ANÁLISE COMPARATIVA ENTRE OS PRINCÍPIOS INFORMADORES DO REGULAMENTO GERAL DE PROTEÇÃO DE DADOS DA UNIÃO EUROPEIA E AS NORMAS DO DIREITO BRASILEIRO

Aluna: Ana Lara Galhano Mangeth
Orientadora: Caitlin Mullholland

Introdução

O advento da tecnologia fez com que fosse necessário novos arranjos para a sociedade e para o poder público. Não raro, a lei não consegue acompanhar as mudanças velozes do mundo conectado, mas há anos que a demanda por leis mais protetivas aos dados pessoais do cidadão ganha espaço entre especialistas e entusiastas da tecnologia.

Isto porque, o cidadão comum, por vezes, não é capaz de reconhecer os riscos e oportunidades criadas para a exploração de seus dados pessoais. Assim, muitas vezes abrem mão de informações pessoais importantes em troca de simples acesso a sites e aplicativos de aparelho celular. Não apenas isto, mas toda a troca de dados realizada em estabelecimentos comerciais físicos e cadastros — quaisquer transações do tipo também deveriam constar no escopo de uma lei geral de proteção de dados.

A União Europeia há alguns anos já gozava de tal proteção com a Diretiva 95/46 CE, a qual buscava regular a coleta, uso e tratamento de dados no território europeu. Porém, acompanhando as tendências de uso global, transferência e necessidade de apagamento ou prestação de contas sobre dados pessoais, um novo Regulamento foi elaborado a fim de expandir a proteção ao indivíduo.

Sendo assim, após um período de dois anos, entrou em vigor o Regulamento Geral de Proteção de Dados europeu — GDPR. Com texto extenso e uma preocupação notável em abranger as mais diversas possibilidades de transação envolvendo dados, o GDPR sagrou-se um marco na proteção de dados e da proteção à privacidade do usuário. Instituiu princípios sólidos e claros, a fim de não abrir margem para interpretações diversas. Assim, o documento cria no indivíduo a possibilidade de domínio sobre os próprios dados, reclamando a

propriedade destes como algo pessoal e não comercial, pertencente às empresas ou amplamente explorado pelo Poder Público.

O Brasil, por sua vez, demora a espelhar as tendências globais e até mesmo sul-americanas em termos de legislação de proteção de dados. Apenas este ano (2018), projetos que versavam sobre o tema caminharam rumo à aprovação do Congresso Nacional. Os principais são o Projeto do Senado nº330/2013 e o Projeto da Câmara nº 5.276/2016. As iniciativas divergem entre si acerca da abrangência do domínio dos titulares sob seus dados, dos princípios informadores adotados, da extensão ao Poder Público das mesmas garantias de coleta e tratamento de dados, e da criação de uma Autoridade de Proteção de dados pessoais.

Tendo em vista serem pontos importantes para que o país tenha uma lei adequada regulando um tema tão caro, aguarda-se o resultado final do processo legislativo.

Objetivos

Os objetivos deste trabalho são: (i) analisar os princípios gerais de proteção de dados adotados pela União Europeia; (ii) investigar a legislação brasileira e iniciativas do legislativo (projetos de lei) a respeito da proteção de dados pessoais; (iii) compilar bibliografia a respeito do tema; (iv) indicar a existência de casos e a jurisprudência sobre o tema, e (v) realizar a comparação entre os ordenamentos europeu e brasileiro.

Metodologia

Consistiu em vasta leitura de doutrina, artigos e teses sobre o tema, direcionados ao advento da tecnologia e seus impacto na proteção da privacidade e de dados. Leitura e análise dos projetos de lei brasileiros sobre proteção de dados e o Regulamento Geral de Proteção de Dados da União Europeia (GDPR), bem como análise dos seus princípios basilares.

