Pontifícia Universidade Católica
do Rio de Janeiro

Sergio Ricardo Correia de Sá Junior

A regulação jurídica da proteção de dados pessoais no Brasil

Monografia apresentada ao Programa de Pós-Graduação em Direito da Propriedade Intelectual da PUC-Rio como requisito parcial para obtenção do título de Especialista em Direito

Orientador: Eduardo Magrani

Rio de Janeiro

17 de dezembro de 2018

AGRADECIMENTOS

Em primeiro lugar, acima de tudo, agradeço imensamente aos meus amados pais, cujo apoio incondicional incentivou-me ao longo de toda uma vida. Com certeza absoluta, qualquer agradecimento será insuficiente para representar toda a sua importância fundamental. Mesmo que um dia o vento leve essas palavras ao esquecimento, o meu profundo sentimento de gratidão permanecerá eterno.

Agradeço ao companheirismo dos meus amigos da PUC-Rio, onde tivemos o prazer de nos conhecer e batalhar juntos diariamente, cuja intensidade durou o tempo necessário para torná-lo inesquecível. Levo comigo, sem sombra de dúvidas, lembranças de amizades raras, que durarão para o resto da vida.

Finalmente, porém não menos importante, agradeço pelos sábios conselhos do professor e orientador Eduardo Magrani. Com toda a admiração e respeito, agradeço pela confiança, aprendizado e fundamentais orientações para a conclusão deste trabalho.

Dessa forma, ainda que neste diminuto espaço, deixo o meu agradecimento a todos pelo apoio nos bons e maus momentos dessa jornada acadêmica. Hoje, sou o resultado da confiança e força de cada um de vocês. Obrigado!

RESUMO

JUNIOR, Sergio Ricardo Correia de Sá. A regulação jurídica da proteção de dados no Brasil. 44 p. Monografia (Pós-graduação em Direito) – Pontifícia Universidade Católica do Rio de Janeiro: Rio de Janeiro, 2018.

O presente trabalho acadêmico tem como escopo promover uma análise da nova sistemática de proteção de dados no Brasil. Esta monografia estudará a evolução legislativa do tema no Brasil e sua problemática, sob a ótica dos novos desafios a serem enfrentados para a efetivação tutela ao direito fundamental da privacidade, a fim de proporcionar instrumentos mais claros e eficazes para os indivíduos zelarem pelas informações que lhe dizem respeito. Por fim, verificar-se-á o papel especial do Poder Público, visando criar políticas públicas capazes de proporcionar segurança jurídica à sociedade, bem como proteger, adequadamente, a privacidade dos indivíduos no âmbito nacional.

Palavras Chave: Direito Constitucional e Civil – Proteção de Dados Pessoais – LGPD – GDPR – Privacidade – Internet das Coisas – Big Data – Responsabilidade Civil – Políticas Públicas.

Abreviações

CC – Código Civil

CDC – Código de Defesa do Consumidor

CF – Constituição Federal

GDPR – *General Data Protection Regulation*

LGPD - Lei Geral de Proteção de Dados Pessoais

SUMÁRIO

INTRODUÇÃO

I. Breve delimitação temática da pesquisa

A sociedade está cada vez mais conectada no mundo contemporâneo. Uma era digital que antes parecia uma promessa tão distante, apenas em cenários de filmes futuristas, agora já faz parte da rotina e hábitos diários das pessoas, trazendo, ao mesmo tempo, soluções e desafios introduzidos nessa nova realidade.

Com a evolução da tecnologia, a interação contínua entre dispositivos inteligentes, sensores e pessoas gera uma quantidade crescente de dados que estão sendo armazenados e processados no nosso cotidiano. Nessa esteira da interatividade em rede, ampliando a comunicação entre indivíduos e máquinas, a chamada Internet das Coisas[1] (ou Internet of Things – "IoT", em inglês) desponta como uma das mais impactantes transformações nas estruturas econômicas e sociais da atualidade.

Isso porque diversos produtos integram esse universo da IoT e podem ajudar a resolver problemas reais enfrentados durante o dia a dia da população. Além de eletrodomésticos sensíveis à internet, peças de vestuário, meios de transporte e até brinquedos estão conectados uns aos outros, para atender ao usuário e facilitar a vida, de modos inimagináveis há uma década.

De fato, o contexto de hiperconectividade em ambientes virtuais é capaz de proporcionar mais comodidade aos consumidores, assim como benefícios econômicos ao Estado e às empresas. Não à toa, esse mercado tem chamado a atenção de investidores do setor privado, tendo em vista o seu potencial de oferecer soluções tanto para a indústria, quanto a antigos desafios da administração pública, em questões envolvendo segurança, mobilidade urbana, saúde e criminalidade, por exemplo.

Com efeito, um estudo do McKinsey Global Institute[2] estima que o impacto de IoT na economia global será de 4% a 11% do produto interno bruto do planeta

---

[1] "De maneira geral, pode ser entendido como um ambiente de objetos físicos interconectados com a internet por meio de sensores pequenos e embutidos, criando um ecossistema de computação onipresente (ubíqua), voltado para a facilitação do cotidiano das pessoas, introduzindo soluções funcionais nos processos do dia a dia." MAGRANI, Eduardo. *A internet das coisas*. FGV Editora: Rio de Janeiro, 2018, p. 20.

[2] LOHR, Steve. The Age of Big Data, New York Times. Disponível em: https://www.nytimes.com/2012/02/12/sunday-review/big-datas-impact-in-the-world.html . Acesso em 10/12/2018.

em 2025 (portanto, entre 3,9 e 11,1 trilhões de dólares). No caso específico do Brasil, a estimativa gira em torno de 50 a 200 bilhões de dólares de impacto econômico anual em 2025.

Em contrapartida, a progressão exponencial dos níveis de conectividade gera significativos desafios nas esferas da segurança e privacidade dos indivíduos. Afinal, quanto mais objetos conectados, maior o fluxo de informações produzidos por esses dispositivos em relação aos seus usuários.

Nessa perspectiva, a IoT se comunica com o conceito de "*big data*" [3], pois quanto maior a quantidade de dispositivos conectados à internet, maior o volume massivo de dados processados e analisados em alta velocidade, a fim de transformá-los em informações. Afinal, tudo o que fazemos deixa vestígios digitais[4].

Ocorre que, os consumidores ainda não conhecem claramente a forma de coleta, compartilhamento e o potencial uso desses dados pessoais – e as vezes íntimos – por terceiros. Ademais, falhas de segurança podem permitir ataques a servidores e dispositivos inteligentes a fim de obter essas informações, em razão do seu alto valor de mercado.

Essa preocupação vem crescendo substancialmente em função dos recentes episódios de vazamentos de dados pessoais, envolvendo usuários do Facebook, Uber, Delta, Equifax, dentre outras empresas. Esses incidentes deixaram expostos milhares de dados cadastrais de consumidores, incluindo nomes, endereços, números de cartões de crédito e até mesmo algumas informações mais sensíveis[5], como o DNA e as origens étnicas de várias pessoas, no caso da plataforma eletrônica "My Heritage"[6].

---

[3] Estudo "The Internet of Things: Mapping the Value Beyond the Hype". Disponível em https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world . Acessado em 10/12/2018.

[4] GRASSEGGER, Hannes; KROGERUS, Mikael. *The data that turned the world upside down.* Motherboard, 2017.

[5] "O segundo grupo (dados sensíveis) seriam aqueles que se referem às convicções filosóficas, morais, sociais, políticas e sindicais, religiosas, questões de origem social e ética, vida sexual, orientação sexual e à saúde, incluindo, mas sem limitação, dados genéticos da pessoa. Os dados sensíveis são, sem dúvida, constitucionalmente protegidos pelo "manto" do direito à privacidade (direito fundamental de qualquer brasileiro ou estrangeiro residente no país". BLUM, Rita Peixoto Ferreira. *O direito à privacidade e à proteção dos dados do consumidor.* São Paulo: Almedina, 2018, p. 168.

[6] Estudo "The Internet of Things: Mapping the Value Beyond the Hype". Disponível em https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world . Acessado em 10/12/2018.

Por essas e outras razões, nota-se cada vez mais a necessidade de se garantir mecanismos que possibilitem à pessoa deter controle sobre seus dados – porquanto expressão direta de sua própria personalidade[7]. Inclusive, diversos ordenamentos jurídicos estão considerando a proteção de dados pessoais como um dos pilares da dignidade da pessoa humana e para a tutela do direito fundamental à privacidade[8].

Tal preocupação aumenta ao passo que os dados pessoais se tornam um elemento estratégico em novos modelos de negócios, seja pela facilidade de sua coleta e armazenamento, ou pela sua utilidade para diversos fins comerciais – muitas vezes alheios ao controle e consentimento da pessoa vinculada àquela informação.

Aliás, muitos negócios *on-line* se baseiam em Termos de Uso que são escritos muitas vezes para não serem lidos pelos usuários, mas configuram esse contrato eletrônico, onde a empresa permite a ampla coleta de dados que não estão necessariamente relacionados com o escopo daquele produto ou serviço ofertado.

Diariamente, algoritmos são alimentados por informações pessoais que indicam como pensamos e quais os nossos desejos, criando perfis de consumo dos usuários, para fins de publicidade direcionada[9] e venda desses dados pessoais para outras empresas. Nesse sentido, a proteção da privacidade passa pela proliferação dessas práticas comerciais de "*big data*", "*targeting*" e "*profiling*" dos usuários, deixando as pessoas presas dentro de uma realidade *on-line* customizada ("*tailored reality*") [10].

Existe uma falta de consciência e autonomia da maioria dos consumidores dentro dessa realidade customizada, bem como, por outro lado, um abuso de algumas empresas nesse cenário da otimização de anúncios publicitários. Isso

---

[7] Direito Privado e Internet / Guilherme Magalhães Martins (coordenador). – São Paulo: Atlas, 2014, p. 62.

[8] DONEDA, Danilo. A proteção de dados pessoais como direito fundamental. Revista Espaço Jurídico 12/103. Joaçaba: Unoese, 2011, p. 103.

[9] Nas palavras de Rita Peixoto Ferreira Blum: *"*Os dados dos hábitos de consumo da pessoa, somados ao seu perfil financeiro, idade, e outros elementos que possam influenciar na decisão de compra de novos e melhores produtos, ou contratação de novos serviços são hoje muito importantes para fins de marketing. Por esta razão têm também valor econômico para os fornecedores. Tais dados são úteis a eles seja para estreitar o vínculo que têm com o consumidor, seja para melhor definir o teor da propaganda que será elaborada e apresentada a um consumidor potencial*."* (BLUM, Rita Peixoto Ferreira. *O direito à privacidade e à proteção dos dados do consumidor*. São Paulo: Almedina, 2018, p. 129).

[10] "Assim, ocorre uma espécie de "hipertrofia de atenção", pois os sites e blogs mais populares são os mesmos constantes nos primeiros lugares das pesquisas dos sites de busca, quando se procura por informação política e por isso propensos à acumulação de novos leitores." MAGRANI, Eduardo. *A internet das coisas*. FGV Editora: Rio de Janeiro, 2018, p. 20.

porque os consumidores não sabem ao certo como os seus dados pessoais estão sendo tratados, para onde estão sendo transferidos e para qual finalidade exatamente serão utilizados.

Segundo alguns teóricos, a sociedade já vive em uma realidade orientada e governada por algoritmos. Em muitas plataformas *on-line*, a navegação dos consumidores é direcionada para conteúdos selecionados pelos algoritmos, conforme as suas supostas predileções, porque quanto mais tempo o indivíduo gastar em um determinado site ou rede social, mais dinheiro é gerado para aquela plataforma eletrônica.

Ademais, essas técnicas deixam os indivíduos presos dentro de um filtro bolha, assistindo, por exemplo, apenas aos filmes enquadrados na categoria que se encaixa nos seus respectivos perfis na plataforma de *streaming*. Além de dificultar uma visão sobre o que está fora desse círculo, os algoritmos geram uma comodidade tremenda aos indivíduos. Contudo, as pessoas precisam ter uma visão crítica para além da comodidade do filtro bolha, que oferece riscos à sociedade[11].

Por outro lado, algoritmos não são suficientemente transparentes ou bem compreendidos, além de selecionarem conteúdos de forma automatizada. Dessa forma, a vida na sociedade hiperconectada é permeada por decisões automatizadas, e vários dos tratamentos algoritmos automatizados são feitos por inteligências artificiais.

