ANÁLISE COMPARADA ENTRE REGULAMENTAÇÕES DE DADOS PESSOAIS NO BRASIL E NA UNIÃO EUROPEIA (LGPD E GDPR) E SEUS RESPECTIVOS INSTRUMENTOS DE *ENFORCEMENT*

Laila Neves Lorenzon[1]

Resumo

A evolução da Internet ao longo dos últimos anos trouxe grandes conquistas para a democratização da informação, novas formas de comércio e interações interpessoais. Paralelamente, trouxe consigo novos desafios no âmbito jurídico para garantir que o espaço virtual seja seguro e que as relações entre consumidores e fornecedores seja equilibrada e justa, com direitos e deveres devidamente estabelecidos por normas nacionais. Nesse sentido, o presente trabalho visa apresentar um panorama geral sobre a construção das atuais regulamentações de dados pessoais existentes na União Europeia e no Brasil, respectivamente o Regulamento Geral sobre Proteção de Dados (GDPR, em inglês) e a Lei Geral de Proteção de Dados (LGPD), ambos recentemente elaborados. O objetivo do trabalho é realizar uma análise sobre como essas normas tratam as relações entre os usuários da Internet e as empresas ou instituições que fornecem serviços, a utilização e o tratamento de dados pessoais e os direitos que os indivíduos detêm sobre eles, e principalmente identificar a forma como essas normas visam garantir a aplicação correta de suas diretrizes, também conhecidos como instrumentos de *enforcement*. Será feita uma análise comparativa entre os instrumentos de *enforcement* de cada lei, no objetivo de chegar a uma conclusão sobre qual dos dois regulamentos oferece instrumentos mais eficazes para garantir que todas as instituições envolvidas realizem o devido *compliance* com a lei, e também ressaltar a importância da existência de tais regulamentações no contexto atual para transformar o mundo online em um ambiente seguramente democrático.

Palavras-chave

Dados pessoais; LGPD; GDPR; Brasil; União Europeia; instrumentos de *enforcement*.

1 Graduanda do curso de Relações Internacionais da UFRJ (IRID-UFRJ), pesquisa pelo Laboratório Orti Oricellari de Economia Política Internacional integração regional na América Latina e pesquisa cibersegurança e proteção de dados no Projeto CyberBRICS no Centro de Tecnologia e Sociedade (CTS) FGV—Direto Rio.

Abstract

Over the past few years, the evolution of the internet has brought great achievements for the democratization of information, new forms of commerce, and interpersonal interactions. In parallel, it has also brought new challenges in the legal field to ensure that the virtual space is safe and that the relationships between consummers and suppliers are balanced and fair, with rights and duties duly established by national standards. In this sense, this work aims to present an overview of the construction of the current regulations on personal data existing in the European Union and Brazil, respectively the General Regulation on Data Protection (GDPR) and the Lei Geral de Proteção de Dados (LGPD), both recently developed. The objective of the work is to carry out an analysis on how these standards deal with the relationship between Internet users and companies or institutions that provide services, the use and treatment of personal data and the rights that individuals have over them, and mainly to identify how these standards aim to ensure the correct application of its guidelines, also known as enforcement instruments. A comparative analysis will be carried out between the enforcement instruments of each law, to reach a conclusion on which of the two regulations offers the most effective instruments to ensure that all institutions involved perform due compliance with the law, and also to emphasize the importance of the existence of such regulations in the current context to transform the online world into a safely democratic environment.

Keywords

Personal data; LGPD; GDPR; Brazil; European Union; enforcement instruments.

INTRODUÇÃO

Nas últimas décadas, a Internet passou por intensos aprimoramentos, que modificaram toda a forma de se relacionar com o outro, a relação do usuário com o mundo virtual e também a maneira como esses são vistos por empresas e novas tecnologias. Atualmente, milhões de dados são produzidos constantemente por cada indivíduo que acessa ou se utiliza de serviços na Internet, e eles foram gradualmente se transformando em uma nova moeda de troca muito valiosa para grandes conglomerados, colocando em risco a privacidade individual de cada usuário. À medida que a Internet evoluiu, também evoluiu o debate sobre direitos e deveres nesse novo mundo ainda não muito conhecido, e viu-se a necessidade de aprimorar regulamentações já existentes para garantir que não houvesse abuso por parte de fornecedores de serviços, na tentativa de tornar a relação entre estes e os usuários mais simétrica. Esse debate visa a possibilitar que indivíduos tenham maior controle sobre os próprios dados pessoais, compreendam melhor a importância que esses possuem no ambiente

With the support of the Erasmus+ Programme of the European Union

FGV RIO DE JANEIRO LAW SCHOOL Jean Monnet Centre of Excellence

virtual e o perigo que se apresenta com a ausência de regulamentações apropriadas para salvaguardar suas informações pessoais.

