RGPD V. LGPD: ADOÇÃO ESTRATÉGICA DA ABORDAGEM RESPONSIVA NA ELABORAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS DO BRASIL E DO REGULAMENTO GERAL DE PROTEÇÃO DE DADOS DA UNIÃO EUROPEIA

GDPR v. GDPL: Strategic Adoption of the responsiveness approach in the elaboration of Brazil's General Data Protection Law and the EU General Data Protection Regulation

Submetido: 05/12/2019
Parecer: 19/12/2019
Aceito: 27/01/2020

Aline Iramina*
ORCID: 0000-0002-5141-9544

DOI: https://doi.org/10.26512/lstr.v12i2.34692

Abstract

Purpose – *The main purpose of this article is to analyze the aspects of the responsiveness approach adopted by European and Brazilian lawmakers in the elaboration of data protection rules, such as GDPR and LGPD.*

Methodology – *The applied methodology is based on the responsive regulation theory and, additionally, the network governance theory, through the comparative analysis of personal data protection legal frameworks in Brazil and the EU.*

Findings – *Based on the comparative analysis of the GDPR and the LGPD, it is verified the adoption of escalated regulatory techniques of Ayres and Braithwaite's enforcement pyramid in the developed of these norms, as a strategy adopted by lawmakers to guarantee a greater compliance from regulated entities.*

Keywords: *Data Protection. Responsive Regulation Theory. Regulatory Authorities. Compliance. Nodal Governance.*

Resumo

Propósito – O propósito do artigo é analisar os aspectos da abordagem responsiva adotados pelos legisladores europeus e brasileiros na elaboração das normas de proteção de dados, como a LGPD e o RGPD.

Metodologia/abordagem/design – a metodologia a ser aplicada terá como base a teoria da regulação responsiva e, subsidiariamente, a teoria da governança em rede, por meio da análise comparativa dos arcabouços legais de proteção de dados pessoais europeu e brasileiro.

*Master of Laws (L.L.M) em Direito da Propriedade Intelectual na University College London (UCL). Coordenadora-Geral de Regulação, Negociação e Análise, da Secretaria de Direitos Autorais e Propriedade Intelectual, do Ministério da Cidadania. E-mail: alineiramina@gmail.com.

Resultados – Por meio da análise comparativa da LGPD e do RGPD, verificar-se-á a adoção de técnicas regulatórias escaláveis da pirâmide de constrangimento de John Braithwaite e Ian Ayres na construção desses atos normativos, como estratégia dos legisladores de buscar maior *compliance* dos entes regulados.

Palavras-Chave: Proteção de Dados. Teoria da Regulação Responsiva. Autoridades Regulatórias. Compliance. Governança Nodal.

INTRODUÇÃO

Em uma sociedade cada vez mais informatizada, na qual o fluxo de dados se tornou um componente crucial para o comércio, as comunicações e as interações sociais, a proteção de dados pessoais passou a ser uma preocupação para grande parte dos países. Nesse contexto, muitos países têm adotado novas regras de proteção de dados ou modernizado as que já tinham, como Coreia do Sul, Chile, Tailândia, Índia, Indonésia e Brasil. Atualmente, já são mais de cem países com marcos regulatórios para proteção de dados pessoais em todo o mundo (CONSUMERS INTERNATIONAL, 2018, p. 2).

Considerando que empresas geralmente operam extraterritorialmente, a convergência global das normas que regulam a proteção de dados tem-se mostrado fundamental, não só para facilitar o fluxo de dados e, consequentemente, o comércio e a cooperação entre as organizações e as autoridades públicas, mas também para aumentar o nível de proteção de dados pessoais em todo o mundo. Não por acaso, grande parte das mais recentes legislações de proteção de dados são inspiradas no Regulamento Geral de Proteção de Dados (RGPD) da União Europeia, em vigor desde maio de 2018, e, portanto, apresentam características similares, como: 1) legislação geral e abrangente (em vez de normas setoriais); 2) proteção de direitos individuais; 3) autoridade supervisora independente (UNIÃO EUROPEIA, 2019a)

No caso brasileiro, em um contexto de adequação progressiva do país às melhores práticas globais na gestão de dados, o Congresso Nacional aprovou a Lei n° 13.709, de 2018, também conhecida como Lei Geral de Proteção de Dados (LGPD) e fortemente inspirada na legislação europeia, que se aplica tanto as empresas estabelecidas em território nacional quanto as com sede no exterior que ofereçam serviços ou tenham operações no país. A LGPD tem previsão de entrada em vigor no país em agosto de 2020. Inclusive, a Autoridade Nacional de Proteção de Dados (ANPD), que será o órgão regulador responsável pela aplicação e fiscalização das novas normas no país, ainda está em processo de formação.

Já sob a perspectiva regulatória, que é objeto principal de análise deste artigo, observa-se que tanto a LGPD quanto o RGPD adotam uma abordagem estratégica para o tratamento de dados pessoais, incentivando as empresas a adotarem boas práticas de privacidade, como forma de investimento e obtenção de vantagem competitiva no uso dos dados pessoais. Nesse sentido, por meio de uma análise comparativa das duas legislações, verifica-se a opção tanto dos legisladores europeus quanto dos brasileiros por aspectos da regulação responsiva, em detrimento dos de comando-e-controle, para aplicação das normas. Em particular, nota-se claramente a adoção pelos legisladores de estratégias regulatórias escaláveis, que partem desde mecanismos de autorregulação regulada até regulação por sanções.

Nesse ínterim, o objetivo deste artigo é demonstrar como as técnicas regulatórias escaláveis da pirâmide de constrangimento de John Braithwaite e Ian Ayres estão presentes nas normas previstas tanto na LGPD quanto no RGPD, assim como a opção dos legisladores pela perspectiva de governança em rede, como forma estratégica para facilitar o trabalho das autoridades regulatórias e buscar maior *compliance* das organizações reguladas em relação às normas de proteção de dados. Para isso, serão apresentadas as principais regras previstas no RGPD, as principais semelhanças e diferenças entre o RGPD e a LGPD, o papel das autoridades nacionais de proteção de dados para implementação e aplicação do regulamento e da lei e, por fim, será feita a análise de como essas normas se inserem em uma abordagem responsiva de regulação, por meio da aplicação, de forma escalada, das medidas regulatórias previstas nas legislações europeia e brasileira na pirâmide de constrangimento de Braithwaite e Ayres.

PRINCIPAIS ASPECTOS NORMATIVOS INTRODUZIDOS PELO RGPD E PELA LGPD NA REGULAÇÃO DA PROTEÇÃO DE DADOS PESSOAIS

Como é possível verificar pela análise das principais regras previstas no Regulamento Geral de Proteção de Dados e na Lei Geral de Proteção de Dados, a lei brasileira tem forte inspiração no regulamento europeu, com a adoção de uma legislação abrangente sobre o tema, o estabelecimento de direitos fundamentais para os titulares dos dados e a criação de uma autoridade supervisora independente. Inclusive em relação às estratégias e aos mecanismos regulatórios previstos em ambas as normativas, como será analisado neste artigo, observa-se que os legisladores optaram pela mesma abordagem responsiva, com base em uma governança nodal, para implementação, aplicação e fiscalização mais efetiva dessas normas pelas autoridades regulatórias.

Regulamento Geral de Proteção de Dados (RGPD) – União Europeia

Em vigor desde 25 de maio de 2018, o Regulamento Geral de Proteção de Dados foi aprovado, em 2016, em substituição a Diretiva de Proteção de Dados de 1995, que estabelecia padrões mínimos para o processamento de dados na União Europeia (CONSUMERS INTERNATIONAL, 2018, p. 1). O RGPD tem como objetivo principal harmonizar as leis de privacidade de dados no bloco europeu, regulando o processamento por indivíduos, empresas ou organizações de dados pessoais relacionados a indivíduos do bloco. Nesse sentido, as grandes novidades trazidas pelo RGPD foram: o fortalecimento dos direitos dos indivíduos sobre seus dados; a obrigação de harmonização das normas sobre o tema para os reguladores europeus; e maior responsabilidade pra as empresas em relação aos dados pessoais que coletam, com sanções mais duras para aquelas que não agirem em conformidade com as novas regras (CONSUMERS INTERNATIONAL, 2018, p. 1).