Ocorre que cada vez mais foge do nosso controle saber como os algoritmos estão chegando àquelas conclusões em cada caso. Para pirar a situação, os algoritmos também estão ficando mais complexos, por causa das técnicas de "*machine learning*", "*deep learning*" e "*neural learning*". Atualmente, já existem algoritmos complexos que se auto programam, sem *imputs* lógicos dos seres humanos, propondo novas saídas para diversos problemas[12].

---

[11] "[...] a própria arquitetura dos sites nos deixa reféns dos algoritmos regulando nosso comportamento assim como o direito e criando obstáculos sérios ao acesso à informação, à autonomia individual, à privacidade e à liberdade de expressão. [...] A premissa do *filter bubble* é que você não decide o que aparece para você dentro da bolha, nem tem acesso ao que fica de fora. [...] Assim, ocorre uma espécie de "hipertrofia de atenção", pois os sites e blogs mais populares são os mesmos constantes nos primeiros lugares das pesquisas dos sites de busca, quando se procura por informação política e por isso propensos à acumulação de novos leitores." (MAGRANI, Eduardo. *Democracia conectada: a internet como ferramenta de engajamento político-democrático*. Curitiba: Juruá, 2014, p. 120-123).

[12] Veja-se o exemplo do Facebook, que colocou dois bots para negociar um produto entre si. Só que eles começaram a fazer novas associações. Eles entenderam que a linguagem humana era ineficiente e criaram uma linguagem própria que deixou de ser compreendida pelos programadores do

A esse respeito, as empresas de tecnologia devem assumir a responsabilidade de acompanhar a capacidade de autoconstrução dos algoritmos e auto evolução da inteligência artificial, principalmente tentando olhar para uma regulação "*by design*", pensando na privacidade durante toda a concepção daquela nova tecnologia.

Portanto, uma vez identificados os potenciais desafios dessa nova realidade, é preciso identificar a resposta jurídica para esses problemas na atualidade. Nesse contexto, buscam-se modelos regulatórios para disciplinar a proteção dos dados pessoais, sem impedir que inovações legítimas beneficiem a sociedade[13].

II. Estrutura do trabalho

Com vistas a proporcionar uma análise lógica e contextualizada do tema acima delimitado, a presente abordagem foi dividida nos próximos três capítulos que compõem este trabalho acadêmico.

Em síntese, a primeira parte do estudo procurará descrever os impactos do novo regramento europeu de proteção de dados pessoais. Neste momento, serão introduzidos alguns aspectos relevantes sobre a sua aplicabilidade, demonstrando como essa regulação impõe limites ao tratamento e processamento de dados pelas empresas, a fim de comparar tais disposições com a posterior regulação no Brasil.

Seguindo essa linha de raciocínio, o segundo capítulo traz a evolução histórica que levou à recente edição do marco regulatório federal para disciplinar a proteção de dados pessoais, de uma forma ampla e unificada, no ordenamento jurídico brasileiro. Aproveitar-se-á esta oportunidade para debater as principais alterações trazidas pela Lei Federal nº 13.709/2018 ("LGPD"), em que pese a ainda escassa doutrina e jurisprudência sobre esse tema.

A seguir, o prosseguimento do estudo se dará à luz das perspectivas para o cenário brasileiro, tendo em vista o papel do Poder Judiciário e dos órgãos de defesa do consumidor, bem como a necessária criação de uma Autoridade Nacional de

---

Faceboook, que desativaram esse projeto. Os bots não tinham recebido essa ordem, mas concluíram que essa forma seria mais eficiente. Notícia disponível em: https://www.tecmundo.com.br/inteligencia-artificial/117983-bots-facebook-criam-linguagem-conta-propria-conversar-melhor.htm. Acessado em 10/12/2018.

[13] Notícia disponível em: https://g1.globo.com/economia/tecnologia/noticia/mark-zuckerberg-depoe-ao-senado-sobre-uso-de-dados-pelo-facebook.ghtml. Acessado em 19/07/2018.
Ver também: https://www.conjur.com.br/2017-mai-16/europa-punir-facebook-violacoes-leis-privacidade. Acessado em 10/12/2018.

Proteção de Dados – ainda pendente de regulamentação – para que o cumprimento da nova legislação ocorra da maneira adequada, protegendo a privacidade dos indivíduos.

Por fim, ante todo o exposto, o trabalho será concluído com breves comentários acerca dos resultados obtidos com o presente estudo acadêmico, considerando o contexto de um mundo cada vez mais dependente da coleta e do tratamento de dados pessoais.

CAPÍTULO 1 – ASPECTOS RELEVANTES DO NOVO REGRAMENTO EUROPEU SOBRE A PROTEÇÃO DE DADOS

À luz desse recorte interdisciplinar, com o objetivo de reduzir os riscos de abusos na coleta, no tratamento, uso e transferência de dados na União Europeia (UE), em 2016, foi publicado o Regulamento Geral de Proteção de Dados ("*General Data Protection Regulation*" - GDPR). Após uma *vacatio legis* de dois anos, essa norma entrou em vigor em maio deste ano, estabelecendo um novo regime regulatório para todos os estados membros da UE e substituindo, assim, a antiga Diretiva 95/46 CE, de 1995[14].

O presente trabalho não pretende exaurir todas as peculiaridades do referido regramento, mas serve para destacar alguns aspectos relevantes sobre a sua aplicabilidade, inclusive para as empresas brasileiras, que possuem relacionamento com clientes ou parceiros europeus[15]. Isto porque, extrapolando os limites da aplicação territorial, o GDPR também afeta as organizações estabelecidas fora da

[14] Desde 24/05/2018 não está mais vigente a Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Tradução livre de "Directive No. 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data". Disponível em: https://wipolex.wipo.int/en/text/313007 . Acessado em 10/12/18.

[15] "A ideia é garantir uma proteção ampla a todos os indivíduos que tiverem seus dados coletados de alguma forma por empresas ou instituições que realizam transferência de dados com organizações europeias, fazendo com que as mesmas prestem contas nesse sentido." MAGRANI, Eduardo. Artigo disponível em: http://eduardomagrani.com/seis-pontos-para-entender-o-regulamento-geral-de-protecao-de-dados-da-ue/ . Acessado em: 10/12/18.

União Europeia, mas que realizem negócios naquele território, ou ofereçam bens e serviços que coletem dados pessoais relacionados à UE[16].

Em linhas gerais, segundo o GDPR, as empresas precisam obter o consentimento expresso e inequívoco dos titulares de dados para autorizar a coleta e tratamento desses dados, devendo expor claramente como essas informações serão utilizadas, além de explicar o mecanismo pelo qual os indivíduos poderão revogar esse consentimento, a qualquer momento.

Outra novidade é o chamado direito ao esquecimento, previsto no art. 17 do GDPR, para casos nos quais a retenção de tais dados infrinja o Regulamento ou a legislação da União ou Estado Membro a que o controlador está sujeito. Assim, o referido dispositivo elenca diversas hipóteses[17] não exaustivas em que esse direito poderá ser requerido, como por exemplo, quando os dados deixam de ser necessários em relação à finalidade que motivou a sua coleta.

Ademais, as empresas ficam obrigadas a cumprir medidas de proteção de dados a partir da criação de qualquer nova tecnologia, garantindo também que os mecanismos de proteção adequada sejam incorporados aos produtos já existentes.

Por outro lado, o princípio da minimização ainda prevê que os dados pessoais devem ser adequados, pertinentes e limitados em relação aos fins para os quais serão processados. Ou seja, as empresas só devem coletar e processar os dados minimamente necessários para uma determinada finalidade e nos limites do consentimento concedido.

Além dessa importante restrição ao uso indiscriminado dos dados pessoais, segundo o princípio "*accountability*", os processadores de dados sujeitos às disposições do GDPR precisarão manter registros detalhados de suas atividades,

---

[16].MAGRANI. Eduardo. Artigo disponível em: https://feed.itsrio.org/seis-pontos-para-entender-a-lei-europeia-de-prote%C3%A7%C3%A3o-de-dados-pessoais-gdpr-d377f6b691dc. Acessado em 10/12/2018.

[17] "Como se percebe, essa nova regulamentação parece bastante alinhada com a ideia de controle de dados pessoais – uma perspectiva mais próxima do art. 7º, X, do Marco Civil da Internet do que do modo como o direito ao esquecimento vem sendo discutido no Brasil. [...] E, embora ainda haja quem defenda que o direito ao esquecimento não existe, tanto doutrina quanto jurisprudência parecem mais inclinadas a debater não sua existência, mas as regras mais adequadas para sua aplicação." BRANCO, Sergio. *Memória e esquecimento na internet*. Porto Alegre: Arquipélago Editorial, 2017, p. 165.
Vide também: "No entanto, nota-se uma ampliação desproporcional do instrumento. Isto porque o conceito "tradicional" de direito ao esquecimento pressupõe uma ponderação mais cuidadosa dos critérios específicos, a fim de não ferir a liberdade de expressão e o acesso à informação." MAGRANI, Eduardo. Artigo disponível em: http://eduardomagrani.com/seis-pontos-para-entender-o-regulamento-geral-de-protecao-de-dados-da-ue/ . Acessado em: 10/12/18.

exigindo-se que as organizações implementem medidas técnicas e organizacionais apropriadas, e sejam capazes de prestar contas e demonstrar sua eficácia, quando solicitadas.

Na Europa, a política de privacidade do Facebook foi objeto de recentes questionamentos à rede social, que teria descumprido a lei francesa de proteção de dados pessoais, ao supostamente vender informações de navegação dos seus usuários para empresas interessadas em realizar anúncios de produtos e serviços, por meio de publicidade direcionada.

Considerando esse cenário, o regramento europeu também exige que as empresas responsáveis pelo processamento de um grande volume de dados poderão ser demandadas a nomear um "*Data Protection Officer*" (DPO), para monitorar essas atividades e garantir o cumprimento do GDPR. Qualquer violação à privacidade de dados pessoais deverá ser notificada ao órgão regulador, no prazo máximo de 72 horas, após identificado o fato ocorrido.

Com efeito, as sanções previstas no GDPR também são mais gravosas, chegando a multas de até 2% do volume anual de negócios mundiais da empresa infratora, com uma multa mínima de 10 milhões de euros.

Dessa forma, espera-se que essa regulação crie limites ao tratamento e processamento de dados pessoais pelas empresas envolvidas nesse contexto. Em abril de 2018, Mark Zuckerberg teve que prestar extenso depoimento em uma audiência no Senado dos Estados Unidos, para explicar como o Facebook reagiu ao vazamento de dados de 87 milhões de pessoas pela consultoria política Cambridge Analytica. Naquela ocasião, o executivo afirmou que a empresa vai investir em medidas para proteger os dados de usuários da rede social[18].

Convém ressaltar ainda que o direito europeu também vai além do conceito básico de dados pessoais (nome, número de identidade, CPF) e considera as informações que, apesar de isoladamente não identificarem alguém, acabam levando a uma possível identificação. Assim, consideram-se dados de localização geográfica, endereço e IP de dispositivos utilizados por pessoas físicas, assim como o perfil comportamental sobre as notícias e anúncios clicados pelos consumidores. Considerando esse conceito amplo, é muito difícil imaginar um cenário em que a referida lei não se aplique no caso concreto.

[18] Direito Privado e Internet / Guilherme Magalhães Martins (coordenador). – São Paulo: Atlas, 2014, p. 62.

Em seu artigo 9º, o GDPR ainda destaca a importância de uma categoria especial para os dados sensíveis, submetidos a um regime específico, que veda o processamento desse tipo de dado pessoal, exceto nas dez hipóteses elencadas no dispositivo. Nesse sentido, salvo raras exceções, o regramento europeu confere uma proteção especial àqueles dados capazes de revelar informações de cunho íntimo, por conter origem racial ou étnica; opiniões políticas; crenças religiosas ou filosóficas; filiação sindical; dados sobre saúde ou vida sexual e orientação sexual; dados genéticos e dados biométricos para fins de identificação pessoal.

Para que esses dados sensíveis possam ser tratados, de forma devida, os critérios de consentimento foram ampliados pelo GDPR, devendo o consentimento ser livre, explícito, inequívoco, informado e específico.

Nesse sentido, já surgem os primeiros litígios envolvendo o GDPR na Europa. A iniciativa surgiu do portal *My Privacy is none of your Business* (NOYB)[19] que ajuizou quatro ações perante autoridades administrativas na Áustria, Bélgica, Alemanha e França, respectivamente contra o Facebook, Instagram, WhatsApp e Google questionando o modelo de consentimento "forçado" dessas plataformas digitais.