O debate sobre questões de privacidade no mundo virtual e o recolhimento de dados de usuários da Internet já se fazia presente no meio jurídico da União Europeia (UE) desde o século passado, mais precisamente em 1995, quando foi aprovada a Diretiva 95/46 CE[2] que unificou regras de proteção de dados entre todos os países participantes da União. Porém, desde então, presenciou-se um crescimento exponencial na complexidade do uso da Internet. Se no início do século XXI sua utilização era ainda pouco difundida ao redor do mundo, e era em certo nível experimental, em apenas poucos anos passou a conectar bilhões de pessoas ao redor do mundo de uma maneira nunca antes vista, e, para tanto, recolhendo quantidades extraordinárias de dados de seus usuários. Assim, para que houvesse uma regulamentação que melhor se adequasse aos novos desafios advindos com o avanço da Internet, foi proposta no ano de 2012 a Regulamentação Geral de Proteção de Dados na União Europeia (GDPR, em inglês), que levou quatro anos para ser elaborada e aprovada, constando em seu corpo de texto 99 capítulos.

Com o prazo de dois anos para que os setores público e privado — dos mais variados tipos de serviços desde farmácias a companhias aéreas — se adequassem a suas exigências, a GDPR marcou um ponto de inflexão no que diz respeito a regulamentações sobre o uso de dados pessoais por parte de qualquer empresa ou instituição, sendo a primeira a munir os usuários de uma ampla gama de direitos perante sua privacidade no mundo virtual e a cobrar atitudes mais responsáveis e seguras dos processadores de dados. Ao longo deste capítulo, será melhor explicitado o funcionamento da Lei bem como os direitos e deveres que ela institui.

Já no cenário brasileiro, o primeiro projeto de regulamentação envolvendo questões do mundo online surgiu em 2009 e ficou conhecido como Marco Civil da Internet,[3] que foi posteriormente transformado em lei em 2014. Apesar de não ter foco no assunto de dados pessoais, foi pioneiro na delimitação de direitos e deveres para os usuários e fornecedores de serviços na Internet, além de estabelecer diretrizes para a atuação do governo brasileiro perante o assunto. Alguns meses depois, no final de 2010, começaram a surgir propostas sobre a criação de uma regulamentação específica sobre atividades envolvendo o uso e armazenamento de dados pessoais. Em 2015, o Governo Federal realizou um debate público sobre o tema que contou com mais de 2.500 contribuições na-

2 WIPO. **Directive No. 95/46/EC of the European Parliament and of the Council**. Disponível em: https://wipolex.wipo.int/en/text/313007. Acesso em: 18 maio 2020.

3 CGI. **Lei do Marco Civil da Internet no Brasil**. Disponível em: https://www.cgi.br/lei-do-marco-civil-da-internet-no-brasil/. Acesso em: 18 maio 2020.

cionais e internacionais vindas de vários setores da sociedade, e que resultou na elaboração do primeiro Anteprojeto de Lei de Proteção dos Dados Pessoais.[4] Três anos depois, o anteprojeto virou o Projeto Lei da Câmara 53/2018,[5] e no dia 14 de agosto de 2018 foi sancionado como lei nº 13.709,[6] passando a ser a primeira lei federal a regular o uso de dados pessoais e criar novos conceitos jurídicos específicos sobre o tema. Nos próximos tópicos serão elencados os principais pontos da Lei Geral de Proteção de Dados, com atenção especial para seus instrumentos de *enforcement* e medidas sobre *compliance* com a lei.

Este artigo foi elaborado principalmente a partir de análises documentais das respectivas leis e artigos explicativos sobre o assunto, que proporcionam um conjunto detalhado de informações para identificar os principais instrumentos de *enforcement* de cada norma e melhor entender como esses são estruturados e aplicados em cada contexto. O foco concentra-se majoritariamente na forma como cada norma assegura que suas diretrizes serão cumpridas por todos os setores da sociedade; portanto, será feita apenas uma breve contextualização sobre a compreensão que cada legislação traz sobre a proteção de dados pessoais e principais obrigações que instituições possuem perante indivíduos portadores desses dados, para posteriormente analisar e comparar seus instrumentos de *enforcement*.

