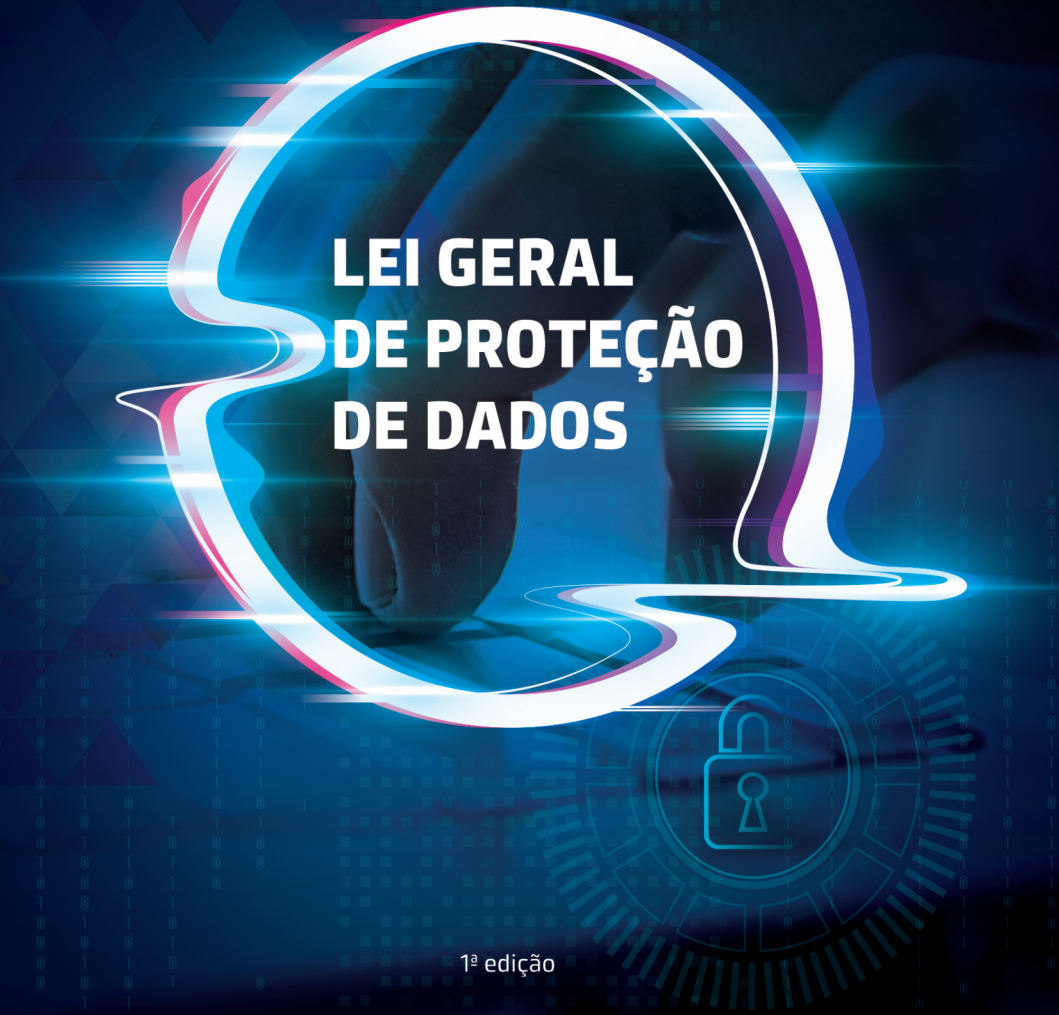
Liane Pointner
Mônica Tais Medeiros Lopes Scariot
Patrícia de Oliveira Vieczorek
Raphael Di Tommaso Lugarinho da Fonseca
Renata Dalla Santa de Carvalho
Vanise Saciloto Camassola

LEI GERAL DE PROTEÇÃO DE DADOS



1ª edição

OAB RIO GRANDE DO SUL Subseção Caxias do Sul
EDUCS
OAB RIO GRANDE DO SUL CDDNT Comissão Direito Digital e Novas Tecnologias

LEI GERAL DE PROTEÇÃO DE DADOS

Organizadores

Liane Pointner
Mônica Tais Medeiros Lopes Scariot
Patrícia de Oliveira Vieczorek
Raphael Di Tommaso Lugarinho da Fonseca
Renata Dalla Santa de Carvalho
Vanise Saciloto Camassola

LEI GERAL DE PROTEÇÃO DE DADOS

Organizadores

Liane Pointner
Mônica Tais Medeiros Lopes Scariot
Patrícia de Oliveira Vieczorek
Raphael Di Tommaso Lugarinho da Fonseca
Renata Dalla Santa de Carvalho
Vanise Saciloto Camassola

EDUCS

OAB RIO GRANDE DO SUL Subseção Caxias do Sul

Revisão de conteúdo: Raphael Di Tommaso Lugarinho da Fonseca
Revisão Final: João Paulo Boeno Pagno
Editoração: Joelma Esteves
Coordenação: Mônica Tais Medeiros Lopes Scariot

Dados Internacionais de Catalogação na Publicação (CIP)
Universidade de Caxias do Sul
UCS - BICE - Processamento Técnico

L525 Lei geral de proteção de dados [recurso eletrônico] / org. Liane Pointer ... [et al] - Caxias do Sul, RS : Educs, 2021.

Dados eletrônicos (1 arquivo)

Apresenta bibliografia

ISBN 978-65-5807-098-6

Modo de acesso: World Wide Web

1. Proteção de dados - Legislação 2. Brasil [Lei geral de proteção de dados pessoais (2018)] .I. Ponntner, Liane, org. [el at]. II. Título

CDU 2. ed: 342.721(094.46)

Índice para o catálogo sistematico:

1. Proteção de dados - Legislação	342.721(094.46)
2. Brasil. [Lei geral de proteção de dados pessoais (2018)]	342.721(81)

Catalogação na fonte elaborada pela bibliotecária
Carolina Machado Quadros - CRB 10/2236

EDITORA AFILIADA

EDUCS – Editora da Universidade de Caxias do Sul
Rua Francisco Getúlio Vargas, 1130 - Bairro Petrópolis - CEP 95070-560 - Caxias do Sul - RS - Brasil
Ou: Caixa Postal 1352 - CEP 95020-972 - Caxias do Sul - RS - Brasil
Telefone/Telefax: (54) 3218 2100 - Ramais: 2197 e 2281 - DDR (54) 3218 2197
Home Page: www.ucs.br - E-mail: educs@ucs.br

ORDEM DOS ADVOGADOS DO BRASIL -
SUBSEÇÃO DE CAXIAS DO SUL
Triênio 2019/2021

Presidente:
Rudimar Luis Brogliato

Vice-Presidente:
Ana Carla Hendler Gava Furlan

Secretário-Geral:
Ivandro Bitencourt Feijó

Secretária-Geral Adjunta:
Eloisa Fatima dos Passos Dahmer

Delegada da CAA/RS Caxias do Sul:
Mariana Carneiro

SUMÁRIO

Rudimar Luis Brogliato
Presidente da OAB -
Subseção de Caxias do Sul

PALAVRA DO PRESIDENTE

Enquanto estamos ensaiando a transformação da sociedade tecnológica para digital, tenho grata satisfação e honra de inaugurar a materialização de um projeto, idealizado e desenvolvido pela nossa laboriosa Comissão de Direito Digital e Novas Tecnologias, que é sumamente engajada em dissecar a Lei Geral de Proteção de Dados (LGPD), dada a sua importância e atualidade no mundo digital.

A satisfação se dá porque sempre fui um ávido leitor e não poderia terminar a gestão sem que tivéssemos dado uma pequena contribuição à literatura e saber jurídico. Honrado fico porque a nossa comissão, liderada pela advogada Renata Dalla Santa de Carvalho, conseguiu materializar este projeto que tivemos ousadia de acreditar.

