Insper

LL.M – Direito do Mercado Financeiro e de capitais

Eduardo Avila Alves de Souza

O impacto da Lei Geral de Proteção de Dados (LGPD) para os gestores de fundos de investimento

São Paulo

2021

Eduardo Avila Alves de Souza

O impacto da Lei Geral de Proteção de Dados (LGPD) para os gestores de fundos de investimento

Trabalho de Conclusão de Curso apresentado ao programa LL.M em Direito dos Mercados Financeiro e de Capitais do Instituto de Ensino e Pesquisa (Insper) como requisito parcial para a obtenção do título de pós-graduado em Direito dos Mercados Financeiro e de Capitais.

Orientadora: Profa. Pamela Gabrielle Romeu Gomes Roque.

São Paulo

2021

Souza, Eduardo Avila Alves de.
O impacto da Lei Geral de Proteção de Dados (LGPD) para os gestores de fundos de investimento.
Eduardo Avila Alves de Souza – São Paulo, 2021.

48f.

Trabalho de Conclusão de Curso – Insper, 2021. Orientadora: Pamela Gabrielle Romeu Gomes Roque.

1. LGPD; 2. Lei Geral de Proteção de Dados Pessoais; 3. Lei 13.709 4. Lei 13.853; 5. Administração de carteira de valores mobiliários; e 6. Gestores de Fundos de Investimento;

Eduardo Avila Alves de Souza

O impacto da Lei Geral de Proteção de Dados (LGPD)
para os gestores de fundos de investimento

Trabalho de Conclusão de Curso apresentado ao programa LL.M em Direito dos Mercados Financeiro e de Capitais do Instituto de Ensino e Pesquisa (Insper) como requisito parcial para a obtenção do título de pós-graduado em Direito dos Mercados Financeiro e de Capitais.

Orientadora: Profa. Pamela Gabrielle Romeu Gomes Roque.

Aprovado em: _____/_____/_____.

Banca Examinadora

_____

Profa. Pamela Gabrielle Romeu Gomes Roque (Orientadora)

_____

_____

Dedico esse trabalho à Artesanal Investimentos e seus sócios,
cuja empreitada não seria possível sem o apoio e o patrocínio fornecidos.

À colega de trabalho Fernanda Murbach Couto,
por abraçar essa iniciativa, apoiando os estudos
e colocando em prática as adequações impostas pela LGPD.

Aos colegas do curso, em especial à Luana Forte Dias,
cujo espírito colaborativo fez toda a diferença.

Por fim, agradeço aos docentes do Insper
especialmente à minha orientadora,
professora Pamela, pela dedicação.

RESUMO

Este artigo científico apresenta como tema central o impacto da Lei n. 13.709, de 14 de agosto de 2018, intitulada Lei Geral de Proteção de Dados ("LGPD") para os gestores de fundos de investimentos e uma proposta de adequação de seus negócios para atender aos novos requisitos legais. A nova legislação gera, por si, grande impacto em todas as instituições, públicas ou privadas, por tratar da proteção de dados pessoais dos indivíduos em qualquer relação que envolva informações classificadas como dados pessoais, por qualquer meio, seja pessoa natural ou jurídica. As consequências de sanções aplicadas por transgressões julgadas variam de multa de 2% do faturamento até R$ 50 milhões por infração, além da possibilidade de um possível reclamante ajuizar ação judicial envolvendo o tema. Além do impacto econômico, há o risco reputacional de uma condenação que, como consequência, poderia inabilitar a empresa condenada nos processos de compras e de fornecimento de serviços de empresas que consideram os malfeitos como critério de exclusão em suas políticas de contratação e parcerias.

Neste contexto, o estudo irá avaliar o impacto direto da lei na atividade de administração de carteira de valores mobiliários, exercida por agentes previamente autorizados pela Comissão de Valores Mobiliários (CVM), conforme as normas estabelecidas pela Instrução CVM n. 558, de 26 de março de 2015. O trabalho de pesquisa e aprofundamento teórico foi realizado a partir da interpretação da lei, apoiado em bibliografias preexistentes sobre a LGPD. Trata-se de um estudo qualitativo, que fez usa da revisão bibliográfica para atender aos seus propósitos. Todo o trabalho de pesquisa, apresentação dos conceitos e historicismo tem o objetivo de identificar os novos requisitos e princípios que devem nortear as atividades e os processos de negócios que lidam direta ou indiretamente com dados pessoais de pessoas físicas e apresentar soluções alternativas para resolver eventuais não conformidades para com a lei a partir do ponto de vista dos Gestores de Fundos de Investimentos. Por fim, verificaremos como conclusão, que a lei impõe mudanças culturais aos agentes que deverá nortear a atividade de tratamento de dados pessoais com base nos princípios da transparência e do respeito à vontade dos titulares.

Palavras-chave: LGPD; Lei Geral de Proteção de Dados Pessoais; Lei n. 13.709; Lei n. 13.853; Administração de carteira de valores mobiliários; Gestores de Fundos de Investimento.

ABSTRACT

This academic article presents as a central theme the impact of LGPD for investment fund managers and a proposal for adequacy.

Law No. 13.709, of August 14, 2018, the General Data Protection Law (“LGPD”) generates, by itself, a great impact on all institutions, whether public or private, as it deals with the protection of personal data of individuals in any relationship involving information classified as personal data, by any means, whether by a natural person or a legal entity. The consequences of sanctions applied for transgressions range from a fine of 2% of billing to BRL $50,000,000.00 for an infraction, without considering the possibility of a possible claimant filing a lawsuit against. In addition to the economic impact, we also have the reputational risk of a conviction that, moreover, it could disable the convicted company in the processes of purchasing and providing services from companies that consider wrongdoing as an exclusion criterion in their hiring and partnership policies.

In this context, we will assess the direct impact of the law on securities portfolio management activity, performed by agents previously authorized by the Securities and Exchange Commission (CVM), in accordance with the rules established in CVM Instruction No. 558 of March 26, 2015. The research work and theoretical analysis was carried out based on the interpretation of the law, supported by preexisting bibliographies on the LGPD. This is a qualitative study, which used a literature review to meet its purposes. All research work, presentation of concepts and historicism aims to identify the new requirements and principles that should guide the activities and business processes that deal directly or indirectly with personal data of individuals and present alternative solutions to solve any compliance failures compliance with the law from the point of view of Investment Fund Managers. Finally, we will verify as a conclusion that the law imposes cultural changes on agents that should guide the activity of processing personal data based on the principles of transparency and respect for the will of the holders.

Keywords: LGPD; Brazilian General Data Protection Law; Brazilian General Data Protection Regulation; Brazilian Data Privacy; Brazilian Law 13.709; Brazilian Law 13.853; Brazilian Capital Markets; Funds Administration.

SUMÁRIO

1	INTRODUÇÃO	09
2	PANORAMA GERAL E A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)	11
2.1	Disposições preliminares	12
2.2	Tratamento de dados pessoais	13
2.3	Do consentimento como base legal	14
2.4	Legítimo interesse	15
2.5	Tratamento de dados pessoais sensíveis	16
2.6	Tratamento de dados pessoais de crianças e adolescentes	16
2.7	Direitos dos titulares	17
2.8	Agentes de tratamento de dados pessoais	18
2.9	Segurança e boas práticas	19
3	GESTORES DE FUNDOS DE INVESTIMENTOS E MODELOS ORGANIZACIONAIS	22
3.1	Departamento pessoal e/ou recursos humanos (RH)	23
3.2	Departamento comercial, cadastro e identificação de investidores dos fundos de investimentos sob distribuição própria	24
3.3	Departamento jurídico	24
3.4	Departamento de tecnologia da informação (TI) e *cybersegurança*	25
3.5	Departamento de processamento de dados e inteligência de negócio	25
3.6	Departamento de *compliance* e/ou controles internos	25
4	DIAGNÓSTICO DE IMPACTO E PROPOSTA DE ADEQUAÇÃO	27
4.1	Departamento pessoal e/ou de recursos humanos (RH)	28
4.2	Departamento comercial e de cadastro e identificação de investidores dos fundos de investimentos sob distribuição própria	29
4.3	Departamento jurídico	32
4.4	Departamento de tecnologia da informação (TI) e *cybersegurança*	33
4.5	Departamento de processamento de dados e inteligência de negócio	34
4.6	Departamento de *compliance* e/ou controles internos	34
4.7	O papel do *compliance* na adequação das empresas à LGPD – uma experiência pessoal	36
5	CONCLUSÃO	38
	REFERÊNCIAS	40

1 INTRODUÇÃO

As obrigações oriundas da Lei n. 13.709/2018, denominada Lei Geral de Proteção de Dados (LGPD), exigiram a adequação em parcela relevante da iniciativa pública e privada no Brasil e no exterior, especialmente em relação ao tratamento e ao armazenamento dos dados pessoais dos cidadãos brasileiros.

O presente artigo pretende apresentar as obrigações trazidas pela nova legislação, as atividades afetadas e as demandas de implementação de um plano de ação para a conformidade e o acompanhamento dos processos críticos de uma gestora de recursos em operação.

Neste contexto, o artigo irá se limitar a explorar as obrigações da lei que potencialmente impactaram nos processos deste negócio no momento da publicação deste artigo. Não obstante, suprimiremos diversos capítulos e artigos da norma em que não agregaram ao desenvolvimento do diagnóstico e plano de conformidade da proposta de adequação na tentativa de formular proposições de boas práticas e de governança sobre a proteção de dados pessoais.