É importante ressaltar a relevância e atualidade do tema em questão devido a GDPR ser um modelo de referência mundial no assunto sobre privacidade digital, e sua regulamentação já ser efetiva em todo território da União Europeia, passível de punição caso não cumprida. Além disso, a aprovação da LGPD no Brasil ocorreu há menos de dois anos e a lei está vigente em suas disposições gerais desde setembro de 2020, o que a torna extremamente passível e urgente de ser estudada. No entanto, é importante ressaltar que as sanções administrativas ainda não estão em vigor, portanto a aplicação de muitas e outros tipos de sanções para aqueles que não estiverem em conformidade com a lei só poderão ser feitas a partir de agosto de 2021. Porém, os titulares que dados já possuem o direito e autonomia para questionarem empresas privadas e órgãos públicos sobre como é feito o tratamento de suas informações pessoais. Assim, a partir de uma análise comparada entre a lei brasileira e o marco regulatório europeu é possível aprender novas formas de aplicabilidade de leis

4 Ministério da Justiça e Segurança Pública. **Lei do Marco Civil da Internet no Brasil**. Disponível em: https://www.justica.gov.br/news/mj-apresenta-nova-versao-do-anteprojeto-de-lei-de-protecao-de-dados-pessoais. Acesso em: 18 maio 2020.

5 Senado. **Projeto Lei da Câmara 53/2018**. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=7761202&ts=1531939522588&disposition=inline&ts=1531939522588. Acesso em: 18 maio 2020.

6 Planalto. **Decreto nº Lei Nº 13.709, de 14 de agosto de 2018**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 18 maio 2020.

With the support of the Erasmus+ Programme of the European Union

FGV RIO DE JANEIRO LAW SCHOOL Jean Monnet Centre of Excellence

com temáticas digitais e melhor compreender a magnitude do papel de dados pessoais no mundo moderno.

1. O PANORAMA LEGAL EUROPEU

É evidente a influência da GDPR em diversas regulamentações nacionais sobre dados pessoais pelo fato de ter sido pioneira no assunto, e até o momento, o marco regulatório mais completo — em termos legais e estruturais — sobre questões de privacidade virtual. O consentimento expresso e inequívoco dos usuários é uma das bases legais principais do seu regimento, e deve ser claro, explícito e anterior à coleta e uso dos dados pessoais, podendo ainda ser revogado a qualquer tempo.[7]

Primeiramente, é imprescindível entender como a norma conceitua dados pessoais, que em seu Artigo 4° são definidos como "qualquer informação relacionada a uma pessoa física identificada ou identificável (titular dos dados),[8] e por qualquer informação entende-se literalmente qualquer informação que pode ser usada para identificar inequivocamente um sujeito direta ou indiretamente, podendo os dados serem físicos ou virtuais. Essa definição abrangente e expansionista tem como motivo a dinamização da legislação, ou seja, faz ela não se tornar obsoleta ou atrasada em meio às mudanças e evoluções constantes do ambiente virtual.

Um ponto que merece destaque é a aplicabilidade extraterritorial das diretrizes da lei, que cobre o tratamento de dados de indivíduos pertencentes à UE ou dados localizados na UE. Isso significa que, independentemente da origem do controlador ou processador (podendo esse ser de caráter público ou privado), se ele estiver realizando procedimentos ou fornecendo serviços nas condições supracitadas, eles devem realizar *compliance* com a GDPR. A definição de "processamento" é apresentada, também no Artigo 4º, como:

> qualquer operação ou conjunto de operações executadas com dados pessoais ou com conjuntos de dados pessoais, independentemente de serem automatizados, como coleta, registro, organização, estruturação, armazenamento, adaptação ou alteração, recuperação, consulta,

7 DE OLIVEIRA, Brenno Henrique; GUERRA, Carolinne Cardoso. O Impacto do Regulamento Geral de Proteção de Dados Pessoais da União Europeia no Brasil. In: **Governança e Direitos Fundamentais**: revisitando o debate entre o público e o privado. 1ª ed. Porto: Universidade de Santiago de Compostela, 2020, p.75-83.