O GDPR[1]

[1] Tema extensivamente tratado no artigo pelos autores MANGETH, A.L. MAGRANI, Eduardo NUNES, Beatriz. Seis pontos para entender a lei europeia de proteção de dados. Disponível em: < https://feed.itsrio.org/seis-pontos-para-entender-a-lei-europeia-de-prote%C3%A7%C3%A3o-de-dados-pessoais-gdpr-d377f6b691dc > Acesso em 24/07/2018

O Regulamento Geral de Proteção de Dados (GDPR) tem por objetivo reforçar e unificar a proteção de dados pessoais na União Europeia (UE), adaptando seus princípios ao mundo conectado, que cada vez mais centra atividades econômicas na coleta e tratamento de dados pessoais, na Internet e fora dela. O GDPR substitui, assim, a antiga Diretiva 95/46 CE, de 1995. Foi aprovado pelo Conselho Europeu em abril de 2016, e tornou-se executável a partir de 25 de maio de 2018, após um período de dois anos para adequação às mudanças implementadas. Por ser um Regulamento, é diretamente aplicável a todos os estados membros da União Europeia, ao contrário da antiga Diretiva. O Regulamento vincula toda e qualquer organização ou empresa que ofereça bens e/ou serviços que coletem dados pessoais de pessoas relacionadas à UE.

O GDPR traz previsões importantes a serem observadas, não apenas pelas entidades que coletam e tratam dados pessoais (estejam elas dentro ou fora da UE), mas também pelos usuários titulares dos dados. Um pilar importante é o consentimento do titular de dados, que tornou-se o elemento protagonista do Regulamento. O consentimento passa a figurar, por exemplo, como elemento principal para autorizar a coleta e tratamento de dados, devendo ser inequívoco e envolver sempre uma postura assertiva. Caso isto seja descumprido, o GDPR prevê diretamente possibilidades de responsabilização daqueles que realizarem a atividade (coleta, tratamento e transferência) inadequadamente.

Ao mesmo tempo, outro elemento discutido é o poder concedido às autoridades fiscalizadoras para aplicar sanções a quem descumprir o GDPR. Sabe-se que sem tais autoridades, a efetividade da lei fica comprometida, porém é preciso se atentar para o grau de ingerência destas nas atividades das empresas. Isto porque, as consequências mais graves podem gerar multas de até € 20 milhões, ou 4% do valor global da empresa. Para monitorar isso, o Regulamento mantém as autoridades públicas já instituídas pela Diretiva, as DPA's (em inglês, *Data Protection Authorities* ou, em português, Autoridades de Proteção de Dados), que ficam encarregadas de supervisionar a aplicação das regras, sendo uma para cada Estado Membro da UE. Além disso, insere a figura do DPO (em inglês, *Data Protection Officer* ou, em português, Diretor de Proteção de Dados), profissional encarregado de prestar contas sobre a atividade da entidade em que se encontra filiado, através da avaliação de possíveis impactos aos titulares de dados, entre outros.

Essas e outras mudanças são novidades que o GDPR com o objetivo claro que sinalizar às organizações a necessidade de comprometimento durante a realização da

atividade. O objetivo é reduzir os riscos de abusos na coleta, no tratamento, uso e transferência de dados. Para isso, uma série de princípios orientam a conduta a ser adotada, os quais serão analisados a seguir.

Princípios

Os princípios garantidos pelo GDPR são: princípio da licitude, lealdade e transparência (*Lawfullness, Fairness & Transparency*); princípio da adequação e limitação da finalidade (*Purpose Limitation*); princípio da necessidade ou minimização (*Data Minimisation*); princípio da qualidade dos dados ou exatidão (*Accuracy*); princípio da limitação da conservação (*Storage Limitation*); princípio da segurança, integridade e confidencialidade (*Integrity and Confidentiality*), princípio da prestação de contas ou responsabilização (*Accountability)*. Estes princípios norteadores serão diretamente aplicáveis, independentemente de internalização por parte dos Estados Membros através da lei nacional.

Como novidades que não constavam na Diretiva 95/46, destacam-se aqui os princípios da necessidade ou minimização e *Accountability*. O princípio da minimização prevê que os dados pessoais devem ser adequados, pertinentes e limitados em relação aos fins para os quais serão processados. O objetivo é diminuir a quantidade de dados, coletando apenas aqueles que sejam essenciais para o produto ou serviço ofertado. O *Accountability* é o princípio segundo o qual exige-se que as organizações implementem medidas técnicas e organizacionais apropriadas, e sejam capazes de prestar contas e demonstrar sua eficácia, quando solicitadas. Para tal, instituiu-se o controlador de dados, profissional responsável, por demonstrar que a organização está agindo em conformidade com os demais princípios estabelecidos pelo Regulamento[2].

Uma aplicação fiel dos princípios, no entanto, não é a única medida a ser cuidadosamente observada pelas organizações. O escopo territorial de aplicação do GDPR também vem suscitando dúvidas.