No artigo "Learning from the EU GDPR: What elements should the US adopt?", o *Centre for Information Policy Leadership (CIPL)* destaca a necessidade dos países, em particular os EUA, seguirem o exemplo europeu e adotarem uma legislação com obrigações específicas que não sejam excessivamente prescritivas e que garantam flexibilidade organizacional na decisão de como alcançar as obrigações, encorajando abordagens inovadoras para o *compliance (*2019a). O foco, portanto, segundo o estudo, deve estar nas obrigações e não em como elas devem ser cumpridas. De acordo com o CIPL, essa abordagem deve garantir que a lei se mantenha atual, seja escalável para pequenas e médias empresas com recursos limitados e não reprima indevidamente a inovação orientada por dados.

Desse modo, em relação aos elementos centrais do RGPD, vale destacar a exigência de consentimento por parte do titular, que deve ser realizado por meio de uma ação clara e afirmativa do indivíduo e que deve ser fornecido para cada operação de processamento ou uso de dados pessoais. As empresas devem, assim, manter um registro de quando e como o indivíduo deu o seu consentimento. No caso de crianças, o consentimento deve vir de seus pais ou responsáveis. Lembrando que dados pessoais para os fins do regulamento são quaisquer informações que se relacionam a um indivíduo identificado ou identificável. Ou seja, dados de pessoas "anônimas" não são considerados dados pessoais.

Nesse sentido, o regulamento proíbe o uso de dados pessoais para um propósito diferente do qual foi coletado originalmente, a não ser que o novo propósito não seja incompatível com o original, segundo o art. 6(4). No art. 9, o regulamento proíbe, também, os usos de dados sensíveis (ex. sobre raça, origem

étnica, opiniões religiosas ou políticas, saúde, orientação sexual etc.), a não ser que o indivíduo tenha fornecido seu consentimento explícito ou sob outras circunstâncias específicas (CIPL, 2019a). Isso porque, ao proteger os dados, não se busca apenas defender um bem ou valor econômico, mas também evitar a manipulação de comportamentos, discriminações, revelações não desejadas da vida privada, em outras palavras, proteger a privacidade como um todo (ROCHFELD, 2018).

Em relação às circunstâncias específicas, o RGPD prevê seis fundamentos jurídicos de processamento ou "bases" para usar dados pessoais, uma dos quais deve ser apresentada para validar a legalidade do processamento. Uma dessas bases é o "interesse legítimo", previsto no art. 6(1)(f), que permite o processamento de informações pessoais quando a organização ou terceiro tem um interesse legítimo no processamento que se sobrepõe aos interesses ou aos direitos dos indivíduos cuja informação pessoal está sendo processada. O regulamento busca assim um equilíbrio entre os interesses dos indivíduos, titulares dos dados, e das organizações que fazem o tratamento desses dados. (CIPL, 2019a)

Além disso, o RGPD incorpora, no Capítulo 3, vários dos direitos individuais de proteção de dados que já estavam previstos na antiga Diretiva de Proteção de Dados da UE (ex. acesso, correção, objeção, "apagamento" de dados) e vários outros novos direitos (ex. portabilidade de dados, transparência na coleta e transmissão de dados e a revisão de decisões puramente automatizadas por pessoas naturais). No caso, o direito à portabilidade e à recuperação dos dados é um elemento novo e essencial do novo sistema, para restituir de fato ao indivíduo o controle sobre os seus dados (MARTIAL-BRAZ, p. 103). Tais direitos, contudo, não são absolutos, estando sujeitos a exceções em circunstâncias específicas, conforme mencionado acima. De qualquer modo, esses direitos fortalecem o posicionamento dos indivíduos e garantem que eles tenham certo controle sobre suas informações (CIPL, 2019a).

Já no tocante a sua forma de aplicação, uma das principais novidades trazidas pelo novo regulamento europeu foi a inclusão do princípio de *accountability* no art. 24, demandando às organizações que: (a) adotem políticas, procedimentos e medidas para implementação das obrigações do RGPD; e b) sejam capazes de demonstrar tal implementação. De acordo com o CIPL, a obrigação de *accountability* promove o tratamento responsável dos dados por organizações e possibilita uma proteção significativa dos dados para os indivíduos, por meio de boas práticas operacionais mandatórias que cobrem os elementos centrais de responsabilização (ex. avaliação de risco, registro dos processos, implementação de medidas de segurança etc.). (2019a)

Nesse sentido, o regulamento prevê, ainda, nos artigos 37, 38 e 39, a necessidade das empresas contratarem um responsável ou encarregado da proteção de dados (*Data Protection Officer – DPO)*, que deve auxiliar aquelas que controlam ou processam dados em questões relacionadas à proteção de dados pessoais, informando e orientando, por exemplo, o controlador ou processador, assim como seus empregados, sobre suas obrigações estabelecidas pela legislação de proteção de dados. Do mesmo modo, esse encarregado da proteção de dados deve monitorar o cumprimento por parte da empresa de toda legislação relacionada à matéria, inclusive em auditorias, atividades de conscientização, assim como em treinamentos da equipe envolvida nas operações de processamento. O encarregado age, também, como ponto focal para recebimento dos requerimentos dos indivíduos a respeito do uso de seus dados pessoais e atua em cooperação com as autoridades regulatórias (UNIÃO EUROPEIA, 2019b).

Nesse contexto, o RGPD incorpora também uma abordagem de avaliação de riscos, no art. 24, que obriga as organizações não apenas a avaliar os riscos de dano aos indivíduos, mas também os benefícios que estão associados a usos específicos de informações pessoais e que possibilitam ações de mitigação de riscos que são elaboradas de acordo com a avaliação de risco/benefício feita pela empresa. De acordo com o regulamento, as organizações têm flexibilidade para determinar suas próprias metodologias de avaliação de riscos e ações de mitigação, de modo a facilitar tanto a melhor proteção da privacidade quanto o uso mais efetivo de dados pessoais (CIPL, 2019a). Quando os dados são considerados de risco, o RGPD, no art. 35, demanda, ainda, que as empresas façam uma avaliação de impacto da proteção de dados (*Data Protection Impact Assessment*) (CIPL, 2019a).

Ainda dentro da obrigação de *accountability*, o regulamento obriga as organizações a notificarem, sem demora e quando possível em 72 horas, a autoridade nacional de proteção de dados (reguladora) sobre qualquer violação de dados que pode resultar em riscos a indivíduos e a notificarem os próprios indivíduos se a violação puder resultar em alto risco para eles, conforme previsto nos artigos 33 e 34. Quando a notificação não for feita em 72 horas, ela, quando encaminhada, deve ser acompanhada das razões para o atraso.

O RGPD requer que as organizações já levem em consideração a proteção de dados quando da fase de concepção de novos produtos, serviços e projetos, o que eles têm chamado de *privacy by design*. Isso porque se entende que a privacidade desde a concepção, juntamente com os elementos de *accountability* organizacional e a abordagem de avaliação de riscos, já mencionados acima, constituem a base fundamental do arcabouço jurídico

moderno de privacidade de dados trazido pelo regulamento europeu (CIPL, 2019a).

Por fim, vale mencionar que o RGPD prevê a figura das autoridades de proteção de dados (DPAs) – ao menos uma para cada Estado Membro da UE - que são responsáveis por supervisionar, por meio de poderes investigativos e corretivos, a aplicação da lei de proteção de dados. Além de fornecer pareceres sobre questões envolvendo proteção de dados, essas autoridades que analisam as denúncias a respeito de violações ao regulamento. Até por isso, a norma dá poderes para que as autoridades de proteção de dados reguladoras imponham multas de até 20 milhões de euros ou 4% do faturamento global para algumas violações do regulamento.