8 Artigo 4º, inciso I do Regulamento (EU) 2016/679. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN. Acesso em: 12 janeiro 2021.

uso, divulgação por transmissão, disseminação ou disponibilização, alinhamento ou combinação, restrição, apagamento ou destruição;[9]

É importante ressaltar que a GDPR não fornece aos indivíduos (*titular dos dados*)[10] propriedade sobre seus dados, mas, sim, o controle sobre o que irá acontecer com eles — como serão armazenados, para que fim serão utilizados e com quem serão compartilhados. Nesse sentido, algumas das garantias da lei aos titulares são o direito de exigir que empresas deletem seus dados pessoais[11] (desde que não sejam necessários para fins científicos, históricos, de saúde pública e estatísticos); direito de acessar e transferir seus dados pessoais de um serviço para o outro sem deixar rastros; e direito à transparência total sobre qualquer operação realizada com seus dados.

Qualquer operação no processamento de dados que signifique uma mudança no teor dos termos de uso assinados e consentidos previamente pelos titulares de dados deve ser informada aos mesmos. Além disso, é obrigatório os responsáveis pelo tratamento de dados informarem, em até 72h, aos titulares e autoridades responsáveis se houver um vazamento de seus dados, sendo passível de multa caso essa obrigação não seja cumprida. Munidos de todos esses direitos, os titulares de dados estão aptos a garantir transparência e responsabilidade no uso de suas informações pelos provedores de serviços e conteúdos que contratam.

Um dos instrumentos de *enforcement* para garantir que esses direitos sejam exercidos, e consequentemente obrigações sejam cumpridas pela outra parte, é a obrigatoriedade da criação de um cargo[12] — tanto em empresas privadas quanto em órgãos públicos — chamado *Data Protection Officer* (DPO, Diretor de Proteção de Dados, em português). O DPO é o responsável por supervisionar as operações envolvendo dados pessoais e garantir que todas estejam em constante *compliance* com a regulamentação. Caso necessário, ele pode ser chamado para prestar esclarecimentos às autoridades reguladoras e/ou o público.

---

9 Artigo 4º, inciso II do Regulamento (EU) 2016/679, op. cit.

10 Ibidem.

11 Também conhecido como "direito ao esquecimento".

12 "No caso da lei europeia, a nomeação de um DPO é obrigatória caso: 1) o processamento for efetuado por uma autoridade pública, 2) as "atividades essenciais" de um controlador/processador de dados requererem o "monitoramento regular e sistemático de dados em grande escala" ou 3) quando as atividades centrais da organização consistirem no processamento em grande escala de categorias especiais de dados, como dados sensíveis (que incluem informações pessoais sobre saúde, religião, raça ou orientação sexual) e/ou dados pessoais relacionados à condenações e delitos penais." A importância da fiscalização da Lei de Proteção de Dados Pessoais. **REAMP**. Disponível em: https://www.reamp.com.br/blog/2018/09/a-importancia-da-fiscalizacao-da-lei-de-protecao-de-dados-pessoais/. Acesso em: 27 maio 2020.

With the support of the Erasmus+ Programme of the European Union

FGV RIO DE JANEIRO LAW SCHOOL Jean Monnet Centre of Excellence

Além do estabelecimento de um DPO, a norma europeia delegou a função mais significativa no que diz respeito ao *enforcement* da lei — de aconselhar, fiscalizar e aplicar multas caso necessário — às *Data Protection Authorities* (DPA, Autoridade de Proteção de Dados, em português) específicas de cada Estado membro. Assim, cada país integrante da UE é responsável por selecionar o conselho que formará autoridade reguladora e também indicar os poderes garantidos à mesma, ou seja, as responsabilidades específicas de cada DPA dependem das leis nacionais de cada país-membro.[13]

Porém, o direito de aplicar multas é garantido a todas as DPAs pelo Artigo 83 da norma, bem como o valor das mesmas, que dependem da gravidade da violação cometida. Para violações severas (listadas nos arts. 83-5), a multa pode chegar ao valor de 20 milhões de euros, ou, no caso de uma empresa, até 4% do faturamento total global do ano fiscal anterior, o que tiver maior valor. Mesmo para violações menos severas (listadas nos arts. 83-4) a multa pode chegar a 10 milhões de euros ou 2% do faturamento nos mesmos termos anteriores.[14] É importante ressaltar que as multas são aplicadas juntamente a outros recursos corretivos como a imposição de uma limitação temporária ou definitiva no processamento de dados e também a obrigação de ajustar o seu processamento à GDPR.