Mas vai muito além de mero capricho de vaidade, sem dúvidas, o assunto abordado no livro vem ao encontro da missão institucional da Ordem dos Advogados do Brasil, pois, como expresso no art. 44 do Estatuto da Advocacia, deve a Ordem primar pela boa aplicação das leis e do aperfeiçoamento jurídico. Não obstante a esses compromissos técnicos jurídicos, também compete a nossa instituição prestar assistência à justiça social e aos direitos humanos, sendo que a pri-

vacidade dos dados certamente insere-se no elenco de proteções da dignidade do ser humano, mormente das pessoas mais vulneráveis.

Com efeito, a popularização do acesso aos meios virtuais, ferramentas úteis e necessárias para a atual vida em sociedade e, sobretudo, na moderna sociedade de consumo, com a crescente facilitação dos mecanismos eletrônicos de busca de dados, compartilhamentos e cruzamento de informações resultam na extrema vulnerabilidade do cidadão, que pode sofrer uma devassa na sua intimidade, na sua privacidade pelo uso indiscriminado e não autorizado das suas informações privadas: "E as incessantes e indesejadas ligações de telemarketing? Nossos dados pessoais estão sendo acessados com muita facilidade. E o acesso aos dados do cartão de crédito basta para contratar além das fronteiras, em nome de outro." Questiona e conclui com propriedade a coautora Liane Pointner.

Destarte, tenho certeza que o livro contribuirá muito para a advocacia, aos operadores de direito em geral e acadêmicos que estudam os mecanismos e alcances da LGPD para que, assim, possamos todos prestar uma melhor assessoria e consultoria jurídica à sociedade.

Nesse norte, posso afirmar, sem falsos sofismas, que, graças ao trabalho da nossa Comissão de Direito Digital e Novas Tecnologias, graças aos brilhantes coautores desse projeto, graças ao engajamento de todos os membros da comissão, estamos entregando uma compilação interessante para a hermenêutica da LGPD.

Esta publicação, portanto, ombreia com outra gama de projetos, eventos e trabalhos desenvolvidos ao longo da nossa gestão, que só se tornaram possíveis pelo empenho abnegado, prestimoso, altruísta e silencioso dos colegas advogados e advogadas e, porque não dizer, amigos e amigas, que participam dos trabalhos da nossa subseção de Caxias do Sul, orgulho de toda advocacia e exemplo no Estado.

Muito obrigado a todos aos coordenadores da Comissão de Direito Digital e Novas Tecnologias, aos coautores do livro - Liane

Pointner, Mônica Tais Medeiros Lopes Scariot, Patrícia de Oliveira Vieczorek, Raphael Di Tommaso Lugarinho da Fonseca, Renata Dalla Santa de Carvalho e Vanise Saciloto Camassola. Também estendo cumprimentos aos membros da comissão, nossos colaboradores e editora da Universidade de Caxias do Sul, que contribuíram para o desenvolvimento de mais esse projeto.

Desejo a todos uma boa leitura!

PREFÁCIO

Fabiano Menke
Professor da Faculdade de Direito e do Programa de Pós-graduação em Direito da UFRGS e advogado.

É motivo de honra poder contribuir com o prefácio do livro sobre a Lei Geral de Proteção de Dados, elaborado a partir da iniciativa da Comissão de Direito Digital e Novas Tecnologias da OAB Caxias do Sul/RS, e de autoria de Liane Pointner, Mônica Tais Medeiros Lopes Scariot, Patrícia de Oliveira Vieczorek, Raphael Di Tommaso Lugarinho da Fonseca, Renata Dalla Santa de Carvalho e Vanise Saciloto Camassola.

O primeiro ponto a ser destacado é o da pertinência da publicação. Como sabemos, a Lei Geral de Proteção de Dados (LGPD), com inspiração no Regulamento Geral de Proteção de Dados da União Europeia, acentua o seu caráter de "geral". A mensagem que ecoa desse atributo da lei é a da transversalidade: desde a sua edição passou a ocorrer um amplo debate nacional, independentemente do setor envolvido, acerca da compreensão de seus conceitos e princípios e de suas repercussões.

Há, praticamente, um consenso no Brasil de que a LGPD é oportuna e de que era necessário avançar para que o nosso país incrementasse o nível de proteção dos titulares de dados pessoais, seguindo os passos do que até mesmo países vizinhos, como Uru-

guai e Argentina, há muito já haviam atingido. Mas é claro, não se pode esquecer que o fluxo informacional também se mostra relevante e consiste em fundamento da disciplina de proteção de dados. Em suma, ninguém vive sem realizar tratamento de dados pessoais, mas ao mesmo tempo é preciso que todos tenham mais cuidado ao lidar com as informações relacionadas à pessoa natural.

Nesse contexto: da compreensão, do debate e da necessidade de esclarecimentos acerca de tão importante temática, o presente livro vem cumprir a fundamental missão de, num formato sucinto, didático e prático, mas ao mesmo tempo rico em conteúdo, auxiliar o leitor a se familiarizar com o que poderia se chamar de conceitos de base da proteção de dados.

Após a publicação do livro ser devidamente introduzida por Renata Dalla Santa de Carvalho, Liane Pointner inicia abordando o conceito de titular de dados pessoais, a partir de uma visão que resgata elementos históricos, mas ao mesmo tempo analisa características da contemporaneidade. Da mesma forma, expõe, de forma precisa e contextualizada, os conceitos de dado pessoal e de dado pessoal sensível, bem como as hipóteses em que esses dados poderão ser tratados (as denominadas bases legais). Um dos capítulos de grande relevância da lei, o relativo aos direitos do titular dos dados, também foi muito bem abordado no texto inaugural de Liane Pointner.

Patrícia de Oliveira Vieczorek contribui com um enfrentamento bastante prático acerca da LGPD nas empresas. Questionando o que se deve fazer para proteger os dados dos funcionários e dos clientes. Sugere um didático caminho envolvendo as etapas da adequação das organizações à lei e conclui com importantes dicas.

Vanise Saciloto Camassola trata da temática da LGPD nos escritórios de advocacia. Aspectos interessantes são ressaltados no texto, como a relação com clientes, e até mesmo com outros escritórios, os correspondentes, que possam vir a interagir com o prestador

de serviços advocatícios e demandar o tratamento de dados pessoais. Na linha prática que marca o livro, Vanise elenca valiosas dicas para os escritórios de advocacia se adaptarem à LGPD.

Raphael Di Tommaso Lugarinho da Fonseca escreve sobre a Autoridade Nacional de Proteção de Dados, a ANPD, chamando a atenção para a sua importância como pilar da regulação sobre a temática. Aborda a composição da Diretoria da ANPD, bem como as atribuições da autoridade brasileira. O autor salienta, outrossim, a importância da atividade de fiscalização, informando sobre o desenvolvimento atual de regra específica. Nesse contexto, calha destacar a função preventiva do monitoramento das atividades da ANPD, de modo a tentar evitar situações que venham a causar riscos aos titulares de dados pessoais.

Por fim, Mônica Tais Medeiros Lopes Scariot aporta ricas contribuições consistentes em glossário contendo diversos conceitos, em muitos casos ilustrados por exemplos, bem como em dicas práticas, que efetivamente poderão auxiliar a todos no dia a dia do trato com dados pessoais.

Ao concluirmos a leitura do livro, temos a certeza de que o nosso nível de compreensão acerca da disciplina foi elevado!

Renata Dalla Santa
de Carvalho

INTRODUÇÃO

A entrada em vigor da Lei n. 13.709/2018 no Brasil, conhecida como Lei Geral de Proteção de Dados Pessoais – ou LGPD – teve fundamental importância para que universidade, empresa, governo e sociedade civil organizada iniciassem um debate mais profundo acerca da exploração econômica de dados da pessoa natural. Em um mundo conectado por meio de internet – onde informações são geradas por meio da combinação de dados a uma velocidade que ultrapassa os dígitos do analógico, a disponibilidade de dados é praticamente irrestrita e o seu uso tem finalidade econômica – sendo crucial a regulação das relações entre mercado e sociedade.