Reforçam a necessidade e a importância da escrita deste artigo no momento da sua publicação a ausência de regras de boas práticas e de governança sobre a proteção de dados pessoais pela Comissão de Valores Mobiliários (CVM) e a Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais (ANBIMA). Esta última, limita-se a publicar medidas técnicas adotadas no âmbito da tecnologia da informação voltadas à garantia da segurança da informação, a exemplo do *Guia de Segurança Cibernética da ANBIMA*.

O artigo aqui proposto divide-se em três âmbitos de discussão: (i) apresentar o panorama geral de proteção de dados no Brasil e trazer as principais definições legais aplicáveis à atividade dos gestores de fundos de investimentos quanto aos processos de coleta, tratamento, armazenamento e uso de informações pessoais; (ii) proposta para estruturar a organização em departamentos cuja atividade envolve processos com dados pessoais e; (iii) diagnosticar o impacto, além de propor adequação aos processos que exigem a conformidade à LGPD. Por fim, apresentaremos uma experiência pessoal que sustenta a importância do papel de *compliance* como o principal agente promotor de adequação das empresas à LGPD.

Quanto à metodologia, o trabalho de pesquisa, quanto ao seu aprofundamento teórico, foi realizado a partir da interpretação da lei, apoiado em bibliografias

preexistentes sobre a LGPD e levantamento de processos inerentes às atividades de gestão de fundos de investimentos. Trata-se de uma pesquisa qualitativa apoiada em revisão bibliográfica, estudo de doutrina, do ordenamento jurídico e de processos.

Soluções hipotéticas serão dadas a partir de propostas de implementação de processos que garantam a condução diligente das atividades relacionadas à coleta, ao armazenamento e ao uso de dados de terceiros nas atividades que um gestor de fundos de investimento pode realizar conforme as normas vigentes.

A análise do impacto da LGPD para os gestores de fundos de investimento se limitará a avaliar as possíveis atividades realizadas pelos gestores, definidas nos normativos da CVM e nos processos inerentes à prestação de serviço de gestão de fundos de investimento. Ainda sobre a delimitação do escopo deste artigo, suprimimos alguns temas tratados na LGPD, por exemplo, o tratamento de dados pessoais pelo poder público, transferência internacional de dados, fiscalização e sanções, detalhamento da governança da autoridade nacional de proteção de dados e disposições finais e transitórias que julgamos irrelevantes para a finalidade deste trabalho.

2 PANORAMA GERAL E A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

A União Europeia é pioneira na proteção de dados pessoais; isto ocorre porque, dentre outras iniciativas, entende que a privacidade deriva da dignidade da pessoa humana, ao considerar a proteção de dados pessoais como direito fundamental. Postura esta que foi amplamente confirmada durante a elaboração da pesquisa e do levantamento de referências para fundamentar a proposta deste artigo.

Neste sentido, corroborando com o cenário descrito, Viviane Nóbrega Maldonado afirma: "é fato que a Europa assumiu o protagonismo em matéria de proteção de dados e estabeleceu *standards* a serem observados em termos mundiais [...]"[1]. Além disso, a Declaração Universal dos Direitos Humanos quanto ao direito da vida privada, rege: "Art. 12 – Ninguém será sujeito à interferência na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataque à honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques".

Neste contexto, em 2016, foi aprovada a *General Data Protection Regulation*[2] (GDPR) visando proteger, coletar, tratar e armazenar os dados pessoais dos cidadãos da União Europeia. Desde a sua entrada em vigorvários países passaram a utilizar as diretrizes previstas na legislação europeia para julgar e analisar situações envolvendo a proteção de dados, dada a inexistência de legislação própria regulamentando o tema.

Essa cooperação entre os países levou vários deles a criarem novas normativas, a maioria espelhada na GDPR. Seguindo essa tendência, o Brasil elaborou a Lei n. 13.709/2018, alterada pela Lei n. 13.853/2019 e, finalmente, promulgada em 18 de setembro de 2020.

"Antes da LGPD, o Brasil dispunha apenas de leis esparsas para tratar de diferentes aspectos das relações jurídicas que envolviam dados pessoais"[3], explicam Ricardo Oliveira e Marcio Cots. Assim, é a partir dessa iniciativa que a discussão central desse artigo toma corpo.

---

[1] MALDONADO, Viviane Nóbrega **LGPD**: Lei Geral de Proteção de Dados Pessoais – manual de implementação. São Paulo: RT, 2019, p. 29.
[2] UNIÃO EUROPEIA. Regulação (EU) 2016/679, de 27 de abril de 2016. Regulação Geral de Proteção de Dados. Disponível em: https://gdpr-info.eu/. Acesso em: 2 fev. 2021.
[3] OLIVEIRA, Ricardo; COTS, Marcio. **Lei Geral de Proteção de Dados Pessoais comentada**. São Paulo: RT, 2018, p. 25.

A Lei Geral de Proteção de Dados – LGPD (Lei n. 13.709), publicada em agosto de 2018, somente entrou em vigor em 18 de setembro de 2020, após inúmeros vetos e alterações (destacando-se aqueles trazidos pela Lei n. 13.853/2019). É o seu art. 1º que define o escopo e a tutela da norma jurídica:

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

Uma análise preliminar do objeto da LGPD revela a consagração da proteção de pessoais naturais contra o tratamento dito ilegal de dados pessoais realizados por qualquer pessoa, seja por outra pessoa natural ou por demais agentes. Seguindo o princípio da GDPR, os direitos de liberdade e de privacidade também são descritos como "direitos fundamentais", corroborando o entendimento de que a legislação brasileira foi inspirada na europeia.

De acordo com Viviane Nóbrega Maldonado e Renato Opice Blum, é importante destacar neste primeiro artigo a "aplicabilidade da Lei também ao tratamento de dados em estado físico ou *offline*, migrando ou não, posteriormente, para o meio digital ou *online*"[4]. Nesse contexto, documentos fisicamente disponíveis também serão tutelados pela nova legislação.

2.1 Disposições preliminares

Em sua estrutura central e mais recente, a lei está dividida em 10 capítulos e 65 artigos, conforme demonstra o quadro abaixo:

Quadro 1 – Estrutura geral da Lei Geral de Proteção de Dados

Capítulo	Descrição	Artigos
I	Disposições Preliminares	1° ao 6°
II	Do Tratamento de Dados Pessoais: Inclui Seção I – Dos Requisitos para o Tratamento de Dados; Seção II – Do Tratamento de Dados Pessoais Sensíveis; Seção III – Do Tratamento de Dados Pessoais de Crianças e Adolescentes; e Seção IV – Do Término de Tratamento de Dados.	7° ao 16°
III	Dos Direitos do Titular	17° ao 22°
IV	Do Tratamento de Dados Pessoais pelo Poder Público: Inclui Seção I – Das Regras; e Seção II – Da Responsabilidade.	23° ao 32°

[4] MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **LGPD** – Lei Geral de Proteção de Dados Pessoais comentada. São Paulo: RT, 2019, p. 20.

V	Da Transferência Internacional de Dados	33° ao 36°
VI	Dos Agentes de Tratamento de Dados Pessoais: Inclui Seção I – Do Controlador e do Operador; Seção II – Do Encarregado pelo Tratamento de Dados Pessoais; e Seção III – Da Responsabilidade e do Ressarcimento de Danos.	37° ao 45°
VII	Da Segurança e das Boas Práticas: Inclui Seção I – Da Segurança e do Sigilo de Dados; Seção II – Das Boas Práticas e da Governança.	46° ao 51°
VIII	Da Fiscalização: Inclui Seção I – Das Sanções Administrativas.	52° ao 54°
IX	Autoridade Nacional de Proteção de Dados (ANPD) e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade: Inclui Seção I – Da ANPD; e Seção I – Do Conselho Nacional de Proteção de Dados Pessoais.	55° ao 59°
X	Disposições Finais e Transitórias	60° ao 65°

Fonte: Autoria nossa.

Para melhor esclarecimento do dispositivo legal no contexto da abordagem deste trabalho, chamamos atenção para os arts. 5º e 6º da legislação, que apresentam, respectivamente, os principais conceitos e princípios norteadores da norma em discussão: “Art. 5º. Para os fins desta Lei, considera-se: [...], I a XIX; Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: [...] I a X

A seguir, exploraremos os principais pontos relacionados à LGPD, enfatizando os capítulos, artigos e parágrafos da lei para investigar o desenvolvimento do capítulo da norma voltado ao diagnóstico de impacto e proposta de adequação.

2.2 Tratamento de dados pessoais

As disposições das hipóteses nas quais os dados pessoais podem ser tratados estão definidas taxativamente no art. 7º da nova lei. São hipóteses que representam as bases legais. Não obstante, destacamos que o atendimento de apenas uma delas já é suficiente para fundamentar a atividade de tratamento dos dados pessoais:

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> I – mediante o fornecimento de consentimento pelo titular;
> II – para o cumprimento de obrigação legal ou regulatória pelo controlador;
> III – pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
> IV – para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
> V – quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

> VI – para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei n. 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
> VII – para a proteção da vida ou da incolumidade física do titular ou de terceiro;
> VIII – para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei n. 13.853, de 2019) Vigência
> IX – quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
> X – para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

Ainda no contexto do tratamento de dados pessoais, destacamos dois conceitos a serem aprofundados: o consentimento como base legal e o legítimo interesse, com foco no art. 10 da lei que aprofunda a sua definição.

