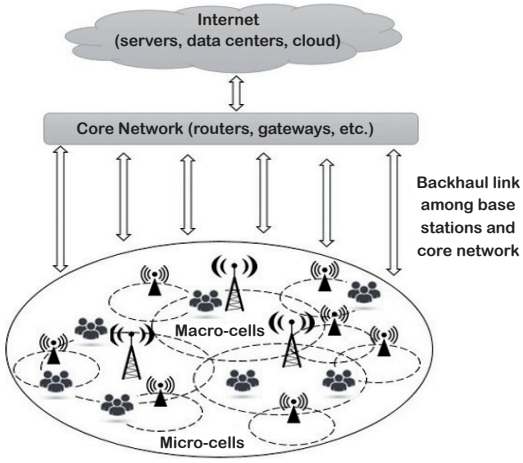
inovações e, depois, estudou a forma como distintos regulamentos jurídicos brasileiros e seus dispositivos serão capazes (ou não) de tratar tais inovações. Para fins de recorte temático, se optou pelos seguintes regulamentos: o Código de Defesa do Consumidor, o Marco Civil da Internet e a Lei Geral de Proteção de Dados. Adicionalmente, analisou a Agência Nacional de Telecomunicações, porquanto será este o órgão responsável por lidar com as empresas responsáveis por ofertar o 5G, as operadoras de telecomunicações.

Destarte, o texto se estrutura da seguinte forma: o capítulo 2 explicará brevemente o 5G (cujo conceito é relativamente desconhecido), o capítulo 3 exporá os impactos à privacidade deste, o capítulo 4 mostrará a forma como o Regulamento Geral de Proteção de Dados europeu lidou com tais impactos, o capítulo 5 tangerá o tema da preparação da Anatel, o capítulo 6 concernirá o Código de Defesa do Consumidor, o capítulo 7 tratará do Marco Civil da Internet, o capítulo 8 analisará a Lei Geral de Proteção de Dados (LGPD) e, por fim, o artigo trará suas conclusões no capítulo 9.

2. A definição do 5G

Antes de se adentrar o tema dos impactos à privacidade em si, a novidade dessa tecnologia e o relativo desconhecimento do público torna necessária a elucidação, ainda que de forma breve, do que é e como funciona a tecnologia 5G.

Em linhas gerais, o 5G é a quinta geração de telecomunicação celular, na qual a comunicação é feita pelo envio e recebimento de ondas de radiofrequência. O seu funcionamento se dá por meio da implementação de pequenas antenas, as quais são responsáveis pelo recebimento de dados de áreas geográficas denominadas "células" (daí o termo *celular*). Ademais, tais antenas são interconectadas a uma rede central, alcunhada de *core*. Esta, por fim, se liga, por meio de servidores e *data centers* à Internet (MARQUES, 2019). A imagem abaixo ilustra, de forma simplificada, tal conceito.



As notas distintivas do 5G em comparação às gerações anteriores são a sua alta velocidade de transmissão de dados, de até 10 Gbps, sua baixa latência, de aproximadamente 1ms (latência, no caso, se constitui no intervalo de tempo entre o envio e o recebimento de uma informação), sua densidade de conexões de 1 milhão de dispositivos por quilômetro quadrado, dentre outros (INTERNATIONAL TELECOMMUNICATION UNION, 2017).

Tais características tornam a tecnologia 5G não apenas inovadora, mas disruptiva, porquanto, devido à alta velocidade de dados permitida, muito maior do que a das gerações anteriores,[1] serão possíveis aplicações em diversas indústrias, como nos setores de saúde (permitindo a realização de cirurgias a distância), agricultura (com a possibilidade de monitorar a situação de colheitas em tempo real), logística (que será integralmente automatizada), transporte autônomo etc. (HUMAYUN *et al.*, 2020).

Nesse sentido, consoante Marques (2019, p. 31), serão três os grandes campos de aplicação do 5G: Banda Larga Móvel melhorada (*enhanced Mobile Broadband ou eMBB*), comunicação massiva *MTC (Machine Type Communication)* e serviços de comunicação ultraconfiáveis e de baixa latência (*Ultra Reliable and Low Latency Communications*). O primeiro se refere à maior capacidade de transmissão de dados, permitindo maior velocidade em jogos *online*, por exemplo. O segundo concerne aos sistemas que permitem a interação entre máquinas em quantidade massiva, como nas cidades inteligentes ou *smart cities*.[2] O terceiro, por fim, tange a aplicações onde certas atividades são optimizadas pelo baixo intervalo de comunicação entre dois dispositivos, como nas denominadas *smart grids*, redes de distribuição de energia elétrica inteligentes e que funcionam sem necessidade de interferência humana.

Em suma, é dessa maneira que o 5G é estruturado e são os traços apontados acima que o distingue das gerações de telecomunicação pregressas. Entretanto, em que pese serem os possibilitadores de um vasto número de aplicações tecnológicas em diversas indústrias, são estas mesmas vantagens que implicarão em diversos problemas relacionados à privacidade, os quais serão melhor explorados no capítulo seguinte.

[1] A velocidade máxima suportada pelo 4G, por exemplo, é de 300 Mbps, ou megabits por segundo.

[2] Cidades inteligentes se refere à integração entre várias máquinas em uma cidade, possibilitando vasta interconexão e melhoramento de diversos serviços, como segurança pública, mobilidade urbana etc.

3. Os impactos do 5G à privacidade

Por se tratar de uma tecnologia ainda em estado de incipiente distribuição comercial, deve-se levar em conta que nem todos os possíveis impactos à privacidade trazidos pelo 5G são conhecidos. Entretanto, diversos autores apontam possíveis brechas a este direito trazidos pela quinta geração de telecomunicações celulares.

Nas palavras de Sicari, Rizzardi e Coen-Porisini (2020, p. 2, tradução nossa):

> Entretanto, já que tais dispositivos estarão conectados à rede o tempo inteiro de uma maneira muito mais ampla, eles poderão ser mais facilmente rastreados e serão mais vulneráveis a vários tipos de ataque [...]. Manter um alto nível de qualidade de serviço em termos de *delay*, quando uma alta quantidade de informação é transferida dentro da rede 5G, enquanto tentar conservar, ao mesmo tempo, a sua confiabilidade da rede em si, é uma tarefa crítica e complexa.

Para Humayun *et al.* (2020, p. 2, tradução nossa), por sua vez:

> O 5G irá providenciar constante conectividade dos aparelhos IoT (Internet of Things ou Internet das Coisas, em português) e espera-se que transfira um alto volume de dados. Essa transferência de informação apresenta vários desafios em termos de privacidade do consumidor.

Em suma, os impactos à privacidade (os quais serão expostos logo abaixo) são resultantes da alta velocidade e quantidade de dados transmitida por meio das redes 5G. Com tantos dados sendo enviados e recebidos em um pouquíssimo espaço de tempo, no denominado *Big Data,*[3] restará difícil para as empresas responsáveis pelo tratamento e controle de dados, nos termos das legislações protetoras de privacidade, como o Regulamento Geral de Proteção de Dados e a Lei Geral de Proteção de Dados, evitarem que ocorram vazamentos.

Liyanage *et al.* (2018), a título exemplificativo, arrola vários desafios à privacidade trazidos pelos 5G, quais sejam:

a) A alta capacidade de transmissão de dados da tecnologia 5G permitirá a atuação de diversos provedores de serviços e operadores, muitos dos quais irão ter contato com os dados dos usuários sem o seu consentimento.