Para que haja uma aplicação consistente da GDPR em toda a União Europeia, foi criado o *European Data Protection Board* (EDPB, Conselho Europeu para a Proteção de Dados em português), um organismo independente cujo objetivo é promover a cooperação e o intercâmbio eficaz de informações entre as DPAs de cada país-membro. Ele é composto por representantes das DPAs e pelo *European Data Protection Supervisor* (EDPS, Autoridade Europeia para a Proteção de Dados em português).[15] Uma de suas principais funções é emitir diretrizes sobre a interpretação dos conceitos centrais da GDPR e "governar por decisões vinculativas sobre disputas relacionadas ao processamento transfronteiriço, garantindo uma aplicação uniforme das regras na UE para evitar que o mesmo caso possa ser tratado diferentemente em várias jurisdições".[16]

A norma europeia também conta com a participação pública no combate contra processamento de dados indevidos, e em seu Artigo 77 garante aos

13 INCE. **Enforcement of the GDPR**. Disponível em: https://www.incegd.com/en/knowledge-bank/enforcement-of-the-gdpr. Acesso em: 27 maio 2020.

14 GDPR-INFO. **Fines/ Penalties**. Disponível em: https://gdpr-info.eu/issues/fines-penalties/. Acesso em: 27 maio 2020.

15 EDPB. **About EDPB**. Disponível em: https://edpb.europa.eu/about-edpb/about-edpb_en. Acesso em: 27 maio 2020.

16 European Comission. **What is the European Data Protection Board (EDPB)?** Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/enforcement-and-sanctions/enforcement/what-european-data-protection-board-edpb_en. Acesso em: 27 maio 2020.

titulares o direito de apresentar uma reclamação junto a uma autoridade supervisora (normalmente DPA) caso percebam que o processamento de seus dados pessoais não segue os princípios da GDPR. Também estão autorizados, pelo Artigo 79, a um recurso judicial efetivo se acreditarem que seus dados foram violados.

Desse modo, ao emitir diretrizes e relatórios públicos sobre a interpretação da norma europeia, a EDPB colabora para a educação e conscientização da população sobre a relevância da proteção de dados pessoais. Esse ponto, aliado ao direito concedido aos cidadãos europeus pelo Artigo 77 da norma, garante uma participação ativa da sociedade civil na defesa de direitos sobre dados pessoais e privacidade online.

No que diz respeito à supervisão interna da própria União Europeia em relação ao *compliance* com a GDPR, são realizadas fiscalizações anuais de instituições governamentais que integram o corpo organizacional da UE, que são escolhidas depois da análise de diversos fatores como "resultados de nossa [EDPS] análise de risco, se categorias especiais de dados são processadas, o tempo decorrido desde a última inspeção e se houve um aumento no número de reclamações".[17] Os relatórios das inspeções já realizadas e seus métodos de análise não são divulgados ao público, mas seus resumos periódicos podem ser encontrados no boletim informativo e relatório anual, disponíveis no site oficial da UE.

Por fim, é crucial ressaltar que a GDPR impõe parâmetros para países que desejarem manter relações comerciais com a União Europeia, ou seja, para dar continuidade a negócios (que em sua maioria envolvem o processamento de dados, nem que seja apenas de funcionários das empresas) é necessário que o país em questão possua uma regulamentação completa e abrangente sobre proteção de dados e uma autoridade reguladora para garantir a eficácia da regulação. Isso é de certa forma um instrumento de *enforcement* com viés internacional, visto que a GDPR conta com o peso da União Europeia no comércio internacional para instituir a obrigação ao resto do mundo de dar a devida atenção ao direito de privacidade e transparência no tratamento de dados pessoais.

2. O PANORAMA LEGAL BRASILEIRO

A Lei Geral de Proteção de Dados brasileira é um marco na legislação nacional por ter formulado diversos conceitos jurídicos novos como "dados pessoais", "dados pessoais sensíveis", "anonimização de dados", "tratamento de dados", entre outros, para tratar do recolhimento, compartilhamento e uso

17 EDPS. **Inspections**. Disponível em: https://edps.europa.eu/data-protection/our-work/our-work-by-type/inspections_en. Acesso em: 27 maio 2020.

With the support of the Erasmus+ Programme of the European Union

FGV RIO DE JANEIRO LAW SCHOOL Jean Monnet Centre of Excellence

de informações pessoais de indivíduos. Por ter sido fortemente inspirada pela GDPR, ambas possuem conceitos e diretrizes parecidas. Também é importante ressaltar que

> a LGPD corresponde a um regulamento geral para proteção de dados pessoais, independentemente destes passarem por fluxos da Internet ou não. Assim, quaisquer estabelecimentos que coletem dados pessoais — como farmácias, locadoras de carro, postos de gasolina — estão submetidos às disposições legais.[18]