Por fim, convém ressaltar que, segundo o artigo 46 do GDPR, uma vez obtido o consentimento expresso e inequívoco do titular de dados, os responsáveis pelo tratamento só poderão realizar a transferência desses dados para outros países ou organizações internacionais, se estes tiverem apresentado leis adequadas de proteção.

Diante desse contexto, o regramento europeu serviu como catalisador para que o Brasil editasse uma legislação específica de proteção de dados pessoais, pois, caso contrário, não poderia realizar troca de dados com a UE. Dessa forma, a não adaptação ao GDPR prejudicaria as atividades das empresas brasileiras, enfraquecendo a competitividade e a inovação na economia nacional, se o país não estabelecesse uma agenda regulatória para se adequar às regras globais sobre o assunto.

---

[19] Disponível em https://noyb.eu/ . Notícia disponível em: https://money.cnn.com/2018/05/25/technology/gdpr-compliance-facebook-google/index.html . Acessado em 10/12/2018.

CAPÍTULO 2 – A NOVA LEI DE PROTEÇÃO DE DADOS PESSOAIS NO BRASIL

No âmbito nacional, essa questão também já vem sendo debatida nos últimos anos há praticamente uma década. No entanto, o ordenamento jurídico brasileiro ainda não possuía um marco regulatório federal para disciplinar a proteção geral de dados pessoais de uma forma completa e unificada; a regulamentação era feita de forma esparsa, carecendo de uniformidade e segurança jurídica[20].

Até então, a Constituição Federal[21] servia como a principal resposta jurídica aos problemas que vinham surgindo nos últimos anos, relacionados ao cenário da crescente hiperconectividade. Embora o constituinte originário não pudesse prever, ao final da década de 80, os riscos que envolvem a proteção de dados atualmente, o artigo 5º, inciso X, da CRFB/88 já previa a inviolabilidade da intimidade, vida privada, honra e imagem das pessoas, garantindo o direito de "indenização pelo dano material ou moral decorrente de sua violação".

Nesse sentido, também eram aplicáveis outros diplomas ainda vigentes, como o Código Civil[22] – dispondo, por exemplo, sobre a proteção à personalidade, imagem e intimidade –, a Lei de Acesso à Informação (LAI)[23], o Código de Defesa do Consumidor[24] (CDC), o Marco Civil da Internet (MCI), a Lei de Cadastro Positivo e a Lei de delitos informáticos.

---

[20] BIONI, Bruno Ricardo. De 2010 a 2018: a discussão brasileira sobre uma lei geral de proteção de dados pessoais. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/de-2010-a-2018-a-discussao-brasileira-sobre-uma-lei-geral-de-protecao-de-dados-02072018. Acessado em: 10/12/2018.

[21] Com efeito, o artigo 5º da Constituição Federal garante a todos os "*brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade"*, alçando a privacidade ao *status* de direito fundamental, decorrente das garantias constitucionais que se relacionam com a dignidade da pessoa humana. Nesse sentido: DONEDA, Danilo. A proteção de dados pessoais como direito fundamental. Revista Espaço Jurídico 12/103. Joaçaba: Unoese, 2011, p. 103.

[22] A Lei Federal nº 10.406, de 10 de janeiro de 2002 ("Código Civil"), em seu artigo 21, prevê a inviolabilidade da vida privada, devendo "o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma".

[23] A Lei Federal nº 12.527, de 18 de novembro de 2011 regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do §3º do art. 37 e no §2º do art. 216 da Constituição Federal, dentre outras providências.

[24]"O Código de Defesa do Consumidor (Lei 8.078/90) foi a primeira lei infraconstitucional a se preocupar com a proteção da privacidade. Por isso, em seu art. 43, estabelece critérios para abertura de cadastros e para a manutenção das informações nele contidas, entre outras provisões." BRANCO, Sergio. *Memória e esquecimento na internet*. Porto Alegre: Arquipélago Editorial, 2017, p. 147.

O CDC[25] define quais são os direitos básicos do consumidor e, dentre as práticas comerciais utilizadas para a captura de dados, algumas já poderiam ser enquadradas como abusivas nesse contexto. Com efeito, o consumidor que tinha seus dados eventualmente coletados pelo fornecedor sem perceber o fato e, portanto, sem anuir com essa conduta, já estava em situação de vulnerabilidade técnica – que pode ensejar manifestação de vontade viciada – uma vez que não lhe foram corretamente informadas as características essenciais do serviço[26].

Tal prática violaria um dos princípios basilares do CDC, qual seja, o da boa-fé, assim como direitos básicos do consumidor à informação adequada e clara sobre o serviço, além da proteção à publicidade enganosa e abusiva.

Assim como o diploma consumerista, o Marco Civil da Internet[27] também demonstrou uma preocupação fundamental com a tutela da segurança e da

---

[25] O artigo 6º do CDC prevê alguns direitos básicos do consumidor, tais como: "a proteção da vida, saúde e segurança contra os riscos provocados por práticas no fornecimento de produtos e serviços considerados perigosos ou nocivos". Ademais, pode-se citar os seguintes dispositivos relevantes:
"Art. 8° Os produtos e serviços colocados no mercado de consumo não acarretarão riscos à saúde ou segurança dos consumidores, exceto os considerados normais e previsíveis em decorrência de sua natureza e fruição, obrigando-se os fornecedores, em qualquer hipótese, a dar as informações necessárias e adequadas a seu respeito."
"Art. 10. O fornecedor não poderá colocar no mercado de consumo produto ou serviço que sabe ou deveria saber apresentar alto grau de nocividade ou periculosidade à saúde ou segurança."
"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.
§1º O produto é defeituoso quando não oferece a segurança que dele legitimamente se espera, levando-se em consideração as circunstâncias relevantes [...]"
"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."
[26] BLUM, Rita Peixoto Ferreira. *O direito à privacidade e à proteção dos dados do consumidor.* São Paulo: Almedina, 2018, p. 61).
[27] O artigo 7º do MCI ressalta que a importância do acesso à internet para o exercício da cidadania, assegurando aos usuários: *"I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação; 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; [...] VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei; [...] IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais; X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei; [...] XIII - aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na internet.;"*.
Ademais, o artigo 11 do MCI prevê que *"em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão*

privacidade dos dados pessoais, ao restringir o acesso ou uso de informações privadas na *internet*.

Não à toa, o MCI prevê o respeito às regras de consumo; inviolabilidade da intimidade da vida privada, bem como do sigilo no fluxo de comunicações pela *internet*; guarda e disponibilização dos registros de acesso a aplicações de *internet*, devendo atender à preservação da intimidade, honra e imagem das partes envolvidas.

Nesse sentido, o art. 7º, X, do MCI já previa o direito do usuário à "*exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros*" [28].

No entanto, em que pese o avanço gradual na tutela da privacidade dos dados pessoais, essa evolução se mostrava lenta frente aos desafios dos novos tempos. No contexto da sociedade da informação, nota-se que o desenvolvimento da tecnologia e das técnicas de marketing ensejam, ao mesmo tempo, benefícios e desafios à tutela de direitos fundamentais.

Assim, percebe-se que a legislação até então vigente se mostrava insuficiente para a proteção da intimidade, vida privada, honra e imagem das pessoas, face aos novos problemas que vêm surgindo na atualidade. A título exemplificativo, o modelo de consentimento para a contratação eletrônica de um serviço ainda é um grave problema a ser resolvido, considerando que muitas pessoas não leem os Termos e Usos das plataformas digitais.

Apesar de termos contratos eletrônicos baseados em Termos de Uso, eles muitas vezes são escritos para não serem lidos. Não temos um modelo perfeito de consentimento nesse tipo de coleta de dados pessoais.

Ademais, alguns conceitos legais ainda estão dispostos de forma genérica, sem uma definição clara e específica, apta a garantir a proteção de dados pessoais e a eficaz segurança de seus titulares. O Decreto nº 8.771/2016, regulamentador do

---

ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros." (Grifou-se)

[28] "Há quem chame esse dispositivo de "direito ao esquecimento de dados pessoais", embora pareça mais adequado incluí-lo apenas entre as previsões de proteção de dados pessoais derivadas da concepção contemporânea do direito à privacidade." BRANCO, Sergio. *Memória e esquecimento na internet*. Porto Alegre: Arquipélago Editorial, 2017, p. 145-146.

Marco Civil da Internet[29], define o que é um dado pessoal, mas não especificou o conceito de dados sensíveis. Essa definição – trazida, como visto, pelo GDPR europeu – ainda não tinha previsão no ordenamento jurídico brasileiro. Nessa realidade digital, onde os dados não têm fronteiras, uma Lei Geral de Proteção de dados pessoais era uma pauta urgente no Brasil, a fim de colocá-lo no mesmo patamar de outros países do mundo.

Analisando uma breve retrospectiva histórica, pode-se entender o contexto que fomentou essa regulamentação local, a partir de fatores sociais e políticos que foram decisivos para impulsionar os trâmites legislativos no Congresso Nacional. A trajetória para o modelo atual começou a partir de 2010, com a primeira consulta pública sobre o tema, em um blog[30] disponibilizado pelo Ministério da Cultura. Naquela ocasião, algumas empresas e pessoas interessadas já puderam contribuir até abril de 2011 com os primeiros debates sobre uma proposta de regulação da proteção de dados pessoais no Brasil.

Em 2013, Edward Snowden, ex-analista de sistemas da CIA, agência central de inteligência dos Estados Unidos, revelou detalhes sigilosos do programa de vigilância global e espionagem do governo norte-americano sobre o tráfego de comunicações e informações de vários países[31].

Esse escândalo causou comoção social e política na época, alertando o Brasil, a União Europeia e outras nações que ainda não estavam participando dessa discussão, tampouco preocupadas com a necessidade de uma mudança de paradigma sobre a proteção dos dados pessoais.

Tal evento ajudou a acelerar o trâmite para a aprovação do Marco Civil da Internet no Brasil, visto inicialmente como um microssistema de proteção de dados pessoais. No entanto, ainda havia a necessidade de se tutelar algumas questões

---

[29] O Decreto nº 8.771, de 11 de maio de 2016 regulamenta o MCI 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. Em seu artigo 14, inciso I, o referido Decreto considera dado pessoal como todo *"dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa."*

[30] Disponível em: http://culturadigital.br/ . Acessado em 18/11/2018.

[31] Disponível em https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1 . Acessado em 18/11/2018.

específicas não tratadas pelo MCI, como por exemplo, a proteção de dados sensíveis na internet.

Em 2016, após uma segunda consulta pública sobre o tema, formou-se uma comissão especial para opinar sobre as propostas legislativas em curso no Congresso Nacional e, naquela ocasião, diversas entidades públicas nacionais e internacionais participaram do debate, contribuindo para amadurecer as ideias ventiladas até então.

A conjuntura política também auxiliou no avanço das discussões sobre um marco regulatório para a proteção de dados pessoais, já que medidas neste sentido poderiam auxiliar no ingresso do Brasil – cujo pedido de adesão ainda está sob análise – no grupo dos países membros da Organização para a Cooperação e Desenvolvimento Econômico ("OCDE").

Somada a essa questão, em março de 2018, o Banco Nacional de Desenvolvimento Econômico e Social (BNDES) divulgou o relatório de um extenso estudo, realizado em parceria com o Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC), para o diagnóstico e a proposição de um plano de ação estratégico com projetos para o país em Internet das Coisas[32].

Tal iniciativa serviu para analisar aspectos regulatórios sobre a proteção de dados pessoais, a fim de promover o desenvolvimento competitivo da economia brasileira.

Ainda no início deste ano, também tivemos o caso da Cambridge Analytica[33], uma empresa privada que combinava mineração e análise de dados com comunicação estratégica para processos eleitorais.

Por fim, em maio de 2018, com a vigência do GDPR, que substituiu uma antiga diretiva da União Europeia, antes facultativa, sobre o tratamento de dados e mostrou ao Brasil a necessidade de uma legislação vinculativa sobre o assunto. Ademais, o regramento europeu dispõe que só pode haver fluxo internacional de dados se o outro país tiver uma lei adequada de proteção da privacidade, semelhante ao GDPR.

---

[32] Disponível em: https://www.bndes.gov.br/wps/portal/site/home/conhecimento/pesquisaedados/estudos/estudo-internet-das-coisas-iot/estudo-internet-das-coisas-um-plano-de-acao-para-o-brasil. Acessado em 20/11/2018.

[33] Notícia disponível em: https://www.theguardian.com/uk-news/cambridge-analytica . Acessado em 10/12/2018.

