

E-BOOK PROTEÇÃO DE DADOS PESSOAIS

Temas em Destaque

Comissão de Privacidade e Proteção de Dados Pessoais



COORDENAÇÃO: Carolina Martins Pinto | Ivonaldo da Silva Mesquita
Apresentação: Ivonaldo da Silva Mesquita



2023

Editorial

Diretoria da Seccional Piauiense (Gestão 2022/2024)

Presidente: Celso Barros Coelho Neto
Vice-presidente: Daniela Carla Gomes Freitas
Secretária Geral: Raylena Vieira Alencar Soares
Secretário Geral Adjunto: Audeiri Martins Carneiro Filho
Diretor Tesoureiro: Marcus Vinícius de Queiroz Nogueira

CONSELHEIROS SECCIONAIS

Maria Fernanda Brito Do Amaral
Maria Da Conceição Carcará
Kadmo Alencar Luz
Damásio de Araújo Sousa
Alexandre Augusto Batista de Lima
Herval Ribeiro
Hilbertho Luis Leal Evangelista
William Palha Dias Netto
Shardenha Maria Carvalho Vasconcelos
José Sérgio Torres Angelim
Thiaga Leandra Alves Ribeiro Learth
Astrobaldo Ferreira Costa
Mauro Benício Da Silva Júnior
José Urtiga de Sá Júnior
Luciano José Linard Paes Landim
Dione Cardoso De Alcântara
Francisca Juliana Castello Branco Evaristo de Paiva
Andréa Bandeira Paz
Andreya Lorena Santos Macêdo
Graciane Pimentel de Sousa
Myrthes Barreira dos Reis
Wilson Spindola Rodrigues Silva
James Araújo Amorim
Justina Vale de Almeida
Juliana Oliveira Soares
Marenize Leite Macena
Antônio Augusto Pires Brandão
Raíssa Mota Ribeiro
Ariane Caiane Melo Mota
Carlos Washington Cronemberger Coelho
Edvaldo Oliveira Lobão
Hamilton Ayres Mendes Lima Júnior
Carolina Lamarca Leal Areias
Sílvia Cristina Carvalho Sampaio Santana
Cheyla Maria Paiva Ferraz Ponce
Cleiton Aparecido Soares da Cunha
Adriano Silva Borges
Luiz Mário de Araújo Rocha
Darlan da Rocha Martins
Luíza Virgínia Macêdo Sales
Francisco de Sousa Vieira Filho
Jedean Gericó de Oliveira
Ravana Medeiros Costa Soares Basílio
Rafael Orsano de Sousa
Karolínna Vasconcelos Pereira
Mara Raylane De Sousa Reis
Rafael Fonseca Lustosa
Jhon Kennedy Teixeira Lisbino
Williams Cardec da Silva
Denize de Maria Dias Gomes e Silva
Luiz Alberto Ferreira Júnior
Silvânia Maria Luz Leal
Aureliano Marques Da Costa Neto
François Lima de Barros
Beatriz de Sousa
Ruan Oliveira Leal
Danielle dos Santos Araripe
Lady Kelly Câmara Lemos de Santana Terto
Alexia Leal de Carvalho Torres
Mayza Allen Lopes Cerqueira Amorim
Marineri Alves de Sousa

CONSELHO FEDERAL

Élida Fabrícia Oliveira Machado Franklin
Shaymmon Emanuel Rodrigues de Moura Sousa
Carlos Augusto de Oliveira Medeiros Júnior
Jamyllé Torres Viana Vieira de Alencar Leite Lima
Isabella Nogueira Paranaguá de Carvalho Drummond

DIRETORIA ESAPI

Diretor Geral
Thiago Anastácio Carcará
Vice-Diretora
Leda Maria Eulálio Dantas Luz Costa
Diretor Administrativo
Ivonaldo da Silva Mesquita
Diretora de Ensino
Marcele Roberta Pizzato
Diretora Acadêmica
Ravana Medeiros Costa Soares Basílio
Diretor Pesquisa de Pós-Graduação
Fabrício de Farias Carvalho
Diretor de Eventos e Relações Institucionais
Jhon Kennedy Teixeira Lisbino
Diretor de Interiorização das Ações da Escola
Johilse Tomaz da Silva

CONSELHO SUPERIOR

José Augusto de Carvalho Mendes Filho
Patrícia Caldas Meneses Pires Ferreira
Roberto Cajubá da Costa Britto
Joseli Lima Magalhães

COORDENADORES ESAPI

Coordenador da Residência Jurídica
Thiago Edirsandro Albuquerque Normando
Coordenadores do Curso de Iniciação à Advocacia
Sílvia Cristina Carvalho Sampaio Santana
Aurélío Lobão Lopes
Coordenadora de Eventos
Michelle Thamyles Melo Abath
Coordenadores de Pesquisa
Gesio de Lima Veras
Cassio Luz Pereira
Coordenadora de Comunicação
Samila Barbosa Milhomem
Coordenador de Interiorização das Ações da Escola
Daniel da Costa Araújo
Coordenador de Atividades de Extensão
Frank Lucio Dantas Noronha
Coordenadora de Biblioteca e Salas de Estudos
Nayara Figueiredo de Negreiros
Coordenadores das Ferramentas Digitais da Advocacia
Helldânio Muniz Barros
Coordenador de Relações Institucionais
Howzembergson de Brito Lima
Coordenador de Altos Estudos da Advocacia
Antônio Augusto Pires Brandão
Coordenador de Programa de Interface da Advocacia
Berilo Pereira da Motta Neto
Coordenador de Ações para Jovem Advocacia
Alina Menezes
Coordenadora de Ações para Mulher Advogada
Letícia dos Santos Sousa
Coordenadora de Pós-Graduação
Vitória Andressa Loiola dos Santos
Coordenador de Ensino
Victor Hugo Leal Silva
Coordenador de Memória e Cultura
Jose Augusto Lima Nery Barbosa

DIRETORIA CAAPI

Presidente
Talmy Tércio Ribeiro da Silva Júnior
Vice- Presidente
Maria Dalva Fernandes Monteiro
Secretária Geral
Ravennya Muara Oliveira Silveira Moreira
Secretaria Geral Adjunta
Jória Maria Batista Nunes Soares
Tesoureiro
Josélio Sálvio Oliveira
Suplentes Diretoria
Gerson Luciano Damasceno de Moraes
Manuela Veras Coimbra Maciel
Conselho Fiscal
Glaylorlane Soares Silva
José Vagner Fonseca Nunes Filho
Lucas Matheus Resende Feitosa
Suplente Conselho Fiscal
Francisca Fábria Viana Monteiro

CONSELHO EDITORIAL

Editores Chefe: Carolina Martins Pinto | Ivonaldo da Silva Mesquita

Editora: EDITORA OAB

Design Editorial: Letícia Florêncio

CONSELHO EDITORIAL

Presidente Executivo - Nestor Alcebíades Mendes Ximenes

Conselheiros

Leandro Cardoso Lages

Adriana Castelo Branco de Siqueira

Alexandre Augusto Batista de Lima

José Octávio de Castro Melo

Ana Letícia Sousa Arraes de Resende

Dados Internacionais de Catalogação na Publicação (CIP) (Câmara Brasileira do Livro, SP, Brasil)

P659p Pinto, Carolina Martins.
E-Book Proteção de Dados Pessoais: temas em destaque. /
Carolina Martins Pinto, Ivonaldo da Silva Mesquita. – Teresina:
OAB-PI, 2023.
26 f.; Il.