A União Europeia criou ainda um grupo com a participação de múltiplas partes interessadas (*Multistakeholder Expert Group*) para auxiliar na identificação de possíveis desafios na implementação do RGPD, sob a perspectiva de diferentes partes interessadas, e orientar a comissão em como resolvê-los. Participam, atualmente, como membros do grupo, representantes de empresas, da sociedade civil e indivíduos com conhecimento na área. Em um relatório publicado, em junho de 2019, com as contribuições do grupo, levantou-se, por exemplo, nesse primeiro momento, entre as várias questões experimentadas pelas organizações para estarem em conformidade com o RGPD, o aumento substantivo dos investimentos para garantir a conformidade com o regulamento, em particular investimentos para garantir *accountability* no processamento dos documentos, renovar o consentimento dos indivíduos, atualizar os contratos e as notificações com informações a respeito da proteção de dados, implementar políticas para lidar com violações de dados, criar novos processos internos de negócios para lidar com requerimentos sobre tratamento de dados ou para validar novos processos operacionais, aumentar a conscientização e treinamentos (MULTISTAKEHOLDER EXPERT GROUP, 2019), o que demonstra a maior responsabilidade das organizações em garantir a aplicação efetiva do regulamento.

Embora o RGPD seja diretamente aplicável nos Estados Membros, é necessário que os estados europeus adotem uma série de medidas legais no âmbito nacional, em particular para estabelecer e alocar poderes para as autoridades nacionais de proteção de dados, como o poder para aplicar multas administrativas (CIPL, 2019a). O trabalho das autoridades nacionais de proteção de dados, em cooperação com o Comitê Europeu de Proteção de Dados (ou *the European Data Protection Board - the Board)*, também é uma questão chave para uma aplicação consistente das novas regras no continente europeu.

Lei Geral de Proteção de Dados (LGPD) e as Principais Semelhanças e Diferenças em relação ao RGPD

No Brasil, a Lei n° 13.709, de 14 de agosto de 2018, estabeleceu a Lei Geral de Proteção de Dados Pessoais (LGPD), prevista para entrar em vigor em agosto de 2020. A lei busca unificar mais de quarenta normas diferentes que regulam a proteção de dados, seja *online* ou *off-line*, no país (KOCH, 2019). Em geral, a lei estabelece regras de coleta, tratamento, armazenamento e compartilhamento de dados pessoais pelas organizações, além de garantir direitos aos titulares das informações, responsabilidades para quem processa dados e estruturas e formas de fiscalização e eventuais sanções em caso de abuso (VALENTE, 2019). Vale lembrar que, no Brasil, a proteção de dados têm também fundamentação legal na Constituição Federal, em particular nas garantias constitucionais de liberdade, privacidade e sigilo de dados (CAVALCANTI & SANTOS, 2018).

A Medida Provisória n° 869, de 2018, editada e aprovada na forma da Lei n° 13.853, de 08 de julho de 2019, instituiu a Autoridade Nacional de Proteção de Dados (ANPD), órgão regulador com autonomia técnica, vinculado à Presidência da República. A ANPD, que ficará responsável pela regulação, aplicação e fiscalização das normas da LGPD, será formada por um Conselho Diretor constituído por cinco diretores, nomeados pelo Presidente da República, e os membros do conselho terão mandato de quatro anos. Há, na lei, o compromisso de revisão da natureza institucional da ANPD após dois anos de sua entrada em vigor.

Assim como na legislação europeia, a LGPD adota um modelo de lei geral, que busca construir uma arquitetura regulatória de modo a consolidar o tema de proteção de dados pessoais como um setor de políticas públicas, composto por instrumentos estatutários, sancionatórios e um órgão administrativo, responsável pela implementação e aplicação da lei (MENDES, 2014, p. 58 *apud* CAVALCANTI & SANTOS, 2018, p. 354). Segundo o art. 5 da LGPD, dados pessoais são quaisquer informações que podem identificar alguém, incluindo aquelas utilizadas para a identificação do perfil comportamental de uma pessoa natural (identificada ou identificável). Dados de crianças e adolescentes, assim como dados considerados sensíveis, como informações a respeito de origem racial ou étnica, convicções religiosas, opiniões políticas e orientação sexual, têm um grau maior de proteção, assim como se verifica no RGPD.

A LGPD tem abrangência extraterritorial e atinge todas as pessoas (físicas ou jurídicas) e atividades realizadas no Brasil que tenham relação com tratamento de dados pessoais, como a coleta, a produção, a classificação, a utilização, o acesso, a reprodução, a transmissão, a distribuição, o

processamento, o arquivamento, o armazenamento, a eliminação, a avaliação ou o controle da informação, a modificação, a transferência, a difusão ou a extração de dados, nos termos do art. 5, inciso XII, da lei. Isso significa que, mesmo que a empresa ou organização não esteja localizada no país, se o tratamento dos dados e a oferta de serviços e bens resultantes desse tratamento são feitos no território nacional, a lei é aplicável. Do mesmo modo, a lei se aplica se os dados pessoais objeto do tratamento tenham sido coletados no território brasileiro (CAVALCANTI & SANTOS, 2018).

Ainda, com base no *Fair Information Principles* e no *Guidelines on the Protection of privacy and Transborder Flows of Personal Data da OCDE*, a LGPD adotou como princípios fundamentais em relação ao tratamento de dados, os princípios da: **finalidade** especificada e informada explicitamente ao titular; **adequação** à finalidade previamente acordada e divulgada; **necessidade** do tratamento, limitado ao uso de dados essenciais para alcançar a finalidade inicial; **acesso livre**, fácil e gratuito das pessoas à forma como seus dados são tratados; qualidade dos dados, deixando-os exatos e atualizados, segundo a real necessidade do tratamento; **transparência** ao titular, com informações claras e acessíveis sobre o tratamento e seus responsáveis; **segurança** para coibir situações acidentais ou ilícitas como invasão, destruição, perda, difusão; **prevenção** contra danos ao titular e a demais envolvidos; **não discriminação**, ou seja, não permite para fins discriminatórios ilícitos ou abusivos; e **responsabilização e prestação de contas** do agente, obrigado a demonstrar a eficácia das medidas adotadas para a observância e cumprimento das normas (CAVALCANTI & SANTOS, 2018).

Assim como no regulamento europeu, a LGPD se preocupa com o empoderamento dos titulares de dados por meio de controle e escolha significativos em relação às suas informações pessoais. Por exemplo, os titulares de dados devem ser devidamente informados sobre o processamento dos seus dados pessoais e essa informação deve ser clara, adequada, facilmente acessível e transparente. A LGPD, no artigo 18, estabelece, assim, nove direitos fundamentais para os indivíduos em relação a proteção de seus dados, no caso:

> I - confirmação da existência de tratamento;
> II - acesso aos dados;
> III - correção de dados incompletos, inexatos ou desatualizados;
> IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
> V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa e observados os segredos comercial e industrial, de acordo com a regulamentação do órgão controlador;

> V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;
> VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;
> VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
> VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
> IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.

Os direitos previstos na LGPD são essencialmente os mesmos previstos no RGPD, embora no regulamento europeu sejam oito e não nove direitos fundamentais. De acordo com Richie Koch, isso se justificaria pois o regulamento prevê um direito mais amplo de acesso à informação *("Right to be Informed"*), enquanto a lei brasileira teria dividido o mesmo direito em dois, ao incluir especificamente o direito de "informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados" (KOCH, 2019).

Ademais, da mesma forma que o regulamento europeu, a lei brasileira prevê uma série de obrigações para as empresas, instituições públicas ou privadas e órgãos do governo, como a necessidade de garantir a segurança das informações e a de notificar os titulares em caso de violações de dados. No entanto, a lei prevê também os casos em que se pode fazer o uso de dados sem necessidade de consentimento do titular, permitindo, por exemplo, a utilização de dados por empresas nos casos em que há "legítimo interesse".

Para adaptar-se às obrigações da nova legislação, os agentes, que podem ser tanto pessoa física quanto jurídica, de direito público ou privado, que coletam e fazem tratamento de dados, têm não apenas investido em tecnologia da informação e segurança da informação, mas também nomeado responsáveis pela proteção de dados, buscado obter consentimento dos clientes para a utilização de seus dados e atualizado documentos, como contratos e políticas internas. Vale ressaltar que, segundo o art. 5, incisos VI e VII, esses agentes podem ser tanto o "controlador", a quem compete as decisões referentes ao tratamento de dados pessoais, quanto o operador, que é quem realiza o tratamento dos dados em nome do controlador, na mesma lógica adotada pelo RGPD.