A regulação desta relação ainda é incipiente no mundo inteiro, visto que data da década de 70, em Hesse, Alemanha, a primeira lei que regula dados. No Brasil, pode-se apontar como ponto de partida a inclusão realizada pela Lei n. 9.296/96 no artigo 5º da Constituição Federal de 1988, quando dispõe que "[...] é inviolável o sigilo da correspondência e [...], de dados e das comunicações [...]. Além da Carta Magna, o Código de Defesa do Consumidor, em 1993, nos arts. 72 e 73 prevê penalidades para casos em que os consumidores forem prejudica-

dos na obtenção de suas próprias informações, bem como por decorrência de inconsistências na qualidade de dados. Dois anos após, a criação da Diretiva 95/46/CE da União Europeia apontou alguns princípios do tratamento de dados que foram incorporados e atualizados pelo Regulamento Geral de Proteção de Dados – GDPR, que entrou em vigor em 2018. Antes do Regulamento Europeu, no Brasil, o Marco Civil da Internet também abordou alguns tópicos acerca de dados, porém foi o GDPR uma das principais referências para a elaboração, no Brasil, de norma específica para tratar do referido tema: a Lei Geral de Proteção de Dados.

É evidente que dados permeiam o mundo físico. Entretanto, com o avanço tecnológico das ferramentas de comunicação na rede mundial de computadores, o acesso e a disponibilidade das informações possuem um alcance substancialmente maior do que se tais dados fossem tratados apenas em âmbito analógico e físico. Portanto, urge a união de diferentes inteligências de diversos segmentos para conhecer, entender, discutir e regular esse tema gerador de riqueza econômica em nossa sociedade. O conhecimento dessa Lei e o debate são importantes para que tal premissa não seja motivo de excessos que confrontem direitos já conquistados como autodeterminação informacional, personalidade, privacidade e a tantos outros direitos garantidos pelos Direitos Humanos e incorporadas às regras já vigentes.

E foi com esse propósito que a Comissão de Direito Digital e Novas Tecnologias da OAB Caxias do Sul/RS (CDDNT – OAB/RS) desenvolveu o presente livro: aproximar colegas da respectiva lei, pois profissionais atuantes da advocacia certamente irão – se ainda não ocorreu – se deparar com temas abordados pela LGPD em suas diferentes áreas de atuação jurídica e também na sua vida, enquanto titulares de dados pessoais. Certamente, esta comissão, por meio do presente trabalho, conseguirá aproximar os profissionais da advocacia a esse tema ainda pouco explorado juridicamen-

te em nosso país.

Por fim, enfatiza-se que neste trabalho, os autores apresentam considerações dos principais elementos da norma e que compõem situações básicas dos trabalhos já desenvolvidos pelos escritórios e profissionais autônomos da advocacia. Portanto, os colegas estão convidados a se familiarizar com a linguagem da respectiva lei. E, assim, deseja-se o despertar do interesse pelo novo revestimento que vem modulando as temáticas abordadas nos escritórios, bem como as ferramentas utilizadas pelos advogados: a inovação e a tecnologia. Faz-se o presente convite ao leitor, no sentido de facilitar o entendimento de que ambos conceitos sejam aliados aos escritórios, cultivando-se uma relação harmônica entre o economicamente viável e a garantia dos direitos dos titulares de dados.

SOBRE OS AUTORES

LIANE POINTNER

É doutoranda em Filosofia do Direito pela Universidade de Caxias do Sul - UCS, bolsista Prosuc-capes, mestre em Direito Privado *stricto sensu* pela Universidade Federal do Rio Grande do Sul – UFRGS. Especialista em Direito do Consumidor e Direitos Fundamentais pela Universidade Federal do Rio Grande do Sul – UFRGS. Bacharel em Ciências Jurídicas e Sociais pela Universidade Federal do Rio Grande do Sul – UFRGS.

MÔNICA TAIS MEDEIROS LOPES SCARIOT

É especialista em Direito Civil, Negocial e Imobiliário pela Anhanguera Uniderp e especialista em Advocacia em Direito Digital e Proteção de Dados pela Ebradi – Escola Brasileira de Direito. Graduada em Direito pela Faculdade da Serra Gaúcha – FSG.

PATRÍCIA DE OLIVEIRA VIECZOREK

É graduada em Direito pela Pontifícia Universidade Católica - PUC-RS, especialista em Direito Civil Aplicado e Processo Civil pela - UFRGS.

RAPHAEL DI TOMMASO LUGARINHO DA FONSECA

É graduado em Direito e em Publicidade e Propaganda pela UCS. Pós-graduado em Multimídia e Comunicação e em Direito Digital. Certificado pela Exin em Privacy & Data Protection Foundation, Privacy & Data Protection Essentials e Information Security Foundation based on ISO/IEC 27001.

RENATA DALLA SANTA DE CARVALHO

É especialista em Direito Digital, pela Fundação Escola Superior do Ministério Público, DPO com certificação pela Assespro-RS.

VANISE SACILOTO CAMASSOLA

É especialista em Direito Digital e pós-graduanda em Direito Penal e Direito Processual Penal ambas pela Fundação Escola Superior do Ministério Público – FMP.

Todos são advogados e membros da Comissão de Direito Digital e Novas Tecnologias da OAB – CDDNT – Caxias do Sul – RS

Liane Pointner

1. TITULAR DE DADOS

1.1 O titular de dados e a cultura da proteção dos dados pessoais

Dados pessoais identificam a pessoa e revelam características da sua personalidade. Permitem estabelecer diferenças e também agrupar as pessoas, conforme as suas características em comum e suas afinidades. A história mostra que houve ocasiões em que foi praticada discriminação e crime contra a humanidade, quando foram descumpridos os direitos fundamentais do ser humano, especialmente a dignidade, a igualdade, a liberdade e a justiça, porque algumas pessoas não eram consideradas como tal (escravos, mulheres, estrangeiros, crianças) ou pertenciam a uma religião ou eram consideradas como "raça inferior" ou se manifestavam politicamente contra o *status quo* vigente. Em que pese a noção de direitos fundamentais seja relativamente recente, infelizmente ainda não superamos esse problema, pois os negros, os índios, os pobres, os imigrantes, os LGBTs e talvez venham a ser os não vacinados contra a Covid-19 e suas variantes, além de outros grupos identificados de pessoas em razão de seus dados pessoais,

continuam a ser discriminados em pleno século XXI.

Fato é que o mundo atual é capitalista, que o mercado é global e liberal e que a vida humana é social, isto é, exige que as pessoas se relacionem umas com as outras e negociem entre si e com pessoas jurídicas. Nessas relações, a pessoa natural assume diferentes status ou posições jurídicas, ora no âmbito familiar, na condição de mãe, pai, marido, esposa, companheiro, filho, avô, avó, neto e assim por diante. No âmbito profissional, as pessoas são empregadoras, empregadas, estudantes, profissionais liberais, comerciantes, etc. Na vida civil, a pessoa é contratante, consumidora - mesmo o empregador e o fornecedor, que, quando adquirem bens e serviços para si próprios, assumem a posição jurídica de consumidores - proprietária, locadora, locatária, contribuinte, etc. No âmbito político, a pessoa é candidata, eleitora, cidadã, voluntária. Na rede mundial de computadores, há fornecedores e usuários. Essas relações, quase todas, não são anônimas, especialmente se considerada a digitalização da vida, proporcionada pelo avançado desenvolvimento tecnológico intensificado iniciado no século XX. E o acesso aos dados pessoais, que é facilitado, permite que esses dados sejam utilizados para fins comerciais, políticos, econômicos e ainda discriminatórios, legais e ilegais. Possibilita ainda que a pessoa seja manipulada de várias maneiras, por exemplo, tendo acesso apenas a notícias que seu governo quer que tenha acesso, como ocorre em países não democráticos, mas que também pode ocorrer em democracias, se a rede social não é neutra, sem que a rede mundial de computadores seja livre. Ou, uma vez elaborado seu perfil de consumo, pode a pessoa natural ser induzida a adquirir produtos que combinam com o seu comportamento e até obrigada a pagar mais por esse produto, conforme a sua geolocalização. A instituição financeira pode lhe negar crédito, a operadora de plano de saúde e a seguradora lhe negar serviços após medirem o risco envolvido nas contratações, embora haja vedação legal expres-

sa para os planos de saúde. E quem garante que esse perfil, hoje criado na maioria das vezes de forma automatizada, pela inteligência artificial, está correto? A simples oferta de entretenimento, bem adaptada aos interesses, conforme o perfil do usuário, pode fazer com que ele permaneça conectado a uma mídia digital, sendo prejudicado o desenvolvimento da sua personalidade e inibido o agir político e social que lhe é inerente enquanto pessoa. E as incessantes e indesejadas ligações de telemarketing? Nossos dados pessoais estão sendo acessados com muita facilidade. E o acesso aos dados do cartão de crédito basta para contratar para além das fronteiras, em nome de outro.