Aplicação Territorial

[2] BURGESS, Matt. What is the GDPR? The summary guide to GDPR compliance in UK. Disponível em: < https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/ > Acesso em 30/07/2018.

Essa questão tornou-se controversa devido à dúvidas com relação a quem seria protegido pelo GDPR, no âmbito da aplicação territorial, uma vez que se tem afirmado que apenas os residentes da UE estariam contemplados. O artigo 3º do Regulamento[3] determina que as regras do GDPR são aplicáveis ao tratamento de dados pessoais efetuado *no contexto das atividades do estabelecimento de um responsável pelo tratamento, ou das atividades de um subcontratante, situado no território da União Europeia, independentemente de o tratamento em si ocorrer dentro ou fora da União*. Mas afinal, quais seriam os limites da territorialidade?

Ocorre que, devido à própria natureza dos dados pessoais, e sua capacidade de dispersão, o conceito de territorialidade é ampliado. Dessa forma, o GDPR será aplicável a: indivíduos — cidadãos europeus ou não — que residem no território da União Europeia, mesmo quando estes não estejam localizados fisicamente na UE, bem como a indivíduos que apenas se encontram na UE (de passagem, à turismo, etc). Estes também estão sob a proteção do Regulamento, uma vez que usam serviços que podem coletar seus dados ou informações pessoais.

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. Fato é que o GDPR apresenta um escopo abrangente, que afetará a política de uso de muitas empresas, cujas bases encontram-se no território da UE (mesmo com sede no exterior), ou mesmo aquelas que recebam dados transferidos/ tratados destas. Portanto, empresas privadas ou públicas brasileiras, que possuem relacionamento com clientes ou parceiros europeus, terão que adequar-se a fim de respeitar o novo Regulamento.

Demais pontos notáveis do Regulamento

Dados Sensíveis

[3] Disponível em: < http://www.privacy-regulation.eu/en/article-3-territorial-scope-GDPR.htm > Acesso em 30/07/2018.

Outro ponto importante é a inclusão, no GDPR, de uma categoria especial para dados sensíveis. O artigo 9º estabelece um regime específico, segundo o qual o processamento desse tipo de dado pessoal é proibido, exceto nas dez hipóteses elencadas no dispositivo como, por exemplo, a proteção de interesses vitais do indivíduo e razões de substancial interesse público. Assim, de acordo com o Regulamento, dados sensíveis são aqueles que revelem 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.

Tendo em vista serem temas delicados, fica clara a necessidade de uma camada extra de proteção aos dados, por serem capaz de revelar informações de cunho íntimo, além do fato de que, quando cruzados, são capazes de identificar individualmente seu titular. Por essa mesma razão, para que os dados sensíveis possam ser tratados, o consentimento deve ser livre, explícito, inequívoco, informado e específico.

Direito à Explicação

O GDPR prevê também o direito de obter uma explicação para qualquer decisão automática feita por algoritmo, e o direito de optar pela não-coleta de dados[4]. Portanto, via de regra, o titular de dados terá o direito de não se sujeitar à decisões tomadas exclusivamente com base em tratamento automatizado, como previsto no artigo 22 do Regulamento.

As exceções a esse direito restringem-se às seguintes situações: se o titular de dados tiver dado consentimento explícito, se o uso for autorizado por lei da União Europeia ou do Estado Membro a que o responsável pelo tratamento estiver sujeito ou, ainda, caso o processamento seja necessário para a celebração ou execução de contrato entre o titular dos dados e o responsável por seu tratamento. O objetivo é justamente explorar meios diversificados para fornecer um maior grau de transparência sobre como os algoritmos tomam decisões que impactam a vida do indivíduo.

O chamado *Right to Erasure*

[4] Disponível em: < https://iapp.org/news/a/is-there-a-right-to-explanation-for-machine-learning-in-the-gdpr/ > Acesso em 29/07/2018

O chamado direito ao esquecimento, denominado pelo GDPR de direito ao apagamento, também foi contemplado de forma explícita pelo Regulamento[5]. Previsto no artigo 17, o dispositivo elenca diversas hipóteses não exaustivas em que o *right to erasure* poderá ser requerido. Um exemplo seria quando os dados deixam de ser necessários em relação à finalidade que primeiro motivou sua coleta, e quando o titular dos dados retira o consentimento sobre o qual é baseado o tratamento. Esta última possibilidade significa grande avanço, uma vez que materializa a premissa de que pertencem ao titular seus dados e o controle sobre eles.