Embora a LGPD tenha sido claramente influenciada pelo regulamento europeu, como já mencionado anteriormente, inclusive tendo objetivos muito similares, há algumas diferenças entre as duas normativas. Por exemplo, em relação aos encarregados da proteção de dados, enquanto o RGDP estabelece,

em seu art. 37, os casos específicos em que é necessário contratar um encarregado, como no caso em que o processamento dos dados é feito por um órgão ou autoridade pública, na LGPD, a redação atual do art. 41 leva ao entendimento de que toda organização que faz o processamento de dados precisaria contratar um encarregado da proteção de dados, embora ainda seja necessária maior clareza a respeito (KOCH, 2019).

Além disso, no tocante às notificações de violações de dados, enquanto o RGPD estabelece que a notificação deve ser feita em 72 horas a partir da descoberta da violação, a LGPD não estabelece um prazo, determinando apenas que a notificação seja realizada em um período razoável de tempo, conforme definido pela autoridade nacional. Dessa forma, caberá a Autoridade Nacional de Proteção de Dados, quando em funcionamento, estabelecer o prazo. Do mesmo modo, o RGPD é bem mais rigoroso em relação às multas possíveis de serem aplicadas por violações de dados se comparado a LGPD. A lei brasileira estabeleceu, no art. 52, que a multa por violação de dados deve ser de " até 2% do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$50 milhões por infração". No câmbio atual, isso equivaleria entre €10 e 11 milhões, o que representaria metade da multa máxima aplicada na União Europeia.

Isso porque, em relação a outras opções de punições possíveis previstas na lei, que haviam sido, em grande parte, replicadas do RGPD, como advertências, multas, bloqueios, suspensões e proibições parciais ou totais do exercício de suas atividades, o atual Presidente da República vetou as duas últimas formas de punição pela autoridade regulatória, com a aprovação da Lei n° 13.853, de 2019, como:

> X- suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;
> XI – suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;
> XII – proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

Justificou-se o veto por entender-se que, ao prever as sanções administrativas de suspensão ou proibição do funcionamento/exercício da atividade relacionada ao tratamento de dados, a lei geraria insegurança aos responsáveis por essas informações e impossibilitaria a utilização e tratamento de bancos de dados essenciais a diversas atividades privadas, podendo acarretar

prejuízo à estabilidade do sistema financeiro nacional, bem como a entes públicos, com potencial de afetar a continuidade de serviços públicos. Observar-se, assim, que mesmo as sanções mais duras previstas no RGPD foram vetadas na redação atual da LGPD.

Ainda no tocante às diferenças, importante mencionar também o rol mais amplo da lei brasileira, se comparado ao do regulamento europeu, em relação à base legal para o processamento de dados. Originalmente o RGPD incluiu como bases legais o consentimento explícito, desempenho contratual, tarefa pública, interesse vital, obrigação legal e interesse legítimo. A LGPD incluiu as seis e acrescentou outras quatro: estudos de um órgão de pesquisa, exercício de direitos em processos judiciais, proteção à saúde e proteção ao crédito. Assim, enquanto a lei brasileira prevê, no artigo 7°, dez circunstâncias legais para o processamento de dados, o regulamento europeu prevê seis. Para Richie Koch, a proteção do crédito como uma base legal para o processamento de dados, sem dúvida, se afasta de forma significativa do disposto no RGPD (KOCH, 2019), sendo, de certo modo, também, questionável a sua previsão.

Assim como ocorreu na União Europeia, com o estabelecimento de autoridades nacionais de proteção de dados em cada Estado Membro, a estruturação da Autoridade Nacional de Proteção de Dados é fundamental para garantir a implementação e a aplicação da LGPD no Brasil, inclusive com o estabelecimento de diretrizes, regulamentação da matéria e aplicação de sanções administrativas para garantir a proteção de dados dos cidadãos brasileiros (CAVALCANTI & SANTOS, 2018). Como a Autoridade deve ter, entre suas funções, a possibilidade de monitorar não apenas empresas privadas, mas também o Estado, ela deve estar em posição para atuar sem intervenções indevidas (ITS, 2018).

A criação do Conselho Nacional de Proteção de Dados, órgão consultivo, com composição multissetorial e competência para propor diretrizes e estratégias, elaborar estudos e disseminar o conhecimento de proteção de dados no país também é fundamental para a aplicação da lei (CAVALCANTI & SANTOS, 2018). Está previsto na lei que o Conselho deverá ser composto por 23 representantes de órgãos públicos e da sociedade civil, com mandato de dois anos.

Por fim, assim como o RGPD, a LGPD cria obstáculos para a transferência internacional de dados pessoais para países que não são considerados com um nível adequado de proteção. Por isso, a importância da convergência global das normas que tratam de proteção de dados e de a lei brasileira ser interoperável com os principais regimes globais de privacidade, entre eles o europeu. Isso porque essa interoperabilidade é essencial para os negócios globais e para o *compliance* por organizações de todos os tamanhos.

PAPEL CENTRAL DAS AUTORIDADES NACIONAIS DE PROTEÇÃO DE DADOS NA IMPLEMENTAÇÃO E APLICAÇÃO DO RGPD E DA LGPD

Tanto o Regulamento Geral de Proteção de Dados quanto a Lei Geral de Proteção de Dados criaram uma nova estrutura de governança, colocando no centro as autoridades nacionais de proteção de dados (no caso da União Europeia, um para cada Estado Membro), como aplicadoras (*enforcers*) das novas regras e os primeiros pontos de contato para as partes interessadas. As novas normas equiparam essas autoridades com maiores poderes de *enforcement*, ao mesmo tempo em que deram maiores responsabilidades para as organizações, fornecendo ferramentas para que possam demonstrar *compliance*, como cláusulas contratuais padronizadas, códigos de conduta setoriais e os mais novos mecanismos de certificação.

No Brasil, originalmente, a Autoridade Nacional de Proteção de Dados foi criada como órgão da administração pública federal, integrante da Presidência da República, segundo o art. 55-A da lei. No entanto, o art. 55-B estabelece que "é assegurada autonomia técnica e decisória da ANPD". De qualquer modo, a lei também prevê que "a natureza jurídica da ANPD é transitória e poderá ser transformada pelo Poder Executivo em entidade administrativa pública indireta, submetida a regime autárquico especial e vinculada à Presidência da República". De acordo com representante do Google:

> "A Autoridade Nacional de Proteção de Dados terá um papel fundamental para guiar a interpretação da lei e unir os objetivos de inovação e supervisão regulatória eficaz, proporcionando transparência e confiança aos cidadãos" (VALENTE, 2019)

Por isso, independentemente da natureza da ANPD, o mais importante é que se garanta a independência técnica e funcional do órgão para cumprir com as suas tarefas, conforme previsto no art. 55-J da lei. Assim, tanto nos países da União Europeia quanto no Brasil, a proposta é que as autoridades nacionais ajam de forma estratégica, tendo como uma de suas bases a confiança e a cooperação com as organizações que eles supervisionam, e não somente a dissuasão (HIJMANS, 2018).

Vale mencionar, nesse sentido, que o que se tem verificado na União Europeia é que, diferentemente do que temiam as partes interessadas, as autoridades nacionais têm adotada uma abordagem equilibrada, focando mais no diálogo do que em sanções, em particular para os pequenos operadores que não processam dados pessoais como atividade central (UNIÃO EUROPEIA,

2019). Isso não significa que, quando necessário, elas deixem de usar seus novos poderes de forma efetiva, abrindo investigações e aplicando multas que podem variar alguns milhares de euros para muitos milhões, dependendo da gravidade da infração.

Por exemplo, na França, a autoridade de proteção de dados do país aplicou, em janeiro de 2019, uma multa de cinquenta milhões de euros ao Google, por acessar dados pessoais de usuários para fins de propaganda, após a denúncia de dois grupos de defesa de proteção de usuários – *None of Yours Business (NOYB)* e *La Quadrature du Net (LQDN)*- em nome de mais de dez mil indivíduos. A Comissão Nacional sobre Informática e Liberdade (CNIL) da França informou que o Google recebeu punição financeira em razão de falta de transparência, informação inadequada e falta de consentimento válido no tocante à propaganda personalizada. Em relação à falta de consentimento, a Comissão entendeu que o consentimento obtido pela empresa não era nem específico nem inequívoco, uma vez que era difícil para os usuários modificarem as preferências quanto a onde seus dados seriam usados, em particular no tocante a anúncios segmentados (EURONEWS, 2019).