Feitas essas considerações, resta claro que quem tem dados pessoais (informação), como titular ou possuidor desses dados, tem poder, obtendo vantagem sobre a concorrência, podendo utilizar esses dados para finalidades diversas e negociar esses dados, obtendo vantagem econômica. Então, para fornecer esses dados, o titular deve ter direito a permitir o acesso somente aos dados essencialmente necessários para possibilitar que o relacionamento pretendido, sob a forma de um negócio livre ou daqueles obrigatórios por força da lei, como, por exemplo, para firmar um contrato de trabalho, para votar nas eleições, para declarar e pagar impostos, para conduzir um veículo, para garantir a segurança e a saúde pública e assim por diante, se realize. E mais: o titular dos dados deve ter a certeza, a segurança e a confiança de que, uma vez fornecidos, esses dados poderão ser tratados na medida de sua finalidade e que serão protegidos e utilizados para os fins legais e legítimos em razão dos quais foram coletados e que serão somente tratados quando o titular der a sua permissão ou quando for legalmente obrigado a fornecê-los, por força de lei. Há, portanto, uma expectativa por parte do titular de dados que deve ser correspondida pelo cumprimento da lei de proteção de dados pelos agentes de tratamento de dados, sob pena de responsabilização em caso de utilização diversa da finalidade de-

clarada, de tratamento de dados pessoais incorretos, de vazamento ou de acesso não autorizado, dentre outras situações que gerem prejuízo ao titular. Então, quanto menos dados pessoais forem fornecidos, mais protegido estará o titular de dados.

É sobre essa matéria que trata a Lei Geral de Proteção de Dados Pessoais – LGPD[1], na forma do seu 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.

No art. 2º, a LGPD define os fundamentos da proteção de dados pessoais em relação ao titular dos dados, a fim de lhe garantir o respeito à privacidade (I); à autodeterminação informativa (II); à liberdade de expressão, de informação, de comunicação e de opinião (III); à inviolabilidade da intimidade, da honra e da imagem (IV); ao desenvolvimento econômico e tecnológico e à inovação (V); à livre iniciativa, à livre concorrência e à defesa do consumidor (VI) e aos direitos humanos, ao livre desenvolvimento da personalidade, à dignidade e ao exercício da cidadania pelas pessoas naturais (VII). E o art. 17 dispõe que 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.

No art. 5º, V, a LGPD define o titular dos dados pessoais como a "pessoa natural a quem se referem os dados pessoais que são objeto de tratamento." Se ainda não temos uma cultura de proteção dos nossos próprios dados pessoais, sabendo dos riscos envolvidos no tratamento desses dados, o mundo digital nos mostra que esse momento chegou.

---

1 BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**.Lei Geral de Proteção de Dados

1.2 Quais são os dados pessoais e os dados pessoais sensíveis?

Existem dados que são sempre considerados dados pessoais e outros dados que, conforme a utilização que deles se possa fazer, também se enquadram nessa mesma categoria. A LGPD define, no art. 5º, dado pessoal como "informação relacionada a pessoa natural identificada ou identificável" (I) e conceitua dado pessoal sensível como "dado pessoal sobre 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 vinculado a uma pessoa natural" (II). Então, nome, CPF, RG, CNH, passaporte, data de nascimento, sexo, endereço, e-mail, estado civil, profissão, escolaridade, número de telefone fixo e móvel, nome dos pais, nome dos filhos são dados pessoais, porque permitem identificar a pessoa a quem corresponde ser o titular desses dados.

Quando são dados que permitem identificar a pessoa fisicamente, como altura, peso, grupo sanguíneo, cor da pele, cor dos olhos, cor dos cabelos, impressão digital, voz, imagem, marcas de nascença, tatuagens, histórico de saúde etc., esses dados são biométricos e sensíveis, porque podem ser utilizados contra a pessoa, em seu prejuízo, ferindo direitos fundamentais e limitando o direito ao livre desenvolvimento da personalidade. Dados que revelam religião, posicionamento político e filosófico também são sensíveis pelo mesmo motivo. Quando utilizados para a concessão de privilégios, o tratamento desses dados fere o princípio constitucional da igualdade em relação aos demais.

E há dados que não seriam considerados sensíveis, mas sua utilização, conforme o caso, pode ensejar os mesmos efeitos discriminatórios que os dados sensíveis revelam sobre o titular. Assim, o estado civil, a formação escolar, as atividades bancárias, as ligações

telefônicas, o histórico de navegação na internet, o histórico de geolocalização (GPS), o endereço de IP, o passaporte de vacinação, que provavelmente será instituído globalmente, os registros e imagens de fronteiras, de pedágios, de câmeras de segurança são exemplos de dados que, conforme o uso que seja feito deles, podem ser considerados sensíveis. Esses dados, ao serem cruzados, atividade na maioria das vezes delegada à inteligência artificial, permitem a criação de perfis do titular, utilizados para os mais diversos fins, legais ou não, dentro e fora do país.

Importante destacar que os dados pessoais identificam a pessoa natural. Então dados que identificam pessoa jurídica, referentes ao CNPJ, não são dados pessoais. Os dados pessoais dos sócios, quando a sua utilização envolve a pessoa natural e não está relacionada à publicidade para identificar o empreendimento, são dados pessoais protegidos pela LGPD. Assim, o tratamento de dados pessoais, cujo acesso é público, deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização (art. 7º § 3º), que aliás são princípios basilares da LGPD.

1.3 Quando o titular pode ou deve fornecer dados pessoais ou sensíveis?

Uma vez que os dados pessoais e sensíveis pertencem ao titular, porque identificam e dizem respeito a apenas uma e determinada pessoa, cabe a ele decidir o que fazer com esses dados. Ele pode ou não fornecer esses dados, a não ser que seja obrigado por força da lei ao fornecimento. Se decidir por fornecer dados pessoais, a regra geral é que ele primeiro deve fornecer o seu consentimento para que esses dados sejam coletados e tratados (art. 7º, I e art. 8º). E consentimento significa manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada (art. 5º, XII). Então, para

fornecer os dados pessoais é preciso estar devidamente informado e saber exatamente quem os solicita e a finalidade para a qual esses dados serão tratados e todos os demais detalhes envolvidos antes de concordar com o tratamento específico desses dados, sendo que as autorizações genéricas para o tratamento de dados pessoais serão nulas (art. 7º, §4º). É preciso que haja total transparência para a obtenção do consentimento pelo titular. Conforme o art.9º, §1º, na hipótese em que o consentimento é requerido, esse será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca.

Então, quem solicita dados pessoais para uma determinada finalidade não vedada por lei pode obtê-los mediante o consentimento do titular, a não ser que tenha acesso a esses dados por meio de exposição pelo próprio titular. É o caso das postagens em rede social. Como o titular torna público o dado pessoal, o consentimento não é exigido (art.7º, §4º), mas os direitos e liberdades fundamentais do titular em relação a esse dado e o tratamento para finalidade legal e lícita deve estar em conformidade com a Constituição Federal, as leis civil e penal, a LGPD e seus princípios, especialmente a boa-fé, considerando a pluralidade das fontes do direito e relação de confiança que existe entre o titular e a plataforma utilizada para a publicação dos dados.