A garantia, portanto, fundamenta-se no direito de direito do titular de dispor dos dados sobre ele coletados, a fim de retificá-los, se assim desejar. Mas, notadamente, a disposição vai além: o titular possui um "direito a ser esquecido", em 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.

No entanto, pode-se dizer que há uma ampliação vasta do instrumento. Isto porque uma perspectiva tradicional do direito ao esquecimento engloba uma ponderação mais cuidadosa dos critérios específicos, a fim de não ferir a liberdade de expressão e o acesso à informação. Já o *right to erasure* não apresenta tais critérios, cabendo a análise ao próprio responsável pelo tratamento daquilo que, em sua opinião, couber. Ou seja, o GDPR inclui hipóteses de remoção muito amplas, ao mesmo tempo que deixa à particulares a decisão daquilo que irão "apagar", a depender do que for alegado pelo titular dos dados.

Transferência Internacional de Dados

Outra exigência importante do GDPR às empresas sujeitas ao Regulamento é que seja realizada uma gestão de dados, no sentido da possibilidade de transferência de dados (artigo 46 do Regulamento). Os responsáveis pelo tratamento só poderão realizar transferência de dados para outros países ou organizações internacionais, se estes tiverem apresentado leis

[5] Disponível em: < https://www.i-scoop.eu/gdpr/right-erasure-right-forgotten-gdpr/ > Acesso em 30/07/2018.

adequadas de proteção[6]. As regras serão aplicáveis a todas as entidades de um grupo empresarial envolvidas em uma atividade econômica conjunta, e a seus funcionários. Além disso, o titular de dados tem direitos oponíveis perante as empresas, e deve consentir não apenas inequivocamente, mas expressamente sobre a transferência dos seus dados, por meio de uma declaração ou ação afirmativa, após ser devidamente informado sobre os riscos envolvidos em tais transferências, mantendo seu consentimento.

Diante desse contexto, o Brasil, por não possuir uma legislação específica de proteção de dados pessoais, em princípio, não poderá realizar troca de dados com a Europa. Uma vez que a tendência é o GDPR ter um efeito viral[7], a não adaptação terá como consequência dificuldades para as empresas aqui instaladas, bem como um enfraquecimento da competitividade e da inovação na economia nacional, caso o país não buscar se adequar às regras globais de proteção.

A proteção de dados pessoais no Brasil[8]

No Brasil, pode-se dizer que a proteção de dados pessoais encontra-se assegurada sob algumas disposições diretas, mas também pelo guarda-chuva da privacidade. Na Constituição Federal, há respaldo na preservação da intimidade e da vida privada enquanto direito fundamental, no inciso X, artigo 5º. No Marco Civil da Internet, é possível encontrar ambas as previsões: em seu artigo 3º, inciso II, a proteção da privacidade é prevista como princípio que disciplina o uso da Internet, assim como a proteção dos dados pessoais, no inciso III.

Além disso, o acesso à internet é considerado pelo MCI, no artigo 7º, como essencial ao exercício da cidadania, e entre os direitos assegurados ao usuário estão: 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; VIII - informações claras e completas sobre coleta, uso,

---

[6] Disponível em: < https://www.whitecase.com/publications/article/chapter-13-cross-border-data-transfers-unlocking-eu-general-data-protection > Acesso em 29/07/2018.

[7] Disponível em: < http://www.meioemensagem.com.br/home/midia/2018/05/21/a-gdpr-tera-um-efeito-viral.html > Acesso em 29/07/2018.

[8] Tema extensivamente tratado no artigo pelos autores MANGETH, A.L. MAGRANI, Eduardo NUNES, Beatriz. A proteção de seus dados pessoais está em jogo no Senado. Disponível em: < https://feed.itsrio.org/senado-vs-c%C3%A2mara-seus-dados-pessoais-em-jogo-97d7b0cefc54> Acesso em 24/07/2018

armazenamento, tratamento e proteção de seus dados pessoais; 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.

No entanto, há situações específicas que demandam previsão direta e assertiva por parte da lei, a saber: a proteção específica à dados sensíveis, o direito à explicação, direito ao apagamento, a transferência internacional de dados, uma autoridade independente que garanta efetividade a tais garantias, entre outros.