ISBN: 978-65-00-87720-5.

1. LGPD. 2. Proteção de dados. 3. Privacidade. 4. Dados
pessoais. 5. OAB-PI. I. Título.

CDD 342.721

Bibliotecário Responsável: Rogério Cunha Teixeira (CRB-3/1077)



Comissão de
Privacidade e
Proteção de Dados

COMISSÃO DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

Carolina Martins Pinto
Presidente

Michelle Thamyles Melo Abath
Vice-Presidente

Bruno Osires Batista Barbosa e Silva
Secretário

Ana Dulce Ribeiro Gonçalves Rehem
Secretária Adjunta

Membros

Arielly Vitória Dantas Peres da Silva
Catarina Queiroz Feijó

Francisco Soares Campelo Filho
Gisela Carvalho de Freitas

Jasmina Bucar Barjud da Costa
Joaquim José da Silva Xavier Neto

Lairys Grazielle Bezerra de Oliveira
Lana Patrícia Vieira de Sousa

Mirlla Wladia Martins Cavalcante
Marcos Luiz da Silva Filho

Polyana Oliveira Eckhardt
Raryssa Nogueira do Nascimento

Rodrigo Lira

Samira Maria de Carvalho Leite
Victória Bezerra Roque da Silva

Victória Hellen Nascimento Oliveira
Wilton Gutemberg da Cruz Pires Júnior

Sumário

- 06 **APRESENTAÇÃO**
Ivonaldo da Silva Mesquita
- 09 **LGPD, GOVERNANÇA E ESG**
Carolina Martins Pinto
- 11 **A IMPORTÂNCIA DA LEI GERAL DE PROTEÇÃO DE DADOS -LGPD- NOS SINDICATOS**
Ana Dulce Rehem
- 13 **A ADEQUAÇÃO À LGPD SOB A ÓTICA DA REGULAMENTAÇÃO DA ANPD-RESOLUÇÃO CD/ANPD Nº 4**
Bruno Osires Batista Barbosa e Silva
- 16 **LGPD NO ÂMBITO DAS RELAÇÕES CONSUMERISTAS**
João Vitor Silva Macêdo
- 18 **PROTEÇÃO DE DADOS APLICADA À ÁREA DE SAÚDE: O PROCESSO DE ANONIMIZAÇÃO NO TRATAMENTO DE DADOS CLÍNICOS**
Raryssa Nogueira do Nascimento
- 20 **LEI GERAL DE PROTEÇÃO DE DADOS (13.709/18) – A NÃO APLICAÇÃO DA LGPD**
Rodrigo Lira
- 22 **AS REDES SOCIAIS E O CONSTANTE COMPARTILHAMENTO DE DADOS: UM RISCO A SUA PRIVACIDADE**
Victória Hellen Nascimento Oliveira
- 24 **A LGPD E A BASE LEGAL PARA EXECUÇÃO DE CONTRATO**
Arielly Vitória Dantas Peres da Silva

Apresentação

Coube-me a honrosa tarefa de apresentar esta Cartilha organizada pela Comissão de Privacidade e Proteção de Dados da Ordem dos Advogados do Brasil – Secção Piauí, sob a presidência da Advogada Carolina Martins Pinto, intitulada “Cartilha de Privacidade e Proteção de Dados”. Antes de discorrer com brevidade sobre a obra, apresso-me em afirmar que um novo trabalho que tem a digital da Advogada Carolina Martins Pinto é sempre um acontecimento no mundo jurídico, haja vista que ela desponta como uma intelectual de escol bastante respeitada entre seus pares. Honesta, ética, amiga, responsável, sempre cultuou bons hábitos. A obra mostra que ela construiu o caminho de passagem, como organizadora e coautora, para as letras dos membros de referida Comissão que se tornaram os seus coautores e dão seu brilho ao trabalho escrito.

A Cartilha organizada pela Comissão de Privacidade e Proteção de Dados da OAB-PI é bastante inovadora no mundo jurídico, pois enfrenta temas e institutos recorrentes do ramo do Direito Digital, apropriando-se de uma metódica conhecida como “resumo expandido”. Em uma forma mais aprofundada, insista-se em dizer que, o objeto de análise perfilhado pelo trabalho é, indubitavelmente, a Lei nº 13.709/2018 - Lei Geral de Proteção de Dados (LGPD). Levando-se em conta esse objeto a obra enfrentou vários impactos da lei em diversos âmbitos. Inicialmente, Carolina Martins Pinto, apresenta uma correlação tríade: “LGPD, Governança e ESG”, apontando que as organizações públicas ou privadas devem priorizar a LGPD na sua governança, visando construir uma nova consciência corporativa e novos modelos empresariais, pautados no compliance proativo de dados. Em seguida, Ana Dulce Rehem aborda a importância da LGPD nos Sindicatos, advertindo-os para uma revisão de suas práticas de coleta e tratamento de dados pessoais. Bruno Osires Batista Barbosa e Silva, no seu articulado “A Adequação à LGPD sob a ótica da Regulamentação da ANPD - Resolução CD/ANPD Nº 4”, comenta o regulamento de dosimetria e aplicação de sanções administrativas da ANPD. Já o impacto da LGPD no âmbito das relações consumerista coube a João Vitor Silva Macêdo alertando para os cuidados que as empresas devem ter como os dados colhidos dos consumidores. Raryssa Nogueira do Nascimento, por sua vez, traça um panorama do impacto da LGPD na área de saúde evidenciando “O Processo de Anonimização no Tratamento de Dados Clínicos”. Rodrigo Lira relaciona

determinadas situações que estão excepcionadas na coleta de dados que não traz riscos à privacidade do indivíduo. No tocante às redes sociais, Victória Hellen Nascimento Oliveira, analisa os constantes compartilhamentos de dados e os riscos à privacidade. E, finalmente, Arielly Vitória Dantas Peres da Silva, leciona “A LGPD e a Base Legal para Execução de Contrato, ou seja, justificativas e argumentos que devem ser utilizados como fundamento pelas empresas para legitimar o tratamento e o uso dos dados pessoais, sobretudo, daquelas informações envolvendo os dados pessoais do contrato de trabalho. Desta feita, o leitor terá a oportunidade de seguir uma verdadeira jornada envolvente que debate o “novo” direito fundamental individual à proteção dos dados, insculpido no art. 5º, LXXIX, da Constituição Federal.