2.3 Do consentimento como base legal

Com base na leitura da lei e análise crítica das fontes bibliográficas utilizadas para a elaboração deste artigo, notamos a boa qualidade de esclarecimento na redação da nova lei. No entanto, um ponto chama atenção: a proposta de interpretação do conceito de consentimento, conforme observam Viviane Nóbrega Maldonado e Renato Opice Blum:

> A legislação não especificou o que se deve entender por livre, informado e inequívoco, o que passamos a fazer a seguir, com base especificamente no entendimento que se pode extrair acerca desses conceitos à luz do *General Data Protection* (GDPR – Regulamento Geral de Proteção de Dados Europeu), especificamente *Guideline* 259/2017, do então denominado *Article 29* (atual *European Data Protection Board* – EDPB), tratamento sobre consentimento[5].

Em síntese, ambos propõem uma série de requisitos mínimos como boas práticas no processo de pedido de consentimento, que impõem apresentar aos titulares dos dados a lista a seguir:

> a) finalidades específicas do tratamento;
> b) forma e duração do tratamento, guardados os segredos comercial e industrial;
> c) identificação e informações de contato do controlador;
> d) informações acerca do uso compartilhado de dados pelo controlador e a finalidade;
> e) responsabilidades dos agentes que realizarão o tratamento; e

[5] MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **LGPD** – Lei Geral de Proteção de Dados Pessoais comentada. São Paulo: RT, 2019, p. 179-180.

> f) direitos do titular, aí se incluindo menção à possibilidade de confirmação de tratamento dos dados, acesso, atualização, retificação, anonimização, eliminação, além de outros dispostos nos artigos 17 a 22 da Lei[6].

Ainda sobre o consentimento, o art. 8º da lei define: "O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular".

Destaca-se ainda a observação analítica de Viviane Nóbrega Maldonado e Renato Opice Blum, cuja interpretação indica que o consentimento pode ser obtido de qualquer forma, desde que guarde a evidência da manifestação. Neste contexto, apresentam como alternativas "métodos tradicionais (contratos ou formulários em papel, por exemplo), ferramentas digitais (por meio de assinatura eletrônica ou digital, telefone, biometria, vídeo, áudio, entre outros), sendo amplas as possibilidades trazidas pela norma"[7].

2.4 Legítimo interesse

Conforme ponderamos sobre o tratamento de dados pessoais, o legítimo interesse é uma das suas bases legais, assim apresentada na lei em seu art. 7º e, posteriormente, explorado e definido quanto à sua utilização no art. 10, o que lhe permite ampla interpretação a respeito da sua aplicação.

Segundo Ricardo Oliveira e Marcio Cots,

> Por seu grau de subjetividade, o legítimo interesse talvez seja a base legal que gerará mais discussão, mas sua criação era medida essencial para que o empreendedorismo e a inovação não sofressem ainda mais os impactos da nova lei, especialmente quanto aos dados pessoais tratados antes que a LGPD regulasse o tema[8].

O art. 10 explora o entendimento e as aplicações do legítimo interesse:

> Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a: [...]

Ao final, Marcio Cots e Ricardo Oliveira defendem:

> Podemos tomar o interesse como aquilo que é importante para alguém e

---

[6] MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **LGPD** – Lei Geral de Proteção de Dados Pessoais comentada. São Paulo: RT, 2019, p. 181.
[7] MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **LGPD** – Lei Geral de Proteção de Dados Pessoais comentada. São Paulo: RT, 2019, p. 181.
[8] OLIVEIRA, Ricardo; COTS, Marcio. **Lei Geral de Proteção de Dados Pessoais comentada**. São Paulo: RT, 2018, p. 99.

> legítimo como justificado ou amparado pelo bom senso. Assim, o início da reflexão parte da pergunta se o tratamento dos dados pessoais pretendidos é importante e se justifica, em relação ao controlador, a ponto de ele não ser obrigado a coletar o consentimento dos titulares[9].

Sendo assim, uma vez atingidos os requisitos citados, haverá fundamentos para o tratamento de dados pelo controlador.

2.5 Tratamento de dados pessoais sensíveis

Em síntese, destacam-se na análise de Viviane Nóbrega Maldonado e Renato Opice Blum as vedações "ao tratamento de dados sensíveis para a execução de contrato, com base em interesses legítimos e para a proteção ao crédito"[10], permanecendo as demais hipóteses com algumas restrições. Os autores entendem ainda que o tratamento de dados deve ocorrer apenas em situações indispensáveis para alcançar a finalidade prevista, conforme observado nos arts. 11, 12 e 13, a seguir:

> Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: [...]
>
> Art. 12. Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido. [...]
>
> Art. 13. Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas. [...]

Por fim, observa-se a necessidade de cuidado e de princípios éticos em qualquer inciativa que considerar o tratamento de dados pessoais sensíveis, além das obrigações taxativas nos respectivos artigos da lei que versam sobre o assunto.

2.6 Tratamento de dados pessoais de crianças e adolescentes

---

[9] OLIVEIRA, Ricardo; COTS, Marcio. **Lei Geral de Proteção de Dados Pessoais comentada**. São Paulo: RT, 2018, p. 99.

[10] MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **LGPD** – Lei Geral de Proteção de Dados Pessoais comentada. São Paulo: RT, 2019, p. 197.

Conforme previsto pela Lei n. 8.069/1990 (Estatuto da Criança e do Adolescente – “ECA”), crianças são pessoas com até 12 anos incompletos e adolescentes, pessoas entre 12 e 18 anos incompletos.

O art. 14 da LGPD apresenta restrições claras e objetivas quanto ao tratamento de dados pessoais desses indivíduos: “Art. 14. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente [...]”

Em conclusão, ao tratar os dados pessoais desse grupo, “deve-se levar em conta o melhor interesse, bem como a necessidade de proteção integral, conforme disciplinado na legislação pertinente (ECA)”[11].

2.7 Direitos dos titulares

Os direitos dos titulares constam em diversos artigos da lei, desenvolvidos na sua maior parte no art. 9º e, posteriormente, apresentados de forma estruturada no capítulo III da Lei, arts. 17 a 22, conforme se vê abaixo:

> Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso: [...]
>
> Art. 17. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei. [...]
>
> Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: [...]
>
> Art. 19. A confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular: [...]
>
> Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade. [...]
>
> Art. 21. Os dados pessoais referentes ao exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo. [...]
>
> Art. 22. A defesa dos interesses e dos direitos dos titulares de dados poderá

[11] MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **LGPD** – Lei Geral de Proteção de Dados Pessoais comentada. São Paulo: RT, 2019, p. 90.

> ser exercida em juízo, individual ou coletivamente, na forma do disposto na legislação pertinente, acerca dos instrumentos de tutela individual e coletiva. [...]

Por fim, verifica-se que a legislação define uma vasta gama de direitos assegurados aos titulares dos dados pessoais, além de discorrer a respeito de regras de proteção vinculadas ao princípio de transparência da informação e representação contra eventuais abusos. Importante destacar que os controladores devem estar preparados para atender às demandas dos titulares e prepostos na prestação de esclarecimentos nos prazos determinados pela lei.

2.8 Agentes de tratamento de dados pessoais

Os agentes de tratamento aqui são representados pelos titulares, controladores e operadores apresentados anteriormente. Os legisladores dedicaram um capítulo específico da lei para tratar as obrigações dos agentes citados no desenvolvimento dos artigos 37 ao 45.

Abaixo, apresentamos na íntegra o trecho da lei que trata essas obrigações, uma vez que ela é comum e gera a necessidade de adequação por parte dos agentes e das gestoras de fundos de investimentos.

> Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse. [...]
>
> Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.
> Parágrafo único. Observado o disposto no *caput* deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados. [...]
>
> Art. 39. O operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria. [...]
>
> Art. 40. A autoridade nacional poderá dispor sobre padrões de interoperabilidade para fins de portabilidade, livre acesso aos dados e segurança, assim como sobre o tempo de guarda dos registros, tendo em vista especialmente a necessidade e a transparência. [...]
>
> Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais.

> Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.
>
> Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem: [...]
>
> Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais: [...]
>
> Art. 45. As hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente.

Em síntese, destacamos as seguintes obrigações: a realização de registros com mapeamento de todas as operações que envolvem o tratamento de dados pessoais previstos na LGPD, especialmente aqueles que tiverem como base legal o legítimo interesse; monitoramento de futuras determinações da autoridade nacional de proteção de dados via regulamentação; observar a existência de formalizações documentadas quando houver a existência de tratamento com figura simultânea de agente operador e controlador; a definição do encarregado, quando couber; a indicação taxativa de ressarcimento de danos causados aos titulares de dados originados, além das multas aplicáveis. Ainda nesse contexto, há previsão de inversão do ônus da prova, que é explicado por Viviane Nóbrega Maldonado e Renato Opice Blum: “a empresa, para exonerar a sua responsabilidade, afastando o nexo de causalidade, terá de fazer prova das suas alegações”[12].