[3] *Big Data* se refere à quantidade extremamente alta de dados possibilitada pelas novas tecnologias de comunicação e armazenamento de informação da Quarta Revolução Industrial.

b) A infraestrutura de uma mesma rede será compartilhada por distintas empresas; tal compartilhamento abrirá margem para ataques aos dados vindos de múltiplas fontes, como o DoS (Denial of Service).[4]

c) A alta conectividade permitida entre os aparelhos do 5G possibilitará que pacotes de dados tramitando dentro das fronteiras de um país acabe migrando, sem a autorização ou conhecimento do usuário, para outra nação. Tal situação pode se tornar preocupante na medida em que nem todas as nações possuem legislações e/ou medidas protetivas de privacidade. Ademais, muitos países possuem critérios distintos para tratamento de dados, podendo levar em conta dados sensíveis, como orientação, etnia, crença religiosa, dentre outros.

d) Com vários atores, como provedores de serviço e operadoras de telecomunicações, coletando os dados dos usuários, haverá maior dificuldade de se identificar, em caso de perda ou roubo de dados, o responsável legalmente.

e) Eventual violação à privacidade pode surtir conflitos de competência jurídica, haja vista que, com o 5G, muitas empresas são de países distintos. No Brasil, por exemplo, a maior fornecedora de equipamentos para as companhias do setor de telecomunicações, a Huawei, é chinesa. Nesse sentido, poderia haver dúvidas quanto à legislação aplicável: a do local da vítima, a do provedor de serviços ou do infrator.

f) Como já dito supra, o 5G permitirá a utilização da mesma infraestrutura por parte de diversas empresas, tanto operadoras de telecomunicação como outras provedoras de serviços. O fato de que muitas dessas empresas serem competidoras em segmentos similares de mercado pode criar óbices para que estas colaborem para garantir os mecanismos de privacidade de dados.

g) A tecnologia 5G dependerá extremamente dos chamados serviços de nuvem. Devido a isso, muitas operadoras de telecomunicação armazenarão os dados de seus usuários na nuvem. Entretanto, tal fato pode ser prejudicial à privacidade, na medida em que muitos desses serviços não são administrados integralmente por essas já mencionadas operadoras, mas por outros provedores. Por conseguinte, o controle sobre as informações coletadas dos usuários estará prejudicado. Outrossim, por questões de competição comercial, tais provedores podem se recusar a revelar às operadoras como funcionam suas medidas de privacidade, dificultando ainda mais o controle de dados.

h) A tecnologia 5G abrirá mais espaço para a atuação de empresas terceiras desenvolvedoras de aplicativos. Tais companhias podem aproveitar o acesso à rede para coletar dados e trocá-los ou até mesmo vendê-los para outros desenvolvedores.

[4] DoS ou Denial of Service ocorre quando várias contas, verdadeiras ou não, acessam um mesmo serviço ao mesmo tempo. O número de acessos é tão grande que acaba sobrecarregando o sistema, criando uma pane no serviço em tela e impossibilitando, temporariamente, seu acesso.

i) O 5G possibilitará maior conectividade entre uma quantidade massiva de aparelhos, na Internet das Coisas. Entretanto, de acordo com o Barr Group (2017), parte considerável dos criadores desses dispositivos ignoram o aspecto da segurança em seu design e quase metade dos seus desenvolvedores não encriptam as comunicações destes.

Além do mais, outros desafios à privacidade também surgem ao se analisar setores específicos, como o dos veículos autônomos. No tocante a esse ponto, Lai *et al.* (2020) apontam a possibilidade de criminosos hackearem outros motoristas e roubarem suas informações.

Outrossim, vale mencionar aspectos concernentes à geopolítica, como a hipótese de roubo de informações de um país por outro, como analisado por Kewalramani e Kanisetti (2019) ao tratar da utilização de equipamentos 5G, por parte da Índia, da empresa Huawei, de origem chinesa.

Em suma, percebe-se que a tecnologia 5G trará vários impactos distintos à privacidade, os quais terão que ser lidados pelos ordenamentos jurídicos dos países de forma inovadora. Nesse sentido, os próximos capítulos explorarão como o ordenamento jurídico europeu e o brasileiro conseguirão lidar com tal temática.

4. 5G e o Regulamento Geral sobre a Proteção de Dados (RGPD)

O fato da tecnologia 5G ainda se encontrar em estado incipiente no Brasil, à espera da realização de seu leilão, faz surgir a necessidade de análise de países onde tal geração de telecomunicações celular esteja mais avançada. A título exemplificativo, consoante dados do European 5G Observatory, pode-se mencionar os Estados Unidos da América, Coreia do Sul, com mais de 115 mil estações de base em meados de 2020, China, Japão e União Europeia (EUROPEAN COMISSION, 2020). Dos locais mencionados supra, o autor optou por este último, devido ao fato de ser disciplinado pelo Regulamento Geral sobre a Proteção de Dados (RGPD, Regulamento UE 2016/679) que constitui a inspiração para a legislação brasileira referente à privacidade de dados, a Lei n. 13.709 de 2018, ou Lei Geral de Proteção de Dados (LGPD). Nesse sentido, a presença de similaridades entre as duas legislações será de grande serventia para o presente artigo, haja vista que a forma da RGPD receber os impactos do 5G à privacidade pode indicar como a LGPD irá fazê-lo.

Na seara de segurança de dados e informação, o RGPD é norteado por sete princípios os quais servem para garantir a privacidade, quais sejam: licitude, lealdade e transparência; limitação das finalidades; minimização dos dados; exatidão; limitação da conservação; integridade e confidencialidade; e, por fim, a responsabilidade.

Entretanto, em que pese tais princípios, determinados aspectos inerentes ao funcionamento da tecnologia 5G podem impedir que tais princípios possam ser efetivados. Nesse sentido, Rizou, Alexandropoulou-Egyptiadou e Psannis (2020) apontam três características do 5G que ameaçam os direitos à privacidade elencados na RGPD: a alta taxa de velocidade de transmissão de dados, a densidade de tráfego de informação e a possibilidade de conectar um número extremamente alto de dispositivos.

4.1. Alta velocidade de transmissão de dados

No concernente à alta taxa de velocidade de transmissão de dados, a tecnologia 5G permitirá uma taxa de transmissão de dados de até 10 Gbps, levando a um aumento expressivo do volume de informação, quantidade esta que pode dificultar e até mesmo impedir que o responsável pelo tratamento dos dados forneça as informações necessárias ao titular de dados, afetando o art. 13 do RGPD. Nesse sentido, Rizou, Alexandropoulou-Egyptiadou e Psannis (2020, p. 5, tradução nossa) aduz: "Velocidades mais altas iriam, de fato, fracassar em informar o titular de dados sobre os elementos do processamento de informação, em resposta à quantidade não administrável sendo processada através das redes 5G [...]".

> Art. 13 – Informações a facultar quando os dados pessoais são recolhidos junto do titular.
>
> 1. Quando os dados pessoais forem recolhidos junto do titular, o responsável pelo tratamento faculta-lhe, aquando da recolha desses dados pessoais, as seguintes informações:
>
> a) a identidade e os contactos do responsável pelo tratamento e, se for caso disso, do seu representante;
>
> b) os contactos do encarregado da proteção de dados, se for caso disso;
>
> c) as finalidades do tratamento a que os dados pessoais se destinam, bem como o fundamento jurídico para o tratamento;
>
> d) se o tratamento dos dados se basear no artigo 6º, n. 1, alínea (f), os interesses legítimos do responsável pelo tratamento ou de um terceiro;
>
> e) os destinatários ou categorias de destinatários dos dados pessoais, se os houver;
>
> f) se for caso disso, o facto de o responsável pelo tratamento tencionar transferir dados pessoais para um país terceiro ou uma organização internacional, e a existência ou não de uma decisão de adequação adotada pela Comissão ou, no caso das transferências mencionadas nos artigos 46 ou 47, ou no

> artigo 49, n. 1, segundo parágrafo, a referência às garantias apropriadas ou adequadas e aos meios de obter cópia das mesmas, ou onde foram disponibilizadas. (EUROPEAN UNION, 2016, tradução nossa).

Da mesma maneira, o art. 14 também será afetado por tal fator.