Afirmo que, com a Cartilha da Comissão, o meio jurídico e a sociedade foram muitíssimos agraciados. Minha percepção sinóptica é que nasceu a “Cartilha de Privacidade e Proteção de Dados” numa conjunção da simplicidade da linguagem clara, coesa e sem hermetismo, mas sem perder o tecnicismo próprio do Direito. A obra pode e deve ser considerado um verdadeiro manual de consulta e aprendizagem, dado tratar-se daqueles tipos de cartilhas que conversam conosco.

Ivonaldo da Silva Mesquita

Diretor Administrativo da ESA-PI
Coordenador da Pós-graduação em Direito Digital
e Proteção de Dados da ESA-PI
Advogado; Professor Universitário;
Mestre em Direito Constitucional (UNIFOR)



LGPD, GOVERNANÇA E ESG

Carolina Martins Pinto¹

A Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD) é a primeira norma brasileira dedicada, exclusivamente, ao tema da proteção de dados pessoais, dispondo sobre o tratamento de dados pessoais, inclusive nos meios digitais, realizado por pessoa natural ou por pessoa jurídica de direito público ou privado, trazendo, para tanto, uma ordem quanto a forma em que os dados de titulares precisam ser tratados dentro das organizações.

A cultura de proteção de dados pessoais, demanda em uma instituição, de forma reflexa, estratégias de governança, de ações transparentes ao público, para que estes possam atestar que a instituição oferece uma segurança “palpável”, garantindo que riscos sejam sanados ou mitigados, evitando, por consequência, quaisquer sanções administrativas e judiciais, bem como os demais impactos negativos que decorram da não observância das diretrizes legais.

Nesse sentido, as estratégias de governança a serem desenhadas além de instrumentalizar a LGPD, auxiliam na consolidação da sigla ESG dentro da organização.

Esse termo, que surgiu em 2004, em uma publicação do Pacto Global da ONU, e tem ganhado projeção e visibilidade no mercado nacional e internacional pode ser definido, de forma simples, pela tríade “Environmental, Social e Governance”, correspondendo às práticas ambientais, sociais e de governança, abrangendo, as práticas sustentáveis da organização, para que a mesma gere impactos ambientais positivos em consequência de suas práticas ou atividades (sigla “E”), a preocupação com impactos e preocupações no âmbito social (sigla “S”) e a governança corporativa, que requer um sistema empresarial que apresente estratégias eficientes na tomada de decisões, no gerenciamento de riscos, na transparência com seus colaboradores, stakeholders e consumidores (sigla “G”).



¹ Advogada com Certificação Profissional em Proteção de Dados pela DPBR e EXIN. Pós-graduada em Direito Constitucional e Administrativo, Pós-graduanda em Direito Digital e Proteção de Dados (UERJ), Idealizadora e atual Presidente da Comissão de Privacidade e Proteção de Dados da OAB-PI (2021-2024). Membro da Comissão de Direito Digital da OAB-PI, Líder da Embaixada Data Privacy em Teresina e Professora de LGPD em Pós-graduações.

Segundo disposto no site da rede Brasil do Pacto Global², ESG é a indicação de solidez, custos mais baixos, melhor reputação e maior resiliência em meio às incertezas e vulnerabilidades, com uma aplicabilidade crescente pelas empresas brasileiras.

Isso significa que quem atua de acordo com os padrões ESG e, conseqüentemente, adota as diretrizes do LGPD, garante que a empresa se preocupa e desenvolve práticas sociais, ambientais e de governança, questões que, cada vez mais, despertam o interesse e o foco da sociedade e, por consequência, daqueles que estabelecem relações com essas organizações.

Não há como imaginar governança sem que a empresa aja em conformidade com a legislação e demais regras de conduta do mercado, sejam elas escritas ou tácitas. Os termos LGPD, governança e ESG estão interligados, convergindo a favor dos resultados das empresas, viabilizando a construção de uma atuação corporativa ética e transparente, trazendo diferenciais à organização frente ao mercado, investidores e, principalmente, ao público consumidor do produto/serviço.

Ademais, a não adequação à LGPD, além de não atender aos pilares da governança e ESG, poderá causar um dano reputacional à instituição, seja esta pública ou privada, maior do que qualquer eventual sanção administrativa prevista em lei. Nesse sentido corrobora Chiara de Teffé³, ao ponderar que a adoção de um programa institucional que tenha atenção aos tratamentos dos dados pessoais, mostra-se essencial para auxiliar no efetivo atendimento aos comandos da lei, de acordo com as particularidades de cada local, bem como para prevenir a ocorrência de violações aos direitos dos titulares dos dados, concretizando, na prática, as premissas da LGPD.

O que se observa, portanto, é que as organizações, sejam públicas ou privadas, devem priorizar a LGPD na sua governança, com vistas à construção de uma nova consciência corporativa e novos modelos empresariais, pautados no compliance proativo de dados, que implicam em uma mudança de práticas e de consciência da equipe, o que leva tempo, planejamento e engajamento, já que tal cuidado atende não apenas as novas exigências da sociedade, mas a própria organização, conseguindo identificar suas vulnerabilidades, reduzirá riscos, tornará o seu ambiente e equipe mais coesos, alcançando melhores resultados e índices a longo prazo, garantindo o compliance⁴ da instituição e ampliando a sua competitividade dentro do setor que integra.

2 Disponível em: <https://www.pactoglobal.org.br/pg/esg>. Acesso em 01 de fevereiro de 2023.

3 TEFFÉ, Chiara Spadaccini de. Dados pessoais sensíveis: qualificação, tratamento e boas práticas. Editora Foco, 2022.

4 A nomenclatura deriva do inglês, que significa cumprir/estar em conformidade, o que pode ser definido, no âmbito da organização, como o alinhamento estratégico das suas práticas e da sua equipe às normas e regulamentos existentes, agregando valor ao negócio desenvolvido.

A IMPORTÂNCIA DA LEI GERAL DE PROTEÇÃO DE DADOS -LGPD- NOS SINDICATOS



Ana Dulce Rehem¹

Foi em 14 de agosto de 2018, que se deu a publicação da Lei ordinária n. 13.709. Inicialmente, ela somente fazia alterações na também Lei ordinária n. 12.965 de 23 de abril de 2016 (Marco Civil da Internet). Ocorre, no entanto, que após a aprovação da Lei n. 13.853, de 2019, passou ela de mera alteração do citado Marco Civil, para uma norma independente, qual seja, a Lei Geral de Proteção de Dados, ou LGPD.

A Lei Geral de Proteção de Dados (LGPD) é uma norma brasileira que entrou em vigor em setembro de 2020 e tem como objetivo garantir a privacidade e segurança das informações pessoais dos cidadãos brasileiros. A lei se aplica a todas as organizações públicas e privadas que coletam, armazenam, processam e compartilham, essas mesmas informações.