Portanto, é necessário frisar a ideia de que dados pessoais podem ser tanto dados eletrônicos quanto físicos, e mesmo que exista maior número de tratamento desses dados na Internet, esse termo significa qualquer informação pessoal que pode ser usada para identificar inequivocamente um indivíduo. Em seu Artigo 5º, a LGPD conceitua novos termos jurídicos, citados anteriormente, com atenção especial para o primeiro inciso do artigo que diz que dado pessoal é "informação relacionada a pessoa natural identificada ou identificável".[19] É importante ressaltar o caráter expansionista dessa definição: isso significa que dados que inicialmente não identificam uma pessoa (como endereço IP, faixa etária, nacionalidade etc.), ao serem conjugados ou enriquecidos, se puderem identificar uma pessoa, serão considerados dados pessoais.[20]

Sobre os dados, a lei assegura aos usuários alguns direitos primordiais como: solicitar exclusão permanente de seus dados, a garantia de que eles serão coletados para um fim específico e saber quais dados as empresas detêm sobre eles. No que concerne sua abrangência, a lei brasileira se aplica para o tratamento de dados feito por empresas ou instituições situadas em território brasileiro e/ou quaisquer dados referentes a cidadãos brasileiros, desse modo, empresas estrangeiras que realizam o tratamento de dados de brasileiros também devem se adequar à Lei.

Um ponto crucial da LGDP é o entendimento de que a privacidade está ligada ao consentimento dado pelo indivíduo, portanto, ele deve ser sempre requisitado pelos fornecedores de serviços de maneira expressa e clara, para que o portador dos dados tenha total controle da maneira como suas infor-

18 CAVALCANTE, Pedro Peres. **Privacidade e proteção de dados pessoais:** Uma análise comparativa dos quadros regulatórios brasileiro e europeu. Trabalho de Conclusão de Curso (Graduação em Direito) - Universidade Federal de Pernambuco — UFPE- Recife, 2018, p. 36.

19 Artigo 5°, inciso I, do Decreto n° 13.709, 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709compilado.htm. Acesso em: 12 janeiro 2021.

20 Lei Geral de Proteção de Dados e seus impactos no ordenamento jurídico. **COTS.** Disponível em: https://www.cots.adv.br/artigo/lei-geral-de-protecao-de-dados-e-seus-impactos-no-ordenamento-juridico. Acesso em: 27 maio 2020.

mações serão usadas nos serviços, e, assim, haja maior equilíbrio entre a relação fornecedor-consumidor. Desse modo, é necessário que os envolvidos no tratamento de dados cumpram certas obrigações — e aqui entende-se tratamento de dados como "toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração".[21] Pode-se dizer que a finalidade é a pedra fundamental no tratamento de dados, aliado ao requerimento claro e expresso do consentimento para o uso de dados do indivíduo.

Além disso, empresas ou instituições que tratam dados pessoais devem ser sempre transparentes a respeito do uso que fazem desses dados e garantir a segurança de todos aqueles que são armazenados e tratados. Na seção II do Capítulo VI da lei é instituído que as empresas tenham um encarregado pelo tratamento de dados pessoais cuja principal função é prestar esclarecimentos para as autoridades do governo e adotar providências a respeito da adequação dos processos institucionais e garantir o cumprimento com a LGPD. Resumidamente, o encarregado pode ser visto como um instrumento de *enforcement* da lei, visto que ele é o intermediário entre os titulares de dados, as empresas e a agência fiscalizadora do governo, a Autoridade Nacional de Proteção de Dados (ANPD).

O encarregado pelo tratamento de dados, que também pode ser chamado de Encarregado de Proteção de Dados,[22] desempenha uma função essencial para garantir transparência no cumprimento da lei, porém o ator supremo no quesito fiscalização é a ANPD. Sua proposta é "orientar, orientar e orientar, preventivamente. Após isso, fiscalizar, advertir e, somente após tudo isso, penalizar, se a LGPD continuar sendo descumprida".[23] Assim, percebe-se que o critério adotado para garantir *compliance* com a lei é baseado na abordagem educativa, apostando na prevenção em detrimento da punição.

Em sua estrutura, a ANPD (que ainda está em processo de formação e não foi oficialmente estabelecida) será composta por 23 titulares, não remunerados, com mandato de dois anos, e de diferentes setores: seis do Executivo Federal; um do Senado Federal; um da Câmara dos Deputados; um do Conselho Nacional de Justiça; um do Conselho Nacional do Ministério Público; um do Comitê Gestor da Internet no Brasil; quatro da sociedade civil com atuação

21 Artigo 5º, inciso X, do Decreto nº Lei 13.709, 14 de agosto 2018, op. cit.

22 Vê-se o paralelo da criação desse cargo com a existência do Data Protection Officer previsto pela GDPR.

23 SERPRO. **Quem vai regular a LGPD?** Disponível em: https://www.serpro.gov.br/lgpd/governo/quem-vai-regular-e-fiscalizar-lgpd. Acesso em: 27 maio 2020.