> Art.14 – [...]
>
> 1. Quando os dados pessoais não forem recolhidos junto do titular, o responsável pelo tratamento fornece-lhe as seguintes informações:
>
> a) a identidade e os contactos do responsável pelo tratamento e, se for caso disso, do seu representante;
>
> b) os contatos do encarregado da proteção de dados, se for caso disso;
>
> c) as finalidades do tratamento a que os dados pessoais se destinam, bem como o fundamento jurídico para o tratamento;
>
> d) as categorias dos dados pessoais em questão;
>
> e) os destinatários ou categorias de destinatários dos dados pessoais, se os houver;
>
> f) se for caso disso, o facto de o responsável pelo tratamento tencionar transferir dados pessoais para um país terceiro ou uma organização internacional, e a existência ou não de uma decisão de adequação adotada pela Comissão ou, no caso das transferências mencionadas nos artigos 46 ou 47, ou no artigo 49, n. 1, segundo parágrafo, a referência às garantias apropriadas ou adequadas e aos meios de obter cópia das mesmas, ou onde foram disponibilizadas. (EUROPEAN UNION, 2016, tradução nossa).

Pelas mesmas razões, não haverá tempo suficiente para se apagar os dados caso o titular assim os queira, afetando o direito de retificação (art. 16), o direito ao apagamento de dados (art. 17), direito à limitação do tratamento (art. 18).

Por sua vez, a obrigação estipulada no art. 33, pela qual o responsável pelo tratamento de dados deve avisar a autoridade de controle acerca de eventual violação de privacidade em até 72 horas, se possível, também será afetada, haja vista que os dados violados serão transmitidos de forma tão rápida, antes de qualquer tomada de ação por parte do responsável pelo tratamento.

4.2. Densidade do tráfego de informação

A alta densidade de tráfico de dados por sua vez também pode apresentar alguns problemas os quais o RGPD não conseguirá lidar. "Densidade", no caso, se refere ao alto número de antenas que será distribuído para possibilitar a emissão das ondas de radiofrequência. Nas palavras de Rizou, Alexandropoulou-Egyptiadou e Psannis (2020, p. 6, tradução nossa): "Devido à alta densidade de células pequenas, o conhecimento desta, que está associado ao titular de dados, pode facilmente revelar a informação de localização deste último". Por conseguinte, será extremamente difícil para o responsável pelo tratamento de dados impedir que estas células não só localizem o usuário, como também tracem um perfil deste, mediante uma decisão automatizada, violando o art. 22 do RGPD.

> Art. 22 – [...]
>
> 1. O titular dos dados tem o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar. (EUROPEAN UNION, 2016, tradução nossa).

4.3. Conexão entre um número extremamente alto de dispositivos

No tocante à questão de vários dispositivos interconectados, no contexto da Internet das Coisas, o fato de que o usuário terá contato com vários dispositivos distintos, operado por várias empresas distintas, constituirá um empecilho adicional. Ora, a quantidade de aparelhos será tão alta que restará difícil para o titular de dados saber quais e quantas empresas coletarão suas informações. Em suma, não saberá quem será a empresa imbuída de tratar os dados nem a de controlá-los. Sem esse tipo de informação, ficará difícil para o titular de dados exercer seus direitos, quais sejam, os já mencionados: direito relacionado a ser informado (arts. 13 e 14), o direito à retificação (art. 16), o direito a ser esquecido (art. 17) e o direito a ser notificado sobre eliminação de dados (art. 19), o direito à portabilidade de dados (art. 20) e o direito à objeção (art. 21).

Exemplo interessante é o mencionado por Rizou, Alexandropoulou-Egyptiadou e Psannis (2020), em sua pesquisa, no qual brinquedos diversos, ligados à IoT, gravam e armazenam conversas de crianças sem o seu consentimento ou de seus

responsáveis. Outrossim, ficaria difícil impedir que tais objetos traçassem o perfil do usuário por decisão automatizada, haja vista estarem em número alto, violando o supracitado art. 22.

Pela mesma razão, a quantidade extremamente alta de *smart objects*[5] abriria margem para várias violações de dados pessoais vindas de diversos objetos, se tornando, por conseguinte, muito difícil para que o responsável pelo tratamento notificasse a autoridade de controle ou ao titular de dados, nos termos do já citado art. 33 e do art. 34 do RGPD, respectivamente.

> Art. 34 – [...]
>
> 1. Quando a violação dos dados pessoais for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento comunica a violação de dados pessoais ao titular dos dados sem demora injustificada. (EUROPEAN UNION, 2016, tradução nossa).

Além dos fatores apontados acima, Del Re (2020) aponta que o RGPD não apresenta medidas de controle anterior ou *a priori* da utilização de dados, além do consentimento. Por conseguinte, o usuário apenas consegue descobrir se houve violação de sua privacidade *a posteriori*, isto é, após o ocorrido.

Poder-se-ia apontar, como contraponto às deficiências da legislação europeia, acima mencionadas, o fato da RGPD prever técnicas de proteção de dados, como a pseudonimização e a cifragem de dados (arts. 25 e art. 32).

> Art. 25 – [...]
>
> 1. Tendo em conta as técnicas mais avançadas, os custos da sua aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos decorrentes do tratamento para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica, tanto no momento de definição dos meios de tratamento como no momento do próprio tratamento, as medidas técnicas e organizativas adequadas, como a pseudonimização, destinadas a aplicar com eficácia os princípios da proteção de dados, tais como a minimização, e a incluir as garantias necessárias no tratamento, de uma forma que este cumpra os requisitos do presente regulamento e proteja os direitos dos titulares dos dados. (EUROPEAN UNION, 2016, tradução nossa).

[5] *Smart objects*, no caso se refere a objetos conectados à Internet, que possuem sensores, processadores e software próprios.

> Art. 32 – [...]
>
> 1. Tendo em conta as técnicas mais avançadas, os custos de aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como os riscos, de probabilidade e gravidade variável, para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento e o subcontratante aplicam as medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco, incluindo, consoante o que for adequado:
>
> a) a pseudonimização e a cifragem dos dados pessoais; [...] (EUROPEAN UNION, 2016, tradução nossa).

Entretanto, há de se apontar que a instalação de tais programas se torna difícil no contexto da Internet das Coisas, haja vista que muitos dos *smart objects* não terão capacidade de processamento o suficiente para garantir a eficácia de tais técnicas. Del Re (2020, p. 237, tradução nossa), aliás, fala sobre isso:

> Entretanto, no momento, todas as técnicas [de segurança] requerem recursos de processamento adequados, os quais, conquanto sejam compatíveis com os presentes sistemas de processamento, são muito intensivos computacionalmente para sua utilização na futura Internet das Coisas, na qual a maior parte dos objetos na rede terão capacidades de processamento muito reduzidas ou muito pobres.

Haja vista o exposto, percebe-se que, em que pese possuir vários artigos que garantam direitos sobre os seus dados, o RGPD apresenta algumas brechas as quais devem ser melhor observadas no contexto de lidar com as caraterísticas do 5G, devido, principalmente, aos três fatores retratados – quais sejam, à alta velocidade de transmissão de dados, à alta densidade de tráfego de dados e à grande quantidade de dispositivos interconectados –, criando óbice para a sua eficácia social. Tais deficiências podem servir de prenúncio para a forma como o ordenamento jurídico brasileiro lidará com o tema, panorama este que será melhor tratado nos capítulos seguintes, em especial no tocante à Lei Geral de Proteção de Dados.

5. Agência Nacional de Telecomunicações (Anatel)

Analisar o preparo da Anatel em receber a tecnologia 5G é parte integrante do presente, haja vista ser o órgão responsável por regular o setor de telecomunicações no Brasil, com fulcro no art. 8º da Lei Geral de Comunicações (Lei n. 9.472 de 1997), o qual diz:

> Fica criada a Agência Nacional de Telecomunicações, entidade integrante da Administração Pública Federal

> indireta, submetida a regime autárquico especial e vinculada ao Ministério das Comunicações, com a função de órgão regulador das telecomunicações, com sede no Distrito Federal, podendo estabelecer unidades regionais. (BRASIL, 1997).