Eis que, finalmente, em 10 de julho de 2018, o plenário do Senado Federal aprovou o Projeto de Lei da Câmara nº 53/2018, que altera o artigo 7º, inciso X e o artigo 16, inciso II, do Marco Civil da Internet, para disciplinar a proteção dos dados pessoais no Brasil e definir as situações em que estes podem ser coletados e tratados, tanto por empresas quanto pelo Poder Público.

Com isso, o Brasil saiu do rol minoritário de países para se juntar a diversos outros do mundo, que já possuem legislação específica sobre o tema. Com a sanção do presidente Michel Temer, a Lei Federal nº 13.709, de 14 de agosto de 2018 entrará em vigor em fevereiro de 2020, após 18 meses de sua publicação no Diário Oficial da União, tratando de diversos pontos que não possuíam previsão legal até então, ou eram tratados apenas de maneira esparsa por leis setoriais, que formavam uma colcha de retalhos sobre o tema.

Ao unificar esses assuntos em 65 artigos, a Lei 13.709/18 (Lei Geral de Proteção de Dados – "LGPD") estabelece uma série de restrições para instituições privadas e públicas que armazenem dados de internautas, consumidores, partes em um contrato, usuários de serviços públicos ou alvos de políticas públicas. Assim, a nova legislação almeja promover a necessária proteção aos direitos fundamentais da liberdade e privacidade dos indivíduos.

Com efeito, a LGPD tem grande influência do regulamento europeu sobre a matéria. Assim como no GDPR, para coletar, processar ou transferir dados de uma pessoa, será preciso obter a permissão do titular dessas informações, sob pena de pagar uma severa multa – no caso do Brasil, de até 50 milhões de reais.

Portanto, nota-se que o diálogo entre o direito regulatório e a tecnologia ficou exponencial nos últimos anos para suprir uma lacuna que havia no quadro legislativo da sociedade contemporânea, especialmente em decorrência do cenário da hiperconectividade e dos riscos trazidos por essa nova realidade.

Mais do que uma modificação legislativa, o advento da LGPD deve representar uma mudança cultural no âmbito da proteção de dados pessoais no Brasil – a exemplo da experiência europeia – proporcionando instrumentos mais claros e eficazes para os indivíduos zelarem pelas informações que lhe dizem respeito.

2.1 Escopo de aplicação e princípios da LGPD

A aplicação da LGPD é basicamente voltada a pessoas físicas e naturais, cujos dados pessoais estejam tendo o tratamento feito por empresas ou órgãos públicos. Veja-se como os objetivos dessa lei ficam claros já no seu artigo 1º:

> *"Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural."* (Grifou-se)

Assim, a LGPD não se aplica a dados relacionados às pessoas jurídicas, porquanto já tutelados na esfera da propriedade intelectual. Por outro lado, segundo o seu artigo 4º, a referida lei também não se aplica ao tratamento de dados pessoais realizados por pessoa natural para fins particulares e não econômicos; ou exclusivamente para fins jornalístico, artístico ou acadêmico; bem como para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais.

Além disso, a LGPD também não se aplica a dados de pessoas falecidas e dados em trânsito, ou seja, aqueles que não têm como destino Agentes de Tratamento no Brasil.

Sobre o âmbito geográfico de proteção, a LGPD será aplicável aos dados tratados no território brasileiro, ainda que envolvendo um estrangeiro. A questão que ainda preocupa e se mostra como um grande desafio se refere à forma de coercitividade dessa norma.

Por sua vez, a nova lei também traz uma série de princípios norteadores dessa regulação, que espelham os principais fundamentos do mencionado regramento europeu. Aliás, já é possível notar que a LGPD e o GDPR têm mais pontos de convergência do que diferença entre si.

Segundo os princípios da finalidade, adequação e necessidade, correspondentes ao "*data minimisation*[34]", os dados pessoais devem ser adequados, relevantes e limitados em relação aos fins específicos para os quais eles são processados. Essa importante garantia busca impedir justamente o uso ilimitado dos

[34] O princípio do "*data minimisation*" está previsto no artigo 5º, 1 (c) do GDPR, exigindo que sejam coletados apenas os dados adequados, relevantes e necessários para a sua respectiva finalidade: "*Personal data shall be: adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')*".

dados pessoais coletados, de forma diversa a que os titulares destas informações poderiam esperar.

Conforme o princípio do livre acesso[35], além de poder obter uma cópia gratuita dos seus dados coletados, o titular também tem o direito de saber a forma pela qual seus dados estão sendo processados pelo controlador, que deverá cumprir com o requisitado dentro do período de 1 (um) mês.

Ainda, pelo princípio da qualidade dos dados[36], estes devem ser precisos e, quando necessário, atualizados. Ademais, tendo em vista os fins para os quais são processados, deve tomar-se todos os passos razoáveis para garantir que os dados pessoais imprecisos serão apagados ou corrigidos sem demora.

Em relação ao princípio da transparência[37], organizações deverão providenciar tanto informações extensivas aos indivíduos quanto ao processamento de seus dados pessoais e que isso deverá ser feito de forma concisa, transparente, inteligível e acessível ao titular dos dados.

Os princípios da segurança e prevenção[38], por sua vez, determinam que os dados sejam processados de forma a garantir a segurança adequada, incluindo a proteção contra o processamento não autorizado ou ilegal. Ademais, estabelece proteção contra perdas, destruições ou danos acidentais, utilizando medidas técnicas ou organizacionais adequadas.

Já o princípio da não discriminação[39], que também encontra correspondência no GDPR europeu, veda a utilização de dados sensíveis. O preâmbulo, em seu item 85, reforça a premissa de que a violação de dados pessoais pode, quando não abordada de forma apropriada, resultar em danos diversos, como perde de controle do titular sob seus próprios dados, roubo de identidade e discriminação. Portanto, assim que o controlador de dados identificar que houve uma violação, deve notifica-la às autoridades de supervisão imediatamente.

---

[35] O princípio conhecido como "*right of information and access*" está previsto no art. 15 do GDPR, assegurando o direito do titular dos dados a obter informações do responsável pelo seu tratamento, bem como o acesso a esses dados pessoais.

[36] Os direitos de retificação e restrição de processamento de dados pessoais ("*accuracy*") estão previstos nos artigos 5º, 1 (d), 16, 18 e 19 do GDPR ("*right to rectification and restriction of processing*").

[37] O art. 5º 1 (a) do GDPR também define que os dados pessoais serão processados de forma legal, justa e transparente em relação à assunto dos dados ("*lawfulness and fairness & transparency*").

[38] Correspondente aos princípios "*integrity & confidentiality*" no GDPR.

39 Em seu preambulo, o GDPR dispõe sobre a possibilidade de processamento de dados pessoais oferecer riscos aos direitos e liberdades de pessoais naturais. Entre danos físicos, materiais e não materiais, destacam-se a perda da confidencialidade dos dados pessoais e a discriminação.

Ocorre que, a LGPG não estabeleceu um parâmetro de tempo para essa comunicação. Como visto, o GDPR, por exemplo, determina que uma empresa deve comunicar aos consumidores em até 72 horas caso haja um vazamento de dados. Como muitas empresas só descobrem um vazamento meses após o ocorrido, as empresas deverão fazer um investimento grande para o "*compliance*" com essa nova exigência do regramento europeu.

Ademais, ainda restam dúvidas sobre a forma de identificar se o algoritmo está dando tratamento discriminatório e violando os Termos de Uso da Plataforma. Órgãos de Defesa do Consumidor, o Poder Judiciário e o Ministério Público deverão cuidar dessas questões, a fim de tutelar os direitos difusos e coletivos.

2.1.1 O direito à explicação na LGPD e problemática das decisões automatizadas

Como visto, além de não serem suficientemente transparentes ou bem compreendidos, os algoritmos selecionam conteúdos de forma automatizada, por inteligências artificiais, que memorizam as predileções dos usuários conforme as suas buscas e acessos na internet.

Entretanto, na medida em que a sociedade está perdendo o controle de como os algoritmos estão chegando às próprias conclusões – muitas vezes se auto programando, sem *imputs* lógicos dos seres humanos – fica cada vez mais difícil aplicar o direito à explicação, concebido como extensão do princípio da boa-fé e do direito à transparência.

Ressalte-se que esse direito, entendido como o "*direito de receber informações suficientes e inteligíveis que permita ao titular dos dados entender a lógica e os critérios utilizados para tratar seus dados pessoais para uma ou várias finalidades*", já existia antes de ser expressamente introduzido pela LGPD.

A sua proteção, no entanto, decorria de uma regulação setorial, disposta no microssistema do CDC e da Lei de Cadastro Positivo, voltada às decisões automatizadas relativas à concessão de crédito, modelagem e cálculo de risco de crédito. Apesar do seu escopo reduzido de aplicação antes da LGPD, é essencial compreender os princípios que fundamentam o direito à explicação na atualidade,

pois ainda são os mesmos que continuam a legitimar a sua expansão, ocorrida em decorrência da situação fática das novas tecnologias.

A fim de garantir o pleno gozo dos direitos dos consumidores, o CDC busca evitar práticas abusivas e discriminatórias, a fim de garantir um ambiente comercial saudável, pautado pelos princípios da transparência e da boa-fé nas relações de consumo.

A teor do disposto no artigo 43 da LGPD, fica claro o direito do consumidor à informação quanto aos seus cadastros, bancos de dados, informações a seu respeito e às respectivas fontes, além de garantir que elas estejam dispostas de uma maneira clara para a sua compreensão. Afinal, o direito à informação não pode ser gozado em plenitude se os arquivos compartilhados são ininteligíveis.

Nesse sentido, o artigo 46 da LGPD dispõe que os consumidores não podem ser induzidos a contrair obrigações se não tiverem a oportunidade de tomar conhecimento prévio do conteúdo do contrato, ou se as informações não forem claras – porquanto redigidas com o propósito de dificultar a compreensão do leitor.

Em compasso com os princípios que regem as relações de consumo, a Lei do Cadastro Positivo (Lei 12.414/2011 - LCP), que busca disciplinar a consulta a banco de dados com informações de adimplemento para a formação de histórico de crédito, também tem como objetivo reduzir a assimetria de informações e a possibilidade da coleta de dados apenas após o consentimento do consumidor.

Assim, em seu art. 5º, incisos IV a VII, a LCP garante o direito à explicação quanto às decisões automatizadas em relações de consumo. Esse é o caso da distinção da taxa de juros entre diferentes consumidores, com base em suas características pessoas, colhidas e armazenadas em bancos de dados.

A norma também limita os tipos de dados que podem ser utilizados para o cálculo do risco de crédito, vedando dados pessoas sensíveis e aqueles relacionados "à origem social e étnica, à saúde, à informação genética, à orientação sexual e às condições políticas, religiosas e filosóficas".

Por vez, cumpre ressaltar o posicionamento firmado pelos tribunais superiores sobre o tema. Após a edição da Súmula 550 do STJ, que permite a utilização de dados pessoas para fins de crédito mesmo sem o consentimento do credor, garantido o direito à explicação, o Tribunal, no julgamento do RESP 1.304.736/RS, estabeleceu que para existir interesse de agir do consumidor quanto

à utilização de suas informações, é necessário que as decisões tenham um impacto específico na vida das pessoas.

No entanto, a restrição do direito à explicação positivada no microssistema de normas é insuficiente para lidar com as situações que se apresentam na vida moderna. Afinal, a implementação de novas tecnologias permite o uso comercial de dados pessoais voltados para cenários além da concessão de crédito aos consumidores, podendo ser aplicados à saúde, com a análise de dados genéticos; à educação, para garantir educação diferenciada a cada criança com base em suas características e inclinações; ao emprego, com a triagem do currículo de candidatos; à informação, com a criação de perfis comportamentais; à liberdade, com a dosimetria da pena; à cidadania, com o acesso a serviços públicos vinculado à pontuações dos cidadãos, em alguns países.

Ante os exemplos apresentados, resta claro que existem casos na vida moderna em que os dados pessoais, apesar de terem relação consumerista - protegidos pelo CDC -, não encontram a devida proteção, tal qual a garantida pela LCP.

A fim de garantir que tais direitos pudessem ser utilizados nas mais diversas situações, a LGPD estabelece o direito à explicação, em concordância com outras normas e no mesmo sentido do entendimento já firmado pelo STF, de que o dever de informação decorre das obrigações derivadas da boa-fé objetiva.

Dessa forma, é garantido aos titulares dos dados *"informações claras, precisas e facilmente acessíveis sobre a organização do tratamento e os respetivos agentes de tratamento."*[40]

Outra garantia do direito à explicação da LGPD não prevista no ordenamento europeu se refere ao tratamento e a re-identificação de dados anonimizados, quando utilizados na formação de perfis comportamentais de pessoas identificadas.