Porém, não obstante a necessidade de ter uma lei geral de proteção de dados pessoais no país ser uma discussão antiga, até recentemente o Legislativo não havia demonstrado interesse em votar projetos que versassem sobre a matéria. Contudo, o escândalo em torno da agência Cambridge Analytica e a entrada em vigor do GDPR impulsionaram o Congresso Nacional a agilizar o andamento dos projetos de lei que já haviam sido propostos. Com isso, tem-se que, inicialmente, tramitavam três projetos de lei para a proteção geral de dados pessoais: o PL n° 330/2013, criado no Senado Federal, e os PLs n° 4.060/2012 e n° 5.276/2016, criados pela Câmara dos Deputados.

Pode-se dizer que destes, destacaram-se o PLC nº 5.276 e o PLS nº 330. Quanto ao conteúdo, o PL nº 330 indicou pouca cautela ao tratar do tema, deixando de espelhar princípios básicos do GDPR. Por esse motivo, passou a ser duramente criticado por especialistas[9]. Entre as lacunas mencionadas, destaca-se: exceções ao Poder Público à medida que não se lhe aplicaria as mesmas regras de proteção de dados como, por exemplo, a possibilidade de o titular de dados se opor ao tratamento de dados por parte do governo ou, ainda, de que teria assegurado o direito à limitação do tratamento dos mesmos, após o prazo necessário para realização da atividade; uma ampliação do rol de exceções, visto que a proteção da lei não se estenderia à coleta de dados para fins de repressão, investigação de infrações penais e atividades de inteligência, o que poderia acarretar em parcialidade quanto à utilização desses dados. Além disso, o projeto não previa a criação de uma autoridade de proteção de dados, considerada essencial para a efetividade da lei.

[9] Disponível em: < https://www.docdroid.net/jPBNsN6/nota-coalizao-pls330-final.pdf > Acesso em 29.07.2018.

Em comparação, o PL 5.276, de iniciativa da Câmara, apresentava um texto mais adequado aos debates atuais sobre proteção de dados e privacidade, uma vez que é fruto de um longo processo e diversas audiências públicas. Em comparação, o projeto traz pontos positivos que refletem as diretrizes do GDPR como, por exemplo, a coleta e uso de dados pessoais mediante consentimento explícito, e a imposição às empresas de coletar apenas dados estritamente necessários para que os seus serviços funcionem, isto é, com finalidade específica, conforme o princípio da adequação e limitação da finalidade. Também deixa clara a distinção entre dados pessoais, anônimos e sensíveis, atribuindo maior rigor a este último.

O mesmo projeto determina a criação de uma Autoridade Nacional de Proteção de Dados, de caráter regulatório. Essa autoridade teria a função de aconselhar, editar normas e fiscalizar o cumprimento da lei, aplicando sanções em caso de violações e/ou abusos , previsão esta relevante como garantia à segurança jurídica.

Diante desse confuso cenário, em meados de maio de 2018, e com a proximidade das eleições e consequente paralisação do Congresso Nacional, tornou-se indispensável o avanço do Senado Federal nas discussões para aprovação de uma Lei Geral de Proteção de dados, em caráter de urgência, considerando que encontra-se preparado para debater a matéria desde 2013, quando o PLS nº 330 entrou em pauta.

O projeto de lei aprovado em 2018

O trajeto para aprovação da lei geral de proteção de dados seguiu turbulento. No final de maio, a Câmara votou e aprovou o PL n° 4.060, incorporando também a redação do PL n° 5.276/2016, em regime de urgência regimental. Cabia, portanto, ao Senado aprovar o PL.

Ocorre que o PLS n° 330/2013, do Senado, permaneceu na Comissão de Assuntos Econômicos (CAE), ao invés de ser remetido à Câmara para votação. Com dois projetos versando sobre o mesmo tema no Senado, houve a saída de pauta do PLS n° 330/2013, que foi apensado ao PL n° 4.060/2012. Ambos se tornaram-se, então, o PLC n° 53/2018 (antigo PL n° 5.276/2016, apensado ao PL n° 4.060/2012 e, por fim, apensado ao PLS n° 330/2013) que aguardava, então, nova aprovação no Senado para, então, ser apreciado pelo Presidente da República.