2.9 Segurança e boas práticas

O tema da segurança é tratado pela LGPD nos artigos 46 ao 51, na qual os agentes de tratamento (controlador e operador) devem, de acordo com Viviane Nóbrega Maldonado e Renato Opice Blum, “implementar medidas de segurança, medidas técnicas e medidas administrativas capazes de proteger os dados pessoais”[13].

Segundo os autores, as boas práticas podem ser lidas como medidas administrativas:

> São exemplos de medidas administrativas: políticas corporativas para

[12] MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **LGPD** – Lei Geral de Proteção de Dados Pessoais comentada. São Paulo: RT, 2019, p. 329.
[13] MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **LGPD** – Lei Geral de Proteção de Dados Pessoais comentada. São Paulo: RT, 2019, p. 329.

> proteção de dados pessoais, contratos de confidencialidade, políticas de privacidade de *sites* e aplicativos, capacitação dos empregados cujas atividades envolvam o tratamento de dados pessoais, controle de acesso aos arquivos físicos, entre outras[14].

Trata-se de uma discussão de grande relevância para o diagnóstico de impacto e proposta de adequação, tema a ser desenvolvido mais adiante. Abaixo, os artigos mencionados:

> Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. [...]
>
> Art. 47. Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término. [...]
>
> Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. [...]
>
> Art. 49. Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares. [...]

Em síntese, a seção anterior, que reúne os artigos 46 ao 49, estabelece a necessidade de se aplicar princípios técnicos e administrativos para nortear controles de segurança da informação dentro de padrões reconhecidos no setor, além de um plano de resposta aos potenciais incidentes, uma vez que as iniciativas devem mitigar os riscos de vazamento, e não eliminá-lo totalmente.

> Seção II
> Das Boas Práticas e da Governança
>
> Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais. [...]
>
> Art. 51. A autoridade nacional estimulará a adoção de padrões técnicos que

[14] MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **LGPD** – Lei Geral de Proteção de Dados Pessoais comentada. São Paulo: RT, 2019, p. 329.

facilitem o controle pelos titulares dos seus dados pessoais.

Por fim, a seção anterior representada pelos artigos 50 e 51 estabelece com elevado grau de importância, a previsão dos controladores e operadores, sozinhos ou coletivamente, definirem suas próprias regras de boas práticas, principalmente quanto aos padrões técnicos a serem adotados, uma vez que a lei não os define.

3 GESTORES DE FUNDOS DE INVESTIMENTOS E MODELOS ORGANIZACIONAIS

Tal como previsto na Instrução CVM n. 558, de 26 de março de 2015., o administrador fiduciário é a pessoa jurídica autorizada pela CVM para atuar na administração de carteiras de valores mobiliários e na administração de fundos de investimentos e demais práticas relacionadas.

Já o gestor de recursos é o responsável profissional pela gestão dos ativos financeiros integrantes da carteira dos fundos de investimentos e as demais práticas relacionadas, conforme a instrução citada e, de forma específica, no Capítulo VIII do Código de Administração de Recursos de Terceiros da ANBIMA. O gestor também poderá atuar como gestor-distribuidor de fundos de investimentos próprios, como previsto pelo art. 30 da Instrução CVM n. 558.

Na administração de empresas, assim como na administração de uma gestora de fundos de investimentos, há uma série de conceitos adotados para a departamentalização das atividades.

Embora a proposta deste artigo não seja aprofundar conceitos de teoria da administração, ou esgotar os modelos organizacionais, durante o processo de pesquisa para fundamentar a proposta de modelo organizacional aqui utilizado, nos deparamos com a definição utilizada por Sérgio Rodrigues: “uma empresa dedicada a um conjunto restrito de produtos e mercados, normalmente opera com base numa estrutura funcional, ou seja, com funções agrupadas por similaridade ou afinidade”[15].

Nosso artigo também não se propõe a definir um modelo rígido de estrutura organizacional, corroborando com o esclarecimento de Sérgio Rodrigues ao mencionar a função da natureza do negócio para essa definição:

> A estrutura organizacional é função da natureza do negócio e das caraterísticas peculiares de cada empresa. Uma empresa de serviços ou uma empresa de utilidade pública (energia elétrica, gás, telefone etc.) tem também suas características totalmente peculiares com direta consequência nas respectivas estruturas de organização[16].

No entanto, verificamos que, para fins práticos, seguir com uma proposta de departamentalização mais segmentada possível seria de maior valia para a

---

[15] RODRIGUES, Sérgio. **Sistemas de informação**: um enfoque gerencial. Edgard Bruno Cornachione Jr. (colab.) 2. ed. São Paulo: Atlas, 2017, p. 84.
[16] RODRIGUES, Sérgio. **Sistemas de informação**: um enfoque gerencial. Edgard Bruno Cornachione Jr. (colab.) 2. ed. São Paulo: Atlas, 2017, p. 88.

apresentação deste trabalho e futuras discussões para os pesquisadores do tema. Não obstante, no momento da publicação deste trabalho, atuávamos como diretor estatutário responsável pela governança e por controles internos de uma gestora de fundos de investimentos com estrutura organizacional equivalente a que será proposta abaixo.

Neste contexto, exploraremos as principais áreas e atividades cujos processos lidam potencialmente com dados pessoais, independentemente da relação de *stakeholder*: "Um bom início deve considerar a elaboração de um mapa do macrofluxo dos dados dentro da sua empresa (*one page view*). Um mapa para cada macroprocesso"[17]. Trata-se de uma lógica dedutiva de trabalho, conforme explica Viviane Nóbrega Maldonado.

Considerando os conceitos de estrutura organizacional e de fluxo de dados pessoais, apresentamos uma proposta de organização das atividades e de macroprocessos em departamentos, a partir da indicação abaixo – suas estruturas e perfis serão exploradas na sequência:

i) departamento pessoal e/ou recursos humanos;
iii) departamento comercial e de cadastro e identificação de investidores dos fundos de investimentos sob distribuição própria;
iv) departamento jurídico;
v) departamento de tecnologia da informação (TI) e *cybersegurança*;
vi) departamento de processamento de dados e inteligência de negócio; e
vii) departamento de *compliance* e/ou controles internos

3.1 Departamento pessoal e/ou recursos humanos (RH)

Em que pese não haver obrigação legal, regulatória ou autorregulatória, as gestoras, observando as melhores práticas de governança e porte, possuem um departamento pessoal responsável, principalmente, pela relação entre colaborador e gestora, além das obrigações decorrentes.

No entanto, é recomendável organizar essa estrutura considerando suas atividades mais específicas, práticas e objetivas para garantir que a empresa esteja

[17] MALDONADO, Viviane Nóbrega **LGPD**: Lei Geral de Proteção de Dados Pessoais – manual de implementação. São Paulo: RT, 2019, p. 48.

de acordo com as leis trabalhistas e as demais aplicáveis para cada regime de contrato a ser celebrado dentro de sua estrutura.

3.2 Departamento comercial, cadastro e identificação de investidores dos fundos de investimentos sob distribuição própria

Desde que observadas as Instruções n. 558, n. 539 e n. 617 da CVM, no Código de Administração de Recursos de Terceiros da ANBIMA, e na Lei n. 9.613/1998, as gestoras podem atuar tanto como gestora quanto como gestora-distribuidora de fundos próprios. Na segunda situação, elas têm obrigações regulatórias e autorregulatórias diferentes das de gestora ou dos administradores fiduciários e demais agentes do mercado de capitais.

Essas obrigações são, principalmente, relativas ao cadastro e à identificação de investidores nos fundos de investimento próprios, especialmente de acordo com o art. 30 da Instrução n. 558 e das Instruções n. 539 e n. 617, todas da CVM.

A depender da estrutura adotada, os colaboradores alocados nesse departamento são responsáveis por contatar o investidor, esclarecer dúvidas, obter informações e documentos, realizar cadastro inicial e atualizações necessárias, além de outros assuntos que guardam relação com o tema.

3.3 Departamento jurídico

Conforme as normas regulatórias e autorregulatórias, as gestoras e gestoras-distribuidoras não são obrigadas a possuir um departamento jurídico próprio, portanto, podem contratar um prestador de serviço para atuar na gestão dos assuntos jurídicos.

O departamento jurídico ou de administração dos assuntos legais seria responsável pela governança dos contratos de todas as espécies firmados pela gestora, incluindo as funções de elaborá-los, revisá-los periodicamente e aprová-los.

3.4 Departamento de tecnologia da informação (TI) e *cybersegurança*

Conforme previsto no Capítulo V, seções III e V do Código de Administração de Recursos de Terceiros da ANBIMA, a gestora deve manter na sua estrutura regras, procedimentos e controles relativos às informações sensíveis e de segurança cibernética.

Para tanto, e visando maior controle e segurança, considera-se a existência de um departamento interno que trata de tecnologia da informação e *cybersegurança* em todas as instâncias da rotina corporativa.

3.5 Departamento de

Conforme as normas regulatórias e autorregulatórias, as gestoras e gestoras-distribuidoras não são obrigadas a possuir um departamento de processamento de dados e inteligência de negócio.

De acordo com Edgard Bruno,

> disseminação de informações numa empresa enquadra-se em uma ou mais das seguintes categorias: resposta a perguntas e questões, relatórios rotineiros produzidos por subsistemas de informação, relatórios especiais, documentos de fábrica e escritórios[18].