No entanto, como está claro pelo próprio regulamento, o objetivo é que o sucesso da normativa não seja medido pelo número de multas aplicadas, mas pelas mudanças verificadas na cultura e no comportamento dos atores envolvidos (UNIÃO EUROPEIA, 2019a). Para Hodges, um engajamento construtivo e responsivo com as partes interessadas é a melhor forma de alterar de fato um comportamento futuro e deve ser a atitude chave a ser adotada pelas autoridades nacionais de proteção de dados (HODGES, 2018, p. 9). Por isso, as autoridades têm outras ferramentas a sua disposição para impor, por exemplo, na União Europeia, limitações temporárias ou definitivas no processamento, incluindo um banimento ou uma ordem de suspensão de fluxo de dados para um receptor em um terceiro país, conforme previsto no artigo 59(2)(f) e (j)(p. 5) do RGPD.

Como se sabe, a LGPD somente entrará em vigor, no país, em agosto de 2020 e a Autoridade Nacional de Proteção de Dados ainda está em processo de formação. Contudo, tendo em vista a similaridade da lei brasileira com o regulamento europeu, em particular no tocante aos mecanismos regulatórios à disposição, a partir da experiência que se verifica nos países europeus, pode-se ter uma ideia do papel que a ANPD deve ter no país e dos desafios que deve enfrentar para a implementação e aplicação da lei.

Assim, importante mencionar que o papel das autoridades nacionais de proteção de dados na Europa tem sido não apenas de garantir o *enforcement* da lei, mas também de conscientizar as empresas e a sociedade, em geral, da importância da proteção dos dados pessoais e dar suporte aos negócios na

economia digital, fornecendo soluções para o futuro. Nesse contexto, o que se já tem verificado é uma mudança de comportamento, que é um dos objetivos do RGPD, com empresas começando a desenvolver ofertas de novos serviços mais atentos à questão da privacidade (ou *privacy-friendly)*. Da mesma forma, há outras companhias que têm desenvolvido serviços baseados nos novos direitos assegurados aos indivíduos, como a portabilidade de seus dados pessoais, e um crescente número de empresas que têm promovido o respeito a dados pessoais como um fator de competitividade e um argumento de venda (UNIÃO EUROPEIA, 2019a).

Além disso, algumas autoridades de proteção de dados de países europeus têm criado novas ferramentas, como linhas de ajuda e *toolkits* para negócios, enquanto outras têm desenvolvido novas abordagens, como isolamento de processos (*sandboxes*) regulatórios para auxiliar companhias nos seus esforços de *compliance* (UNIÃO EUROPEIA, 2019a). Embora ainda haja reclamações por parte de algumas partes interessadas, em particular de pequenas e médias empresas, no tocante ao auxílio e às informações prestadas pelas autoridades nacionais, há investimentos, inclusive por parte da Comissão Europeia, para remediar essa situação. Ou seja, o papel das autoridades nacionais de proteção de dados na Europa para implementação e aplicação do regulamento vai muito além do *enforcement*, e é isso que se espera da Autoridade Nacional de Proteção de Dados brasileira quando estiver em pleno funcionamento.

ADOÇÃO ESTRATÉGICA DA ABORDAGEM RESPONSIVA NA LGPD E NO RGPD: APLICAÇÃO DOS MECANISMOS REGULATÓRIOS NA PIRÂMIDE DE CONSTRANGIMENTO

Após uma análise comparativa das regras previstas no Regulamento Geral de Proteção de Dados e na Lei Geral de Proteção de Dados Pessoais, pode-se observar claramente a opção dos legisladores por aspectos da abordagem responsiva na regulação da proteção de dados nos territórios brasileiro e europeu, com uma estratégia de maior *accountability* para as organizações, diminuindo, em parte, a responsabilidade do Estado na aplicação das normas. Em busca de maior nível de *compliance,* tanto na União Europeia quanto no Brasil, verifica-se a opção, assim, pela adoção de métodos de governança regulatória, cuja característica fundamental está na necessidade de que os próprios regulados exercitem, em maior grau, habilidades colaborativas e assumam responsabilidades por seus atos (ARANHA, 2019).

Seguindo essa lógica de governança regulatória, a teoria da regulação responsiva, ao adotar como uma de suas estratégias a autorregulação regulada,

parte do pressuposto de que as organizações têm maior capacidade de regular suas atividades do que o governo (ARANHA, 2019). No entanto, esta forma de autorregulação não é voluntária, havendo ainda a necessidade de certa intervenção estatal, mesmo que em menor grau. Dessa forma, como afirma o autor Márcio Iorio Aranha:

> "Uma teoria de regulação responsiva de persuasão e punição proporá modalidades regulatórias partindo do pressuposto de que os regulados agem segundo mecanismos de convencimento (persuasão) e punição integrados em um desenho institucional que os reforce e os nutra constantemente" (2019)

Na regulação responsiva, entende-se, portanto, que "a efetividade da regulação depende da criação de regras que incentivem o regulado a voluntariamente cumpri-lo" (ARANHA, 2019), em um ambiente de constante diálogo entre regulado e regulador, como se verifica tanto no RGPD quanto na LGPD, quando o legislador prevê a obrigação de *accountability* para as empresas que processam dados pessoais. Há, inclusive, argumentos, no tocante à implementação do RGPD, no sentido de que a adoção de medidas de proteção de dados, além de melhorar a imagem da empresa, garante maiores investimentos e vantagem competitiva no mercado.

No âmbito do RGPD, por exemplo, sob a perspectiva do princípio da *accountability*, previsto nos artigos 5(2) e 24, espera-se que as empresas implementem um amplo programa regendo todos os aspectos da coleta e uso de informações pessoais e que sejam capazes de verificar e comprovar a existência e a efetividade desses programas, seja internamente (para sua diretoria e gestores), seja externamente quando solicitada (para autoridades regulatórias, indivíduos ou parceiros comerciais). A adoção de um programa como esse, que inclua, por exemplo, a adoção de boas práticas operacionais mandatórias que cubram os elementos centrais de responsabilização (ex. avaliação de risco, registro dos processos, implementação de medidas de segurança, transparência, treinamentos etc.) é fundamental para garantir a observância ou conformidade das empresas com as obrigações previstas no regulamento (CIPL, 2019b). Além disso, como se verifica nos *Recitals* 98, 99 e 100 do RGPD, há incentivos também para que as empresas adotem medidas voluntárias, como a adoção de cláusulas contratuais padronizadas, códigos de conduta setoriais ou, até mesmo, mecanismos de certificação, como forma de alterar, assim, o próprio comportamento das empresas em relação à cultura de proteção de dados.

O objetivo das normativas brasileira e europeia, desse modo, é que adoção do princípio da *accountability* forneça não apenas as ferramentas necessárias para a proteção de dados pessoais, mas também atribua a responsabilidade de garantir essa proteção às organizações que fazem uso desses

dados (CIPL, 2019b). Vale lembrar que outro elemento próprio da autorregulação regulada da teoria responsiva está em se exigir da empresa que internalize custos de fiscalização por intermédio da criação de departamento ou grupo de conformidade interno à empresa com o objetivo de monitorar a observância das normas e recomendar ações disciplinares contra os infratores (ARANHA, 2019). Nesse sentido, de forma similar, tanto o RGPD quanto a LGPD dispõem sobre a necessidade de contratação, por parte das empresas, de um encarregado da proteção de dados (um *Data Protection Officer*), que deve cumprir com essa função de monitorar a observância das normas e fazer recomendações a empresa e a seus funcionários.

Como entende o CIPL, a previsão de *accountability* no RGPD não se trata de simples autorregulação, mas sim a operacionalização e a tradução de regras legais fundamentadas em princípios em políticas, procedimentos, controles e governança concretas para alcançar o *compliance*. A *accountability* não substitui exigências legais, mas se aplica em conjunto com elas. Como é comum que leis que incluem *accountability* sejam baseadas em princípios, isso possibilita a adaptação de tais princípios a setores da indústria específicos e a diferentes níveis de risco (CIPL, 2019b). A previsão de *accountability* minimiza o risco de *non-compliance* e prepara as organizações para serem responsivas e responderem quando incidentes com danos por violação de dados ocorram (CIPL, 2019b).