Os dados, conforme a LGPD, são definidos em duas categorias: pessoais e pessoais sensíveis, em suma, são os mesmos, mas que, a depender da sua origem, torna seu tratamento mais restrito.

Ademais, no que lhe toca, serão considerados sensíveis quando são de origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando se encontre vinculados a uma pessoa natural.

Quando se indica a filiação a sindicato, não se trata de simples dado pessoal, mas sim, de dado pessoal sensível. Este, nas palavras de Bruno Ricardo Bioni^[1] são: “uma espécie de dados pessoais que compreendem uma tipologia diferente em razão de seu conteúdo oferecer uma especial vulnerabilidade, discriminação”. Entretanto, no que respeita a filiados de entidades sindicais, requer-se, para essas informações, um tratamento mais rigoroso.

Os sindicatos são organizações que representam os interesses de trabalhadores de diferentes setores e atividades econômicas. Essas entidades costumam coletar e armazenar dados pessoais de seus membros, como nome, endereço, CPF, telefone, e-mail, entre outros, revelando que essas informações são importantes para que os sindi-

¹ Advogada, Encarregada de Dados do Sebrae-PI e membra da Diretoria da Comissão de Privacidade e Proteção de Dados da OAB-PI (2021-2024).

catos possam prestar serviços aos seus associados, como orientação jurídica, negociação coletiva e organização de eventos.

No entanto, a coleta e o tratamento desses dados devem ser realizados de acordo com as normas estabelecidas pela LGPD. Isso significa que os sindicatos devem tomar imprescindíveis medidas para garantir a privacidade e segurança dessas informações, além de obter o consentimento dos seus titulares, a fim de, legalmente poder utilizá-los.

As entidades sindicais que possuem bases de dados com pessoas filiadas e desfiladas, assemelham-se à figura do Controlador, que, na forma do inciso IV, do artigo 5º, da LGPD, é a “pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.”

Nessa qualidade, conforme artigo 37, deve-se manter registro de todas e quaisquer operações de tratamento que realizarem, especialmente quando baseado em seu legítimo interesse ou de seus associados. Além disso, quando determinar alguma das citadas operações, além do consentimento específico e não genérico dos titulares de dados, deve-se, também, instruí-las de forma clara, aos operadores que irão realizar o tratamento dos dados recebidos.

É também de exigência da lei, que a entidade sindical indique um Encarregado de Dados Pessoais (DPO), para atuar como ponto focal para questões relacionadas à LGPD, a elaboração de uma política de privacidade, a implementação de medidas de segurança da informação e a realização de treinamentos para conscientização dos colaboradores sobre a importância da proteção dos referidos dados pessoais.

A conformidade com a LGPD pode, e deve, aumentar a confiança dos trabalhadores nos seus sindicatos, pois, demonstra que a organização se preocupa com a privacidade e a segurança dos dados pessoais dos seus filiados. Além disso, a conformidade com a LGPD pode ser vista como um diferencial competitivo em relação a outras organizações que não adotam medidas de proteção de dados das pessoas sobre as quais devem se preocupar.

Além disso, a lei prevê sanções para as organizações que descumprirem as normas estabelecidas pela lei, como multas que podem chegar a R\$ 50 milhões por infração.

Dessa forma, a LGPD se torna extremamente importante para os sindicatos, pois estas entidades precisam garantir que estão em conformidade com a lei para evitar possíveis sanções e prejuízos financeiros, além de preservar a confiança e credibilidade dos seus associados.

Portanto, é fundamental que os sindicatos realizem uma revisão de suas práticas de coleta e tratamento de dados pessoais, implementem as medidas de segurança da informação exigidas pela LGPD e promovam a conscientização dos seus colaboradores sobre a importância da respectiva proteção. A adoção dessas medidas pode contribuir para fortalecer a relação de confiança e transparência entre os sindicatos e seus associados, além de evitar possíveis problemas com o preceito normativo ora em questão.

A ADEQUAÇÃO À LGPD SOB A ÓTICA DA REGULAMENTAÇÃO DA ANPD-RESOLUÇÃO CD/ANPD N° 4

Bruno Osires Batista Barbosa e Silva¹

A construção histórica e legislativa que o Brasil atravessou desde 2010 permitiu que a Lei Geral de Proteção de Dados – 13.709/2020 – entrasse em vigor em setembro de 2020. O surgimento da lei promoveu, ou deveria promover, significativos movimentos na área pública e privada na busca da adequação. De fato, algumas instituições têm buscado consultorias ou, por si mesmas, feito ajustes com vistas a buscarem uma adequação aos diversos objetivos a que a lei se propõe.

A Autoridade Nacional de Proteção de Dados foi o órgão criado pela nova Lei com as atribuições, dentre outras, de elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade, editar regulamentos, bem como deliberar, na esfera administrativa, sobre a interpretação da LGPD, além de promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança. Durante muito tempo a ANPD se preocupou em endereçar para a sociedade e para àqueles que deveriam se adequar a lei a busca pelo:

1. Conhecimento de que a lei existe, do que se trata e quem deve buscar a necessidade de criar mecanismos e procedimentos com vistas à adequação;
2. Conscientização de que, majoritariamente, as práticas adotadas não estavam, quando da entrada em vigor, em conformidade com o estipulado pela lei, e principalmente pelos princípios que a regulam.



¹ Advogado e membro da Diretoria da Comissão de Privacidade e Proteção de Dados da OAB-PI (2021-2024).

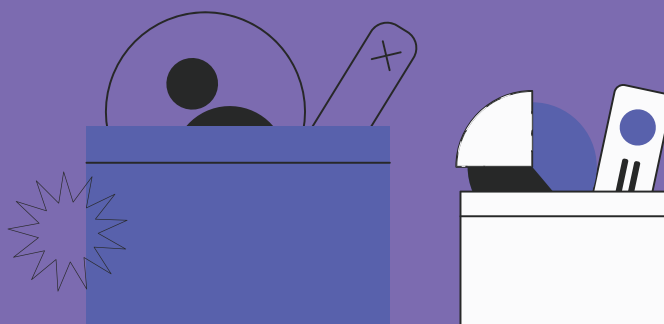
No tocante especificamente ao segundo ponto, a ANPD não trouxe, de cara, a ideia de sancionar órgãos públicos e privados. É fato que este é um tema e uma preocupação nova no país, reforçada pela ausência de uma lei específica (até 2020) tratando sobre privacidade e proteção de dados. Logo, seria desarrazoável que se trouxesse o caminho pela adequação à base de sanções administrativas estipuladas pela lei. A ideia passou então por uma ampla agenda de reuniões, audiências públicas, emissão de documentos, guias de implementação e mecanismos facilitadores para que os atores públicos e privados pudessem endereçar esforços com vistas a um início de adequação.