Neste contexto, a evolução dos negócios caminhou para as empresas se especializarem e se organizarem para atender à demanda de processamento de dados e inteligência de negócio instituindo departamentos especializados para este propósito.

3.6 Departamento de *compliance* e/ou controles internos

Conforme previsto pelos arts. 4º, IV, § 3º e 19 da ICVM 558; art. 7º da ICVM 617; e art. 10 do Código de Administração de Recursos de Terceiros da ANBIMA, os administradores de carteiras de valores mobiliários devem manter uma área segregada para o desenvolvimento e a implementação de regras, controles internos e procedimentos que mantenham a aderência da empresa nas normas legais,

---

[18] RODRIGUES, Sérgio. **Sistemas de informação**: um enfoque gerencial. Edgard Bruno Cornachione Jr. (colab.) 2. ed. São Paulo: Atlas, 2017.

regulatórias e autorregulatórias.

Tendo em vista a responsabilidade do *compliance* em promover e desenvolver controles internos e procedimentos, é natural que a responsabilidade pela gestão do mapeamento, pela implementação e pela manutenção das regras apresentadas pela Lei Geral de Proteção de Dados caiba ao departamento em questão.

4 DIAGNÓSTICO DE IMPACTO E PROPOSTA DE ADEQUAÇÃO

O diagnóstico de impacto representa a análise das principais atividades com o objetivo de se implementar a conformidade de acordo com a LGPD, observando para tanto os princípios, os conceitos e as terminologias trazidos pela lei e explorados na seção anterior.

De acordo com Patricia Peck Pinheiro, o início do processo de implementação é o levantamento de dados pessoais através do mapeamento de "quais são e onde estão"[19].

Neste contexto, Viviane Nóbrega Maldonado observa:

> Devem ser consideradas no escopo todas as áreas de negócio que tratam dados pessoais: que coletam, armazenam, processam, transferem ou recebem dados pessoais de titulares de dados – clientes, consumidores, *prospects*, funcionários, candidatos a vagas de emprego, parceiros e fornecedores[20].

É importante mapear todas as atividades relacionadas ao processamento de dados pessoais previstos na lei e suas respectivas finalidades considerando todas as bases legais previstas, por exemplo, as previsões legais e regulatórias que justificam a coleta, o armazenamento, o tratamento e o compartilhamento das informações pessoais e direitos dos titulares de acessar, retificar, solicitar a exclusão de dados, transferir, limitar ou se opor ao tratamento, e retirar o consentimento conforme previsto e apresentado na LGPD.

A partir do levantamento dessas informações, Patricia Peck acredita que será possível desenvolver "o mapa de risco e elaborar o plano de ação" que será base para o esforço necessário em relação à adequação à Lei[21].

Segundo a autora, o esforço pode ser classificado em quatros frentes ou "níveis", assim explicados: i) nível técnico representado por ferramentas e/ou sistemas; ii) documental, que implica a atualização de normas, políticas, contratos e afins; iii) procedimental, representado pelas adequações de governança e de gestão dos dados pessoais e processos afins; e iv) cultural, através de iniciativas de treinamentos, campanhas de conscientização de equipes, parceiros fornecedores e clientes. Dentro desse panorama, inclui-se o seguinte ponto de atenção:

---

[19] PINHEIRO, Patricia Peck. **Proteção de dados pessoais** – Comentários à Lei n. 13.709/2018 LGPD. São Paulo: Saraiva Educação, 2018, p. 44.
[20] MALDONADO, Viviane Nóbrega. **LGPD**: Lei Geral de Proteção de Dados Pessoais – manual de implementação. São Paulo: RT, 2019.
[21] PINHEIRO, Patricia Peck. **Proteção de dados pessoais** – Comentários à Lei n. 13.709/2018 LGPD. São Paulo: Saraiva Educação, 2018, p. 44.

> Dependendo do ramo do negócio, da empresa e da maturidade da governança de dados pessoais, é fundamental criar um programa de *compliance* digital, com *risk assessment*, planos de repostas a incidentes, treinamentos e comunicação*, due diligence* de terceiros em um contexto multisetorial dentro do negócio [...] [22].

Logo, verificamos que o escopo do plano de ação é relativo à complexidade da estrutura organizacional que se pretende analisar e atender. E que a melhor proposta de adequação é a criação de um programa de proteção de dados que promova as melhorias de forma contínua.

4.1 Departamento pessoal e/ou de recursos humanos (RH)

O departamento pessoal e/ou de recursos humanos é impactado pela LGPD diretamente por conta do colaborador pessoa física, da seleção de candidatos, contratação e manutenção, até a rescisão do vínculo.

No primeiro momento, o responsável por selecionar os candidatos deverá observar como os currículos foram obtidos, já que não pode ser armazenado ou compartilhado, exceto se autorizado expressamente pelo candidato ou se as informações foram obtidas de canais digitais; no segundo cenário, o documento não será armazenado fora desse ambiente.

Ademais, é vedado expressamente que os dados pessoais sensíveis[23] sejam utilizados como critério de seleção dos candidatos.

No momento da contratação, o colaborador propõe utilizar um termo de consentimento detalhando o uso e o compartilhamento dos seus dados pessoais. Entretanto, não há obrigação legal para essa conduta, visto que os dados coletados são obtidos para cumprir obrigações legais, contratuais e/ou regulatórias[24], além da utilização da biometria, quando necessário, para o acesso a determinadas áreas da empresa que vier a utilizar esse recurso tecnológico cada vez mais comum na gestão de acessos.

Importante salientar que a gestora tem obrigação regulatória[25] e autorregulatória de manter determinados departamentos segregados dos demais,

---

[22] PINHEIRO, Patricia Peck. **Proteção de dados pessoais** – Comentários à Lei n. 13.709/2018 LGPD. São Paulo: Saraiva Educação, 2018, p. 45 (*ebook*).
[23] Nesse caso específico, além das hipóteses previstas no art. 5º, II, da LGPD, também são considerados dados pessoais sensíveis informações que possam ser utilizadas de forma discriminatória, ou sem qualquer razão de ser, como endereço, gênero ou *status* de relacionamento.
[24] BRASIL. Lei n. 13.709/2018. Lei Geral de Proteção de Dados. Art. 7º, II e V.
[25] Conforme artigo 24, I, da ICVM 558, e artigo 12 do Código de Administração de Recursos da ANBIMA.

inclusive fisicamente. As salas em questão possuem restrição de acesso, dessa forma, o colaborador, quando contratado, será informado da situação e deverá consentir expressamente para o compartilhamento da sua biometria, já que se trata de um dado sensível[26].

Durante a vigência do vínculo entre o colaborador e a gestora, a depender do regime jurídico, os dados pessoais coletados no momento da contratação serão compartilhados com órgãos federais, estaduais, municipais, regulatórios e autorregulatórios, além de empresas contratadas pela gestora para o cumprimento das obrigações contratuais, legais ou regulatórias[27]. O departamento jurídico irá monitorar os respectivos contratos, observando cláusulas relativas à Lei Geral de Proteção de Dados.

Na rescisão contratual, todos os dados pessoais, sensíveis ou não, serão expurgados, mantendo, pelo prazo previsto, apenas os que são obrigatórios pela legislação aplicável.

4.2 Departamento comercial e de cadastro e identificação de investidores dos fundos de investimentos sob distribuição própria

Quando analisamos a incidência da LGPD na atividade citada, verificamos que há a coleta, o tratamento e o compartilhamento de vários dados pessoais[28]. Entretanto, pela própria estrutura do mercado de capitais, são informações compartilhadas com os administradores dos fundos visando especificamente efetuar, manter e promover os investimentos requeridos.

Nesse sentido, em que pese o compartilhamento seja indispensável para a realização dos investimentos[29], a gestora, por mera liberalidade e para sempre informar os investidores das razões que justificam a coleta dos dados, propõe-se a utilizar e enviar um termo de ciência no início do relacionamento, quando são apresentadas as razões para coletar, armazenar, tratar e compartilhar suas informações[30].

Com a promulgação da Lei, os investidores que já possuíam cadastro,

---

[26] BRASIL. Lei n. 13.709/2018. Lei Geral de Proteção de Dados. Art. 5º, II.
[27] As empresas podem ser, por exemplo, empresas de plano de saúde, benefícios e contadores.
[28] Tal como prevê o Anexo 11-A da ICVM 617.
[29] BRASIL. Lei n. 13.709/2018. Lei Geral de Proteção de Dados. Art. 7º, V.
[30] BRASIL. Lei n. 13.709/2018. Lei Geral de Proteção de Dados. Arts. 6º a 9º.

receberiam dos departamentos comercial e de *Compliance*, uma comunicação (e-mail por exemplo) solicitando a manutenção dos dados, frisando sempre que armazenar e compartilhar as informações seria indispensável para efetuar os investimentos.