Embora incentivem um engajamento construtivo e responsivo das autoridades reguladoras com os entes regulados, como forma de garantir não apenas maior *compliance*, mas principalmente um mudança de comportamento futuro, tanto o RGPD quanto a LGPD também preveem como ferramenta de *enforcement* a possibilidade de aplicação de sanções duras por parte das autoridades, até para que se dê suporte ao seu engajamento construtivo. Isso porque, como afirma Hijmans, nem toda organização necessariamente investe em "fazer a coisa certa". Ou seja, segue-se a lógica da pirâmide de constrangimento da teoria da regulação responsiva, na qual há três tipos de atores da base ao topo da pirâmide, que se comportam de formas distintas e podem ser representados na pirâmide de perfis regulados, por três tipos: o virtuoso, o racional e o irracional (ARANHA, 2019).

No entanto, Hijmans destaca que essas sanções administrativas devem ter como alvo apenas aquelas atividades que não cumprem com a norma de forma deliberada, voluntariosa, seriamente negligente, repetitiva ou particularmente séria. Até porque, como ele ressalta, os poderes de *enforcement* devem ser exercitados apenas de vez em quando, se não perdem seu sentido (2018). Essa é a própria lógica da abordagem responsiva de regulação, que, conforme afirma Braithwaite, estabelece que a aplicação da lei somente deveria

ser responsiva ao quão efetivamente os cidadãos e as empresas estão se autorregulando, antes de decidir se deve escalar-se no nível de intervenção (2006). Adota-se, assim, diferentes estratégias e mecanismos regulatórios escaláveis, partindo de técnicas de persuasão e de punição, para garantir o maior cumprimento da lei pelo ente regulado. Neste caso, a previsão de mecanismos de autorregulação regulada não exclui a necessidade de prever-se também sanções administrativas, até porque elas não se excluem, mas, sim, se reforçam.

Como afirma o autor Márcio Iorio Aranha, ao citar Braithwaite e Ayres, a adoção de "uma abordagem regulatória de reação equivalente implica, por parte do regulador, o comportamento de se abster de aplicar sanções enquanto a empresa for cooperativa" (2019). Isso porque, em regra, essa postura tende a maximizar os resultados de conformidade à norma e minimizar os custos regulatórios, sendo benéfica tanto para o regulador quanto para o regulado, enquanto ambos adotarem posturas cooperativas. (ARANHA, 2019). Desse modo, a utilização de sanções se justificaria apenas quando o ente regulado, no caso as empresas que fazem o tratamento de dados, não cumpra, por exemplo, voluntariosamente ou negligentemente com a norma.

Além da abordagem responsiva, observa-se tanto no RGPD quanto na LGPD a opção por uma estratégia de governança nodal. Não necessariamente como forma alternativa aos constrangimentos estatais da pirâmide de constrangimento, como proposta na pirâmide de regulação em rede de John Braithwaite para os países em desenvolvimento, mas de forma complementar. Assim, as legislações europeia e brasileira utilizam-se da estratégia de governança nodal no sentido de que incentivam a participação efetiva de indivíduos e instituições variadas, principalmente do setor privado, que possuem um conjunto de tecnologias, conhecimentos e modos de pensar variados, para buscar contornar o déficit de capacidade regulatória de alguns dos países, desonerando a estrutura estatal do ônus de implementar todas as medidas de incentivo à conformidade normativa do regulado.

Isso se verifica na constituição, por exemplo, do grupo de múltiplas partes interessadas (*Multistakeholder Expert Group*), que auxilia a Comissão Europeia na identificação de possíveis desafios para implementação do RGPD, e na própria constituição do Conselho Nacional de Proteção de Dados e Privacidade, órgão consultivo da ANPD, com composição multissetorial e competência para propor diretrizes e estratégias, elaborar estudos e disseminar o conhecimento de proteção de dados no Brasil. Sem esquecer, também, o papel dos indivíduos que têm plena capacidade assegurada no regulamento não só para demandar seus direitos junto às empresas que fazem o tratamento dos dados, mas também para buscar ter seus direitos garantidos, por meio de reclamações junto às autoridades nacionais de proteção de dados.

Essa opção pela governança nodal é uma forma de onerar menos o Estado, partindo do pressuposto de que nenhum governo é capaz de garantir a aplicação de todas as leis, conforme entendimento dos teóricos da regulação responsiva (BRAITHWAITE, 2006). Assim, tanto na elaboração da LGPD quanto do RGPD, entendeu-se que a participação dos demais atores envolvidos no tema é fundamental para a aplicação efetiva das leis.

Aplicação dos Mecanismos Regulatórios do RGPD na Pirâmide de Constrangimento

Segundo o autor Marcio Iorio Aranha, "o caráter gradual de escalada na pirâmide de constrangimento se apresenta como outra marca identificadora da regulação responsiva" (2019). Por isso, pode-se afirmar que os legisladores europeus optaram por uma abordagem responsiva ao estabelecer as normas gerais de proteção de dados pessoais do bloco. Isso fica mais claro quando se analisa os mecanismos regulatórios previstos no regulamento, que preveem desde a adoção de boas práticas voluntárias pelos próprios entes regulados até a aplicação de multas milionárias e a suspensão do fluxo de dados.

No art. 57 do RGPD, estão previstas as atribuições das autoridades nacionais de proteção de dados, dentre as quais se inclui a de controlar e executar a aplicação do regulamento. Assim, cabe a essas autoridades aplicar as sanções previstas no art. 58, como:

> "a) Fazer advertências ao responsável pelo tratamento ou ao subcontratante no sentido de que as operações de tratamento previstas são suscetíveis de violar as disposições do presente regulamento;
>
> b) Fazer repreensões ao responsável pelo tratamento ou ao subcontratante sempre que as operações de tratamento tiverem violado as disposições do presente regulamento;
>
> c) Ordenar ao responsável pelo tratamento ou ao subcontratante que satisfaça os pedidos de exercício de direitos apresentados pelo titular dos dados nos termos do presente regulamento;
>
> d) Ordenar ao responsável pelo tratamento ou ao subcontratante que tome medidas para que as operações de tratamento cumpram as disposições do presente regulamento e, se necessário, de uma forma específica e dentro de um prazo determinado;
>
> e) Ordenar ao responsável pelo tratamento que comunique ao titular dos dados uma violação de dados pessoais;
>
> f) Impor uma limitação temporária ou definitiva ao tratamento de dados, ou mesmo a sua proibição;
>
> g) Ordenar a retificação ou o apagamento de dados pessoais ou a limitação do tratamento nos termos dos artigos 16, 17 e 18, bem

como a notificação dessas medidas aos destinatários a quem tenham sido divulgados os dados pessoais nos termos do artigo 17 (2), e do artigo 19;

h) Retirar a certificação ou ordenar ao organismo de certificação que retire uma certificação emitida nos termos dos artigos 42 e 43, ou ordenar ao organismo de certificação que não emita uma certificação se os requisitos de certificação não estiverem ou deixarem de estar cumpridos;

i) Impor uma multa nos termos do artigo 83, para além ou em vez das medidas referidas no presente número, consoante as circunstâncias de cada caso;

j) Ordenar a suspensão do envio de dados para destinatários em países terceiros ou para organizações internacionais