A LGPD define as finalidades para tratamento e compartilhamento de dados pessoais no art. 7º, isto é, quando esses dados podem ser coletados e tratados. São as seguintes: mediante o consentimento do titular (I); para o cumprimento de obrigação legal ou regulatória pelo controlador (II); pela administração pública, para a execução de políticas públicas legalmente previstas (III); para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais (IV); quando necessá-

rio para a execução de contrato, inclusive na fase pré-contratual (V); para o exercício regular de direitos em processo judicial, administrativo ou arbitral (VI); para a proteção da vida ou da incolumidade física do titular ou de terceiro (VII); para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária (VIII) quando necessário para atender aos interesses legítimos do controlador ou de terceiro, prevalecendo os direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais (IX).

Então, algumas dessas finalidades dependem apenas do consentimento do titular, enquanto outras exigem que o titular forneça os dados. Para cumprir obrigação legal, por exemplo, na formalização de um contrato de trabalho, o e-Social exige que o empregador preencha dados pessoais e sensíveis obrigatórios. Assim também para a prestação de serviço médico ou na adoção de medidas sanitárias para evitar a propagação de doenças, podem ser solicitados dados pessoais e sensíveis, devendo o titular, após devida e satisfatoriamente informado, de forma transparente, fornecer esses dados.

Para possibilitar a execução de contratos, pode ser necessário o acesso a dados pessoais do titular. É o caso dos contratos de financiamento bancário, compra e venda de imóveis. O importante é que a finalidade não encontre vedação na lei e que ao titular dos dados sejam conferidos todos os direitos à proteção de dados constantes na LGPD.

Para comprar um produto em uma loja física, é preciso fornecer dados pessoais? Em compras à vista, em dinheiro, não é necessária a identificação da pessoa. Se envolve crédito ou houver obrigação legal em fornecer algum dado ou o fornecimento do dado pessoal for condição para a realização do negócio, então o fornecimento é obrigatório, sob pena de não se concretizar a negociação. Para comprar um produto em uma loja virtual, são necessários o

fornecimento do endereço para a entrega e a identificação do comprador para o fim de comprovar que pagou o preço, por meio dos dados do cartão de crédito ou para a emissão de boleto, e para que possa desistir da compra, devolvendo o produto para exercer o direito de arrependimento, como previsto no Código de Defesa do Consumidor. A LGPD exige que o comprador também seja informado sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa (art. 18, VIII). Quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular será informado com destaque sobre esse fato e sobre os meios pelos quais poderá exercer os direitos do titular elencados no art. 18 da lei (art. 9 § 3º).

Quando o titular de dados participa de promoções na internet, publica suas imagens, responde a questionários, visita sites e faz pesquisas na internet, ele fornece dados pessoais e sensíveis, em geral coletados por *cookies*, mesmo que essas atividades não sejam manifestamente comerciais. Assim, é preciso que o titular dos dados seja informado sobre quais dados serão coletados, como os seus dados pessoais serão tratados e para qual finalidade, etc. para fornecer seu consentimento. Se soubesse quais dados são tratados e para qual finalidade, talvez preferisse não os fornecer.

Há exceções nas quais a LGPD não se aplica, como define o art. 4º: quando o tratamento dos dados for realizado por pessoa natural para fins exclusivamente particulares e não econômicos (I); para fins exclusivamente jornalísticos e artísticos (a); ou acadêmicos (b) (II), para fins exclusivos de segurança pública (a); defesa nacional (b); segurança do Estado (c) atividades de investigação e repressão de infrações penais (d) ou provenientes de fora do território nacional, na forma de lei específica e regulamento pela Autoridade Nacional de Proteção de Dados (III e IV). À exceção do inciso I, trata-se de situações em que prevalece o direito da coletividade em relação

ao direito individual da pessoa, com a finalidade de fornecer a todos segurança e proteção estatal, como exemplo, medidas para combater o terrorismo.

1.4 Direitos do titular de dados

Além do já referido nos arts. 1º, 2º e 17, que consagram o direito da pessoa natural a ter assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade, de privacidade e o livre desenvolvimento da sua personalidade, bem como que os dados pessoais referentes ao exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo (art. 21), o titular de dados tem direito a obter toda a informação necessária relativamente ao tratamento de dados que é ou que será realizado para que forneça o seu consentimento, mesmo nas situações em que é obrigado a fornecer esses dados e naquelas que dispensam a obtenção do consentimento.

Antes de consentir em fornecer dados pessoais e/ou dados sensíveis, na forma do art. 9º, o titular deve saber qual a finalidade específica do tratamento (I), a forma e duração do tratamento, observados os segredos comercial e industrial (II), quem é o controlador e suas informações de contato (III e IV); informações acerca do uso compartilhado de dados pelo controlador e a finalidade (V) responsabilidades dos agentes que realizarão o tratamento (VI) e os direitos do titular, com menção explícita aos direitos contidos no art. 18 da LGPD (VII). O titular tem direito à informação e transparência relativamente ao tratamento dos dados e seu consentimento deve ser livre.

Para fornecer dados pessoais sensíveis, que possam causar dano ao titular, a LGPD exige que o consentimento seja específico e destacado para finalidades específicas (art. 11, I), sendo que não é necessário consentir para fornecer dados sensíveis (art.11, II), quando for indispensável para: a) cumprimento de obrigação legal ou

regulatória pelo controlador; b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral; e) proteção da vida ou da incolumidade física do titular ou de terceiro; f) tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; ou f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

E quando o titular de dados não pode consentir validamente com o fornecimento dos dados pessoais, como no caso das crianças e adolescentes, idosos ou incapazes sob tutela ou curatela? A LGPD regulou a situação das crianças e adolescentes da seguinte forma: o tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, na forma da lei (art. 14). Nos dados de crianças, o tratamento deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal (§ 1º), sendo que o "controlador deve realizar todos os esforços razoáveis para verificar que o consentimento foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis (§ 5º); devendo os controladores manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos a que se refere o art. 18 desta Lei (§ 2º)"; tratar informações pessoais apenas estritamente

necessárias para jogos, aplicações de internet ou outras atividades (§ 4º). Apenas se a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento de que trata o § 1º, é que poderão ser coletados dados pessoais de crianças sem consentimento de pelo menos um dos pais ou do responsável legal (§ 3º).

A LGPD ainda levou em consideração a vulnerabilidade da criança e do adolescente no que diz respeito ao dever de informar, determinando que as informações sobre o tratamento de dados deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança (§ 6º).

Com relação aos incapazes, embora a LGPD não tenha capítulo específico, entende-se aplicável o art. 14, porque os incapazes são titulares de dados representados pelo tutor ou curador. Já os idosos são plenamente capazes de direitos e obrigações, mas, assim como as crianças e adolescentes, têm a vulnerabilidade agravada. É preciso que haja maior transparência e pleno cumprimento do dever de informação e de boa-fé, levando em consideração a vulnerabilidade agravada para a obtenção do consentimento e tratamento de dados pessoais, seja pelo Poder Público ou por empresas privadas. Na relação de consumo, o art. 39, IV do Código de Defesa do Consumidor define como prática abusiva prevalecer-se da fraqueza ou ignorância do consumidor, tendo em vista sua idade, saúde, conhecimento ou condição social, para impingir-lhe seus produtos ou serviços.

Então, mesmo quando dispensado o consentimento e ainda que o tratamento seja realizado por órgãos ou entes públicos ou seja compartilhado, a utilização dos dados e do compartilhamento deve atender a finalidades específicas de execução de políticas públicas e atribuição legal, respeitados os princípios de proteção de dados pessoais elencados no art. 6º (art. 26), devendo ser dada publicidade à dispensa de consentimento, nos termos do inciso I do *caput* do art. 23 e art. 11 § 2º.