Nasce, assim, como consequência para o direito à explicação - que consiste em não estar sujeito a decisões totalmente automatizadas - o *direito à revisão*, no qual o titular dos dados pode postular que a decisão, com impacto em seus

[40] Dispõe o artigo 6º da Lei de Proteção de Dados Brasileira: as atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: (...) VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial". Ver: BRASIL (2018).

interesses, seja novamente analisada por uma pessoa natural para deixar claro os critérios utilizados naquela decisão.

Afinal, se não forem claras as informações prestadas, necessárias para que o particular exerça seu direito à oposição, é necessário que ele entenda, também, como o próprio sistema funciona.

Diante da possibilidade de recusa da empresa gestora dos dados em fornecer as explicações solicitadas, ganha destaque o papel exercido pela futura Autoridade Nacional de Proteção de Dados. Essa, que pode, após processo administrativo, realizar auditorias nos sistemas da entidade[i] a fim de verificar a existência de aspectos discriminatórios no uso de dados pessoais. Em razão dessas distinções serem um trabalho extremamente técnico, resta clara a necessidade do corpo da ANPD contar com profissionais altamente especializados e preparados.

2.2 Responsabilidade civil no âmbito da proteção de dados

Como visto, cada vez mais uma parte expressiva do ser humano está no ambiente digital, reduzindo a distinção entre a vida *on-line* e a *off-line*. A quantidade de informações pessoais disponibilizadas na internet representa quem nós somos, o reflexo direto da nossa personalidade. Sendo assim, há uma necessidade de se considerar a proteção de dados pessoais como um direito fundamental para a proteção da pessoa humana[41].

Poucos setores jurídicos têm passado por mudanças tão drásticas e rápidas quanto a responsabilidade civil. Agora é o momento ideal para analisar o conceito do dever de reparar danos, porquanto inserido em circunstâncias novas. Em alguns casos, no contexto da proteção de dados, é possível aplicar a responsabilidade civil para a reparação *in natura* e compensação pecuniária.

Com efeito, nota-se que as empresas tendem a investir muito mais em segurança para a proteção dos dados, quando estão sujeitas ao dever de reparação civil por eventuais danos decorrentes da sua falha.

[41] Direito Privado e Internet / Guilherme Magalhães Martins (coordenador). – São Paulo: Atlas, 2014, p. 62.

A responsabilidade civil, no âmbito da proteção de dados, é uma obrigação derivada, que nasce de outra relação na qual uma obrigação primária foi descumprida.

Com efeito, as empresas devem passar por uma reavaliação dos seus termos de consentimento, cumprindo com os requisitos de informação, sendo uma das obrigações que possivelmente irão gerar dever de indenizar no cenário da proteção de dados.

Sobre os registros de processamento, o art. 37 da LGPG dispõe sobre o controlador e operador de dados, instituindo uma nova obrigação de registrar o processamento de dados, como se fosse um "livro caixa".

Ademais, a comunicação sobre o vazamento de dados, previsto no art. 48 da referida Lei também pode gerar dever de indenizar, a cada vez que a violação comprometer a integridade, disponibilidade, confidencialidade dos dados.

Assim, será necessário verificar se a providência tomada pela empresa em termos de segurança era ou não suficiente, pois esse grau de cautela exercerá uma influência determinante na caracterização de responsabilidade civil das partes envolvidas.

A Avaliação de Impacto, prevista no art. 38 da LGPD, é um dos instrumentos mais importantes, no cenário de proteção de dados, mas ainda está sujeita à regulamentação. Aliás, como será salientado mais adiante, esse é mais um dos motivos para termos uma constituição rápida da Autoridade Nacional, para definir o que é padrão de mercado em termos de proteção de dados no Brasil.

Em relação aos novos atores desse novo cenário, o titular dos dados se equipara ao consumidor nas relações de consumo. O fornecedor de produtos e serviços já se subdivide entre o controlador e o operador de dados, dependendo das funções desempenhadas. Quando fala-se em "agentes" está se referindo ao coletivo de operador/controlador.

O controlador ("*data controller*") é quem decide o que vai ser feito com os dados, e o operador ("*data processor*") é quem, sob as ordens do controlador, faz o tratamento de dados. Então, uma empresa que terceiriza a folha de pagamento, por exemplo, é a controladora – que decide o que fazer com as informações dos empregados – enquanto o departamento de contabilidade é o operador, que faz o tratamento desses dados, conforme as instruções da empresa.

O art. 42 da LGPD é muito parecido com a cláusula geral de responsabilidade civil, prevista no art. 186 do Código Civil brasileiro. Quem causa dano tem o dever de repara-lo. Há uma obrigação solidária do operador, mas somente nas hipóteses em que ele próprio descumprir as regras de proteção de dados, ou não cumprir as determinações do controlador.

Já o art. 43[42] da LGPD tem uma redação parecida com os artigos 12 e 14 do Código de Defesa do Consumidor, sobre a responsabilidade civil pelo fato do produto ou do serviço. Os incisos do art. 43 trazem as excludentes de responsabilidade dos agentes, nos casos em que a ação não existiu, a conduta não é ilícita, ou o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiros.

Por outro lado, o art. 44[43] da LGPD determina quando haverá ato ilícito, para fins de apuração da responsabilidade civil. Nas hipóteses em que as empresas não observarem a legislação ou quando a segurança oferecida falhou, não era suficiente ou adequada, a conduta da empresa pode ser enquadrada como passível de responsabilização nessa esfera civil.

Ocorre que, nenhum tipo de segurança consegue cobrir todos os riscos da atividade. A partir do momento em que se fala em responsabilidade objetiva, muda-se o foco da culpa para a assunção de risco, que pode ser controlado. Evidentemente, esse risco não pode ser zerado, mas a ausência de mecanismos de controle pode ensejar a responsabilidade civil por esse descuido das partes envolvidas.

A seu turno, a LGPD também prevê ferramentas de segurança para analisar a ilegalidade de uma conduta. Contudo, a lei não deixou claro quais ferramentas serão utilizadas nesse contexto. Segundo o conceito aberto, tais medidas poderiam

---

[42] Segundo o art. 43 da LGPD, os agentes de tratamento só não serão responsabilizados quando provarem: *"I - que não realizaram o tratamento de dados pessoais que lhes é atribuído; II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro."*

[43] "*Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais:*
I - o modo pelo qual é realizado;
II - o resultado e os riscos que razoavelmente dele se esperam;
III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.
Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano."

ser providências aptas a proteger os dados pessoais de acessos não autorizados[44] - considerando o estado da arte, até para que o texto legal não perca o seu objeto em poucos anos, com os avanços tecnológicos.

Assim, a Autoridade Nacional poderá dispor sobre esses padrões técnicos mínimos, seja como diretriz ou práticas de governança corporativa. A *International Organization for Standardization* já tem um grupo de normas técnicas internacionalmente conhecidas como melhores práticas atualmente. Essa é, por exemplo, uma diretriz objetiva que poderá ser utilizada por enquanto.

Contudo, nada impede que experimentos e novas técnicas sejam empregadas e, caso cumpram o proposito para o qual foram implementadas, não há razão para negar que o modelo utilizado é compatível com o modelo de proteção de dados. Por exemplo, a privacidade diferencial é uma técnica por meio da qual se consegue obter respostas estatisticamente válidas sobre uma base de dados, sem conferir acesso à mesma para quem for analisar. Ainda que não tenha se tornado recomendação expressa da autoridade de dados, nem prevista na lei, essa técnica já vem sendo discutida e pode ser implementada.

Uma das novidades que precisamos nos acostumar é essa técnica de incorporar a segurança no desenvolvimento do projeto ("*privacy by design*"). O §2º do art. 46 da LGPD diz que todos os projetos de ofertas de serviços que posteriormente vão tratar dados precisam incorporar as melhores práticas de segurança desde o início.

Trocando em miúdos, ao adotar o conceitodo *privacy by design*, uma empresa demonstra que tomou cautelas de segurança suficiente desde a fase de desenvolvimento do produto. Ou seja, é o dever geral de cautela, que não combina com a responsabilidade objetiva, onde se despensa qualquer avaliação de culpa.

Por outro lado, apenas a vontade de que ninguém invada o seu sistema ("privacy by desire"), ou seja, a esperança de que ninguém perceba a falha se segurança, não é a concepção mais adequada para efetivar uma proteção aos dados pessoais.

---

[44] "*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."*

A LGPD não tem critério para aferir tamanho de indenização. No caso da Cambridge Analytica foram utilizados certos critérios para avaliar a multa em 500 mil libras pelo *Information Commissioner's Office* (ICO-UK). Critérios como: (i) afetar um número grande de indivíduos, (ii) e o volume de dados dos cidadãos colocados em risco sério, por exemplo. No final do relatório, analisou como a empresa foi lenta de 2015 até 2018 para tomar medidas efetivas dar resposta a algumas coisas. Todos esses critérios deverão ser utilizados pelo regulador brasileiro, ou pelo Judiciário na hora de avaliar o dever de indenizar.

No último e mais recente caso, tratando da investigação da Boa Vista pelo MPDFT, se teve a notícia de que a base de dados tinha vazado. O MP levou essa base ao conhecimento da sua divisão interna de segurança e análise, descreve as diligências, descobriu-se a vulnerabilidade de uma determinada aplicação; que a base de dados tinha sido violada; mas era uma base de teste, que não tinha dados armazenados.

Dessa forma, decidiu-se arquivar o procedimento, porque essa base violada não continha os dados que estavam sendo procurados naquela investigação.

Portanto, o melhor cenário, em termos de responsabilidade civil relacionada à proteção de dados seria encontrar o ponto de equilíbrio entre três fatores: empreendedor (uso legítimo e responsável de dados para gerar desenvolvimento econômico sustentável), indivíduo (garantia de direitos fundamentais, recolocando-o um pouco mais na cadeia de controle de aspectos de sua personalidade) e consultorias (seguramente boas oportunidades profissionais a partir de agora e pelos próximos anos).

Se o empreendedor tiver interesse em usar dados no seu negócio, que faça essa utilização de maneira responsável, para que o indivíduo tenha seus direitos respeitados – porquanto garantidos em lei e reflexos da sua personalidade.

Assim, embora não tenhamos controle sobre todos os nossos dados, podemos pelo menos interferir na forma como eles são colocados, questionando o controlador e, se necessário, pedindo para apagar.

2.2.1 A importância do conceito de "*privacy by design*"

Diante de todos esses avanços tecnológicos, a legislação vigente ainda fica muito defasada, de modo que se faz necessário garantir valores na técnica de concepção dessas novas tecnologias. Nesse sentido, nota-se uma preocupação crescente em garantir direitos humanos e fundamentais de outra forma, assegurando valores desde o momento da elaboração do design do produto.

A esse respeito, já discute-se formas de as empresas deixarem os processos de design mais inclusivos, aplicando o que se chama de "*inclusive engeneering*". Isto porque, ao invés de se pensar somente na fase da reparação de danos, os advogados em geral têm dificuldade em enxergar a priori e entender o trabalho dos engenheiros, nessa etapa inicial de concepção do produto.

A esse respeito, cumpre ressalta que as empresas têm responsabilidade em relação a essa fase inicial de produção, de modo que é preciso acompanhar a capacidade de autoconstrução dos algoritmos e auto evolução da inteligência artificial, principalmente tendo em vista uma legislação "*by design*", que tutele esses pontos ainda pendentes de regulação jurídica, tal como previsto no art. 46 do GDPR.

Além desse conceito de "privacy by design", também é preciso pensar na chamada "segurança by design", como, por exemplo, no caso das "*smart guns*" (arma com chip que só dispara na mão do dono). O Brasil vive um momento em que o armamento ou desarmamento da população é um assunto em pauta de discussão nacional. Várias armas de militares acabam na mão de criminosos, assim como armas dos pais podem acabar na mão das crianças.

Sendo assim, a sociedade poderia aproveitar esse ensejo para embutir o valor da segurança no design desses artefatos técnicos, pois, se houvesse um dispositivo controlando o disparo apenas na mão do dono, muitos acidentes poderiam ser evitados.

Da mesma forma, o exemplo do "*car tech*" também se aplica nesse caso. Com efeito, muitas vidas poderiam ter sido salvas com a implementação de um bafômetros em automóveis, de modo a impedir o acionamento de carros se o motorista estiver embriagado.