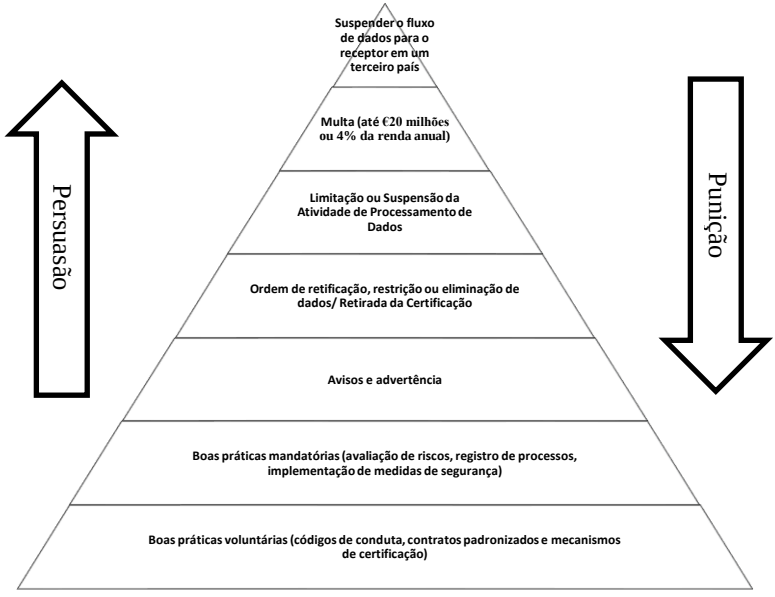

Figura 1 – Pirâmide de Constrangimento do RGPD da UE

Como se verifica, na base da pirâmide de constrangimento do RGPD, estão previstas as boas práticas voluntárias, como as que envolvem a adoção de códigos de conduta e de certificação (artigos 40 e 43), como estratégia de autorregulação regulada. Logo acima, encontram-se as boas práticas mandatórias, como avaliação de risco e registro dos processos (artigos 30 e 35). Apenas na terceira camada da pirâmide, iniciam-se as sanções previstas no artigo 57 do regulamento, partindo das menos "punitivas", como o aviso de

violação e advertência, escalando até a suspensão do fluxo de dados para o receptor de um país estrangeiro ou uma organização internacional.

Portanto, verifica-se que há uma gradação na aplicação das sanções, embora se possa discutir se a suspensão do fluxo de dados pode ser considerada mais punitiva do que uma multa, por exemplo, se a multa for no teto de vinte milhões de euros. De qualquer modo, o RGPD deixa claro que não se trata de mecanismos regulatórios excludentes. Por exemplo, no *recital* 150, que prevê a competência das autoridades nacionais de impor multas, de acordo com a natureza, a gravidade, a duração da violação e suas consequências, está expresso, também, que a imposição de uma multa ou o envio de um aviso não afeta o exercício de outros poderes das autoridades ou a aplicação de outras sanções previstas no regulamento.

No caso, o RGPD prevê apenas sanções administrativas, deixando a critério dos Estados-Membros a previsão de sanções penais pelo descumprimento de normas do regulamento. Vale lembrar, que "o conjunto de instrumentos persuasivos depende do setor regulado, da cultura de negócios, da tradição jurídica, enfim, de circunstâncias, cabendo ao regulador desenhar a pirâmide regulatória segundo as características do setor regulado" (ARANHA, 2019).

Aplicação dos Mecanismos Regulatórios da LGPD na Pirâmide de Constrangimento

Da mesma forma como se pode verificar no RGPD, a Lei Geral de Proteção de Dados Pessoais brasileira também adotou mecanismos regulatórios escalonáveis, que podem ser facilmente visualizados quando aplicados na pirâmide de constrangimento de Braithwaite e Ayres. Assim como no regulamento europeu, que serviu de base para a lei brasileira, observa-se que o legislador partiu dos mecanismos de persuasão, como a previsão de adoção voluntária de práticas de boa governança pelos entes regulados, para os de sanção, sendo a mais punitiva, a aplicação de multas que podem chegar a 50 milhões de reais.

Na LGPD, o artigo 52 trata das sanções administrativas a serem aplicadas pela Autoridade Nacional de Proteção de Dados, como:

> I - advertência, com indicação de prazo para adoção de medidas corretivas;
>
> II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;

III - multa diária, observado o limite total a que se refere o inciso II;

IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;

V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;

VI - eliminação dos dados pessoais a que se refere a infração; (…)

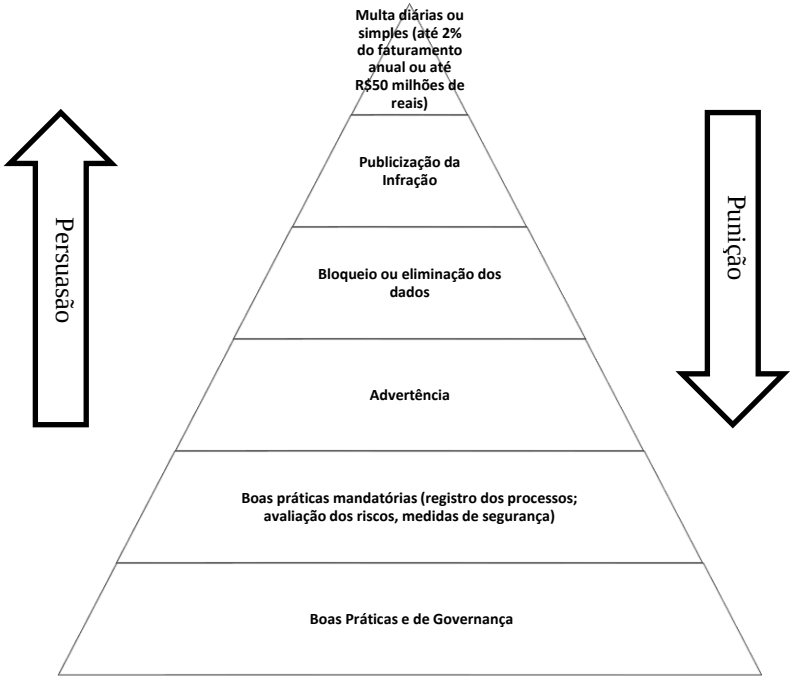

Figura 2 – Pirâmide de Constrangimento da LGPD do Brasil

Desse modo, assim como na pirâmide de constrangimento do RGPD, na da LGPD, na base, também estão as boas práticas de governança (artigo 50), que, em regra, podem ser adotadas de forma voluntária pelos controladores e operadores. Contudo, fica clara a opção do legislador por uma estratégia de autorregulação regulada novamente neste caso, em razão da obrigação desses atores de publicarem e atualizarem periodicamente as suas regras de boas

práticas e de governança, que poderão ser reconhecidas e divulgadas pela autoridade nacional (art. 50, § 3º).

Logo na camada acima da pirâmide, seguindo a lógica adotada pelo RGPD, estão as boas práticas mandatórias, como o registro dos processos, a necessidade de avaliação dos riscos e as medidas de segurança para proteger os dados pessoais (artigos 37, 38 e 46). Na parte mais acima da pirâmide, que trata das sanções, observa-se que a LGPD prevê menos opções de sanções administrativas a serem aplicadas pela ANPD, se comparada ao RGPD. No caso, como já foi mencionado anteriormente, na redação final da Lei n° 13.709, de 14 de agosto de 2018, após as mudanças introduzidas pela Lei n° 13.853, de 08 de julho de 2019, foram vetados três incisos que tratavam de sanções administrativas, sendo uma delas a possibilidade de suspensão da atividade de processamento de dados temporariamente (inciso XI), prevista no regulamento europeu. No entanto, a LGPD inova em relação ao RGPD e traz a possibilidade de publicização da infração, como uma forma de sanção.

Em relação aos mecanismos disponíveis, pode-se dizer que a Autoridade Nacional de Proteção de Dados brasileira tem "menos dentes" que as autoridades nacionais europeias, não apenas por contar com menos opções de sanções, mas também por ser a sua sanção mais "dura" a de aplicação de multa, cujo valor máximo de R$50 milhões por infração equivale praticamente apenas a metade do valor máximo que pode ser aplicado por suas contrapartes europeias, no caso €20 milhões.

Como afirma o autor Marcio Iorio Aranha:

> "Quanto mais distante for o topo da pirâmide da base, melhores serão os resultados de conformidade projetados pela atuação responsiva. Isso significa dizer que o arsenal de sanções disponíveis ao regulador deve ser o mais poderoso possível, gerando a imagem, no regulado, de que a agência reguladora é uma grande arma benigna" (2019).