Conforme rege o capítulo III[31] da LGPD, os titulares de dados pessoais têm determinados direitos, e em face deles, os departamentos envolvidos deverão seguir certas diretrizes, conforme indicadas abaixo:

Observar quem solicitou o pedido. Apenas o titular do dado ou o seu representante legal pode realizar o pedido, nesse caso, deve-se atentar se o meio de comunicação utilizado era aquele que constava no cadastro, como *e-mail* e número de telefone;
As informações enviadas devem ser claras, simplificadas e informar exatamente o que foi solicitado pelo titular;
As informações podem ser enviadas física ou digitalmente, dependendo da solicitação do titular.
A informação repassada não pode conter dado sigiloso ou determinante aos negócios.
Como regra geral, os pedidos devem ser cumpridos em até 15 dias úteis[32], porém, na impossibilidade do cumprimento desse prazo, o *compliance* deverá ser informado para analisar a questão, discutir um novo prazo e, eventualmente, informar o solicitante a respeito.

Abaixo, estão previstas as solicitações que podem ser feitas pelos titulares e eventual observação para a conduta da gestora:

Confirmação de existência de tratamento e acesso aos dados;
Correção de dados incompletos, inexatos ou desatualizados; quando o titular solicita a atualização das informações, após o cumprimento, deverá ser informado do resultado;
Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados de forma diversa ao previsto na Lei. Em princípio não há coleta de dados ‘desnecessários’, porém, é importante que o *compliance* seja envolvido na demanda

[31] BRASIL. Lei n. 13.709/2018. Lei Geral de Proteção de Dados. Art. 17 e seguintes.
[32] Até o momento a única previsão da legislação é o prazo de 15 dias para que as solicitações sejam cumpridas no prazo indicado. BRASIL. Lei n. 13.709/2018. Lei Geral de Proteção de Dados. Arts. 18, §§ 3º e 5º, e art. 19, II.

para auxiliar na verificação, se o dado é desnecessário e se é possível que ele seja anonimizado, bloqueado ou eliminado, especialmente pelas obrigações legais e regulatórias; ao final, o titular deverá ser informado via *e-mail* da conclusão do pedido ou da negativa[33].

Portabilidade dos dados a outro fornecedor de serviço ou produto. Visto que não há regulamentação específica da ANPD, os casos deverão ser analisados junto ao *compliance* para efetivar a portabilidade requerida.

Eliminação dos dados pessoais. O *compliance* deve ser envolvido, visto que determinadas informações não podem ser eliminadas em razão de obrigação legal ou regulatória. Assim, após a análise conjunta e o cumprimento/negativa da solicitação, o titular deverá ser informado por e-mail da conclusão do pedido.

Informação das entidades privadas com as quais o controlador realizou uso compartilhado de dados[34]. Caso o investidor solicite essas informações, é importante que sejam transmitidas exatamente conforme solicitadas pelo titular.

Informação sobre a possibilidade de não fornecer consentimento e a respeito das consequências da negativa[35].

Revogação do consentimento. Se o titular revogar o consentimento do compartilhamento de dados, o relacionamento será encerrado imediatamente, porém, serão mantidos os dados pessoais objeto de obrigação legal e regulatória que possam, porventura, ser requeridos pelos órgãos reguladores, autorreguladores e autoridades judiciais[36].

Revisões de decisões tomadas com base em tratamento automatizado de dados pessoais, incluídas as destinadas a definir o perfil pessoal ou de crédito (*suitability*). A revisão, após solicitada, pode ser feita de forma automatizada já que não há exigência da LGPD para que uma pessoa natural revise as informações. Assim, o sistema que "errou" informará ao investidor os critérios utilizados (sem revelar informações que acarretem a continuidade e o segredo do negócio). Diante disso, ele poderá questionar as informações apresentadas, e se for necessário, as bases e o resultado serão alterados.

---

[33] Comunicações deverão ser elaboradas pelo *compliance.*
[34] Comunicações deverão ser elaboradas pelo *compliance.*
[35] Comunicações deverão ser elaboradas pelo *compliance.*
[36] Comunicações deverão ser elaboradas pelo *compliance*. Destacam-se aqui as informações requeridas pelo Anexo 11-A da ICVM n. 617 e artigo 10 da ICVM n. 539.

Respeitando os princípios da LGPD, conforme o art. 6º, em especial os da necessidade e da finalidade, e os arts. 7º, 8º e 9º, caberá à gestora coletar dados pessoais das pessoas físicas que optarem por investir em fundos próprios nos quais a gestora figure como distribuidora.

Conforme o Anexo 11-A da Instrução 617 da CVM, o gestor-distribuidor tem a obrigação de coletar determinados dados pessoais dos investidores pessoa física. Em razão disso, ao iniciar o relacionamento, o investidor é submetido ao termo de ciência, no qual será indicada detalhadamente a razão legal e técnica para colher aquelas informações, além de informar com quais instituições os dados serão compartilhados e o motivo dessa conduta.

Importante também salientar que os dados deverão ser mantidos no arquivo da gestora por pelo menos 5 anos, conforme os arts. 31, 10 e 26, respectivamente das Instruções n. 558, n. 539 e n. 617 da CVM. Ademais, poderão ser compartilhados com órgãos judiciais, regulatórios e autorregulatórios (art. 7º, VI, da LGPD).

Corroboram ainda com os levantamentos, o primeiro comunicado da CVM referente à matéria, em Ofício-Circular n. 4/2020-CVM/SMI-SIN – Rio de Janeiro, de 11 de dezembro de 2020. Sua redação indica que as previsões contidas na Lei n. 13.709/2018 (“Lei Geral de Proteção Dados”) esclarecem que o agente, no caso, a gestora, possui mandato para a eventual prospecção de informações adicionais, fundamentando para isso que a utilização desses insumos por parte da pessoa obrigada não deve, para efeitos da Prevenção à Lavagem de Dinheiro e ao Financiamento de Terrorismo (“PLDFT”), ultrapassar o escopo das Leis n. 9.613/1998, n. 13.260/2016 e n. 13.810/2019.

Além disso, o titular dos dados poderá, a qualquer tempo, revogar seu consentimento para compartilhar as informações. No caso da gestora, os dados necessários serão armazenados, mas o relacionamento será encerrado no mesmo momento.

4.3 Departamento jurídico

No que tange ao tema da LGPD, o departamento é responsável por mapear os contratos firmados antes do início da vigência da lei e atualizá-los, se for o caso, além de inserir uma cláusula sobre o tema conforme o escopo de cada contrato.

Após a vigência da LGPD, todos os contratos firmados entre a gestora e os

parceiros, especialmente aqueles cujo objeto envolve o compartilhamento de dados pessoais, possuem uma cláusula de aderência e de compartilhamento da Lei. Entretanto, a prática não obsta o envolvimento do *compliance* nos processos de *due dilligence*, tanto no caso de participantes do mercado, como nas demais empresas.

De forma breve, visto que o assunto será abordado no departamento de *compliance*, a diligência também se presta a encontrar notícias desabonadoras e eventuais práticas que infringem a proteção de dados conforme regulamentada pela legislação.

Particularmente, os contratos cujos fundos figurem como parte, devem ser elaborados e assinados em conjunto com o administrador do fundo, por conta das previsões constantes nas Instruções n. 356 e n. 555 da CVM.

4.4 Departamento de tecnologia da informação (TI) e *cybersegurança*

Em que pese as medidas implementadas para evitar o vazamento de dados pessoais, todos os controladores e operadores de dados pessoais estão sujeitos a incidentes de vazamento de dados, portanto, devem manter um plano de resposta[37] que apresente as ações a serem praticadas nessas situações.

O departamento de tecnologia da informação e *cybersegurança*, em conjunto com o departamento de *compliance*, serão os responsáveis pela manutenção e pela atualização do plano, especificando seus riscos, prazos e ações a serem executadas se houver incidente de vazamento de dados, observando que em até 72 horas do evento, o responsável como encarregado[38] comunicará os titulares dos dados vazados e a ANDP sobre o episódio, indicando eventuais riscos decorrentes.

Para minimizar a ocorrência de incidentes, são adotadas medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situação acidental ou ilícita de destruição, perda, alteração, comunicação ou qualquer outra forma de tratamento inadequado ou ilícito dos dados pessoais.

Apenas para reforçar a ideia, todos os colaboradores cujas atividades são envolvidas diretamente na obtenção, tratamento e análise dos dados pessoais devem ser submetidos a treinamentos sobre o tema.

---

[37] BRASIL. Lei n. 13.709/2018. Lei Geral de Proteção de Dados. Art. 50, I, “g”.
[38] BRASIL. Lei n. 13.709/2018. Lei Geral de Proteção de Dados. Art. 5º, VIII.

4.5 Departamento de processamento de dados e inteligência de negócio

Contando com o apoio do departamento de *compliance*, o departamento de processamento de dados assegurará a aderência de todos os processos envolvendo dados pessoais de investidores dos fundos de investimento sob distribuição, especialmente no que tange aos prazos de armazenamento dispostos na regulação e na autorregulação, nos arts. 31, 10 e 26, das Instruções n. 558, n. 539 e n. 617, respectivamente, da CVM.

Considerando a previsão da LGPD, o departamento em questão será responsável pelos processos internos que irão controlar os prazos de armazenamento dos dados pessoais, visando cumprir estritamente os prazos das obrigações legais e regulatórias e do requerido pelo titular no caso de revogação de consentimento.

No caso da gestora que atuar com operações de crédito na atividade de inteligência de negócio, como por exemplo, a prática de monitoramento de *credit scoring*, estará autorizada a operar nos limites da legislação pertinente.