Dessa forma, nota-se que a fase de design exerce uma importante influência nas consequências do produto, salvo nas hipóteses em que os seus efeitos eram indeterminados, pois não dependiam das ações de outros atores, além dos designers.

É o caso do comportamento do robô/inteligência artificial que pode vir dos "*imputs*" dos consumidores, levando a máquina a agir de modo diverso daquele previamente programado. Nessas hipóteses, excepcionalmente, é preciso levar em consideração o que estava nas esferas de controle e influência dos designers e outros agentes de produção. Isso vai exigir uma aproximação do trabalho da sociedade com o trabalho dos engenheiros.

Portanto, é necessário um debate mais aprofundado sobre essa questão envolvendo a produção e a regulação "by design". Fica claro todo o impacto que essa automação, inteligência artificial e funcionamento dos algoritmos exerce na sociedade e na proteção dos dados pessoais.

2.3 Tratamento de dados pessoais pelo Poder Público.

Com o advento da LGPG também surgem questionamentos sobre a efetividade dessa norma, em relação à forma que o Poder Público pretende tratar os dados pessoais dos indivíduos.

A LGPD traz algumas definições sobre o tema no caso do Poder Público. A primeira delas é esse cenário de órgão de pesquisa (art. 5º, XVIII[45]), segundo a qual institutos de pesquisas estarão interessados nessa definição.

O art. 7º da LGPD dispões sobre os requisitos para o tratamento de dados pessoais, ou, como é chamado internacionalmente, as bases legais para essa prática. São dez hipóteses legais de tratamento e, no que se refere ao Poder Público, interessa notar o inciso III do referido artigo.

A definição do artigo art. 5º, X também dispõe que o tratamento é considerado como toda operação realizada com dados pessoais. Trata-se, portanto, de um conceito amplo que engloba toda operação realizada com dados pessoais,

[45] LGDP: "*Art. 5º Para os fins desta Lei, considera-se:*
XVIII - órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico."

desde a coleta da informação até o seu descarte. O mero armazenamento "*backup*" também é considerado como um tratamento. Nesse sentido, nota-se porque a LGPD tem tantos impactos nesse aspecto do setor público.

Sobre as hipóteses legais de tratamento, o *caput* do art. 7º deixa claro que se o tratamento de dados não se enquadrar nessas dez hipóteses taxativas, então não poderá ser realizado. Não existia esse cenário até então.

A primeira delas é justamente a figura do consentimento pelo titular. A LGPD definiu esse consentimento no art. 5º, XII[46], sendo caracterizado, no mínimo, pela manifestação livre, informada e inequívoca do titular em relação ao tratamento dos seus dados pessoais, para uma finalidade determinada. Então, todo consentimento tem que ser livre, e isso foi interpretado pelas autoridades europeias de proteção de dados como sendo uma escolha real/significativa que o titular pode exercer.

Por exemplo, no âmbito das relações de trabalho, várias autoridades de proteção de dados da Europa entendem que não existe o consentimento livre nessas relações, em razão da subordinação entre o empregado e a empresa. Então, o ICO orienta o DPA do Reino Unido nesse sentido.

Sobre a questão de o consentimento ser informado, o titular deve saber para quais finalidades ele consente. Isso é importante, porque não se usa bases legais diferentes para a mesma finalidade. Então, apesar de muitos enxergarem o consentimento como a base legal principal, é importante notar que, quando notamos as exigências que o consentimento traz, somado ao fato de que para qualquer mínima mudança de finalidade, exige uma renovação – se a empresa quiser insistir naquela base legal de consentimento para as finalidades adicionais.

Em relação ao art. 7º, II da LGPD, nota-se que o tratamento poderá ser realizado para o cumprimento de obrigação legal ou regulatória pelo controlador. Isso é muito comum no setor financeiro, porque o Banco Central tem uma série de normas e diretrizes exigindo que o controlador (empresa que toma as decisões a respeito do que vai ser feito com os dados) tenha que guardar essas informações.

Então, o banco é obrigado a guardar transações pelo prazo de cinco anos, até para fins de combate à lavagem de dinheiro. O que muda nesse novo paradigma

---

[46] LGPD: "*Art. 5º Para os fins desta Lei, considera-se:*
XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada."

da LGPD? A finalidade dessa obrigação legal é combater lavagem de dinheiro. No âmbito da LGPD, o marketing pode aproveitar esses dados para mandar e-mail direcionado? Não, se a hipótese legal for de cumprimento de obrigação legal ou regulatória (limitada à finalidade para qual foi criada essa obrigação). Porém, se o banco puder se basear em outra base legal (consentimento, livre interesse, etc) pode sim usar essa base de dados para outra finalidade.

Quando a lei fala que o consentimento deve ser inequívoco, não pode haver dúvida de que o titular de dados consentiu com aquelas condições. Sobre o consentimento ser inequívoco, isso quer dizer o ônus que o controlador – quem vai tomar essas decisões a respeito desses dados – tem de provar que o consentimento foi obtido.

Na prática, os usuários se baseiam na maioria das vezes em contratos eletrônicos e Termos de Uso. Nos EUA, o conceito desse mero aviso ao consumidor de que a política foi atualizada vale. Por outro lado, no direito brasileiro e europeu o paradigma é diferente: é necessário provar a existência do consentimento.

O art. 7º, III[47] é um tremendo guarda-chuva e deixar um amplo espectro de atuação para a administração pública, ao prever que o tratamento de dados pessoais poderá ser realizado "para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas".

Ainda em relação às hipóteses para o tratamento de dados pessoais, o Inciso V, do art. 7º[48] prevê essa possibilidade quando necessário para a execução de contratos, a pedido do titular dos dados. Essa é a base legal utilizada quando uma empresa terceirizada é a responsável por fazer a instalação de um aparelho de acesso à internet na casa do usuário, por exemplo.

Embora o consentimento tenha ocorrido entre o consumidor e a operadora de telefonia contratada, a hipótese legal em referência pode ser aplicada nesse caso, autorizando o tratamento de dados no âmbito da execução do contrato.

---

[47] O artigo 7º da LGPD inaugura a seção I do capítulo II, prevendo os requisitos para o tratamento de dados pessoais e as restritas hipóteses nas quais esse tratamento poderá ser realizado. O inciso III desse dispositivo dispõe que a administração pública somente poderá realizar *"o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei"* (grifou-se).

[48] LGPD: "*Art. 7 O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:*
V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados."

A partir de 2020 essa empresa terceirizada só poderá fazer o tratamento desses dados coletados para aquela finalidade, sendo vedada a sua utilização para fins diversos.

No final, utiliza-se uma combinação dessas bases legais e é preciso entender em qual delas a finalidade da empresa se encaixará, para justificar como o tratamento de dados se justificará ou não.

Ressalte-se ainda o inciso IX do art. 7º[49], segundo o qual o tratamento de dados poderá ser realizado "quando necessário para atender aos legítimos interesses do controlador ou de terceiro". Para esclarecer esse conceito, o *Information Commissioner's Office* (ICO-UK) orienta o DPA do Reino Unido com um guia[50] para quem decidir utilizar essa base legal.

Esse "teste" possui algumas premissas. A primeira delas é questionar se existe e qual seria de fato esse legítimo interesse. Nesse sentido, o tratamento de dados poderia ser justificável para analisar o comportamento de um usuário a fim de combater fraudes, por exemplo.

A segunda etapa desse "teste" é questionar o tratamento de dados seria mesmo necessário para alcançar o interesse legítimo. Assim, pode-se questionar a terceira e mais relevante premissa, quanto à possível violação de algum direito fundamental do titular de dados.

Toda base legal envolve conflitos de escolha entre benefícios e prejuízos daquela situação. O conceito de interesse legítimo não é diferente, pois precisa ser documentado[51] com uma descrição específica de como a empresa, ao utilizar um interesse legítimo, pretende mitigar os riscos desse tratamento.

Ou seja, quais os mecanismos operacionais e técnicos foram utilizados para adotar esse legítimo interesse. Se a Autoridade Nacional discordar da interpretação dada pela empresa sobre o suposto legítimo interesse, entendendo-o inexistente, a

---

[49] LGPD: "*Art. 7 O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:*
IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais."

[50] Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection-404/. Acessado em 20/11/2018.

[51] LGPD: "*Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas [...]*
§ 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial."

empresa está sujeita às sanções de multa e outras penalidades previstas na LGPD, bem como à interrupção daquele tratamento de dados.

Ressalte-se que a publicidade direcionada pode ser enquadrada no âmbito do legítimo interesse, sendo, inclusive, a base legal utilizada na maioria dos casos pelo setor de publicidade *on-line*, quando o endereço eletrônico não exige "*login*" do usuário – nem, portanto, um consentimento.

Nesse modelo de conteúdos gratuitos na internet, pode-se entender que existe o legítimo interesse das empresas que fazem o rastreamento de dados nas páginas, bem como do próprio portal de notícias, por exemplo, que se sustenta o seu modelo de negócios por meio da publicidade, que, por sua vez, precisa ser customizada para ser eficaz.

Portanto, nota-se que o Poder Público tem um amplo espectro de atuação no que se refere ao tratamento de dados, especialmente com base na permissão legal para a execução de políticas públicas, conforme previsto na LGPD. Contudo, é preciso que haja uma base legal específica e condizente com a respectiva finalidade[52] pretendida em cada caso, a fim de fundamentar o tratamento de dados pessoais.

Novamente, essas e outras questões também devem ser esclarecidas com a criação de uma Autoridade Nacional de Proteção de Dados (ANPD), que deverá emitir opiniões técnicas para definir a interpretação dos conceitos genéricos previstos na LGPD.

2.3.1 As controvérsias envolvendo a exigência de compartilhamento de dados pelos Municípios brasileiros

A exigência do compartilhamento de dados às empresas que prestam o Serviço de Transporte Individual Privado é uma realidade em diversos municípios[53]

[52] Conforme o disposto no §1º do art. 10 da LGPD, *"Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados."* Essa redação abre uma larga margem de atuação ao Poder Público.

[53] Lei Municipal nº 10.751/18 de Fortaleza/CE; Lei Municipal nº 717/2018 de Porto Velho/RO; Lei Municipal nº 5.104/17 de Rio Claro/SP; Lei Municipal nº 20.309/17 de Santarém/PA; Lei Municipal nº 15.539/17 de Campinas/SP; Decreto Municipal nº 29/18 de Ribeirão Preto/SP; Decreto Municipal nº 56.981/16 de São Paulo/SP; Decreto Municipal nº 16.770/16 de Vitória/ES; Decreto Municipal 1.302/17 de Curitiba/PR; Lei Municipal nº 4.040/17 de Balneário Camboriú/SC; Lei Municipal nº 6.683/17 de Maceió/AL; Decreto Municipal nº 2.890/17 de Goiânia/GO; Decreto Municipal nº

do Brasil (São Paulo, Campinas, Porto Velho, Campo Grande, Fortaleza e outros). Sob o pretexto dos dados estarem sendo colhidos para a regulação de políticas públicas de mobilidade urbana[54], é possível notar que a exigência de dados básicos referentes à cada viagem intermediada (origem e destino, tempo e distância, mapa do trajeto, preço pago, identificação do condutor e avaliação do serviço pelo passageiro)[55] é comum entre a maioria das normas que regulamentam a atividade.

Sob a mesma linha argumentativa, alguns municípios inovam e requerem dados dos aplicativos de transporte que, a princípio, não são de sua natureza comercial e/ou exigem uma infraestrutura de rede desnecessária para o mero funcionamento do aplicativo.

Nesse sentido, a regulamentação do Distrito Federal exige que sejam enviados mensalmente mapas de calor por CEP de origem e destino das viagens, além de um relatório com a quantidade agregada de quilômetros percorridos pelos usuários.[56] Quanto à capacidade da infraestrutura, a norma de Palmas, por vez, requer, de maneira inovadora, que os dados sejam compartilhados com o ente municipal em tempo real.

Apesar das diferenças municipais, o sigilo e a confidencialidade com os dados colhidos estão presentes em quase todas as legislações – mesmo que sem regulamentação posterior detalhando a forma como os dados serão tratados a fim de terem sua confidencialidade garantida.

Nesse quesito, merece particular destaque a regulamentação paulistana, que oferece às plataformas de transporte a possibilidade de pleitearem a restrição de acesso a informações compartilhadas com a Prefeitura.[57]

Não à toa, atualmente, a exigência do compartilhamento de dados é discutida em âmbito judicial na cidade de São Paulo e no Distrito Federal pelos principais *players* do mercado, quais sejam: Uber do Brasil, 99 Tecnologia e Associação Brasileira de Online to Offline (ABO2O).