With the support of the Erasmus+ Programme of the European Union

FGV RIO DE JANEIRO LAW SCHOOL Jean Monnet Centre of Excellence

comprovada em proteção de dados pessoais; quatro de instituição científica, tecnológica e de inovação; e quatro de entidade do setor empresarial ligado à área de tratamento de dados pessoais.[24] Apesar de ainda não ter sido criada, o Artigo 55 da LGPD define a agência reguladora como órgão integrante da Presidência da República e lhe garante autonomia técnica, bem como especifica suas funções, sendo as principais (elencadas visando ao objetivo da elaboração deste trabalho):

> III — elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade;
> IV — fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso;
> XI — solicitar, a qualquer momento, às entidades do poder público que realizem operações de tratamento de dados pessoais informe específico sobre o âmbito, a natureza dos dados e os demais detalhes do tratamento realizado, com a possibilidade de emitir parecer técnico complementar para garantir o cumprimento desta Lei;
> XVI — realizar auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização de que trata o inciso IV e com a devida observância do disposto no inciso II do *caput* deste artigo, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluído o poder público;
> XXIII — articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação;[25]

Portanto, tem-se como principal instrumento de *enforcement* da LGPD a instituição da agência reguladora, ANPD, que é a autoridade suprema na fiscalização do cumprimento da lei e aplicação de sanções caso não o haja. No que se refere às sanções administrativas, podem ser 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 — ou multa diária, observado o limite total a que se refere o inciso II.[26] Além de multas,

24 Ibidem.
25 Artigo 55-J, incisos III, IV, VI, XVI, XXIII, do Decreto nº Lei 13.709 de agosto de 2018, op. cit.
26 Artigo 52º, incisos II, III, do Decreto nº Lei 13.709 de agosto de 2018, op. cit.

o Artigo 52 estabelece outras formas de penalidade para aqueles que não garantirem *compliance* com a lei:

> I — advertência, com indicação de prazo para adoção de medidas corretivas;
> 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;
> 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.[27]

3. CONCLUSÃO

Diante de todo o exposto, é possível perceber grandes similaridades entre ambas as normas, como a obrigação de provedores de serviço e conteúdo terem um Encarregado de Proteção de Dados, o estabelecimento de uma agência reguladora nacional, e os detalhamentos das multas, o que é compreensível visto que a GDPR serviu de inspiração para a elaboração da LGPD. No entanto, é possível afirmar que a norma europeia atualmente tem um conjunto de instrumentos de *enforcement* mais completo do que a lei brasileira, exclusivamente pelo fato crucial da norma ter nascido com uma agência regulatória já estabelecida e ela já estar em vigor, e tendo aplicado multas e sanções, como será mostrado adiante.

A ANPD tem suas principais obrigações e funções descritas na LGPD, porém desde que foi sancionada em 2018 até hoje, a agência não foi criada de fato pois nenhum de seus cargos foi preenchido, e com a ausência de uma agência reguladora é impossível haver uma fiscalização com o cumprimento da lei. Além disso, a sua não criação causa grande insegurança jurídica, o que desmotiva a maior parte de empresas e estabelecimentos a iniciar processos

27 Artigo 52°., incisos I, IV, V, VI, X, XI, XII, do Decreto n° Lei n° 13.709 de agosto de 2018, op. cit.

With the support of the Erasmus+ Programme of the European Union
FGV RIO DE JANEIRO LAW SCHOOL Jean Monnet Centre of Excellence

administrativos internos para se adequarem à lei, como mostrado na pesquisa feita pela ICTS Protiviti, na qual 84% das empresas[1] continuam despreparadas. Sem a ANPD não é possível orientar, fiscalizar nem multar aqueles que descumprem as diretrizes da lei, e isso aliado ao adiamento da vigência das sanções administrativas (para o ano 2021)[2] em um momento tão delicado quanto o que está sendo vivido devido à pandemia causada pela Covid-19, só colabora para criar um ambiente instável e descredibilizar a seriedade e a importância da proteção de dados dos cidadãos.