O mesmo diploma normativo, por sua vez, garante a privacidade como um direito dos usuários das telecomunicações ao elencar a inviolabilidade e o segredo de comunicação no rol do seu art. 3º, *in verbis*:

> O usuário de serviços de telecomunicações tem direito:
>
> [...]
>
> V - à inviolabilidade e ao segredo de sua comunicação, salvo nas hipóteses e condições constitucional e legalmente previstas; [...]

Porém, o mero fato de estar expresso em sua legislação não se traduz em preparo para garantir o direito à privacidade em face do 5G.

Pois bem, ao se realizar tal análise, vale lembrar que o 5G não será apenas uma nova evolução tecnológica, mas um marco disruptivo, totalmente distinto das quatro gerações de telecomunicações anteriores. Nesse sentido, a quinta geração de telecomunicações carregará características próprias, com as quais a Anatel nunca se deparou, e que podem apresentar desafios regulatórios para esta última.

Nesse sentido, vale transcrever trecho de Lehr, Queder e Haucap (2021, p. 2, tradução nossa), o qual diz:

> O 5G difere das gerações anteriores de padrões celulares em vários aspectos chave. Primeiramente, o design do 5G tem sido menos centrado em Operadoras de Telecomunicações Móveis e têm envolvido um conjunto maior de atores em seu desenvolvimento. De fato, uma das novas habilidades chave é o potencial de entregar redes 5G *standalone*,[6] privadas, que são separadas das redes das Operadoras Móveis. [...] As melhorias de grande ordem de magnitude ao longo de virtualmente toda dimensão de desempenho irão permitir que o 5G melhore grandemente a performance de aplicações (como serviços de multimídia de banda larga móvel epitomizados por smartphones e tablets) e também melhor lidar com novas oportunidades de mercado para a Internet das Coisas, veículos autônomos [...]. Em luz da complexidade e das muitas opções incluídas dentro do

[6] *Standalone* é termo que se refere aos casos no qual a rede de equipamentos do 5G apenas utilizam dispositivos do 5G, haja vista existir a possibilidade se misturar, na mesma infraestrutura, partes da rede 4G junto a do 5G.

> quadro de padronização do 5G, é mais apropriado ver o 5G como uma caixa de capacidades do que uma tecnologia um "tamanho serve para todos" que seja rigidamente definida por um certo conjunto de características.

Extrai-se do trecho acima aspectos relacionados à constante inovação tecnológica, com a qual a Anatel, acostumada aos serviços tradicionais de telecomunicação, terá que lidar. Em teoria, a Lei Geral de Comunicações não teria problemas em receber tais tecnologias, haja vista que o conceito de telecomunicações usado em seu texto é flexível, podendo ser alterado consoante a hipótese. Nesse sentido, Carlos Sundfeld (2007, p. 159) diz:

> Com a inovação tecnológica, as telecomunicações deixavam de comportar uma só modalidade importante; havia agora a telefonia móvel, as televisões a cabo e por satélite etc. Daí a primeira característica importante da LGT: a de haver tratado as telecomunicações não como um serviço, mas um complexo de serviços (art. 2º-III), cuja definição exata poderia ser feita e refeita pela regulamentação (arts. 62, 63 e 69). Abria-se espaço para que, no lugar do velho serviço público de telefonia, surgissem muitos serviços, de contornos flexíveis e mutáveis (arts. 128 e 130), sem que a lei precisasse ser alterada.

Entretanto, há de se imaginar que boa parte dos quadros da Anatel não possui a experiência necessária para lidar com esse tipo de tecnologia, não podendo usar sua experiência anterior como base de referência.

Como aponta Cave (2018), o 5G será extremamente descentralizado, com a instalação de pequenas células em vários locais distintos. Tal fato pode levar a uma inadequação entre a regulação da Anatel, mais genérica, com as características particulares de cada lugar. Nesse aspecto, a agência reguladora pode não conseguir garantir que as operadoras cumpram o disposto no supracitado art. 3º, inciso V.

Da mesma forma, o 5G permitirá que as operadoras de telefonia móvel ofereçam sua estrutura para que outras companhias disponibilizem serviços para os seus usuários, as denominadas Operadoras de Rede Móvel Virtuais. Muitas delas oferecerão aplicações para segmentos específicos da indústria, os chamados *verticais*,[7] como as áreas de saúde e de finanças, para citar alguns.

Por conseguinte, a Anatel terá que lidar com diversas empresas diferentes as quais surgirão, em um número muito maior do que as que a agência está acostumada a lidar nas últimas décadas e em indústrias as quais ela possui pouco contato. Afinal,

[7] Verticais são empresas especializadas em um único ramo específico do mercado. Por exemplo, uma fintech éum exemplo de vertical, por lidar apenas com tecnologia de operações bancárias e financeiras.

como mostrado pelo próprio órgão regulador em relatório recente, de 2020, o mercado de telecomunicações brasileiro é extremamente concentrado, na prática, um oligopólio, dominado por quatro companhias: Vivo, Claro, Tim e Oi (ANATEL, 2020).

A Anatel, habituada a lidar com apenas quatro empresas, provavelmente terá dificuldades em aplicar suas disposições, inclusive no concernente à privacidade, a atores os quais desconhece e que surgirão em quantidade relativamente alta e em pouco espaço de tempo. Ademais, como já dito, tais companhias oferecerão aplicações em áreas das indústrias as quais os membros da agência reguladora em tela possuem pouca *expertise*.

Por razões similares, a Anatel encontrará dificuldades em garantir a segurança de informações ao se lidar com outra característica própria do 5G, qual seja, a possibilidade de compartilhamento do espectro de radiofrequência por diversas empresas distintas. Nesse aspecto, Lehr, Queder e Haucap (2021, p. 4, tradução nossa), afirmam: "O futuro do 5G será um de muitas redes heterogêneas sem fio sob o controle de diversos operadores independentes, que precisarão coexistir na sua utilização do espectro nos mesmos locais e nos mesmos instantes".

Outrossim, a existência de tal quantidade de empresas operando na mesma rede pode levar a problemas envolvendo a competição. Afinal, companhias rivais poderiam se recusar a cooperar entre si para colocar em eficácia mecanismos garantidores de privacidade de dados ou para resolver um vazamento de informação.

Nesse aspecto, é cediço que a Lei Geral de Comunicações e também a Anatel são norteadas pelos princípios da regulação social e pró-competição, as quais foram arroladas, no mesmo patamar de importância, nos incisos I e III, respectivamente, do art. 2º do diploma normativo em tela (SUNDFELD, 2007).

Entretanto, tais princípios podem ser prejudicados em uma situação de diversos atores operando as redes 5G, muitos dos quais irão, inevitavelmente, competir sem limites entre si.

Talvez a existência de mecanismos como o Conselho Consultivo (art. 33, Lei n. 9.472/1997) ou as consultas públicas (art. 19, inciso III, Lei n. 9.472/1997) possam servir de meio para que a população possa garantir que as operadoras de rede móvel assegurem, de forma integral, sua privacidade. Entretanto, seria uma relação assimétrica, não suficiente para atender tal escopo, haja vista que as companhias, nesse caso, possuem muito mais conhecimento técnico da área, além de terem maior poder financeiro para contratar melhores consultores e advogados em hipóteses de litígios.

Em suma, percebe-se que a Anatel está apenas parcialmente preparada para lidar com os impactos à privacidade trazidos pelo 5G. Sua legislação norteadora, a Lei n. 9.472 de 1997, possui determinados dispositivos que garantem o direito à privacidade, a competição justa entre empresas (as quais supostamente serviria para evitar uma situação de não colaboração na hipótese de violação das informações dos usuários), o interesse social

e mecanismos populares. Entretanto, tais artigos podem se tornar ineficazes ao se lidar com as mudanças tecnológicas do 5G quais sejam: o alto número de empresas a prestarem serviços no ramo, compartilhando a mesma infraestrutura das grandes companhias já existentes no mercado nacional; a descentralização da rede, a qual levará a um conflito entre a regulação geral e as particularidades locais; o relativo desconhecimento, por parte dos membros da agência reguladora, das novas operadoras de rede móvel virtuais que surgirão.