Em caso de descumprimento da LGPD, pelo poder público ou não, o titular pode se opor a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento (art. 18, § 2º), podendo o titular revogar o consentimento, caso haja alterações de finalidade das quais discorde (art. 9, § 2º e art. 8º, § 6º). O tratamento posterior dos dados pessoais [...] poderá ser realizado para novas finalidades, desde que observados os propósitos legítimos e específicos para o novo tratamento e a preservação dos direitos do titular, assim como os fundamentos e os princípios previstos na LGPD (art. 7º, § 7º).

Conforme o art. 8º, § 5º, o consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do *caput* do art. 18.

Fornecidos os dados, o que pode ter ocorrido antes da LGPD (2018), o titular dos dados pessoais tem direito ao acesso facilitado aos seus dados pessoais de quem quer que os trate. As informações deverão ser disponibilizadas de forma clara, adequada e ostensiva sobre o tratamento de seus dados (art. 9º). E se forneceu os dados pessoais por meio do consentimento (art. 7º, I), tem direito a obter do controlador a cópia eletrônica integral de seus dados pessoais (art.19, §3º).

O titular de dados tem direito, conforme o art. 18, a obter do controlador, em relação aos dados por ele tratados, a qualquer momento e mediante requisição administrativa: confirmação da existência de tratamento (I); acesso aos dados (II); correção de dados incompletos, inexatos ou desatualizados (III); anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei (IV); portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial (V); eliminação dos dados pessoais

tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 (VI); informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados (VII); informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa (VIII); revogação do consentimento, nos termos do § 5º do art. 8º desta lei (IX).

A LGPD não proíbe que sejam criados perfis pessoais, profissionais, de consumo e de crédito ou os aspectos da personalidade do titular de dados, que afetem seus interesses, mas, se a criação desses perfis ocorrer de forma automatizada (exemplo, por inteligência artificial), o titular dos dados tem o direito de solicitar informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial (art. 20, §§ 1° e 2º) e revisar as decisões tomadas unicamente com base em tratamento automatizado de dados pessoais (art. 20).

Caso os dados pessoais sejam tratados de forma irregular ou indevida, em desacordo com a finalidade declarada, se os dados pessoais e perfis estão incorretos, se há vazamento ou acesso não autorizado aos dados pessoais, dentre outras situações decorrentes do descumprimento da LGPD que possam gerar ou que gerem prejuízo ao titular, configurando dano patrimonial, moral, individual ou coletivo, haverá a responsabilização do agente de dados, na forma da lei (art. 42).

Para exercer seus direitos, o titular de dados pode fazer requerimento expresso, diretamente ou por meio de representante legalmente constituído, ou por intermédio de órgãos de defesa do consumidor (art.18, §§ 1º, 3º e 8º), junto ao controlador ou a outro agente de tratamento (encarregado). As solicitações podem ser feitas à Autoridade Nacional de Proteção de Dados - ANPD, podendo ensejar a realização de auditoria (art. 20, § 2º). Os direitos do titular de dados podem ser exercidos judicialmente, através de ações individuais ou coletivas (art. 22), havendo hoje advocacia especializada em matéria de proteção de dados.

Patrícia de Oliveira Vieczorek

LGPD NAS EMPRESAS

2.

O primeiro questionamento das pessoas jurídicas de direito privado, ou simplesmente "empresas", em relação à LGPD é "isso se aplica a mim?". E a resposta é, SIM. Independentemente do tamanho da empresa, seu regime tributário, sua atividade, todas as empresas[2] precisam estar com suas políticas internas adequadas às disposições da LGPD. Isto porque todas as empresas, de alguma forma, quer seja em meio físico ou digital, quer seja de consumidores, fornecedores ou funcionários, são responsáveis pelo gerenciamento de bases de dados pessoais. É importante lembrar que são dados pessoais o e-mail ou o CPF de qualquer pessoa física, mesmo que ela represente uma empresa[3].

2 Segundo dados disponibilizados pela SERPRO em seu site institucional, dentre os ramos de atividade mais impactados pela LGPD estão as empresas de Software e tecnologia, escritórios de advocacia, empresas das áreas financeira e seguros, comércio digital, pesquisa e perfilamento, saúde privada e planos, publicidade e marketing. Disponível em: https://www.serpro.gov.br/lgpd/empresa/o-impacto-lgpd-nos-negocios. Acesso em: 25/06/2021

3 Manual Prático de Adequação à Lei Geral de Proteção de dados para Micro e Pequenas empresas elaborado e disponibilizado pelo IDEC (Instituto Brasileiro de Defesa do Consumidor), p. 12. Disponível em. https://idec.org.br. Acesso em: 25/06/2021.

As questões envolvendo a proteção de dados pessoais há muito já vêm sendo discutidas no cenário mundial e até mesmo em virtude da economia globalizada e da necessidade de manutenção de relações comerciais/econômicas com outros países, o Brasil também regulamentou o tratamento de dados pessoais por meio da Lei 13.709/2018, LGPD.

Estamos migrando de um cenário de abundância de dados, muitas vezes fornecidos por seus titulares de forma totalmente despretensiosa por meio de formulários na web, nas redes sociais, em compras on-line, dentre outros, para um cenário de restrição tanto em relação à coleta quanto, e principalmente, com relação ao armazenamento e utilização destes dados.

Neste sentido, as empresas também precisam adequar suas rotinas e políticas internas a essa nova realidade. Então, o que fazer para proteger os dados de seus funcionários e de seus clientes?[4]

Para tanto, sugerimos alguns passos básicos.[5] O primeiro passo para iniciar o projeto de adequação é definir os objetivos da empresa (além de cumprir as obrigações legais e evitar multas),[6] como por exemplo: reduzir a coleta de dados ao mínimo necessário para realizar as suas atividades; justificar a coleta e o tratamento desses dados de forma consistente e granularizada, com base nas justificativas que a lei traz; implementar mecanismos técnicos e administrativos de proteção de dados, para evitar a ocorrência de incidentes; criar parâmetros claros para o compartilhamento de dados com eventuais operadores ou contratantes dos serviços.

Após definidos os objetivos do projeto de adequação é preci-

---

4 Assim como os clientes, os funcionários da empresa são titulares de dados tratados por ela em suas rotinas internas. No que diz respeito aos funcionários, eles têm seus dados coletados tanto na fase pré-contratual (recrutamento, seleção, entrevista, etc.), como contratual, com o preenchimento de sua ficha cadastral e demais documentos elaborados e geridos pela empresa durante a relação de trabalho (PPP, CAT, exames periódicos, laudos, atestados médicos, guias de recolhimentos, etc).

5 IDEC, ob. cit. pp. 31-46.

6 Enfim, os principais objetivos que guiam a adequação de uma micro empresa à LGPD estão ligados à eliminação de captações de dados desnecessárias e à criação de processos eficientes que demonstrem para a ANPD e para titulares de dados que a instituição está cuidando bem do seu banco de informações. (IDEC p.33).

so conscientizar e capacitar a equipe de colaboradores para a aplicação da LGPD nos processos da empresa. É importante ressaltar que mesmo que a empresa defina pessoas específicas para tratar dados pessoais, é importante que todos da equipe sejam apresentados aos principais conceitos da lei, seus princípios, justificativas para tratamento de dados dos titulares e possíveis sanções. Também é importante criar uma cultura de proteção de dados na empresa e torná-la um tema de formação constante.

Para implementar o projeto de adequação, a instituição precisará do auxílio de profissionais qualificados para conscientizar os colaboradores sobre a importância da adequação das rotinas internas à LGPD; capacitar o encarregado de dados; analisar os fluxos de dados da sua instituição e propor os ajustes necessários; revisar os contratos celebrados pela empresa; criar cláusulas e avisos sobre captação de dados; redigir os documentos específicos da sua política de proteção de dados; criar listas de condutas (*cheklists*); monitorar a finalização do processo de adequação, etc. Estes profissionais farão o *data mapping*, um raio X de todos os processos da empresa que envolvem o tratamento de dados pessoais, desde sua captação até o descarte.