Ocorre que, mais de 2 anos e meio depois da entrada em vigor da lei, esse caminho inicial vem se esgotando, dando espaço a efetiva atuação da lei em diferentes espaços administrativos e judiciais. Aqui o foco será voltado à atuação administrativa da ANPD. Inicialmente a autoridade nacional era órgão integrante da Presidência da República e, portanto, subordinado ao Chefe do Executivo Federal. Mais recentemente foi promulgada a Lei 14.460/22, que transforma a Autoridade Nacional de Proteção de Dados (ANPD) em uma autarquia, passando a ter autonomia administrativa e financeira. O objetivo da mudança passa precipuamente pela busca de confiabilidade, independência e compatibilidade com outros regimes regulatórios internacionais.

Após traçar mecanismos iniciais, a ANPD emitiu a Resolução CD/ANPD Nº 4, em 24/02/2023, aprovando o Regulamento de Dosimetria e Aplicação de Sanções Administrativas. Aqui cabe ressaltar que quando da entrada em vigor da lei não existia, até a entrada em vigor da citada Resolução, a possibilidade de aplicação de sanções pecuniárias, por expressa vedação prevista no artigo 53, da LGPD

O artigo 7º do Regulamento trouxe os critérios e parâmetros que serão utilizados pela ANPD determinar a sanção: gravidade e natureza da infração; grau do dano; vantagem econômica e a condição econômica do agente de tratamento; reincidência do agente de tratamento; cooperação, boa-fé e a adoção de medidas de boas-práticas e de governança pelo agente de tratamento; e a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

Importante notar que a adoção de boas práticas de governança e tratamento de dados pessoais são consideradas na dosimetria da multa a ser arbitrada pela Autoridade Nacional de Proteção de Dados,



o que novamente reforça a ideia de que a implantação da lei em órgãos públicos e privados é medida que se impõe desde já, demonstrando boa-fé com a busca pela adequação. Corroborando tal entendimento, o artigo 13 traz como atenuante a “implementação de política de boas práticas e de governança ou de adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar os danos aos titulares”.

A publicação do Regulamento, que traz o completo procedimento a ser seguido (desde o procedimento preparatório, perpassando pela defesa e instrução processual, até decisão em primeiro grau passível de recurso), se soma a diversas outras possibilidades de sanção dos agentes de tratamento. Um programa de adequação robusto e adequado à realidade de cada órgão, é ferramenta que além de mitigar a ocorrência de incidentes de segurança, diminuem os possíveis danos em caso de eventual ocorrência. Além disso, é meio comprobatório para a ANPD de boa-fé na eventual ponderação do valor a ser arbitrado em sanção de multa, constituindo-se em circunstância atenuante.

Por fim, é esperado que a Autoridade Nacional de Proteção de Dados se torne cada vez mais atuante, e que as primeiras sanções pecuniárias sejam aplicadas ao longo de 2023. A necessidade da adoção de um programa de governança efetivo, adequado e voltado às necessidades de cada órgão é medida urgente, haja vista os potenciais danos em eventual incidente de segurança, sejam pelos prejuízos decorrentes do acontecimento em si, seja pelas medidas administrativas possíveis de serem instauradas pela ANPD. Além disso, não ficam prejudicadas ações judiciais individuais ou coletivas, podendo culminar em eventuais indenizações por danos materiais e/ou morais.



LGPD NO ÂMBITO DAS RELAÇÕES CONSUMERISTAS

João Vitor Silva Macêdo¹

O LGPD é um diploma legal que abrange acerca dos dados pessoais do indivíduo, no tema em questão, do consumidor, certo que nos dias atuais alguns fornecedores solicitam dados do cliente para dar continuidade a uma compra ou para a concessão de uma devolução de uma mercadoria ou serviço, haja vista que este fato analisado por um espectro jurídico

Com a massificação do consumo, o analfabetismo digital e a atuação desmuniada da legislação pelo consumidor leigo perante uma compra seja virtual seja em loja física, ocorre esse determinado fato, muitas lojas impulsionam o consumidor a colocar o CPF em troca de ter o seu direito de devolução de tal produto, evidentemente esta situação configura publicidade enganosa, que é o fornecedor ou comerciante fazer afirmação falsa da garantia de um produto ou serviço, porque fundamentadamente, para trocar um produto, não é preciso informar o CPF, basta apresentar a nota fiscal.

Destarte, essa forma de abordagem dos lojistas requerendo o CPF dos clientes para obtenção ou continuidade de tal ocasião que envolva

1 Estudante de direito do 9º Período da UNIFSA e membro da Comissão de Privacidade e Proteção de Dados da OAB-PI (2022-2024).



a relação de consumo, pode ser altamente arriscado ao consumidor, pois com o surgimento de tantos crimes e das intensas mensagens instantâneas virtuais ao consumidor, que atormentam o seu cotidiano, é considerada falta de privacidade aos dados pessoais do consumidor, além de alguns fornecedores de má-fé se aproveitarem de informações dos devidos clientes para manobras fraudulentas em compras não consentidas pelo mesmo, abarcando grandes prejuízos à situação do consumidor.

No ambiente do e-commerce, a lei de nº 13.709/2018 preceitua acerca do tratamento dos dados pessoais das empresas públicas e privadas e proteção de dados de clientes, fornecedores e colaboradores da empresa, em especial das lojas virtuais, no entanto se as empresas não seguirem o ordenamento jurídico estabelecido, estarão submetidas a sanções como advertências de grau de grande intensidade e multas, em virtude dessas empresas estarem corresponsáveis, pois possuem a função de coleta, uso e armazenamento e até compartilhamento de dados pessoais de clientes.

Nessa órbita, pelo fato da Lei Geral de Proteção de Dados ter entrado em vigor em 1º de agosto de 2021, há entraves quanto à adoção do regimento para dispor de credibilidade quanto à privacidade de dados e à aplicação do Agente de Tratamento de Dados. De fato, vender online consistirá, conforme percurso da compra, com base nos preceitos da proteção dos direitos fundamentais da liberdade e o livre desenvolvimento da personalidade natural.

Cabe ressaltar que por meio do Decreto nº 10.474, de 26 de agosto de 2020, aduz acerca da incumbência da ANPD (Autoridade Nacional de Proteção de Dados), que consiste, em caso de insegurança jurídica em razão do vazamento de dados quando da realização da compra virtual, convém à ANPD comunicar às autoridades competentes as infrações penais das quais tiver conhecimento e a implantação de mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com a Lei nº 13.709, de 2018.

Em última perspectiva, convém ao animus do Poder Público estimular a validade legal do ordenamento da Proteção de Dados, no quesito aplicação de punições mais cogentes aos fornecedores de má-fé, de dentro do comércio eletrônico. Conforme se vê nas seguintes alíneas do art. 4º do referido decreto acerca da competência do Conselho Diretor.