6. Código de Defesa do Consumidor

Expor a forma como a Lei n. 8.078 de 1990, ou o Código de Defesa do Consumidor (CDC), receberá as mudanças relacionadas à privacidade originadas do 5G ganha sentido por duas razões. Em primeiro lugar, porque a relação entre os diversos atores da indústria, sejam operadoras de telecomunicação, fornecedoras de equipamentos e empresas terceiras fornecedoras de aplicativos e demais serviços, para com os usuários, podem ser vistas sob uma ótica consumerista. Em segundo lugar, mas não menos importante, porquanto o CDC perfaz parte das quatro leis responsáveis, no Brasil, por lidar com eventuais danos oriundos de novas tecnologias, junto ao Código Civil (Lei n. 10.406 de 2002), ao Marco Civil da Internet (Lei n. 12.965 de 2014) e à Lei Geral de Proteção de Dados (Lei n. 13.709 de 2018).

Tendo em vista tais fatores, o presente capítulo lidará com os dispositivos do CDC que garantirão uma eventual proteção consumerista aos futuros usuários da tecnologia 5G e se tais dispositivos serão suficientes para assegurar eventual responsabilização das empresas da rede por eventuais danos relacionados ao âmbito da privacidade.

Entretanto, tal análise, para ser eficaz, deve ser tripartite, porquanto também são três as possibilidades de relação existentes: dos clientes para com as operadoras de telecomunicação, dos clientes para os fornecedores de equipamentos e, por fim, dos clientes para com as companhias terceiras fornecedoras de serviços.

Antes de se adentrar nos subcapítulos propriamente ditos, entretanto, vale frisar que a interpretação do direito à privacidade como protegido pelo CDC, em que pese não estar este presente no rol do art. 6º, é perfeitamente possível, haja vista a leitura do art. 7º de tal Códice, *in verbis*:

> Art. 7°. Os direitos previstos neste código não excluem outros decorrentes de tratados ou convenções internacionais de que o Brasil seja signatário, da legislação interna ordinária, de regulamentos expedidos pelas autoridades administrativas competentes, bem como dos que derivem dos princípios gerais do direito, analogia, costumes e equidade. (BRASIL, 1990).

Por fim, para fins de se evitar repetição de termos no conteúdo *infra*, é importante aduzir o seguinte: o usuário da rede 5G será sempre enquadrado como consumidor que, nos termos do art. 2º do CDC, "é toda pessoa física ou jurídica que adquire ou utiliza produto ou serviço como destinatário final" (BRASIL, 1990). As operadoras, os fornecedores de equipamento e as empresas terceiras, por sua vez, serão consideradas fornecedores, nos ditames do art. 3º, *caput*:

> Art. 3º. Fornecedor é toda pessoa física ou jurídica, pública ou privada, nacional ou estrangeira, bem como os entes despersonalizados, que desenvolvem atividade de produção, montagem, criação, construção, transformação, importação, exportação, distribuição ou comercialização de produtos ou prestação de serviços. (BRASIL, 1990).

6.1. Operadoras de Telecomunicação

As operadoras de telecomunicação serão as principais responsáveis por gerir as redes 5G e, por conseguinte, proteger seus usuários de eventuais danos à privacidade. Nesse sentido, caso ocorra algum dano à privacidade por parte dos usuários, essas companhias poderão ser responsabilizadas objetivamente, nos termos do art. 14, *caput*:

> Art. 14. O fornecedor de serviços responde, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos. (BRASIL, 1990).
>
> § 1° O serviço é defeituoso quando não fornece a segurança que o consumidor dele pode esperar, levando-se em consideração as circunstâncias relevantes, entre as quais:
>
> I - o modo de seu fornecimento;
>
> II - o resultado e os riscos que razoavelmente dele se esperam;
>
> III - a época em que foi fornecido. (BRASIL, 1990).

Por sua vez, poder-se-á considerar a oferta do 5G como defeituosa, em caso de violação à privacidade, ao se considerar que o serviço em questão não ofertou a segurança devida ao usuário. Destarte, seria exequível aplicar os incisos I e II, § 1º do art. 14 do CDC, pelo modo errôneo de fornecimento e pela extrapolação de riscos esperados, respectivamente.

6.2. Fornecedores de equipamentos

Sob ótica análoga a dos operadores de telecomunicações, os fornecedores dos equipamentos das redes 5G também poderiam ser responsabilizados em caso de danos à privacidade dos usuários, mas nos termos do art. 12 do CDC, por se tratar de um produto. O dispositivo mencionado aduz:

> Art. 12. O fabricante, o produtor, o construtor, nacional ou estrangeiro, e o importador respondem, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos decorrentes de projeto, fabricação, construção, montagem, fórmulas, manipulação, apresentação ou acondicionamento de seus produtos, bem como por informações insuficientes ou inadequadas sobre sua utilização e riscos.
>
> § 1° O produto é defeituoso quando não oferece a segurança que dele legitimamente se espera, levando-se em consideração as circunstâncias relevantes, entre as quais:
>
> I - sua apresentação;
>
> II - o uso e os riscos que razoavelmente dele se esperam;
>
> III - a época em que foi colocado em circulação. (BRASIL, 1990).

Nesse aspecto, vale frisar que muitos dos problemas de privacidade podem ser evitados se aplicando técnicas de segurança no próprio *design* do dispositivo em si. Nas palavras de Del Re (2020, p. 236): "Segurança e privacidade são implementados no *design* desde o desenvolvimento inicial de um aplicativo/serviço e estão sob o controle do titular de dados por soluções técnicas eficientes, as mais simples quanto possível".

Destarte, consoante tal possibilidade técnica, o fornecedor de equipamentos da rede 5G terá a obrigação, para com os eventuais usuários da rede 5G, em garantir, no próprio *hardware* de seus aparelhos, mecanismos de segurança de informações.

Sob tal ótica, seria possível, aliás, combinar a interpretação do art. 12 do CDC com o art. 46, § 2º da Lei Geral de Proteção de Dados, que visa garantir a segurança desde o momento da criação do aparelho:

> Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.
>
> [...]

> § 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução. (BRASIL, 2018).

No concernente a possíveis atualizações posteriores à entrega do equipamento, em seus sistemas digitais, e que possam, outrossim, ocasionar brechas na privacidade dos usuários, o art. 12 do CDC ainda poderia ser aplicado, consoante interpretação de Carlos Edison do Rêgo Monteiro Filho e Nelson Rosenvald (2020, p. 554):

> A responsabilidade se impõe mesmo que esses defeitos apareçam após a colocação em circulação do produto, desde que o fornecedor ainda esteja no controle de atualizações da tecnologia ou providencie serviços digitais. Portanto, o momento em que um produto é colocado no mercado não estabelece um limite rígido de responsabilidade do fornecedor. Quando o defeito surge como resultado da interferência do fornecedor com o produto já colocado em circulação (*v.g.*, por meio de uma atualização de *software*) ou da omissão do fabricante em interferir no momento adequado, ele deve ser considerado um defeito no produto para o qual o fornecedor é responsável. Por conseguinte, o fornecedor deve permanecer responsável quando o defeito tem sua origem em um componente digital defeituoso, parte digital auxiliar ou em outros conteúdos ou serviços digitais fornecidos para o produto após a colocação em circulação do produto ou na ausência de uma atualização do conteúdo digital ou da prestação de um serviço digital que seria necessário para manter o nível esperado de segurança dentro do período pelo qual é obrigado a fornecer tais atualizações.