Outro ponto que merece atenção é o caráter independente das agências reguladoras europeias em comparação com a ANPD, que é um órgão vinculado à Presidência da República, contando com o apoio administrativo e técnico da Casa Civil. Essa questão é crucial, pois pode acarretar na diminuição do poder de supervisionamento da ANPD, na medida pode colocar entraves à sua fiscalização perante órgãos do governo brasileiro. A existência subordinada da Agência Nacional à administração pública pode causar obstáculos na garantia do cumprimento da LGPD por todos os setores da sociedade. Portanto, vê-se que as DPAs europeias possuem maior autonomia para colocar em prática suas diretrizes e proteger os direitos de indivíduos e, assim, garantir uma aplicação rápida e segura da lei.

Também é importante ressaltar a excelente estruturação da regulamentação europeia no que diz respeito ao diálogo entre as diversas agências reguladoras dos países-membros, vide a existência da EDPB, que permite uma rica troca de informações sobre o andamento da aplicação da lei ao redor da União, o que pode ser muito benéfico para estimular novas formas de garantir *compliance* com a lei e fiscalizar empresas, uma vez que a troca de informações e práticas legais são sempre bem-vindas. Não há, porém, como compará-la com a ANPD brasileira, visto que no Brasil existe apenas uma única agência reguladora, e não várias como no caso da União Europeia.

Depois de dois anos em vigor, é possível observar como a GDPR está sendo bem sucedida na luta pelo direito à privacidade e proteção de dados e também na conscientização da sociedade civil sobre a importância desse assunto, visto que metade do total de 280 mil notificações (no primeiro ano de vigência da lei) corresponde a reclamações de indivíduos que encontraram problemas acessando seus dados ou estavam preocupados sobre divulgações e proces-

1 E-Commerce Brasil. **LGPD: mesmo com adiamento, 84% das empresas continuam despreparadas.** Disponível em: https://www.ecommercebrasil.com.br/noticias/lgpd-adiada-empresas-continuam-despreparadas-pesquisa/. Acesso em: 27 maio 2020.

2 DEMARTINI, Felipe. Senado aprova adiamento da LGPD para agosto de 2021. **Canal Tech.** Disponível em: https://canaltech.com.br/legislacao/senado-aprova-adiamento-da-lgpd-para-agosto-de-2021-162863/. Acesso em: 27 maio 2020.

samento não autorizado dos mesmos.[3] Ademais, o valor de multas aplicadas a empresas que não estão em conformidade com a lei já soma 114 milhões de euros.[4]. A maior de todas até o momento foi a multa de 50 milhões de euros aplicada pela agência reguladora francesa à Google pelo fato da multinacional não deixar claro aos usuários de seu serviço quais dados são coletados e de que forma eles utilizam.[5]

Portanto, conclui-se diante de todos os fatos expostos, que, apesar da grande similaridade de riqueza teórica e maturidade civil entre as duas normas regulatórias, a GDPR garante maior autonomia às suas agências reguladoras e, assim, permite que haja uma fiscalização mais efetiva e, consequentemente, a aplicação mais sólida da lei. Também foi possível observar o sucesso da aplicação da GDPR e seus instrumentos de *enforcement*, que não se resumem apenas na aplicação de sanções e multas, mas também contam com a orientação para empresas e instituições sobre a interpretação da lei. Dessa maneira, a GDPR contribui de forma positiva para a educação da população sobre a importância de proteger seus dados pessoais e reforça o entendimento de que usuários possuem uma gama de direitos perante os serviços e aplicações que utilizam, e devem reivindicá-los.

3 VENTURA, Ivan. **Um ano de GDPR: estudo mostra o impacto da proteção de dados na Europa**. Disponível em: https://www.consumidormoderno.com.br/2019/05/27/estudo-impacto-protecao-dados-europa/. Acesso em: 27 maio 2020

4 LGPD Brasil. **GDPR já atingiu US$ 126 milhões em multas por privacidade de informações.** Disponível em: https://www.lgpdbrasil.com.br/gdpr-ja-atingiu-us-126-milhoes-em-multas-por-privacidade-de-informacoes/. Acesso em: 27 maio 2020.

5 CONJUR. **França multa Google em US$ 57 milhões por falta de proteção de dados de usuários**. Disponível em: https://www.conjur.com.br/2019-jan-21/franca-multa-google-us-57-milhoes-falta-protecao-dados. Acesso em: 27 maio 2020.

With the support of the Erasmus+ Programme of the European Union

FGV RIO DE JANEIRO LAW SCHOOL Jean Monnet Centre of Excellence