Sendo assim, cabe ao Governo juntamente com Órgãos de Inteligência e de Armazenamento de Dados, a especialização entre os profissionais atuantes da Lei de Proteção de Dados de forma proba e que traga bons resultados para segurança cadastral de cada cidadão e ao Poder Disciplinar a aplicação de medidas punitivas mais pujantes aos empresários que agem de má-fé no tocante às informações ao consumidor e à infração a ser cometida pelo mesmo nexu causal.

PROTEÇÃO DE DADOS APLICADA À ÁREA DE SAÚDE: O PROCESSO DE ANONIMIZAÇÃO NO TRATAMENTO DE DADOS CLÍNICOS

Raryssa Nogueira do Nascimento¹

A proteção de dados é um elemento fundamental da sociedade digital e é crucial para garantir a privacidade e segurança dos dados pessoais. Não à toa que a nossa Carta Magna, em seu artigo 5º, LXXIX da CF assegura a proteção de dados como garantia de direito fundamental. E em uma sociedade da informação, o que se tem de mais precioso são as informações pessoais, e, por isso, a importância da criação de um regulamento de controle das atividades das organizações.

Na área de saúde, o impacto tornou-se ainda maior, sobretudo, em razão do grande volume de dados pessoais sensíveis² operados diariamente. A proteção de dados na área de saúde é crucial para garantir a privacidade e confidencialidade dos pacientes, já que incluem informações sobre o estado de saúde, histórico médico, resultados de exames, tratamentos, entre outros. Além disso, o acesso inadequado a essas informações pode ocasionar graves consequências para a privacidade e bem-estar dos pacientes, incluindo discriminação e violação de direitos fundamentais.

¹ Advogada, Consultora em proteção de dados pessoais com Certificação Profissional em Formação DPO com foco na LGPD, ISO 27001 e ISO 27701. Pós-Graduada em Direito Digital e Compliance. Pós Graduada em Direito do Trabalho e Direito Processual do Trabalho. membro da Comissão de Privacidade e Proteção de Dados da OAB-PI (2022-2024).

² Dados pessoais sensíveis: são dados cujo tratamento pode ensejar a discriminação do seu titular por se referirem, por exemplo, à opção sexual, convicções religiosas, dado referente a saúde ou opinião política.



Com a informatização dos prontuários médicos, os registros médicos estão disponíveis em tempo real, o que significa que os médicos e outros profissionais de saúde têm acesso a informações mais precisas e atualizadas sobre o paciente, resultado, por vezes, no uso indevido das informações clínicas. Neste sentido, é importante considerar a proteção de dados e a privacidade como questões necessária a serem abordadas e garantidas ao longo do processo de informatização.

Em seu artigo 5º, XI, a LGPD preceitua a anonimização de dados como “utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo”; Isso significa que o dados pessoais, ao passarem pelo processo de anonimização, não mais podem ser associados a uma pessoa natural, o que concede ao Controlador de Dados³, maior liberdade no tratamento de dados.

Na saúde, a anonimização de dados é uma prática importante para ajudar a proteger a privacidade dos pacientes, evitando que informações sensíveis sejam compartilhadas ou usadas sem o consentimento dos mesmos, além de permitir a melhoria dos estudos de saúde, pesquisas médicas e análises de dados de saúde, o que pode levar a avanços na compreensão e tratamento de doenças.

Existem vários métodos de anonimização de dados, incluindo a remoção de informações identificáveis, como nomes, endereços, números de telefone e números de identificação, o uso de identificadores únicos que não podem ser associados aos indivíduos, ou combinando informações de vários pacientes ou agrupando dados em categorias amplas.

No entanto, é importante lembrar que a anonimização não é uma garantia absoluta de privacidade. Em alguns casos, é possível que informações identificáveis sejam recuperadas por meio de técnicas de reidentificação, portanto, faz-se necessário que a escolha das ferramentas de anonimização seja feita de forma cautelosa, a fim de buscar o que há de mais moderno e eficaz no mercado. Além disso, após realizada a técnica, verifique regularmente o processo de anonimização, para garantir que ele esteja funcionando corretamente e para que as possíveis falhas sejam identificadas prontamente.

Adotar medidas de segurança de dados rigorosas, treinar a equipe, monitorar o acesso, manter sistemas de segurança atualizados e cumprir as leis de privacidade são algumas das maneiras pelas quais as instituições de saúde podem proteger os dados de saúde dos pacientes e garantir que os direitos instituídos pela Constituição Federal, pela Lei Geral de Proteção de Dados e demais normas de proteção de dados, sejam respeitados.

³ Controlador de dados é o agente responsável por tomar as principais decisões referentes ao tratamento de dados pessoais e por definir a finalidade deste tratamento.

LEI GERAL DE PROTEÇÃO DE DADOS (13.709/18) – A NÃO APLICAÇÃO DA LGPD¹

Rodrigo Lira.²

A Lei Geral de Proteção de Dados surgiu no intuito de tutelar os dados da pessoa natural dos abusos cometidos pelas empresas e mercado de consumo, pois, com tamanha conectividade, as instituições privadas passaram a ter acesso às informações mais íntimas e a processá-las como queriam. Portanto, a LGPD trata da regulação do fluxo dessas informações entre pessoas jurídicas, independente da complexidade do banco de dados, aplicável tanto os que são automatizados como para os que ainda são manuais. Não obstante, a norma traz situações que excepciona sua aplicação, pois apesar de haver coleta de dados, não há um viés mercadológico e não põe, *a priori*, risco à privacidade do indivíduo (MENEZES; COLAÇO, 2018).

Expresso no art. 4º da LGPD apresenta situações como manipulação de dados realizados por pessoa natural sem fins econômicos, pois a comunicação humana não ocorre sem a troca de informações, e se essa

1 Resumo do artigo “Tratamento de informações pessoais: análise do limite legal para o uso de dados pessoais pelas instituições privadas” In: Direito: Diálogos e pesquisas sobre temas contemporâneos.1 ed. Rio de Janeiro: E-Publicar, 2022, v.1, p. 1-309.

2 Advogado, pós-graduado em Direito Digital e em Direito do Trabalho e Previdenciário, e membro da Comissão de Privacidade e Proteção de Dados da OAB-PI (2022-2024).



comunicação se apresenta no aspecto pessoal. Quando se conhece alguém é comum trocar e-mail, nome, endereço, chegando muitas vezes nos considerados dados sensíveis como orientação sexual e religiosa, apesar disso, não será necessário a aplicação da lei, o que poderia estender bastante sua aplicação e complexidade, podendo interferir em situações muito íntimas entrando em contradição com sua finalidade. Mas, se fizer uso indevido dessas informações, poderá acarretar em danos morais e ilícito penal (MENEZES; COLAÇO, 2018).