Porém, tão importante quanto tocar a votação daquele momento em diante, seria preservar ao máximo as diretrizes do PL nº 5.276. O objetivo deveria ser buscar a aprovação de uma lei de proteção de dados robusta, que fosse igualmente aplicável aos setores público e privado, sem distinções[10]. Após algumas semanas, o PLS nº 330 acabou sendo superado, após trabalho e discussões concomitantes entre Senado e Câmara. Isto representou uma vitória não apenas para a Câmara, mas para a sociedade como um todo, que se beneficiará do texto mais protetivo composto pelos PLs nº 4.060 e 5.276.

Por fim, no dia 10 de julho de 2018, o Senado aprovou o referido PLC nº 53, representando um momento histórico para o país. É inegável o avanço alcançado, porém até o presente momento alguns questionamentos importantes ainda subsistem e podem ameaçar a evolução conquistada. Isto porque, o veto presidencial ainda é uma possibilidade, que se faz ainda mais preocupante com as discussões atuais em torno da inconstitucionalidade da lei por vício de iniciativa.

Argumenta-se que não é possível uma iniciativa do Poder Legislativo criar um órgão como a Autoridade Nacional de Proteção de Dados que, segundo a versão atual do PL, teria natureza de autarquia especial, estaria vinculada ao Ministério da Justiça e gozaria de independência administrativa, ausência de subordinação hierárquica, mandato fixo e estabilidade de seus dirigentes e autonomia financeira. Tal função caberia apenas ao Presidente da República, conforme o artigo 63, § 1º, II da Constituição Federal[11].

Além disso, o governo vem apresentando certa resistência à criação da Autoridade e propondo que tal tarefa seja desempenhada junto a outro órgão já existente. Justificam isto por questões jurídicas e de falta de orçamento para criar uma nova autoridade. As opções ventiladas são a Secretária Nacional de Relações do Consumidor (Senacon), que integra o Ministério da Justiça, ou algum órgão vinculado ao Gabinete de Segurança Institucional (GSI), que controla a Agência Brasileira de Inteligência (Abin). Porém, ambas as

---

[10] Disponível em: < https://www1.folha.uol.com.br/colunas/ronaldolemos/2018/06/governo-e-acusado-de-vender-dados.shtml > Acesso em 29/07/2018.

[11] Tema extensivamente tratado no artigo pelos autores MANGETH, A.L. TEFFÉ, C.A.S. Lei de dados pessoais precisa de uma Autoridade independente. Disponível em: < https://feed.itsrio.org/lei-de-dados-pessoais-precisa-de-uma-autoridade-independente-34137c7bbc64 > Acesso em 30/07/2018.

possibilidades não parecem adequadas, uma vez que a Autoridade deve ter, entre suas funções, a possibilidade de monitorar o próprio Estado, ela deve se encontrar em posição que lhe permita atuar sem intervenções indevidas. Por tudo isso, especialistas no tema vêm afirmando que eventual veto[12] presidencial à Autoridade ameaçaria o fino equilíbrio alcançado.

Nesse ponto, quais seriam, então os possíveis rumos para a Lei Geral de Proteção de Dados? Uma saída possível para tal imbróglio seria o Presidente vetar o trecho do PL que fala na criação da Autoridade e criar a autarquia por meio de Medida Provisória. Outra possibilidade que vem sendo alegada é que, em virtude da redação aprovada no PLC nº 53 se valer fortemente do projeto de lei apresentado pelo Poder Executivo em 2016 e dos debates e consultas que vinham sendo realizados desde 2010, este estaria revestido de legitimidade para a propositura de criação da Autoridade. Destaca-se que a proposta do Executivo, mesmo que não criasse explicitamente a autoridade nos moldes aprovados, já previa a designação de um órgão competente para a proteção de dados pessoais no País[13][14].

Fato é que a experiência de outros países mostra a relevância da existência de uma Autoridade específica para a aplicação eficiente de suas respectivas leis de proteção de dados. O mecanismo permite alcançar uma tutela efetiva da privacidade dos cidadãos, enquanto propicia segurança jurídica na aplicação da lei. Sua autonomia e independência são, sem dúvidas, essenciais para a efetividade das proteções dispostas para a privacidade e os dados pessoais, razão pela qual o país teria muito a perder com a retirada de sua figura da Lei.

Comparação principiológica entre o GDPR e o PL nº 53

O artigo 6º do PL nº 53/2018 é inteiramente dedicado aos princípios que deverão reger a Lei Geral de Proteção de Dados. O *caput* inicia a ideia determinando que a boa-fé

---

[12] Disponível em: < https://www1.folha.uol.com.br/opiniao/2018/07/laura-schertel-mendes-e-danilo-doneda-lei-de-protecao-de-dados-nao-pode-morrer-na-praia.shtml?loggedpaywall#_=_ > Acesso em 31/07/2018.