1.394/17 de Palmas/TO; Lei Municipal nº 12.126/16 de Porto Alegre/RS; Decreto Municipal nº 17.188/17 de Piracicaba/SP; Decreto Municipal nº 17.462/17 de São José dos Campos/SP; Decreto Municipal nº 13.157/17 de Campo Grande/MS; Lei Distrital nº 5.691/16 do Distrito Federal/DF.

[54] Art. 17, Lei Municipal 10.751/2018 (FOR); Art. 4, Decreto Municipal 13.157/17 (CGR); Art. 4, Decreto Municipal 17.462/17 (SJCAM); Art. 4, Decreto Municipal 17.188/17 (PRCCB); Art. 3, Lei Municipal 12.162/16 (POA); Art. 8, Lei 2.330/17 (PMW); Art. 2, Lei Municipal 6.683/17 (MCO); Art. 4, Decreto Municipal 1.302/17 (CWB); Art. 4, Decreto Municipal 16.770/16 (VIT) e outros

[55] Art. 14, Decreto Municipal 16.770/2016;

[56] Art. 21, I e II, Decreto Distrital 38.258/17

[57] Art. 6, §1, Resolução CMUV nº 13.

Mutatis Mutandis, o objeto das ações judiciais, discutidas em mandados de segurança e ações ordinárias, recai sobre a exigência do compartilhamento de dados com o ente público, envolvendo, nesse ponto, (i) a constitucionalidade dos diplomas regulamentadores; (ii) a proibição do serviço em decorrência da não apresentação das informações requisitadas; e (iii) a suspensão de eventuais penalidades.

Os autores dessas ações argumentam haver incompatibilidade das exigências entre às regulamentações locais e a norma federal, que obriga o compartilhamento somente dos *"dados cadastrais que informem qualifiação pessoal, filiação e endereço"*[58] do usuário (motoristas e passageiros).

No entanto, o principal argumento elencado como óbice para a exigência de compartilhamento de dados é o risco de violação ao sigilo e segurança das informações compartilhadas, ante a fragilidade do sistema de coleta e tratamento de dados.

Nota-se, após a promulgação da norma paulistana, o município falhou em atender as exigências estabelecidas na legislação que garantiriam um mínimo de proteção aos dados e não nomeou a tempo o denominado *"Gestor da Informação"*, responsável pelo guarda das informações.

Já no Distrito Federal, a discussão tomou outro rumo. O órgão responsável pelo recebimento e tratamento dos dados defendeu que o risco de vazamento de dados não passa de uma afirmação genérica sem qualquer suporte fático, fundamentando a confiança do sistema nos "perfis com privilégios específicos", que permitem que apenas alguns usuários tenham acesso à rede, a depender de sua função no órgão público – rebatida pela autora em relatório técnico apresentado posteriormente.

Nesse contexto da discussão sobre a regulamentação no Município de São Paulo e no Distrito Federal, o Poder Judiciário vem adotando posições antagônicas quanto à exigibilidade dos dados. Devido à postura das autoridades municipais quanto à adoção das medidas legais de proteção aos dados, as Varas da capital paulista decidem à favor das operadores de aplicativo, ao passo que em Brasília é a regulamentação local que vem sendo consolidada pelo Judiciário local.

---

[58] Art. 11, §2º, Decreto 8.771/2016: *"São considerados dados cadastrais: I - a filiação; II - o endereço; e III - a qualificação pessoal, entendida como nome, prenome, estado civil e profissão do usuário."*

A razão pela qual o compartilhamento de dados em São Paulo vem sendo suspenso nas ações judiciais decorre, principalmente, da postura que o próprio município vem tomando nos autos. Nesse sentido, admite a procedência dos pedidos das autoras, em reconhecimento à não implementação de todas as medidas legais que possam garantir a segurança dos dados colhidos. Assim, ante a própria confissão da autoridade municipal, que gerencia aquela que deveria armazenar os dados e mantê-los seguros, a posição do judiciário não poderia ser outra, se não conhecer dos pedidos.

Cenário diverso é enfrentado pela 99 Tecnologia no Distrito Federal, ante as posturas refutativas do ente distrital e da autoridade local, que argumentam estar em consonância com as exigências legais de proteção de dados.

Dessa forma, com a argumentação da autora ficando restrita à produção de provas, teve sua liminar negada, uma vez que o risco de vazamento *"constitui mera presunção da autora, não baseada em qualquer dado concreto"*.

Tal argumento também foi repetido pelos réus, que alegam que o temor da 99 não passa de "alegações genéricas", visto que os ditames da lei são cumpridos de maneira rigorosa e suficientes para garantias a confidencialidade das informações. Em contraponto, a autora produziu relatórios técnicos apontando as falhas do sistema de dados da SEMOB e sugeriu melhorias para ele, ao passo que o ente distrital não produziu nenhuma prova que sustente a segurança do sistema.

Finda a produção de provas em 1ª instância, ainda assim o magistrado entendeu que: (i) o compartilhamento de dados é uma exigência razoável, visto que constitui uma obrigação secundária para o cálculo do preço público; (ii) não há violação ao Marco Cívil, pelo fato das normas não tratarem sobre os dados dos passageiros, mas sim dos condutores, cujo exercício é regulamentado pelas normas distritais; (iii) o risco de vazamento não é tão grande, uma vez que há qualquer dado concreto que ampare a insegurança do sistema.

CAPÍTULO 3 – PERSPECTIVAS PARA O CENÁRIO BRASILEIRO

Tendo em vista os riscos envolvendo a proliferação de modelos de negócio baseados na coleta e tratamento de dados pessoais, nota-se uma demanda por

especial atenção do Poder Público, a fim de criar políticas públicas capazes de proporcionar segurança jurídica à sociedade, bem como proteger, adequadamente, a privacidade dos indivíduos.

Conquanto a LGPD represente um avanço sobre a matéria, na fase de sanção presidencial, contudo, foram realizados vetos importantes ao texto legal, esvaziando todo o seu capítulo IX, que também tratava da Autoridade Nacional de Proteção de Dados (ANPD) e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade.

Essa lacuna legislativa representa uma significativa perda na estrutura de proteção de dados pessoais no Brasil. Como 51 (cinquenta e um) dispositivos da LGPD mencionam essa Autoridade Nacional, a Lei não tem condições de, por si só, atingir os seus objetivos, porquanto necessita de uma regulamentação para possibilitar a fiscalização de seu cumprimento e sua devida aplicação pelas instituições[59].

Sobre esse aspecto regulatório, convém ressaltar que as inovações tecnológicas beneficiaram de forma definitiva as relações de consumo ao facilitar o comércio em escala global. Mais do que viabilizar diferentes oportunidades de negócios bilaterais, o processo de evolução digital revoluciona a estrutura econômica da sociedade, criando novos serviços e melhorando a qualidade de vida das pessoas[60].

Sendo assim, deve-se atentar para a importância de essas regulações de privacidade não serem editadas de modo a inibir as inovações tecnológicas. Como elas impõem riscos às empresas e aos titulares de dados. Não podemos correr o risco dessa lei servir como instrumento do vigilantismo estatal, ao invés de tutelar

---

[59].TEFFÉ, Chiara Spadaccini de. MAGRANI. Eduardo. VIOLA, Mario. Artigo "5 pontos sobre a importância de uma autoridade nacional de proteção de dados". Disponível em: https://medium.com/@ITSriodejaneiro/5-pontos-sobre-a-import%C3%A2ncia-de-uma-autoridade-nacional-de-prote%C3%A7%C3%A3o-de-dados-4cf8137cf59e. Acessado em 10/12/2018.

[60] O economista Joseph Schumpeter já escrevia a respeito da lógica da inovação ou, como ele mesmo dizia, da "destruição criadora", nos anos 1940: "*A abertura de novos mercados nacionais ou externos e o desenvolvimento das organizações produtivas [...] constituem exemplos do mesmo processo de mutação industrial – se me permitem essa expressão biológica – que revoluciona incessantemente, de dentro, a estrutura econômica, destruindo continuamente seus elementos envelhecidos e criando do mesmo modo elementos novos*." Schumpeter, Joseph A. *Capitalism, Socialism and Democracy.* New York: Harper Perennial Modern Thought, nova edição publicada em 2008.

a proteção de dados pessoais. A intervenção estatal deve ser cuidadosa, para não inviabilizar a atividade que está sendo regulada[61].

Para que o cumprimento dessas disposições ocorra da maneira adequada, vai depender das sanções. O Judiciário precisa estar preparado e entender as complexidades que esse tema envolve. O Poder Judiciário tem, portanto, o nobre papel de controle sobre esses atos regulatórios[62], na salvaguarda das liberdades constitucionais e na garantia de que forças de captura regulatória não criem empecilhos a inovações legítimas que beneficiem a sociedade como um todo[63].

Por outro lado, os avanços nesse contexto também vão depender da criação de uma Autoridade Nacional, com corpo técnico qualificado, autonomia administrativa, financeira e política, com participação social e transparência; caso contrário, a sua ausência pode representar um cenário de falta de "*enforcement*", com uma lei "sem dentes, sem garras" no Brasil. Portanto, precisamos desses órgãos públicos capacitados para tentar tutelar a privacidade dos dados pessoais.

Se essa autoridade tiver um papel relevante e atuante, é possível que ela consiga estabelecer diretrizes, orientações e práticas capazes de diminuir a judicialização de futuras demandas sobre questões envolvendo a proteção de dados no Brasil.

---

[61] Não por outra razão, o ganhador do Prêmio Nobel em Ciências Econômicas Milton Friedman aponta que deve-se "*analisar tanto os benefícios quanto os custos das propostas de intervenção do governo e exigir uma justificativa muito clara a favor dos benefícios em vista dos custos antes de adotá-las*" (FRIEDMAN, Milton; FRIEDMAN, Rose. *Livre para escolher.* Trad. Ligia Filgueiras. 1ª ed. Rio de Janeiro: Record, 2015. p. 62).

[62] Nas palavras do Professor Ragazzo: *"(...) o Poder Judiciário exercerá uma dupla função na revisão de marcos regulatórios: (i) evita arbitrariedades e regulações que são resultados de influência indevida de grupos de interesse, impondo limites substantivos a serem observados pelo Poder Legislativo e demais órgãos reguladores; e (ii) estimula o Poder Legislativo e as agências reguladoras a desenvolverem uma capacidade analítica maior, com a imposição de requisitos procedimentais em hipóteses específicas, a fim de que os órgãos reguladores identifiquem claramente os objetivos regulatórios, bem como a alternativa que represente a melhor relação de custo e benefício, contribuindo para o aumento da transparência e, portanto, da participação democrática."* (RAGAZZO, Carlos. *Regulação Jurídica, racionalidade econômica e saneamento básico*. Renovar: Rio de Janeiro, 2011, p. 267-268).

[63] A intervenção do Poder Judiciário se faz imperiosa. Atualmente, *"a análise jurídica tradicional e isolada é incompleta quando não abrange as influências externas (sociais, econômicas, políticas etc.) dentro do contexto de suas transformações tecnológicas, que podem afetar o comportamento humano em geral e desenvolver aspectos importantes de um corpo social"*. Dessa forma, *"a necessária análise inter-relacionada entre Direito e tecnologia deve alcançar não apenas a atividade legislativa propriamente dita, mas também as decisões dos Tribunais, a atuação administrativa e mesmo a formulação e execução de políticas públicas"* (Arbi, Abhner Youssif Mota. Direito e tecnologia: relação cada vez mais necessária. Revista Eletrônica JOTA. Publicado em 04/01/2017). Disponível em: https://goo.gl/gjavsA.

Além do papel de fiscalizar e sancionar, essa Autoridade Nacional tem o papel de orientar a sociedade sobre as formas de cumprimento à LGPD. Na ausência da ANPD, o Ministério Público e outros órgãos devem assumir a função fiscalizatória e sancionatória, mas essas autoridades não devem exercer a atribuição de orientar, até por falta de competência nesse sentido.

Sobre os longos e confusos Termos de Uso adotados por diversas empresas, a melhor prática de mercado parece ser utilizar basicamente 4 documentos. Além do documento com os Termos de Uso, a Política de Privacidade sobre a forma de tratamento de dados[64], um resumo para o usuário e, por fim, seria uma política que explique o que está sendo feito com os dados, independente de consentimento, ou seja, com fundamento em outras bases legais.

Embora não seja obrigatória, recomenda-se que essa prática seja implementada pelas empresas por enquanto, como medida de cautela neste cenário de insegurança jurídica, diante das lacunas legislativas ainda existentes.