O processamento de dados para fins jornalísticos, também está dentro da exceção de aplicabilidade direta da norma, já que considera-se uma instituição que busca o debate, a liberdade de expressão e a transmissão da verdade, e por isso, não poderia haver algum tipo de censura ou limitação para atuação desses profissionais, entretanto, exige-se uma atividade verdadeira, sem inclinações pessoais ou ideológicas, mantendo sempre a idoneidade da informação transmitida. Um exemplo são os jornalistas esportivos, que preparam matérias sobre os atletas, abrangendo o desempenho e suas características físicas, como número de chutes a gols, quantidade de gols marcados por determinado atleta, idade, altura, peso, distância percorrida no campo. Ainda que informações como estas sejam consideradas dados pessoais e as conclusões obtidas pelo jornalista sejam resultado de tratamento, não há necessidade de aplicação da LGPD, pois a finalidade é somente informativa.

Porém, se um portal de notícias analisa seus visitantes e desenvolve padrão de consumo, tempo médio de permanência online, tipo de conteúdo pesquisa, essas informações passam a possuir alto valor e importância de mercado, pois podem direcionar as empresas ao que apresentarem online para aquela pessoa. Sendo assim, situações como esta, mesmo estando relacionada ao jornalismo, devem se submeter às normas da LGPD.

O tratamento para fins acadêmicos também está excluído da regulamentação, tendo sua autonomia para o desenvolvimento de conhecimento, pesquisas e manifestação de pensamento assegurada pela Constituição Federal, segundo o art. 218, CF/88. Apesar de ficar de fora da aplicação dessa norma, o controle e a fiscalização no ambiente acadêmico ocorre pelos comitês de ética, sem a necessidade de uma matéria especial para controle de pesquisas (BRASIL, 1988).



AS REDES SOCIAIS E O CONSTANTE COMPARTILHAMENTO DE DADOS: UM RISCO A SUA PRIVACIDADE

Victória Hellen Nascimento Oliveira¹

A sociedade está em constante transformação, e o direito deve acompanhá-la. Entretanto, é difícil o sistema legal acompanhar a evolução social e, com o advento da tecnologia a velocidade é ainda maior, diariamente. A internet é hoje muito mais que transferência de dados ou correio eletrônico – o e-mail, pois através dela são oferecidos diversos serviços, que podem ser bancários, educacionais, e até comércio de bens e serviços.

Para entender um pouco de como funciona o ecossistema de proteção de dados pessoais, é preciso saber que há leis que abrangem o ambiente off-line, como no caso do Código de Defesa do Consumidor, e leis que abrangem o ambiente online, o Marco Civil da Internet, que como já apontado é um microssistema de proteção de dados pessoais e que regula todas as nossas relações travadas na internet.

Ou seja, antes da Lei Geral de Proteção de Dados Pessoais, existiam várias peças espalhadas, como um quebra cabeça que muitas vezes não tinham sintonia, e por isso não poderiam ser agregadas facilmente. Com o seu advento, tendo em vista que privacidade é um direito humano fundamental que pertence a todos os indivíduos, houve a regulação de dados pessoais.

Já dizia a famosa frase do matemático britânico Clive Humby: “Dados são o novo petróleo” (Data is the new oil), bem como a publicação da *The Economist*: “O recurso mais valioso do mundo não é mais o petróleo, mas dados” (The world’s most valuable resource is no longer oil, but data), que tem sido muito citadas pelo mercado e executivos mundo afora, apontando que aqueles que possuem dados terão um recurso muito valioso em mãos.

Em uma esfera cujas mídias digitais prestam seus serviços aos usuários sem que estes paguem alguma tarifa diretamente, não se percebe que a conjuntura financeira vai além disso. O documentário da *Netflix* “O dilema das redes” traz uma frase bastante tocante ao se referir às redes sociais reproduzida por Tristan Harris: “Se você não paga pelo produto, você é o produto”.

¹ Advogada, pesquisadora acadêmica, pós-graduanda em Lei Geral de Proteção de Dados e membra da Comissão de Privacidade e Proteção de Dados da OAB-PI (2022-2024).

Neste caso, a finalidade econômica encontra-se na coleta dos dados dos usuários, que, na maior parte dos casos, fornecem eles involuntariamente. Assim, há a coleta de dados que, além de passarem por tratamento, são, em muitos casos, vendidos ou compartilhados com terceiros, gerando enormes somas de dinheiro, resultado de um mercado que se apoia na publicidade direcionada.

Pode-se afirmar que *Facebook*, *Instagram*, *Twitter*, *WhatsApp* e *TikTok* são as redes sociais mais utilizadas atualmente. Na prática, escândalos como o da Cambridge Analytica e Facebook, relatados no documentário “Privacidade Hackeada” na Netflix, contribuem para que o poder da rede faça com que estejamos atentos aos riscos de utilizar redes sociais, tendo em vista que dados são excessivamente coletados.

Além disso, a gigante de tecnologia Meta, responsável por *Facebook*, *Instagram* e *WhatsApp*, entre outros, foi multada em 265 milhões de euros, cerca de R\$ 1,4 bi, por não ter conseguido evitar que dados pessoais de 533 milhões de usuários da rede social Facebook ao redor do mundo fossem coletados automaticamente de forma criminosa por terceiros.

O algoritmo das redes sociais programa-se para de fato instigar seus usuários a fornecer informações e consumir o que melhor funciona para cada indivíduo de acordo com o seu perfil de consumo, o que Shoshana Zuboff denominou de “capitalismo de vigilância” e faz com que as redes sociais falhem em sua missão de proteger o usuário.

A economia movida a dados e o capitalismo de vigilância andam lado a lado, por ser a extensão do mercado baseado em dados pessoais, e exigir a expansão da vigilância. Portanto, os dados pessoais configuram-se como um “ativo econômico” na contemporaneidade, sendo o avanço tecnológico o propulsor da virtualização das informações como “fator crítico da atividade empresarial”.

São páginas e páginas de termos misteriosos, usadas por sites e redes sociais para explicar os seus direitos e deveres. Alguns têm palavras e piadas, outros escondem cláusulas abusivas. No final, você concorda com todas. A construção de instrumentos para facilitar a comunicação e interação entre pessoas estão entre as aplicações das tecnologias de informação de maior destaque hoje.

Com preferências e receios na mão de grandes empresas de tecnologia, pode-se afirmar que somos frequentemente influenciados nas mãos de gigantes que prevalecem em suas vontades em um perigoso jogo de poder. Entretanto, é dever também do usuário conhecer a proteção de dados para proteger ao máximo a sua privacidade, pois frequentemente se colocam em risco ao disponibilizarem tantas informações em redes sociais. Portanto, é essencial falar em privacidade tendo em vista o valor dos dados, apesar de parecer utópico.