[13] Disponível em: < https://www.jota.info/tributos-e-empresas/regulacao/ha-vicio-de-iniciativa-na-criacao-da-autoridade-nacional-de-protecao-de-dados-26072018 > Acesso em 31/07/2018.

[14] Disponível em: < https://www.jota.info/opiniao-e-analise/artigos/constitucionalidade-da-criacao-da-autoridade-nacional-de-protecao-de-dados-24072018 > Acesso em 31/07/2018.

deve guiar todas as atividades de tratamento de dados pessoais. Nos incisos seguintes, o legislador elenca os demais princípios escolhidos, indicando ainda as definições adotadas, quais sejam:

> I - Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
>
> II – Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
>
> III – Necessidade: limitação do tratamento ao mínimo necessário para a realização das suas finalidades, com 7 abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
>
> IV – Livre acesso: garantia aos titulares de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade dos seus dados pessoais;
>
> V – Qualidade dos dados: garantia aos titulares de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
>
> 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;
>
> VII – Segurança: utilização de medidas 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 difusão;
>
> VIII – Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
>
> IX – Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios, ilícitos ou abusivos; e
>
> X – Responsabilização e prestação de contas: demonstração pelo agente da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais, inclusive da eficácia das medidas.

Nota-se a intenção do legislador brasileiro em estabelecer princípios amplos, alinhando-se ao GDPR, à medida que espelha os princípios de adequação e limitação da finalidade, necessidade, qualidade e *accountability*. Com a distinção de que no PL nº 53, o princípio da qualidade equivaleria ao princípio *accuracy* do GDPR, mantendo, porém, o mesmo conteúdo. O princípio da não discriminação, contido no PL nº 53, reflete em seu significado a ideia de *lawfullness* e *fairnes*, ou seja, de um tratamento de dados guiado pela licitude e lealdade, e nunca para fins discriminatórios ou abusivos.

Conclusões

A proteção de dados pessoais é um tema de grande importância tendo em vista o mundo conectado no qual vivemos. A todo momento nossas informações são coletadas fora da rede ou dentro dela, através de compras online, redes sociais, plataformas, e o potencial que nossos dados tem quando reunidos é grande, razão pela qual é necessário uma lei específica para resguardá-los.

Em 2018, a Europa foi contemplada pelo Regulamento Geral de Proteção de Dados Pessoais (GDPR), legislação considerada abrangente na proteção do titular de dados e com medidas assertivas em relação a condutas a serem tomadas pelo Poder Público e por empresas que realizem coleta, tratamento ou transferência de dados. O consentimento por parte do titular firmou-se como o critério chave da legislação, o que denota a opção clara do legislador europeu em proteger o indivíduo, em detrimento de interesses econômicos ou públicos.

O Brasil, por outro lado, nunca teve uma lei de proteção de dados, estando na contramão de uma orientação que é não apenas global, mas também sul-americana. Com isso, finalmente em 2018 o país se viu confrontando diretamente tal necessidade e os principais projetos de lei sobre o tema progrediram em seu andamento no Congresso Nacional.

A primeira iniciativa, do Senado, não refletia as orientações do GDPR, ao não instituir, por exemplo, uma Autoridade de Proteção de dados. Por outro lado, a iniciativa da Câmara se mostrou madura e fortalecida por debates e Audiências Públicas, sendo considerada a proposta mais adequada por especialistas da área.

Por fim, em julho, o projeto final — PLC 53/2018 — foi aprovado e agora aguarda a sanção presidencial. Não obstante, dúvidas quanto à constitucionalidade do projeto por vício de iniciativa ainda pairam, criando dúvidas de um possível veto por parte do Presidente. Ainda assim, até o momento subsiste o anseio de que o texto seja preservado em sua totalidade, inclusive com a criação da Autoridade de Proteção de dados pessoais, haja vista que esta é essencial para a efetividade da Lei, preservada sua imparcialidade e autonomia.