6.3. Empresas terceiras fornecedoras de serviços

Como já foi exposto no capítulo 5, a tecnologia 5G permitirá que outras empresas utilizem a mesma rede das operadoras de telecomunicação para ofertar os mais diversos serviços, das mais distintas naturezas: jogos *online,* aplicativos de saúde, finanças, entre outros. Nesse aspecto, em caso de violação de privacidade, lógica similar à utilizada para as operadoras de telecomunicações deve ser aplicada, considerando-se tal evento como exemplo de serviço defeituoso, incidindo, portanto, o art. 14 do CDC.

7. Marco Civil da Internet

Na seara da privacidade, a Lei n. 12.965 de 2014, também alcunhada de Marco Civil da Internet, arrola a privacidade como um de seus princípios norteadores, como expresso em seu art. 3º, inciso III, o qual aduz:

> Art. 3º. A disciplina do uso da internet no Brasil tem os seguintes princípios:
>
> [...]
>
> III - proteção dos dados pessoais, na forma da lei; [...] (BRASIL, 2014).

Entretanto, a tecnologia 5G apresentará duas particularidades as quais podem entrar de confronto com o disposto no Marco Civil, qual seja, o *network slicing* ou fatiamento de rede e a sua conexão massiva com outros dispositivos, a já citada Internet das Coisas.

7.1. Fatiamento de rede (*network slicing*)

Smirnova *et al*. (2019, p. 1.516, tradução nossa) dão, de forma sucinta, a definição do fatiamento de rede:

> A divisão de uma única rede física em várias redes virtuais com diferentes características de performance. O fatiamento de rede iria permitir que provedores de serviço de internet diferenciassem níveis de qualidade de serviço de acordo com os diversos requerimentos de aplicações verticais providenciados mediante fatiamento de rede específico. Significa que cada fatia da rede estaria ajustada a uma aplicação vertical específica que não poderia ser ofertada pela melhor internet.

Destarte, múltiplas empresas fornecedoras de serviço poderiam utilizar a mesma rede 5G para ofertar aplicações com qualidades distintas, a depender do usuário. Uma fábrica, por exemplo, poderia pedir uma fatia de rede especificamente com menor latência, para seus robôs de linha de produção e outra fatia com banda larga melhorada (*enhanced-MBB*). Porém, tal possibilidade poderia ferir o princípio da neutralidade da rede, isto é, o tratamento isonômico, por parte das provedoras, de pacotes de dados na Internet, cristalizada no art. 9º do Marco Civil:

> Art. 9º. O responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação.

> § 1º A discriminação ou degradação do tráfego será regulamentada nos termos das atribuições privativas do Presidente da República previstas no inciso IV do art. 84 da Constituição Federal, para a fiel execução desta Lei, ouvidos o Comitê Gestor da Internet e a Agência Nacional de Telecomunicações, e somente poderá decorrer de:
>
> I - requisitos técnicos indispensáveis à prestação adequada dos serviços e aplicações; e
>
> II - priorização de serviços de emergência.
>
> § 2º Na hipótese de discriminação ou degradação do tráfego prevista no § 1º, o responsável mencionado no caput deve:
>
> I - abster-se de causar dano aos usuários, na forma do art. 927 da Lei n. 10.406, de 10 de janeiro de 2002 - Código Civil;
>
> II - agir com proporcionalidade, transparência e isonomia;
>
> III - informar previamente de modo transparente, claro e suficientemente descritivo aos seus usuários sobre as práticas de gerenciamento e mitigação de tráfego adotadas, inclusive as relacionadas à segurança da rede; e
>
> IV - oferecer serviços em condições comerciais não discriminatórias e abster-se de praticar condutas anticoncorrenciais.
>
> § 3º Na provisão de conexão à internet, onerosa ou gratuita, bem como na transmissão, comutação ou roteamento, é vedado bloquear, monitorar, filtrar ou analisar o conteúdo dos pacotes de dados, respeitado o disposto neste artigo.

Tal conflito poderia surtir riscos à privacidade do usuário, já que as operadoras poderiam obter indevidamente tais dados, sob a prerrogativa de estarem oferendo serviços especiais. Nesse sentido, mesmo a aplicação dos incisos I, II, III e IV e § 3º do artigo supracitado poderia se tornar ineficaz devido à alta velocidade de transmissão de dados permitida pelo 5G. Ademais, o compartilhamento de recursos no fatiamento de rede também aumentará a interferência de uma conexão de um usuário a rede de outro cliente, que também poderá ser vítima desses danos. Nesse sentido, Yoo e Lambert (2019, p. 28-29, tradução nossa) afirmam:

> [...] As redes já passaram há muito tempo dos dias [...] quando [...] o seu uso era completamente independente e não impunha nenhum impacto prejudicial na utilização por parte de outras pessoas. [...] O advento do fatiamento de rede irá acentuar a grau de compartilhamento de recursos ainda mais. Permitir que usuários acessem recursos em

> uma base multilocal e transacional faz com que seja quase inevitável que o uso de uma pessoa afete o dos outros.

Vale citar, outrossim, que uma solução buscada nas hipóteses permitidas de discriminação de dados pelo Decreto n. 8.771 de 2016 não encontraria respaldo. Nesse aspecto, o art. 5º desta lei elenca todas as possibilidades de tal discriminação, isto é, os requisitos técnicos indispensáveis para a prestação adequada de serviços.

> Art. 5º. Os requisitos técnicos indispensáveis à prestação adequada de serviços e aplicações devem ser observados pelo responsável de atividades de transmissão, de comutação ou de roteamento, no âmbito de sua respectiva rede, e têm como objetivo manter sua estabilidade, segurança, integridade e funcionalidade.
>
> § 1º Os requisitos técnicos indispensáveis apontados no caput são aqueles decorrentes de:
>
> I - tratamento de questões de segurança de redes, tais como restrição ao envio de mensagens em massa (spam) e controle de ataques de negação de serviço; e
>
> II - tratamento de situações excepcionais de congestionamento de redes, tais como rotas alternativas em casos de interrupções da rota principal e em situações de emergência [...]. (BRASIL, 2016).

Como se pode observar pela simples leitura dos incisos acima, nenhum deles cobre a hipótese de oferta de serviços com qualidades específicas, no contexto do fatiamento da rede.

7.2. Internet das Coisas

De forma breve, também vale citar como a massiva conexão com outros dispositivos, no âmbito da já mencionada Internet das Coisas, apresentará riscos à privacidade.

O Marco Civil da Internet obriga os provedores de conexão a guardar, sob sigilo, os registros de conexão dos usuários, nos termos do art. 13, e os provedores de aplicações, a guardar, também sob sigilo, consoante o art. 15, os registros de acesso às aplicações na Internet.

Entretanto, com a conexão com outros dispositivos, tais dados podem ser facilmente transferidos para terceiros, sem o consentimento do usuário. Por razões similares e também devido à alta velocidade de mais de 10 Gbps, o inciso X do art. 7º também pode se tornar ineficaz, porquanto o provedor pode não ter tempo suficiente para excluir os dados pessoais antes que estes tenham sido enviados para outrem.

8. Lei Geral de Proteção de Dados (LGPD)

Para se estudar a forma como a Lei n. 13.709 ou Lei Geral de Proteção de Dados (LGPD) lidará com os impactos do 5G à privacidade, o autor utilizará método análogo ao do capítulo 4, acerca do RGPD, analisando se os dispositivos da lei brasileira serão eficazes o suficiente para garantir a proteção dos dados pessoais dos usuários em face das mudanças tecnológicas do 5G.

É importante apontar que a alta velocidade de dados, já mencionada no capítulo 4, pode afetar o tempo de ação e reação dos usuários e dos responsáveis pelo tratamento e controle dos dados. Nesse sentido, os dados do usuário podem ser facilmente transferidos para outrem antes que ele dê o seu consentimento, ferindo o art. 7º, inciso I, ou antes que ele o revogue, de acordo com o art. 8º, § 5º:

> Art. 7º. O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
>
> I - mediante o fornecimento de consentimento pelo titular; [...] (BRASIL, 2018).
>
> Art. 8º. O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.
>
> [...]
>
> § 5º O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei. (BRASIL, 2018).