A LGPD E A BASE LEGAL PARA EXECUÇÃO DE CONTRATO

Arielly Vitória Dantas Peres da Silva¹

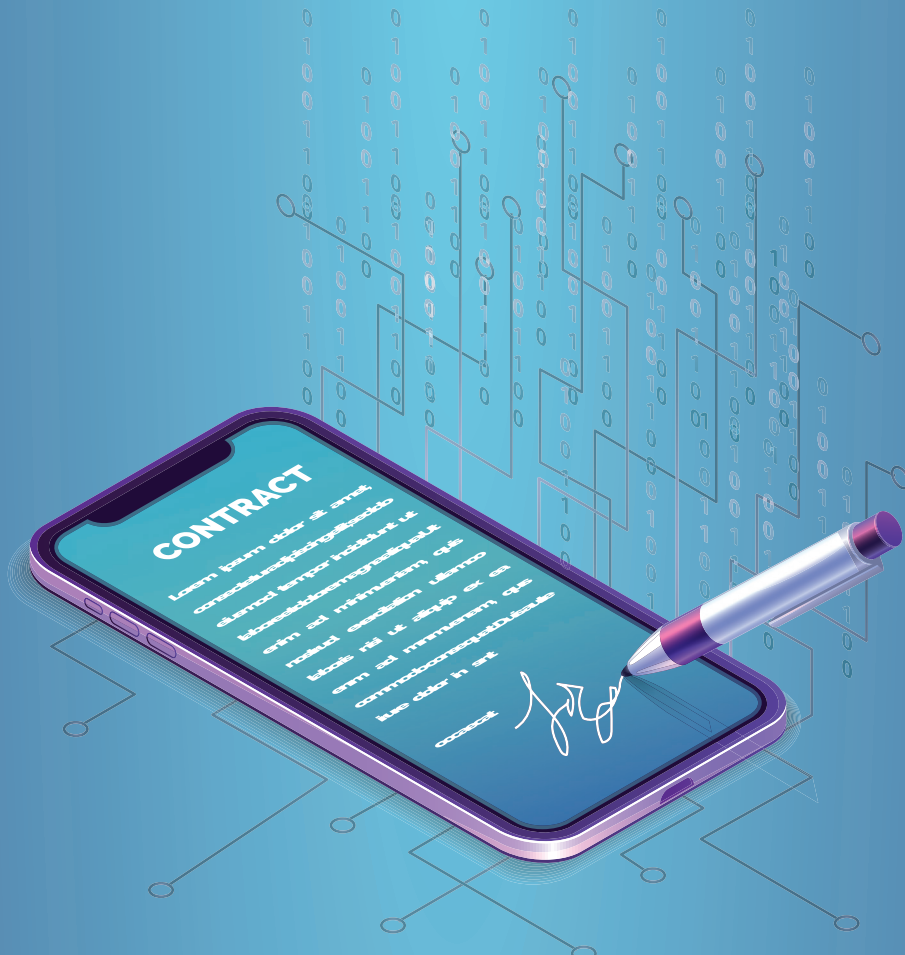
É cediço que a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados) foi introduzida no Brasil para atender a necessidade de proteção dos direitos fundamentais de liberdade e de privacidade e a livre formação da personalidade de cada indivíduo.

A Lei versa sobre o tratamento de dados pessoais, dispostos em meio físico ou digital, feito por pessoa física ou jurídica de direito público ou privado, englobando um amplo conjunto de operações que podem ocorrer em meios manuais ou digitais.

O objetivo da norma é estabelecer um cenário de segurança jurídica, utilizando-se da padronização de regulamentos e práticas para promover a proteção aos dados pessoais de todo cidadão que esteja no Brasil.

Para alcance desse objetivo a Lei oferece as denominadas “bases legais”, ou seja, justificativas e argumentos que devem ser utilizados como fundamento pela empresa para legitimar o tratamento e o uso dos dados pessoais.

1 Advogada. Bacharel em Direito. Pós-graduanda em Direito Digital e Proteção de Dados. Pós-graduanda em Lei Geral de Proteção de Dados. membro da Comissão de Privacidade e Proteção de Dados e Direito Digital da OAB-PI (2022-2024).



Pois bem, se a sua empresa coleta, manipula, armazena ou utiliza de qualquer forma dados pessoais, ela precisa estar enquadrada em pelo menos uma das 10 (dez) bases legais da LGPD.

Conjeturando essa realidade, o art. 7º, inciso V da LGPD prevê como hipótese autorizadora do tratamento de dados a execução de contrato ou de procedimentos preliminares relacionados ao contrato do qual seja parte o titular de dados, a seu pedido.

Nessa situação, o tratamento de dados se dará a pedido do próprio titular dos dados para garantir a execução de um contrato ou de seus procedimentos preliminares. Essa hipótese se assemelha um pouco com o tratamento de dados via consentimento, outra base legal fixada pelo art. 7º, I, da LGPD. Contudo, é possível diferenciá-las uma vez que ao utilizar a base legal para execução de contratos, o titular dos dados não poderá revogar o seu fornecimento a qualquer momento, visto que a outra parte estará resguardada pela LGPD para poder manter os dados fornecidos pelo titular enquanto durar a vigência do contrato celebrado (GROSSI, 2020).

Cita-se ainda que os deveres de informação, proteção e lealdade do controlador (pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais) não se limitam apenas à execução do contrato, mas, repercutem também na fase pós contratual, implicando ao controlador de dados a possível reparação do dano provocado em decorrência da aplicação da teoria da culpa post pactum finitum (RODOVALHO, 2021).

Apesar de não haver expressamente na lei o período de tempo que uma empresa pode armazenar os dados pessoais de um ex-empregado, por exemplo, o artigo 15, inciso III, da LGPD, dispõe que o término do tratamento dos dados pessoais ocorrerá quando da comunicação do titular solicitando que os dados sejam eliminados.

Ocorre que, sobrevindo solicitação do empregado demitido para que a empresa empregadora exclua os seus dados, esta poderá não acatar o pedido do titular dos dados. Isso porque o artigo 16, inciso I da LGPD determina que a empresa poderá reter os dados de determinados trabalhadores, durante certo período de tempo, com o objetivo de cumprir uma obrigação legal ou regulatória.

Contudo, deve-se sublinhar que apesar do amparo da lei no tocante ao armazenamento de dados pessoais de ex-empregados, a empresa não poderá repassar tais informações com o intuito de causar prejuízo, tendo em vista o direito à privacidade e à intimidade do ex-empregado.

“A proteção de dados pessoais deve definir, mais que tudo, a quem cabe o controle sobre os dados pessoais - e assim, conseqüentemente, realizar uma forma de distribuição de poder na sociedade que favoreça a autonomia do indivíduo.”

*Danilo Doneda**



**Professor Danilo Doneda, um dos maiores estudiosos da privacidade e proteção de dados pessoais do Brasil.*



Comissão de
Privacidade e
Proteção de Dados

Acesse o site:

www.oabpi.org.br

Siga-nos:



@OABPiaui