Assim, embora as diferenças não sejam substantivas, o menor poder de *enforcement* da ANPD, em razão de menor arsenal de sanções e uma pirâmide "menos alta", pode ter influência na possibilidade de uma aplicação menos efetiva da lei de proteção dos dados no país, se comparada ao RGPD. No entanto, partindo do pressuposto que a teoria da regulação responsiva tem como um de suas bases também a ideia de vantagem comparativa das medidas conciliatórias, em relação às de comando e controle, para o alcance efetivo de metas regulatórias, poderia apostar-se também numa aplicação da lei no território brasileiro tão efetiva quanto se tem hoje na Europa, considerando que as medidas voluntárias são muito similares nas duas legislações. Tudo

dependerá, na realidade, de quão efetiva será a atuação da ANPD e de seu grau de independência e liberdade de atuação no seu funcionamento.

CONCLUSÃO

Com a aprovação da LGPD, em 2018, criou-se um marco legal para o uso de dados pessoais no Brasil, com o estabelecimento de regras claras e abrangentes, com ferramentas de controle e transparência, para garantir o uso adequado de dados pessoais no país. Com forte inspiração no Regulamento Geral de Proteção de Dados Europeu, os legisladores brasileiros adotaram estrategicamente, como verificado ao longo deste artigo, uma abordagem responsiva na elaboração da LGPD, prevendo não apenas a possibilidade de aplicação de sanções administrativas pela autoridade nacional, mas também mecanismos de *accountability*, como forma de compartilhar a responsabilidade e garantir maior compliance por parte dos entes regulados, sob uma perspectiva de governança em rede.

Nesse novo arcabouço legal, observa-se o papel fundamental que deve ter as autoridades nacionais, tanto no Brasil quanto nos países europeus, para aplicação e regulamentação das normas de proteção de dados. Embora a autoridade nacional brasileira tenha menos mecanismos de sanção, em outras palavras "menos dentes", se comparada às autoridades europeias, nota-se que a estratégia de "enforcement" adotada pelos legisladores é similar, com a previsão de mecanismos de persuasão e punição, que devem ser aplicadas de forma escalável e complementar.

Vale destacar, ainda, que embora o RGPD tenha servido de inspiração para a elaboração da lei brasileira e possa servir de base também para a implementação e aplicação do novo regime de proteção de dados no Brasil, sabe-se que o país deve lidar com suas particularidades e seus próprios desafios nesse processo. Até a entrada em vigor da lei, em agosto de 2020, espera-se que os indivíduos e as organizações, do setor público e privado, adaptem-se a uma nova cultura para a utilização e o tratamento de dados pessoais no Brasil, que deve ser um processo contínuo e conjunto desses atores e do Estado.

De qualquer modo, independentemente das diferenças e semelhanças entre os dois regimes, o que se sabe ao certo é que um sistema de proteção de dados exitoso demanda autoridades fiscalizatórias efetivas, trabalhando de maneira efetiva (HIJMANS, 2018), por isso a importância das autoridades nacionais. Para garantir essa efetividade, a expectativa é que a opção por uma abordagem responsiva da regulação, sob uma perspectiva de governança nodal, auxilie a Autoridade Nacional de Proteção de Dados na implementação e aplicação da lei no país.

REFERÊNCIAS BIBLIOGRÁFICAS

ARANHA, M. I. ***Manual de Direito Regulatório: Fundamentos do Direito Regulatório,*** 5a ed. rev. ampl, London: Laccademia Publishing, 2019.

ARANHA, M. I. Telecommunication Regulatory Design in Brazil: Networking around State Capacity Deficits. ***Economia Pubblica***, v. 25, n. 2, p. 83-105, 2016.

BENADY, D. **GDPR: Europe is taking the lead in data protection. Raconteur, 2018**. Disponível em: < https://bit.ly/33rbSBT>. Acesso em: 21/10/2019.

BRAITHWAITE, J. Responsive Regulation and Developing Economies. ***World Development,*** v. 34, n. 5, p. 884-898, 2006.

BURRIS, S; DRAHOS, P; SHEARING, C. Nodal Governance. ***Australian Journal of Legal Philosophy 30***, p. 30–58, 2005.

CAVALCANTI, N; SANTOS, L. Lei Geral de Proteção de Dados do Brasil na Era do Big Data. *In:* FERNANDES, R; CARVALHO, A. ***Tecnologia Jurídica & Direito Digital: II Congresso Internacional de Direito, Governo e Tecnologia – 2018***, Belo Horizonte: Fórum, 2018. p. 351 - 365.

CENTER FOR INFORMATION POLICY LEADERSHIP. ***Learning from the EU GDPR: What Elements Should the US Adopt?*** 2019. Disponível: em: <https://bit.ly/3hwehjR>. Acesso em: 1º/12/ 2019.

CENTER FOR INFORMATION POLICY LEADERSHIP. **CIPL Accountability Q&A.** 03 de julho de 2019. Disponível em: <https://bit.ly/2Rr38Gg>. Acesso em: 1º/12/2019)

CONSUMERS INTERNATIONAL, Coming Together for Change. **The State of Data Protection Rules around the World: a briefing for consumer organisations.** Disponível em: <https://bit.ly/3bZeOJV>. Acesso em: 02/12/2019.

EURONEWS. ***France fines Google €50 million using EU's transparency and consent law.*** Publicado: 21 de janeiro de 2019. Disponível em: <https://bit.ly/2RsocMx >. Acesso em: 1º/12/2019.

HIJMANS, H. How to enforce the GDPR in a strategic, consistent and ethical manner? A reaction to Christopher Hodges. ***European Data Protection Law Review,*** v. 4, n. 1, p. 80- 84, 2018.

HODGES, C. Delivering data protection: Trust and Ethical Culture. ***European Data Protection Law Review,*** v. 4, n. 1, p. 65- 79, 2018.

KOCH, R. ***What is the LGPD? Brazil's version of the GDPR.*** Disponível em: <https://bit.ly/2RptBUD>. Acesso em: 30/11/2019.

MARTIAL-BRAZ, N. O direito das pessoas interessadas no tratamento de dados pessoais: anotações da situação na França e na Europa. ***Revista de Direito, Estado e Telecomunicações***. v. 10, n. 1, p. 85-108, 2018.

ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO. ***OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data***, 2013.

ROCHFELD, J. Como qualificar os dados pessoais? Uma perspectiva teórica da União Europeia em face dos gigantes da Internet. ***Revista de Direito, Estado e Telecomunicações***, v. 10, n. 1, p. 61-84, 2018

UNIÃO EUROPEIA. Comissão Europeia. (2019a) ***Communication from the Commission to the European Parliament and the Council: Data Protection Rules as a trust-enabler in the EU and Beyond – taking stock. Brussels,*** 24.7.2019 COM(2019) 374 final. Disponível em: <https://bit.ly/2Rwwral>. Acesso em: 04/12/2019.

_____. Comissão Europeia. (2019b) ***EU Data Protection Rules***. Disponível em: <https://bit.ly/2RwwSkZ>. Acesso em: 01 de dezembro de 2019)

_____. Multistakeholder Expert Group to Support the Application of Regulation (EU) 2016/679. ***Contribution from the Multistakeholder Expert Group to the Stock Taking Exercise of June 2019 on the Year of GDPR Application.*** Relatório: 13 de junho de 2019. Disponível em: <https://bit.ly/33rQJaL>. Acesso em: 02/12/2019.

TEFFÉ, C. S. & VIOLA, M. ***Proposta para Criação da Autoridade Brasileira de Proteção de Dados.*** Disponível em: <https://bit.ly/2RsRGt>. Acesso em: 30/11/2019.

VALENTE, J. ***Lei de Proteção de Dados traz desafios a empresas, cidadãos e governo.*** AGÊNCIA BRASIL: Publicado em 25/08/2019. Disponível em: <https://bit.ly/3khXTFu>. Acesso em 1º/12/2019.

Normas de Julgados

UNIÃO EUROPEIA. **Regulação (EU) 2016/79 do Parlamento Europeu e do Conselho Europeu de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE** (Regulamento Geral sobre a Proteção de Dados).

BRASIL. **Lei n° 13.709, de 14 de agosto de 2018**. Publicado em: 15/08/2018. Edição: 157. Seção: 1. Página: 59.

_____. **Lei n° 13.853, de 08 de julho de 2019.** Publicado em: 09/07/2019. Edição: 130. Seção: 1. Página: 1.