Para realizar este mapeamento de dados (*data mapping*), é preciso fazer as seguintes perguntas (e registrar detalhadamente as respostas[7]): I) Como os dados pessoais entram na sua instituição?; II) Por quais tratamentos cada tipo de dado passa em cada área ou setor da instituição?; III) Quais são as finalidades de cada informação coletada pela instituição? Todas as informações coletadas são necessárias para o desenvolvimento de suas atividades? IV) Há dados sensíveis? Quais?; V) Há dados que são compartilhados? Quando e com quem?;

7 Tão importante quanto mapear os documentos e a realizar as adequações necessárias à sua conformidade com a LGPD, é documentar muito bem todas as justificativas e definições e organizar os dados em documentos com acesso restrito às pessoas que precisam trabalhar com eles, para evitar vazamentos de dados. É importante sempre considerar a especificidade de proteção dos dados sensíveis. Além de restringir ainda mais o acesso ou o tempo de armazenamento destes dados, a empresa pode elaborar um termo de confidencialidade para colaboradores que trabalhem com essas informações.

VI) Como as informações são armazenadas e descartadas?

Obtidas as respostas para estas perguntas e identificados os documentos utilizados para captação de dados pessoais (fichas de cadastro, contratos, termos, etc.) e quais as finalidades dos tratamentos de dados pessoais feitos pela organização (compartilhamento, análise, etc.) é necessário adequá-los à LGPD. Para isso é necessário incluir cláusulas sobre proteção de dados em todos os contratos e termos; eliminar a captação de dados sem necessidade real para o desenvolvimento das suas atividades; quando possível, anonimizar dados sensíveis ou que não precisam ter seus titulares identificados; elaborar justificativas para as coletas e tratamentos dos dados que serão mantidos, a partir das bases legais que a lei traz; definir tempo de armazenamento dos dados e sua forma de exclusão.

Quanto às bases legais para o tratamento de dados pessoais tem-se que a LGPD não é suficientemente clara quanto à possibilidade de cumulação das hipóteses elencadas em seu art. 7º. Assim, considerando-se os crescentes estudos acerca da matéria, vem tomando força o entendimento que uma mesma operação de tratamento de dados pode ser enquadrada em mais de uma base legal.[8]

Cumpridas estas etapas preliminares é hora de criar (ou ajus-

8 Em recente artigo sobre a possibilidade de cumulação de bases legais nas operações de tratamento de dados pessoais, Fabiano Menke defende que a necessidade de fundamentar adequadamente o tratamento de dados pessoais em base legal é um traço da escola europeia de proteção de dados e assim sendo, por influência dos artigos 6º e 17 do GDPR, afigura-se possível o enquadramento em bases legais cumulativas. Sublinha ainda o Dr. Menke que analisando-se a literalidade do art. 7º da LGPD não há "comando expresso para que apenas uma base legal seja adotada quando do tratamento de dados pessoais" e que segundo Mario Viola e Chiara Spadaccini de Teffé, em sua obra Tratado de Proteção de Dados Pessoais, é possível "o encaixe do tratamento em pelo menos uma das hipóteses legais para que ele seja considerado legítimo e lícito, sendo possível inclusive cumular as mesmas, assim como no GDPR". Paralelamente, é trazida a lume a hipótese da cumulação de bases legais sendo uma delas a do legítimo interesse. Neste caso, em específico, é recomendada a realização de teste de proporcionalidade, em homenagem ao disposto no art. 10, § 3º da Lei.
Neste passo, Fabiano Menke conclui asseverando a viabilidade de enquadramento da operação de tratamento de dados pessoais em mais de uma base legal mediante uma interpretação do art. 7º da LGPD à luz dos princípios norteadores da própria Lei (boa-fé, finalidade, adequação, transparência, prestação de contas, etc.) e do texto do GDPR (matriz europeia em que a lei brasileira foi cunhada), cumprindo a análise da adequação das bases cumulativamente aplicadas, casuisticamente, pela ANPD.

tar, caso já existam) os documentos que comprovam que a empresa está adequada ao que a LGPD estabelece. Estes documentos são:

• **POLÍTICA DE PRIVACIDADE:** deve estar acessível aos titulares de dados e deve conter: a) quem é o encarregado de dados (DPO) da empresa e como entrar em contato; b) como ocorre a captação de cada tipo de dado pessoal e para qual a finalidade; c) quais os mecanismos de proteção das informações captadas; d) quais os programas e softwares utilizados para tratar as informações; e) quais são os operadores envolvidos no tratamento de dados e se esses dados são compartilhados com terceiros, e, ainda se esse compartilhamento é feito dentro ou de fora do país e qual sua finalidade; f) qual o período de armazenamento e a maneira de descarte das informações captadas.

• **AVISO DE *COOKIES* (rastreadores):** é preciso informar que o site utiliza *cookies*, o que é rastreado e qual a finalidade do rastreamento. O ideal é que, quando possível, a instituição invista em tecnologias que permitam ao titular de dados desativar cookies para poder acessar seu site sem ser rastreado;

• **POLÍTICA INTERNA DE PROTEÇÃO DE DADOS:** este documento deve conter a finalidade e a justificativa legal para cada tipo de informação coletada; as regras de compartilhamento e exclusão de dados; as funções básicas e os contatos do DPO e todos os conceitos que serão utilizados neste e nos demais documentos da empresa relacionados direta ou indiretamente à LGPD.[9]

9 Em resumo, a Política interna de proteção de dados é um manual no qual devem estar registradas todas e quaisquer informações que os colaboradores da empresa (não só o DPO) precisam saber para garantir a aplicação da LGPD, como por exemplo, critérios para identificação de dados sensíveis, recomendações de anonimização; regras para o compartilhamento (fornecimento) de informações com outras empresas, jornalistas, fornecedores, etc.

• **POLÍTICA DE PROTEÇÃO DE DADOS PESSOAIS DE COLABORADORES:** informa ao colaborador o interesse da instituição na captação de seus dados pessoais (tanto na fase pré-contratual como na contratual), justificando e elencando as bases legais para tais procedimentos. A política de proteção de dados pessoais de colaboradores deve conter: a) os tipos de dados coletados em processos seletivos e na hora da contratação; b) eventuais diferenças existentes entre contratação de profissionais *freelancers* e efetivo; c) diferenciação entre dados tratados por obrigação legal e por legítimo interesse do controlador; d) explicação sobre os serviços de monitoramento das atividades dos funcionários e da empresa, como ponto biométrico e câmera de vídeo; e) explicação de como se dá o monitoramento da navegação na internet e o uso do telefone, se houver; f) apresentação dos direitos dos funcionários em relação aos seus dados; g) o período de retenção dos dados coletados tanto no processo de seleção quanto na contratação; g) apresentação das situações em que os dados obtidos na contratação podem ser compartilhados, com quem e por quais razões.

• **POLÍTICA DE SEGURANÇA DA INFORMAÇÃO:** essa política irá orientar a equipe interna da empesa ou terceirizados sobre as condutas adequadas para proteger a confidencialidade, a integridade e a disponibilidade dos dados coletados e armazenados pela empresa, enfatizando a responsabilidade da conduta de cada um por esse cuidado. Esse documento irá consolidar a política de proteção de dados da empresa e pode ser solicitado pela ANPD em caso de incidente de vazamento de dados (podendo atenuar a responsabilidade do controlador em caso de vazamento de dados). Basicamente, uma política de segurança da informação deve conter: principais conceitos relacionados à segurança da informação; classificação de cada tipo de informação em níveis de confidencialidade; quais são os provedores de armazenamento e proteção dos arquivos da institui-

ção; quais as recomendações dadas aos (às) funcionários (às) sobre o uso de computadores e internet dentro da empresa, o acesso à arquivos ou *download* de programas ou conteúdos; apresentação do responsável de TI da instituição, seja um(a) profissional da sua equipe ou terceirizado(a).