Por essas e outras razões, até a conclusão deste trabalho, a criação da ANPD estava na pauta da Presidência da República, na forma de uma secretaria vinculada à Casa Civil. Parece haver um clamor tão grande que motivou um manifesto conjunto de 43 instituições pela criação imediata dessa Autoridade, ainda em 2018, "*de modo a permitir a estruturação de todo o arcabouço normativo e diretrizes necessários para a aplicação e eficácia da LGPD quando da sua entrada em vigor em fevereiro de 2020.*"[65].

Não obstante as discussões sobre a melhor forma de implementar essa mudança legislativa – seja por lei ou medida provisória – é fundamental que a

---

[64] Veja-se, por exemplo, os Termos de Uso da empresa "Tumblr" sobre a exigência de idade mínima para usar essa plataforma. Neste caso, logo após a cláusula contratual, o vocabulário jurídico foi substituído por uma mensagem mais clara e ao consumidor, alertando-o para a seriedade da regra e sugerindo de forma bem humorada outras formas de entretenimento aos mais jovens: "*You have to be the Minimum Age to use Tumblr. We're serious: it's a hard rule. "But I'm, like, almost old enough!" you plead. Nope, sorry. If you're not old enough, don't use Tumblr. Ask your parents for a Playstation 4, or try books."* Disponível em: https://www.tumblr.com/policy/en/terms-of-service . Acessado em 20/11/2018.

§ 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial."

[65] O Manifesto destaca ainda que "a criação da Autoridade com essas características é essencial para consolidar no país uma estrutura institucional, apta a propiciar segurança jurídica para o tratamento de dados no país, dar efetividade aos direitos assegurados na LGPD e possibilitar que o Brasil participe do livre fluxo internacional de dados.". Disponível em: https://brasscom.org.br/autoridade-nacional-de-protecao-de-dados-anpd-clamor-pela-criacao-ainda-este-ano/?fbclid=IwAR0sgr5UAapQLGWlwdQO3MZCTNsEbfCQSuF_irivtGEa5yEr7sy8LuiWFOY. Acessado em: 13/12/18.

ANPD seja estabelecida nos moldes do que havia sido proposto no Projeto de Lei da Câmara n. 53/18, o qual se encontrava alinhado com excelentes modelos e práticas internacionais, bem como havia sido objeto de amplo debate público, democrático e multissetorial[66].

A experiência internacional mostra a relevância da existência da ANPD para a aplicação eficiente de suas respectivas leis de proteção de dados pessoais, como nos casos do Reino Unido, França, Itália, Argentina e Uruguai, que devem servir de inspiração para o modelo brasileiro.

Com efeito, a Autoridade deve ter, entre suas funções, a possibilidade de monitorar tanto o Estado quanto sujeitos privados, ela deve se encontrar em posição que lhe permita atuar sem intervenções indevidas.

Afinal, a existência de uma Autoridade Nacional independente e com elevada autonomia é um dos requisitos para que o Brasil e sua legislação sejam reconhecidos como adequados ao modelo de tratamento de dados pessoais estabelecido na Europa por meio do GDPR[67].

CONCLUSÃO

Pode-se notar que a sociedade ainda não tem consciência plena de todos os potenciais benefícios e riscos desse recente cenário digital de hiperconectividade, entre objetos inteligentes (sensores), *big data* e inteligência computacional, no chamado ABC[68] das tecnologias da informação e comunicação (*analytics* + *big data* + *cloud computing*).

Com a evolução da Internet das Coisas, o seu crescimento exponencial levará à criação de novos modelos de negócios, serviços e produtos que podem alterar ainda mais a relação entre produtor e consumidor[69].

---

[66] "Esse é, vale ressaltar, o entendimento majoritário dos diversos setores da sociedade que vêm discutindo a regulação do tratamento de dados pessoais no País, nos últimos anos." TEFFÉ, Chiara Spadaccini de. MAGRANI. Eduardo. Artigo "Proposta para a criação da Autoridade Brasileira de Proteção aos Dados Pessoais. Disponível em: https://itsrio.org/wp-content/uploads/2018/12/autoridade-protecao-de-dados.pdf . Acessado em: 10/12/18.

[67] Idem.

[68] CAVALCANTI, José Carlos. *"The new ABC of ICTs (analytics +big data + cloud computing: a complex tradeoff between IT and CT costs"*. Hershey: IG Global, 2016.

[69] "Na esfera do poder público, os benefícios da IoT podem oferecer maior eficiência à gestão pública. A partir do uso de tecnologias integradas e do processamento massivo de dados, soluções mais eficazes para problemas como poluição, congestionamentos, criminalidade, eficiência

Como visto, em muitos negócios *on-line*, o consumidor aceita os termos de uso – escrito muitas vezes para não serem lidos – e acaba permitindo que empresas prossigam com a coleta e tratamento de seus dados pessoais, que não necessariamente tem relação com o produto ofertado.

No entanto, observa-se um cenário de mudanças nas posturais governamentais em relação a esse tema, em plena discussão na atualidade, seja pelos recentes escândalos de vazamentos de dados pessoais, ou pela percepção geral de que as inovações tecnológicas trouxeram sérios desafios a serem enfrentados pela sociedade moderna.

Nesse sentido, é necessário que as legislações acompanhem os avanços tecnológicos na mesma velocidade em que o uso de bens e serviços *on-line* cresce no mundo globalizado. Por essa razão, os países estão buscando modelos de regulações sobre o tratamento de dados pessoais, tendo em vista o papel essencial que essas disposições exercem na garantia dos direitos fundamentais para a proteção da dignidade da pessoa humana.

Ao contrário de outros países que estão reformando ou atualizado os seus modelos nacionais existentes, o Brasil está implementando um novo marco regulatório e estabelecendo uma mudança cultural no âmbito da proteção de dados. Dessa forma, espera-se proporcionar instrumentos mais claros e eficazes para os indivíduos zelarem pelas informações que lhe dizem respeito.

Afinal, a proteção do consumidor e do direito fundamental à privacidade encontram amparo no princípio fundamental da dignidade da pessoa humana, de modo que o indivíduo não pode ser tratado como uma coisa ou objeto, cujos dados possam ser tratados sem o devido respeito às normas vigentes[70].

No entanto, em que pese o avanço legislativo sobre essa matéria, ainda há um longo caminho a ser percorrido para que as disposições da LGPD estejam aptas a efetivamente garantir a proteção de dados pessoais e a segurança de seus titulares. Isto porque, ainda não foram definidas algumas questões relevantes sobre as formas

---

produtiva, entre outros, têm sido identificadas e implementadas." MAGRANI, Eduardo. Artigo "A Internet das Coisas no Brasil: Estado da arte e reflexões críticas ao fenômeno. Disponível em: https://igarape.org.br/wp-content/uploads/2018/11/A-Internet-das-Coisas-no-Brasil-Estado-da-arte-e-reflexo%CC%83es-cri%CC%81ticas-ao-feno%CC%82meno-Eduardo-Magrani.pdf . Acessado em: 10/12/18.

[70] BLUM, Rita Peixoto Ferreira. *O direito à privacidade e à proteção dos dados do consumidor.* São Paulo: Almedina, 2018, p. 169.

de cumprimento à LGPD, que carece de regulamentações a respeito das suas sanções.

Sendo assim, é necessária a criação de uma Autoridade Nacional de Proteção de Dados – que promova a conscientização das instituições, empresas e pessoas físicas – principalmente nesse período inicial de implementação de uma nova sistemática, para que o cumprimento dessa legislação ocorra da maneira adequada, protegendo a privacidade dos indivíduos.

Nesse sentido, segundo o entendimento dos Professores Eduardo Magrani e Chiara Teffé, "*para que o Brasil alcance um patamar elevado de proteção aos direitos humanos e de desenvolvimento enquanto nação, defende-se a necessidade da criação de uma Autoridade Nacional de Proteção de Dados Pessoais que goze de autonomia, seja amplamente independente, apresentando as disposições presentes no PLC n. 53/18, e detenha características semelhantes àquelas preconizadas na norma europeia de proteção de dados*"[71].

Enquanto essa lacuna legal não for preenchida, convém observar algumas boas práticas e princípios gerais comuns que devem nortear a coleta, uso e guarda dos dados pessoais dos consumidores, a exemplo das diretrizes implementadas na União Europeia. Recomenda-se uma especial atenção aos chamados "dados sensíveis", que somente devem ser coletados, armazenados ou divulgados em situações excepcionais, dentro dos parâmetros legais[72].

[71] TEFFÉ, Chiara Spadaccini de. MAGRANI. Eduardo. Artigo "Proposta para a criação da Autoridade Brasileira de Proteção aos Dados Pessoais. Disponível em: https://itsrio.org/wp-content/uploads/2018/12/autoridade-protecao-de-dados.pdf . Acessado em: 10/12/18.
[72] BLUM, Rita Peixoto Ferreira. *O direito à privacidade e à proteção dos dados do consumidor.* São Paulo: Almedina, 2018, p. 159.

BIBLIOGRAFIA

ARBI, Abhner Youssif Mota. Direito e tecnologia: relação cada vez mais necessária. Revista Eletrônica JOTA. Publicado em 04/01/2017). Disponível em: https://goo.gl/gjavsA;

BIONI, Bruno Ricardo. De 2010 a 2018: a discussão brasileira sobre uma lei geral de proteção de dados pessoais. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/de-2010-a-2018-a-discussao-brasileira-sobre-uma-lei-geral-de-protecao-de-dados-02072018.
Acessado em: 10/12/2018;

BLUM, Rita Peixoto Ferreira. *O direito à privacidade e à proteção dos dados do consumidor*. São Paulo: Almedina, 2018;

BRANCO, Sergio. *Memória e esquecimento na internet*. Porto Alegre: Arquipélago Editorial, 2017;

CAVALCANTI, José Carlos. *"The new ABC of ICTs (analytics +big data + cloud computing: a complex trade off between IT and CT costs"*. Hershey: IG Global, 2016;

DONEDA, Danilo. A proteção de dados pessoais como direito fundamental. Revista Espaço Jurídico 12/103. Joaçaba: Unoese, 2011;

Direito Privado e Internet / Guilherme Magalhães Martins (coordenador). – São Paulo: Atlas, 2014;

FRIEDMAN, Milton; FRIEDMAN, Rose. *Livre para escolher*. Trad. Ligia Filgueiras. 1ª ed. Rio de Janeiro: Record, 2015;

GRASSEGGER, Hannes; KROGERUS, Mikael. *The data that turned the world upside down.* Motherboard, 2017;

LOHR, Steve. The Age of Big Data, New York Times. Disponível em: https://www.nytimes.com/2012/02/12/sunday-review/big-datas-impact-in-the-world.html . Acesso em 10/12/2018.

MCKINSEY. Estudo "The Internet of Things: Mapping the Value Beyond the Hype". Disponível em https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world. Acessado em 10/12/2018.

MAGRANI, Eduardo. *A internet das coisas*. FGV Editora: Rio de Janeiro, 2018;

MAGRANI, Eduardo. Artigo disponível em: http://eduardomagrani.com/seis-pontos-para-entender-o-regulamento-geral-de-protecao-de-dados-da-ue/ . Acessado em: 10/12/18;

MAGRANI, Eduardo. Democracia conectada: a internet como ferramenta de engajamento político-democrático. Curitiba: Juruá, 2014;

RAGAZZO, CARLOS. *Regulação Jurídica, racionalidade econômica e saneamento básico*. Renovar: Rio de Janeiro, 2011;

SCHUMPETER, Joseph A. *Capitalism, Socialism and Democracy.* New York: Harper Perennial Modern Thought, nova edição publicada em 2008;

TEFFÉ, Chiara Spadaccini de. MAGRANI. Eduardo. VIOLA, Mario. Artigo "5 pontos sobre a importância de uma autoridade nacional de proteção de dados". Disponível em: https://medium.com/@ITSriodejaneiro/5-pontos-sobre-a-import%C3%A2ncia-de-uma-autoridade-nacional-de-prote%C3%A7%C3%A3o-de-dados-4cf8137cf59e. Acessado em 10/12/2018.

TEFFÉ, Chiara Spadaccini de. MAGRANI. Eduardo. Artigo "Proposta para a criação da Autoridade Brasileira de Proteção aos Dados Pessoais. Disponível em: https://itsrio.org/wp-content/uploads/2018/12/autoridade-protecao-de-dados.pdf . Acessado em: 10/12/18.

[i] Art. 20, §2