Para Viviane Nóbrega Maldonado e Renato Opice Blum[39], nesse caso, o processo de análise de crédito e o uso de dados pessoais estão fundamentados em lei setorial, argumento exposto em recurso especial do Superior Tribunal de Justiça:

> O STJ já decidiu que a prática de *credit scoring* é lícito, desde que na avaliação do risco de crédito sejam respeitados os limites estabelecidos pelo sistema de proteção do consumidor no sentido da tutela da privacidade e da máxima transparência nas relações negociais, devendo ser a ele fornecidos esclarecimentos, caso solicitados, acerca das fontes dos dados considerados (histórico de crédito), bem como as informações pessoais valoradas[40].

Neste sentido, recomenda-se o monitoramento contínuo das eventuais diretrizes e normativas pelas autoridades do mercado financeiro quanto às melhores práticas de análise de crédito no que tange à utilização de dados pessoais de terceiros.

4.6 Departamento de *compliance* e/ou controles internos

O departamento de *compliance* deve mapear e identificar quais são os departamentos mais expostos à coleta, tratamento e armazenamento dos dados

---

[39] MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **LGPD** – Lei Geral de Proteção de Dados Pessoais comentada. São Paulo: RT, 2019, p. 47.

[40] BRASIL. Superior Tribunal de Justiça. Recurso Especial 1419697-RS, 2ª Seção, Rel. Min. Paulo de Tarso Sanseverino, j. 12-11-2014.

pessoais. Na sequência, criar um plano de ação que, posteriormente, será encaminhado aos departamentos sensíveis, além de treinar os colaboradores de acordo com o nível de exposição.

Sugerimos a criação de uma política[41] que defina as principais diretrizes, independentemente do nível de exposição das áreas, sugestão explorada por Viviane Nóbrega Maldonado e Renato Opice Blum na forma de "medidas administrativas"[42].

Porém, a atuação do *compliance* se estende, não somente com a gestão das práticas mencionadas, mas por meio do auxílio direto aos colaboradores que eventualmente possuírem algum questionamento, e no contato com os titulares dos dados pessoais que podem solicitar o expurgo dos seus dados ou trazer questionamentos suplementares.

O *compliance* também deve buscar a aderência e o cumprimento das referidas normas na realização das diligências em relação aos parceiros (KYP[43] e DDQ[44]), nas quais são observados notícias e processos que possam ter ligação com o descumprimento de normas relativas à proteção de dados.

No exercício de suas funções, como a área de *compliance* também lida com dados pessoais, tanto na análise de perfil de investidor (KYC[45]) como na análise dos possíveis novos colaboradores (KYE[46]), suas equipes devem realizar cursos relacionados ao tema, o que possibilita que os dados sejam analisados para o único fim a que foram obtidos, nesses casos, atribuir risco ao perfil do investidor e aprovar o perfil do colaborador.

Por fim, destacamos o desafio da área de *compliance* nesta seção. Eduardo Montenegro Dotta[47] ressalta em sua obra um trabalho elaborado por Amanda Gouvêa

---

[41] "Políticas representam aquilo que a direção quer que a organização faça"; "[...] política é um instrumento de grande utilidade para dar orientação consistente e uniforme na busca dos objetivos". RODRIGUES, Sérgio. **Sistemas de informação**: um enfoque gerencial. Edgard Bruno Cornachione Jr. (colab.) 2. ed. São Paulo: Atlas, 2017, p. 64.

[42] "São exemplos de medidas administrativas: políticas corporativas para proteção de dados pessoais, contratos de confidencialidade, políticas de privacidade de *sites* e aplicativos, capacitação dos empregados cujas atividades envolvam o tratamento de dados pessoais, controle de acesso aos arquivos físicos, entre outras". MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **LGPD** – Lei Geral de Proteção de Dados Pessoais comentada. São Paulo: RT, 2019, p. 47.

[43] *Know Your Partner* no contexto de PLDFT e Boas Práticas de Governança.

[44] *Due Diligence Questionnaire* no contexto de PLDFT e Boas Práticas de Governança.

[45] *Know Your Client or Customer* no contexto de PLDFT e Boas Práticas de Governança.

[46] *Know Your Employee* no contexto de PLDFT e Boas Práticas de Governança.

[47] BARRETO, Amanda Gouvêa Toledo. *Regtechs* e fundos de investimentos disciplinados pela Instrução CVM n. 555/2014 *apud* DOTTA, Eduardo Montenegro. **Responsabilidade civil dos administradores e gestores de fundos de investimento**. São Paulo: Almedina, 2018.

Toledo Barreto que tem como foco da discussão o uso de *regtechs*.

Parafraseando Amanda, o autor destaca "a ampliação do desafio de *compliance* imposto aos administradores e gestores de fundos de investimento, seja para a manutenção de controles simples até funções mais complexas" como o desafio de *compliance* na adequação das empresas à Lei Geral de Proteção de Dados Pessoais.

4.7 O papel do *compliance* na adequação das empresas à LGPD – uma experiência pessoal

Este subcapítulo tem por objetivo apresentar e fundamentar a importância do papel de *compliance* como promotor e garantidor na adequação dos processos na atividade das empresas em conformidade com a nova Lei Geral de Proteção de Dados.

As áreas de tecnologia e de sistemas da informação (TI) e de negócios têm papel fundamental na adequação às novas regras, uma vez que os sistemas, em muitos casos, deverão ser atualizados. No entanto, a área de *compliance* deve estar presente em todas as etapas de adequação e, posteriormente, no monitoramento das regras de negócio e respectiva conformidade com a LGPD.

A seguir, nosso intuito é fundamentar o posicionamento acima, com base em material de pesquisa, de ampla acreditação no âmbito de governança corporativa e *compliance*; por fim, apresentaremos caso prático da nossa experiência profissional.

A palavra *compliance*, quando traduzida do inglês para o português, tem o significado amplamente aceito de "conformidade", cujo verbo objetiva estar em conformidade com uma ordem, uma regra ou uma solicitação. Quando o termo é associado ao universo corporativo, passou a representar uma função fundamental na atividade das empresas, principalmente àquelas que seguem os princípios mais modernos de governança corporativa[48] promovidos pelo Instituto Brasileiro de Governança Corporativa (IBGC) de atender aos acionistas, ponderando os interesses de outros grupos de *stakeholders*, considerando como critério o valor da empresa no longo prazo.

Neste contexto, o *compliance* tem a função organizacional de promover a "conformidade com os seus princípios e valores, refletidos em políticas, procedimentos e normas internas, e com as leis e os dispositivos regulatórios a que

[48] IBGC. **Instituto Brasileiro de Governança Corporativa**. Código das melhores práticas de governança corporativa 5. ed. São Paulo, SP: IBGC, 2015, p. 20.

esteja submetida”[49]. Portanto, o gerenciamento de ações relacionadas em conformidade com a legislação vigente e normas internas e externas, num sistema de governança efetivo, deve estar submetido à coordenação da área de *compliance*.

Por fim, conforme proposta inicial, apresentamos um exemplo prático na forma de experiência própria, alcançada em âmbito profissional, cuja empresa atua como administradora de carteiras de fundos de investimentos nos termos da Instrução CVM n. 558/2015. Numa reunião de trabalho com as equipes de negócio, TI e *compliance*, verificamos que os profissionais desta equipe multidisciplinar atingiram a eficácia necessária para resolver alguns desafios trazidos pela LGPD, como a necessidade de eliminar[50] e de anonimizar[51] dados pessoais de clientes que encerraram o seu ciclo de relacionamento com a empresa, e que não haviam consentido[52] a nenhum dispositivo que mantivesse seus dados e informações, anteriores à vigência da lei, por tempo indeterminado.

Neste caso, a solução proposta pelas áreas de TI com a anuência da equipe de negócios foi eliminar os dados dos clientes inativos. No entanto, a área de *compliance*, presente na reunião, alertou sobre a obrigação legal e regulamentar de manter os dados de identificação dos clientes, por no mínimo 5 anos. Diante disso, o que de fato poderia ser praticado naquela circunstância era uma anonimização parcial, para preservar as obrigações previstas na LGPD sem violar a legislação[53] e demais normativas de PLDFT.

---

[49] IBGC. **Instituto Brasileiro de Governança Corporativa**. Código das melhores práticas de governança corporativa 5. ed. São Paulo, SP: IBGC, 2015, p. 20.

[50] BRASIL. **Lei n. 13.853, de 14 de agosto 2019**. Altera a Lei n. 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Artigo 5º, X, que dispõe sobre a definição de eliminação de dados pessoais.

[51] BRASIL. **Lei n. 13.853, de 14 de agosto 2019**. Altera a Lei n. 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências; Artigo 5º, XI, que dispõe sobre definição de anonimização de dados pessoais.

[52] BRASIL. **Lei n. 13.853, de 14 de agosto 2019**. Altera a Lei n. 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Artigo 5º, XII, que dispõe sobre consentimento ao tratamento de seus dados pessoais.

[53] BRASIL. **Lei n. 9.613, de 3 de março de 1998**. Dispõe sobre os crimes de “lavagem” ou ocultação de bens, direitos e valores; a prevenção da utilização do sistema financeiro para os ilícitos previstos nesta Lei; cria o Conselho de Controle de Atividades Financeiras – COAF, e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9613.htm. Acesso em: 31 out. 2019.