Referências

BAIÃO, Kelly Sampaio; GONÇALVES, Kalline Carvalho. A garantia da privacidade na sociedade tecnológica: um imperativo à concretização do princípio da dignidade da pessoa

humana. Civilistica.com. Rio de Janeiro, a. 3, n. 2, jul.-dez./2014. Disponível em: < http://civilistica.com/a-garantia-da-privacidade-na-sociedade-tecnologica-um-imperativo-a-concretizacao-do-principio-da-dignidade-da-pessoa-humana >. Acesso em: 27/07/2018.

BIONI, Bruno. Xequemate: o tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil. São Paulo: GPoPAI/USP, 2015.

BURGESS, Matt. What is the GDPR? The summary guide to GDPR compliance in UK. Disponível em: < https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/ > Acesso em 30/07/2018.

DIAS, Tatiana. Como a falta de noção do governo, militares e os bancos podem melar a lei de de dados pessoais. Disponível em: < https://theintercept.com/2018/07/17/lei-de-dados-pessoais-governo/ > Acesso em 30/07/2018.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006.

DONEDA, Danilo. SCHERTEL, Laura. Lei de proteção de dados não pode morrer na praia. Disponível em: < https://www1.folha.uol.com.br/opiniao/2018/07/laura-schertel-mendes-e-danilo-doneda-lei-de-protecao-de-dados-nao-pode-morrer-na-praia.shtml?loggedpaywall#_=_ > Acesso em 30/07/2018.

GALLINDO, Sergio. STIVELBERG, Daniel. Constitucionalidade da criação da Autoridade Nacional de Proteção de Dados. Disponível em: < https://www.jota.info/opiniao-e-analise/artigos/constitucionalidade-da-criacao-da-autoridade-nacional-de-protecao-de-dados-24072018 > Acesso em 30/07/2018.

MANGETH, A.L. TEFFÉ, C.A.S. Lei de dados pessoais precisa de uma Autoridade independente. Disponível em: < https://feed.itsrio.org/lei-de-dados-pessoais-precisa-de-uma-autoridade-independente-34137c7bbc64 > Acesso em 30/07/2018.

MANGETH, A.L. MAGRANI, Eduardo NUNES, Beatriz. A proteção de seus dados pessoais está em jogo no Senado. Disponível em: < https://feed.itsrio.org/senado-vs-c%C3%A2mara-seus-dados-pessoais-em-jogo-97d7b0cefc54 > Acesso em 24/07/2018

MANGETH, A.L. MAGRANI, Eduardo NUNES, Beatriz. Seis pontos para entender a lei europeia de proteção de dados. Disponível em: < https://feed.itsrio.org/seis-pontos-para-entender-a-lei-europeia-de-prote%C3%A7%C3%A3o-de-dados-pessoais-gdpr-d377f6b691dc > Acesso em 24/07/2018

MENDES, Laura. DONEDA, Danilo. Lei de proteção de dados não pode morrer na praia. Disponível em: < https://www1.folha.uol.com.br/opiniao/2018/07/laura-schertel-mendes-e-danilo-doneda-lei-de-protecao-de-dados-nao-pode-morrer-na-praia.shtml?loggedpaywall#_=_ > Acesso em 30/07/2018.

MORAES, Maria Celina Bodin de. O princípio da Dignidade Humana. *Princípios do Direito Civil Contemporâneo.* Renovar, 2006.

PAULA, Felipe de. NAEGELE, Vitor. Há vício de iniciativa na criação da Autoridade Nacional de Proteção de Dados? Disponível em: < https://www.jota.info/tributos-e-empresas/regulacao/ha-vicio-de-iniciativa-na-criacao-da-autoridade-nacional-de-protecao-de-dados-26072018 > Acesso em 30/07/2018.

PERLINGIERI, Pietro. Normas constitucionais nas relações privadas. *Revista da Faculdade de Direito*, Rio de Janeiro, Renovar, p. 63-77.

PERLINGIERI, Pietro. Princípios. *Perfis do Direito Civil.* Rio de Janeiro, São Paulo: Renovar, 2002, 2. ed., p. 35-56.

PERLINGIERI, Pietro. Situações subjetivas existenciais. *Perfis do Direito Civil.* Rio de Janeiro, São Paulo: Renovar, 2002, 2. ed., p. 153-199.

RODOTÀ, Stefano. A Vida na Sociedade da Vigilância: a privacidade hoje. Rio de Janeiro: Editora Renovar, 2007.

SOLOVE, Daniel. A Taxonomy of Privacy. University of Pennsylvania Law Review, 2006. Vol. 154, n. 3.