Pela mesma razão, tais dados podem ser enviados para terceiros antes que o término do tratamento de dados se concretize, nos termos do art. 15, ou antes que o titular de dados possa pedir revisão de decisões automatizadas, nos ditames do art. 20, respectivamente:

> Art. 15. O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:
>
> I - verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;
>
> II - fim do período de tratamento;

> III - comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º desta Lei, resguardado o interesse público; ou
>
> IV - determinação da autoridade nacional, quando houver violação ao disposto nesta Lei. (BRASIL, 2018).
>
> Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade. (BRASIL, 2018).

Tal brecha de informação pode até ocorrer antes que o controlador possa comunicar à autoridade nacional, violando o art. 48:

> Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.
>
> § 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:
>
> I - a descrição da natureza dos dados pessoais afetados;
>
> II - as informações sobre os titulares envolvidos;
>
> III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
>
> IV - os riscos relacionados ao incidente;
>
> V - os motivos da demora, no caso de a comunicação não ter sido imediata; e
>
> VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo. (BRASIL, 2018).

Outrossim, a alta quantidade de informação transmitida em pouco espaço do tempo criaria óbices ao direito do titular em obter dados do controlador, já que a quantidade de informação de magnitude extremamente alta, indo de confronto com o art. 18, inciso II.

> Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:
>
> [...]
>
> II - acesso aos dados; [...] (BRASIL, 2018).

Ademais, a conexão com vários outros *smart objects*, no contexto da Internet das Coisas, também constituiria em obstáculos para a eficácia de outros dispositivos da LGPD, já que os dados poderiam ser facilmente roubados, dos provedores dos responsáveis pelo seu tratamento, por tais objetos. Dessa forma, o sigilo garantido pela legislação estaria comprometido, como expresso no art. 46, *caput*:

> Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. (BRASIL, 2018).

A conexão entre um *smart object* em território brasileiro e com outro em território estrangeiro também poderia levar à transferência de dados para um país que não possua legislação protetora de dados, ou em hipóteses não contempladas pelo art. 33 da LGPD.

> Art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos:
>
> I - para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei; [...] (BRASIL, 2018).

Quanto às técnicas de segurança de dados, previstas pelo LGPD, como a anonimização e a pseudoanonimização, Del Re (2020), como já mencionado, já apontou a insuficiência técnica dos *smart objects* para garantir tais medidas.

Em suma, conclui-se que a Lei Geral de Proteção de Dados, em que pese seu arcabouço de dispositivos e medidas, possui algumas insuficiências as quais devem ser observadas, consoante a evolução do 5G no Brasil, ao se tratar da alta velocidade de dados e a conexão massiva com vários *smart objects*.

9. Conclusão

Haja vista o exposto nos capítulos acima, percebe-se que o ordenamento jurídico pátrio apresenta algumas insuficiências, que devem ser observadas com cuidado. A depender da capacidade tecnológica do 5G nos próximos anos, tais falhas podem abrir espaço para os mais diversos danos ao direito à privacidade.

O problema, nesse caso, não está relacionado à ausência de princípios e dispositivos garantidores de privacidade (que aliás, como mostrado pelo capítulo 4 e 7, estão presentes em grande número), mas pela sua ineficácia em lidar com as novas características técnicas do 5G, não presentes nas gerações de telecomunicação anteriores:

a alta velocidade de dados, a alta densidade do tráfego de informação e a conectividade massiva com outros dispositivos (Internet das Coisas).

Nesse aspecto, o capítulo 4 serviu como prenúncio para tal observação, revelando inadequações do RGPD em garantir os direitos de proteção dos dados dos titulares. Ao se transportar tal análise para o contexto brasileiro, conclusões semelhantes foram retiradas.

No tocante à regulação setorial, tratada no capítulo 5, a Anatel apresenta algumas deficiências: sua experiência com as gerações de telecomunicações pregressas não será de grande valia em momento posterior, devido ao surgimento de número elevado de novas empresas, as quais usarão a mesma rede. Adicionalmente, as denominadas Operadoras de Rede Móvel Virtuais constituirão um desafio, porquanto, a agência reguladora não está acostumada a lidar com tais atores, habituada a um cenário dominado por 4 empresas (Vivo, Oi, Tim e Claro). O traço descentralizador das redes 5G também criará uma dicotomia entre a regulação federal e a regulação local.

No que tange à regulação legal, dos três ordenamentos estudados, o Marco Civil da Internet, a Lei Geral de Proteção de Dados e o Código de Defesa do Consumidor, apenas este último apresenta mecanismos suficientes para lidar com o 5G, oferecendo diversas possibilidades de responsabilização objetiva para as empresas envolvidas, sejam operadoras de telecomunicação, fornecedoras de equipamentos e companhias terceiras desenvolvedoras de aplicativos, como mostrado no capítulo 6.

O Marco Civil da Internet, por sua vez, como estudado no capítulo 7, encontrará óbices para a efetivação de seus artigos em face do *network slicing* ou fatiamento de rede, o qual entrará em tensão com o princípio de neutralidade de rede. Da mesma maneira, a conexão com vários outros aparelhos aumentará a chance de brecha de bancos de dados que guardem os registros de conexão e de acesso dos provedores da Internet.

A Lei Geral de Proteção de Dados, por sua vez, apresenta também falhas, mencionadas no capítulo 8. A transmissão rápida de informação poderá afetar vários direitos, como o consentimento, comunicação à autoridade responsável, dentre outros. A presença de *smart objects* também e sua interconexão criará rotas alternativas de fluxo de dados, que podem ser enviados para outros países ou empresas sem a anuência do titular.

Em face de tais conclusões, delineia-se um futuro talvez sombrio para a privacidade, inclusive no contexto brasileiro. Por mais robustas que sejam, existe o risco das legislações concernentes à privacidade não conseguirem acompanhar os avanços tecnológicos do futuro, já prenunciados pelo 5G, deixando margem para a exposição indevida de milhões de pessoas para empresas, criminosos e governos autoritários. Como se extrai do texto, pode haver, no porvir, um descompasso entre as disposições normativas

e os novos elementos do 5G, os quais tornarão tais legislações um mero pedaço de papel, sem eficácia real e social.

Serão necessárias pois um grande investimento em medidas voltadas mais ao campo tecnológico do que propriamente jurídico que, sozinho, não conseguirá lidar com os impactos em tela. Entretanto, o atraso tecnológico presente no Brasil, refletido na falta de *expertise* técnica de boa parte da população, operadores do direito aliás, dificultará sobremaneira a solução de tal problemática.

Por fim, deve-se ter receio se o vislumbre atual de governos e da mídia com o 5G não se assemelha à curiosidade de Pandora, que, consoante a lenda grega, abriu uma caixa contendo todos os males do mundo. Em suma, deve-se questionar se o 5G será realmente a porta de entrada de uma nova revolução tecnológica ou a morte do direito à privacidade.

São Paulo, setembro de 2022.

Referências

ANATEL. *Relatório de acompanhamento do setor de telecomunicações*: telefonia móvel, 2º semestre de 2020. Brasília, DF, abr. 2021. Disponível em: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?eEP-wqk1skrd8hSlk5Z3rN4EVg9uLJqrLYJw_9INcO4NT86aq4DZSJMWh9gBoilhtRgvXnEhjT6dqYhPLeIC2xMriZOLrD6LEYnf1psEzlLJAq9-LHel_G9fbuXRs7UR. Acesso em: 15 jun. 2021.