5 CONCLUSÃO

Conforme visto na introdução e no panorama geral deste artigo, a proteção de dados se tornou um tema popular, comum na agenda mundial, gerando efeitos diretos na legislação brasileira através da concretização da LGPD. Não obstante, as gestoras de fundos de investimentos, que apesar de atuarem sobre rígidos normativos e princípios éticos inspirados na experiência internacional, devem considerar a nova legislação como parte dos seus deveres fiduciários.

A lei impõe mudança de cultura aos agentes que atuam como controladores e operadores, mudança essa que deverá nortear a atividade de tratamento de dados pessoais com base nos princípios da transparência e do respeito à vontade dos titulares, agindo além da sua conveniência. A lei ainda prevê o respeito à livre iniciativa, à inovação, ao empreendedorismo, aos investimentos de pesquisa e ao desenvolvimento e segredos de negócio, desde que os agentes controladores e operadores atuem conforme os contornos da LGPD.

Sobretudo, evidenciamos que a LGPD, em sua compreensão meramente teórica, não esgota os métodos e os processos que devem ser utilizados pelos agentes para atender aos requisitos em ações objetivas e cumprir as determinações legais. Neste sentido, este artigo torna-se uma relevante referência para este nicho específico de empresas, qual seja, as gestoras de fundo. Elas poderão atuar minimamente na proposta de adequação apresentada aos processos mais comuns com base nos indicativos desse trabalho.

A despeito dessa relevância, o papel da área de *compliance* é fundamental neste processo. No entanto, as empresas não devem se limitar em promover a participação do *compliance* nos grupos de trabalho para conduzir o diagnóstico e o plano de ação visando imediata adequação. O *compliance* deverá também orientar os recursos necessários à atividade da área para rever seus códigos de ética e de conduta, programas de treinamento direcionados aos colaboradores e promover efetivamente junto à cultura e aos valores da empresa os princípios da LGPD em seus negócios.

Por fim, destacamos a importância de os obrigados monitorarem as futuras normativas emitidas pela autoridade nacional de proteção de dados (ANPD), normativas da CVM e autorregulação da ANBIMA, todas dirigidas ao setor em que atuam as gestoras. Isto porque estas instituições, conforme vimos no início desse

artigo, podem determinar novos padrões técnicos de segurança da informação a serem perseguidos e implementados nas gestoras de fundos de investimento.

REFERÊNCIAS

ABELHA, André; GOMIDE, Alexandre Junqueira. A aplicação da Lei n. 13.709/2018 (Lei Geral de Proteção de Dados – LGPD) aos condomínios edilícios. **Site Migalhas**. Disponível em: https://www.migalhas.com.br/Edilicias/127,MI300087,71043-A+aplicacao+da+lei+137092018+Lei+Geral+de+Protecao+de+Dados+LGPD+aos. Acesso em: 15 ago. 2019.

ANBIMA. **Estatuto Social da ANBIMA** – Associação brasileira das entidades dos mercados financeiros e de capitais. 2018. Disponível em: https://www.anbima.com.br/data/files/A3/E7/F0/A6/4FC575106582A275862C16A8/Estatuto_20ANBIMA_1_.pdf. Acesso em: 15 ago. 2019.

BRASIL. **CVM e MPF prorrogam Termo de Cooperação Técnica**. Disponível em: http://www.cvm.gov.br/noticias/arquivos/2018/20180626-1.html. Acesso em: 15 ago. 2019.

CÓDIGO ANBIMA. **Regulação e melhores práticas para administração de recursos de terceiros**. Disponível em: https://www.anbima.com.br/pt_br/autorregular/codigos/administracao-de-recursos-de-terceiros.htm. Acesso em: 15 ago. 2019.

COELHO, Gabriela. **MP-DF pede a condenação de banco por vazamento de dados pessoais de clientes**. 2018. Disponível em: https://www.conjur.com.br/2018-jul-31/mp-df-condenacao-banco-vazamento-dados-pessoais. Acesso em: 15 ago. 2019.

DATT, Felipe. **Mercado se adapta às novas exigências**. 2019. Disponível em: https://www.valor.com.br/financas/6316209/mercado-se-adapta-novas-exigencias. Acesso em: 15 ago. 2019.

DOTTA, Eduardo Montenegro. **Responsabilidade civil dos administradores e gestores de fundos de investimento**. São Paulo: Almedina, 2018.

FRAZÃO, Ana. **A nova Lei Geral de Proteção de Dados Pessoais**. Publicado em: 13-12-2018. Disponível em: http://anafrazao.com.br/files/publicacoes/2018-12-13-A_nova_Lei_Geral_de_Protecao_de_Dados_Pessoais_Principais_repercussoes_para_a_atividade_empresarial_controversias_em_torno_do_direito_a_explicacao_e_a_oposicao_diante_de_decisoes_totalmente_automatizadas_Parte_XVI.pdf. Acesso em: 15 ago. 2019.

IBGC. **Instituto Brasileiro de Governança Corporativa**. Código das melhores práticas de governança corporativa. 5. ed. São Paulo, SP: IBGC, 2015.

INSPER. LL.M. **Direito dos mercados financeiro e de capitais**. Disponível em: https://www.insper.edu.br/pos-graduacao/direito/direito-dos-mercados-financeiro-e-de-capitais/. Acesso em: 16 ago. 2019.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **LGPD** – Lei Geral de Proteção de Dados Pessoais comentada. São Paulo: RT, 2019.

MALDONADO, Viviane Nóbrega. **LGPD**: Lei Geral de Proteção de Dados Pessoais – manual de implementação. São Paulo: RT, 2019.

MONTEIRO, Renato Leite. **Lei Geral de Proteção de Dados do Brasil (LGPD)**. Disponível em: https://igarape.org.br/wp-content/uploads/2018/12/Existe-um-direito-a-explicacao-na-Lei-Geral-de-Protecao-de-Dados-no-Brasil.pdf. Acesso em: 15 ago. 2019.

MUKINICKA, Rosana. Você está em *compliance* com a LGPD? **O Estado de S. Paulo**, 2018. Disponível em: https://politica.estadao.com.br/blogs/fausto-macedo/voce-esta-em-compliance-com-a-lgpd/. Acesso em: 15 ago. 2019.

OLIVEIRA, Ricardo; COTS, Marcio. **Lei Geral de Proteção de Dados Pessoais comentada**. São Paulo: RT, 2018.

PINHEIRO, Patricia Peck. **Proteção de dados pessoais** – comentários à Lei n. 13.709/2018 LGPD. São Paulo: Saraiva Educação, 2018 (*ebook*).

RODRIGUES, Sérgio. **Sistemas de informação**: um enfoque gerencial. Edgard Bruno Cornachione Jr. (colab.) 2. ed. São Paulo: Atlas, 2017.

SETTI, Rennan. **Condenados na CVM, crimes de informação privilegiada chegam pouco à Justiça**. 2019. Disponível em: https://oglobo.globo.com/economia/condenados-na-cvm-crimes-de-informacao-privilegiada-chegam-pouco-justica-22394865. Acesso em: 15 ago. 2019.

UNIÃO EUROPEIA. Regulação (EU) 2016/679, de 27 de abril de 2016. Regulação Geral de Proteção de Dados. Disponível em: https://gdpr-info.eu/. Acesso em: 2 fev. 2021.

Legislação

BRASIL. **Lei n. 13.853, de 14 de agosto de 2019**. Altera a Lei n. 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13853.htm. Acesso em: 14 ago. 2019.

BRASIL. **Lei n. 6.385, de 7 de dezembro de 1976**. Dispõe sobre o mercado de valores mobiliários e cria a Comissão de Valores Mobiliários. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L6385compilada.htm. Acesso em: 15 ago. 2019.

BRASIL. **Lei n. 9.613, de 3 de março de 1998**. Dispõe sobre os crimes de “lavagem” ou ocultação de bens, direitos e valores; a prevenção da utilização do sistema financeiro para os ilícitos previstos nesta Lei; cria o Conselho de Controle de Atividades Financeiras – COAF, e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9613.htm. Acesso em: 31 out. 2019.

Referências normativas

ABNT NBR 6023: 2018 – Informação e documentação – Referências – elaboração

ABNT NBR 6022:2018 – Informação e documentação – Artigo em publicação periódica técnica e/ou científica – Apresentação

ABNT NBR 6027: 2012 – Informação e documentação – Informação e documentação – Sumário – Apresentação

ABNT NBR 14724: 2011 – Informação e documentação – Trabalhos acadêmicos – Apresentação

ABNT NBR 15287: 2011 – Informação e documentação – Projetos de pesquisa – Apresentação

ABNT NBR 6034: 2005 – Informação e documentação – Índice – Apresentação

ABNT NBR 12225: 2004 – Informação e documentação – Lombada – Apresentação

ABNT NBR 6024: 2003 – Informação e documentação – Numeração progressiva das seções de um documento escrito – Apresentação

ABNT NBR 6028: 2003 – Informação e documentação – Resumo – Apresentação

ABNT NBR 10520: 2002 – Informação e documentação – Citações em documentos – Apresentação

INSPER. **Manual para elaboração de trabalhos**. Biblioteca Telles (s/d). Disponível em: http://arquivos.insper.edu.br/downloads/2021/biblioteca/manual_normalizacao_abnt.pdf. Acesso em: 07 jun. 2021.