BARR GROUP. 2017 *Embedded systems safety & security survey*. Germantown, 2017. Disponível em: https://barrgroup.com/sites/default/files/downloads/barr_group_2017_embedded_systems_safety_security_survey.pdf. Acesso em: 16 jul. 2021.

BRASIL. Decreto n. 8.771, de 11 de maio de 2016. Regulamenta a Lei n. 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações. *Portal do Planalto*, Brasília, DF, 11 maio 2016. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8771.htm. Acesso em: 9 jul. 2021.

BRASIL. Lei n. 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. *Portal do Planalto*, Brasília, DF, 12 set. 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 8 jul. 2021.

BRASIL. Lei n. 9.472, de 16 de julho de 1997. Dispõe sobre a organização dos serviços de telecomunicações, a criação e funcionamento de um órgão regulador e outros aspectos institucionais, nos termos da Emenda Constitucional n. 8, de 1995. *Portal do Planalto*, Brasília, DF, 17 jul. 1997. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9472.htm. Acesso em: 7 jul. 2021.

BRASIL. Lei n. 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. *Portal do Planalto*, Brasília, DF, 24 abr. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 11 jul. 2021.

BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). *Portal do Planalto*, Brasília, DF, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 10 jul. 2021.

CAVE, Martin. How disruptive is 5G? *Telecommunications Policy*, London, v. 42, n. 8, p. 653-658, Sept. 2018. Disponível em: https://www.sciencedirect.com/science/article/pii/S0308596118301654/pdfft?md5=7fdac69a12b3a179c2dd10f0a9fceb50&pid=1-s2.0-S0308596118301654-main.pdf. Acesso em: 25 jul. 2021.

DEL RE, Enrico. Which future strategy and policies for privacy in 5G and beyond? *In*: IEEE 5G WORLD FORUM (5GWF), 3., 2020, Bengalore. *Anais* [...]. Bengalore: IEEE Xplore, 2020. Disponível em: https://ieeexplore.ieee.org/document/9221371/references#references. Acesso em: 4 jul. 2021.

EUROPEAN COMMISSION. *5G observatory*: quarterly report 10. Luxembourg, Dec. 2020. Disponível em: http://5gobservatory.eu/wp-content/uploads/2021/01/90013-5G-Observatory-Quarterly-report-10.pdf. Acesso em: 29 jun. 2021.

EUROPEAN UNION. Regulation (EU) 2016/679. *Official Journal of the European Union*, Brussels, v. 59, L 119, p. 1-88, 4 May 2016. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN. Acesso em: 14 out. 2021.

HUMAYUN, Mamoona; JHANJHI, Noor Zaman; ALRUWAILI, Madallah; AMALATHAS, Sagaya Sabestinal; BALASUBRAMANIAN, Venki; SELVARAJ, Buvana. Privacy protection and energy optimization for 5G-aided industrial internet of things. *IEEE Access*, Piscataway, v. 8, p. 183.665-183.677, 2020. Disponível em: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9214512. Acesso em: 4 jul. 2021.

INTERNATIONAL TELECOMMUNICATION UNION. *Report ITU-R M. 2410-0*: minimum requirements related to technical performance for IMT-2020 radio interface(s). Geneva, Nov. 2017. Disponível em: https://www.itu.int/dms_pub/itu-r/opb/rep/R-REP-M.2410-2017-PDF-E.pdf. Acesso em: 30 jun. 2021.

KEWALRAMANI, Manoj; KANISETTI, Anirudh. 5G, Huawei & geopolitics: an Indian roadmap. *Social Science Research Network*, Rochester, 32 p., 19 June 2019. (Takshashila Discussion Document 2019-02). Disponível em: https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3414860_code3037852.pdf?abstractid=3414860&mirid=1. Acesso em: 29 jul. 2021.

LAI, Chengzhe; LU, Rongxing; DONG, Zheng; SHEN, Xuemin. Security and privacy challenges in 5G-enabled vehicular networks. *IEEE Network*, Piscataway, v. 34, n. 2, p. 37-45, Mar./Apr. 2020. Disponível em: https://ieeexplore.ieee.org/abstract/document/9055735. Acesso em: 4 jul. 2021.

LEHR, William; QUEDER, Fabian; HAUCAP Justus. 5G: a new future for mobile network operators, or not? *Telecommunications Policy*, London, v. 45, n. 3, p. 1-14, Apr. 2021. Disponível em: https://www.sciencedirect.com/science/article/pii/S0308596120301762/pdfft?md5=b86a5e9a3fc1f36ce327706ef8945aac&pid=1-s2.0-S0308596120301762-main.pdf.

LIYANAGE, Madhusanka; SALO, Jukka; BRAEKEN, An; KUMAR, Tanesh; SENEVIRATNE, Suranga; YLIANTTILA, Mika. 5G privacy: scenarios and solutions. *In*: IEEE 5G WORLD FORUM (5GWF), 2018, Silicon Valley. *Anais* [...]. Silicon Valley: IEEE Xplore, 2018. p. 197-203. Disponível em: https://ieeexplore.ieee.org/abstract/document/8516981. Acesso em: 4 jul. 2021.

MARQUES, Eduardo Moreno. *Sistemas celulares 5G, características, desafios para a implantação no Brasil e aplicações*. Orientador: Paulo Cardieri. 2019. 82 p. Dissertação (Mestrado em Engenharia Elétrica) – Faculdade de Engenharia Elétrica e de Computação, Universidade Estadual de Campinas, Campinas, 2019. Disponível em: http://repositorio.unicamp.br/Busca/Download?codigoArquivo=545365. Acesso em: 4 jul. 2021.

MONTEIRO FILHO, Carlos Edison do Rêgo; ROSENVALD, Nelson. Riscos e responsabilidades na inteligência artificial e noutras tecnologias digitais emergentes. *In*: TEPEDINO, Gustavo; SILVA, Rodrigo da Guia (coord.). *O direito civil na era da inteligência artificial*. 1. ed. São Paulo: Thomson Reuters Brasil, 2020. p. 543-564.

RIZOU, Stavroula; ALEXANDROPOULOU-EGYPTIADOU, Eugenia; PSANNIS, Konstantinos E. GDPR interference with next generation 5G and IoT networks. *IEEE Access*, Piscataway, v. 8, p. 108.052-108.061, June 2020. Disponível em: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9110555. Acesso em: 4 jul. 2021.

SICARI, Sabrina; RIZZARDI, Alessandra; COEN-PORISINI, Alberto. 5G In the internet of things era: an overview on security and privacy challenges. *Computer Networks*, Amsterdam, v. 179, 12 p., Oct. 2020. Disponível em: https://www.sciencedirect.com/science/article/pii/S1389128620300827. Acesso em: 4 jul. 2021.

SMIRNOVA, Inga; LIPENBERGS, Elmars; BOBROVS, Vjaceslavs; GAVARS, Peteris; IVANOVS, Girts. Network slicing in the scope of net neutrality rules. *In*: PHOTONICS & ELECTROMAGNETICS RESEARCH SYMPOSIUM, 2019. Rome. *Anais* [...]. Rome, June 2019. p. 1.516-1.521. Disponível em: https://ieeexplore.ieee.org/document/9017846. Acesso em: 15 ago. 2021.

SUNDFELD, Carlos Ari. Meu depoimento e avaliação sobre a Lei Geral de Telecomunicações. *Revista de Direito de Informática e Telecomunicações*, Belo Horizonte, v. 2, n. 2, p. 55-84, jan./jun. 2007.

YOO, Christopher S.; LAMBERT, Jesse. 5G and net neutrality. *In*: THE 47th RESEARCH CONFERENCE ON COMMUNICATIONS, INFORMATION AND INTERNET POLICY, 2019, Washington, DC. *The future of the internet*: innovation, integration and sustainability. Baden-Baden: Nomos, 2019. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3429948. Acesso em: 29 jul. 2021.

ZUBOFF, Shoshana. *The age of surveillance capitalism*: the fight for a human future at the new frontier of power. London: Profile Books, 2019.