• POLÍTICA DE INCIDENTE DE SEGURANÇA:[10]

A política de incidente de segurança é um manual com as informações acerca dos procedimentos a serem adotados quando e se ocorrer alguma quebra da segurança. Este documento deve conter: a) definição sobre o que é um incidente de segurança; b) definição de quem vai formar a equipe de resposta a esse incidente ou de quem ficará responsável para lidar com o incidente junto ao DPO; c) apresentação de áreas de suporte nessas situações: jurídico, TI, e DPO; d) indicação de como colaboradores devem proceder ao perceber a falha; e) indicação de como a equipe de resposta deve avaliar a gravidade do incidente; f) apresentação de exemplos de incidentes.[11]

É importante que a política de incidente de segurança seja constantemente atualizada e que suas orientações estejam em consonância com o disposto pela ANPD que disponibiliza em seu site institucional, além dos procedimentos a serem adotados pelo controlador, um formulário de comunicação de incidente de segurança com dados pessoais.

• Definir o encarregado de dados: encarregado de dados ou DPO[12] é a pessoa (física ou jurídica) responsável pelas atividades de tra-

---

10 Infelizmente os incidentes de quebra de segurança aumentam na medida que a inclusão digital avança. Esses incidentes podem ocorrer mesmo após a adoção de todos os meios disponíveis para a implementação de medidas de segurança de dados e de adequação à LGPD. O importante é que a empresa tenha se precavido antes, implementando todas as medidas que estavam ao seu alcance para a proteção dos dados por ela tratados e armazenados, e, que depois do incidente reaja da melhor forma (isso pode atenuar eventuais penalidades por danos provocados a titulares de dados).

11 Para avaliação da gravidade de um incidente de quebra de segurança (vazamento de dados), sugere-se a utilização de matrizes de risco e de severidade.

Disponível em: https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca .Acesso em: 26/06/2021

tamento de dados pessoais e pelo contato com a ANPD e com os titulares. Em razão de suas atividades é essencial que o encarregado entenda bem os conceitos da LGPD e os fluxos de dados da empresa, sendo capaz de operar seus mecanismos de proteção de dados. Suas principais funções são: a) aceitar reclamações e comunicações dos titulares de dados e encaminhar suas demandas à área responsável, para tratamento; b) receber comunicações da ANPD e adotar as providências cabíveis; c) orientar colaboradores e parceiros da empresa sobre conceitos e práticas que garantam a proteção de dados pessoais.

Além disso, o encarregado deve ser capaz de monitorar o funcionamento da estrutura de proteção de dados criada a partir da adequação à LGPD, bem como manter atualizado o mapeamento dos fluxos de dados da empresa e comunicar internamente à ANPD e aos titulares de dados eventuais mudanças na captação e tratamento de dados, sempre com base na justificativa prevista na lei dentre outras atividades relacionadas às boas práticas de tratamento de dados.

Vale lembrar que a duração do projeto de adequação à LGPD varia de acordo com o engajamento dos gestores da empresa, com o seu número de colaboradores, com o volume/fluxo de tratamento de dados e com o risco envolvido nas atividades de tratamento dos dados.

2.1 Dicas importantes

O processo de adequação à LGPD não precisa ser caro e deve se adaptar à realidade da empresa. Este processo de adequação à Lei é bastante específico para cada instituição e deve ser feito sob medida para sua realidade.

12 Vide no glossário, no tópico 5 a definição de encarregado e sua função, que embora tenha essa nomenclatura na lei brasileira, também é conhecido como Data Protection Officer (DPO) por ter a nomenclatura em inglês.

Todas as empresas têm condições de cumprir o que a LGPD determina. A implementação de programas de governança de dados é um investimento nos processos e estruturas de dados da organização que, além de garantir a adequação às exigências legais, poderá aumentar a eficiência da sua instituição e aumentar as possibilidades da empresa de receber investimento e realizar parcerias com empresas e instituições filantrópicas estrangeiras que já tenham se adequado à legislação de proteção de dados europeia, por exemplo.

A empresa pode implementar a LGPD com a estrutura já existente. Não é necessária a criação de um setor de tecnologia da informação.

Não é preciso coletar o consentimento de titulares de dados para toda ação que envolve seus dados, desde que se enquadrem em base legal que não seja o consentimento. Vale lembrar que o consentimento deve ser a exceção!

A LGPD não impede que a empresa monitore seus colaboradores, durante o exercício de suas atividades laborais ou requisite os seus antecedentes criminais, quando isso for justificável e tenha previsão legal. O monitoramento de colaboradores não é proibido, mas, com a aplicação da lei, as pessoas devem conhecer o funcionamento e a finalidade desse monitoramento.

Antecedentes criminais podem ser solicitados em casos específicos já identificados pela Justiça do Trabalho, como para as posições de motorista, trabalhadores que atuem nas áreas de segurança privada, com informações sigilosas, entre outras.

Vanise Saciloto Camassola

3. LGPD E OS ESCRITÓRIOS DE ADVOCACIA

Os escritórios de advocacia têm um grande compromisso com a Lei Geral de Proteção de Dados, de modo que, praticamente todos os atos em que se realiza a prestação de serviço, há dados pessoais envolvidos, seja no primeiro contato com cliente diante de documentação recebida, ou ainda na sua procuração, contrato de honorários, e na petição inicial, defesa, indicação de testemunha ou produção de provas.

Os dados pessoais do seu cliente e de terceiros envolvidos ao fato que se trata estarão em constante nível de tratamento, o que merece grande atenção. Atualmente, os processos eletrônicos já são uma realidade no meio jurídico, porém, ainda existem muitos processos físicos em fase de adaptação e transição para o meio digital, fato que admite que o profissional advogado possua documentos em âmbito físico e digital.

Inicialmente, é importante que o advogado possa validar os documentos que possui em ambiente físico, documentos que constem dados pessoais e valide a necessidade para sua posse e arquivo, bem como a finalidade a que se destinam. Ainda é de grande valia

levar em consideração a digitalização destes documentos, passando a eliminar ou até mesmo devolver aos titulares os documentos contidos em excesso, que estejam duplicados ou que não mais serão utilizados nas demandas contratuais, de maneira a limitar o tratamento e preservá-lo durante a retenção destes documentos.

É importante salientar que alguns documentos são utilizados durante o processo judicial em diversas etapas, o que não obriga sua inutilização ou exclusão devido a sua manutenção necessária justificadamente pelo procedimento extrajudicial ou judicial, mas o indicado é deixá-los em um ambiente seguro para evitar qualquer incidente. Ainda, caberá ao advogado demonstrar ao seu cliente sua transparência em tratar seus dados pessoais, de modo a que exerça boas práticas e cultura de proteção de dados e possibilite que o cliente exerça seus direitos de autodeterminação informativa e respeito para com a privacidade do cliente. É muito comum ainda que profissionais autônomos, ou propriamente os escritórios de advocacia, precisem realizar diligências em comarcas diferentes, muitas vezes distantes das suas próprias. Viajar até lá implicaria em gastos com transporte, alimentação e possivelmente até mesmo hospedagem, assim, uma alternativa mais vantajosa é delegar o serviço para um advogado local, o chamado então correspondente jurídico.

É inevitável que, para isso, seja necessário compartilhar informações do seu cliente para o correspondente jurídico realizar a diligência necessária na comarca em que você não atua. Pois bem, esta situação também é protegida pela Lei Geral de Proteção de Dados e você, advogado autônomo ou escritório, deverá atentar-se e evidenciar seu cuidado para com esses dados. Atualize seus contratos com seus correspondentes, bem como, alerte seus clientes que a situação poderá ocorrer e, se for o caso, permita que o titular de dados lhe forneça o consentimento necessário para o tratamento daquelas informações.

Para isso, é necessário que se observe a necessidade de conter evidências que comprovem a boa atuação legal, por meio de políticas, conscientizações, treinamentos, termos, e documentos necessários para comprovação a atuação legal. Isso inclui a mudança de cláusulas contratuais no contrato de honorários realizado diretamente com o cliente. Atente-se a estas informações.

Importa salientar que o sigilo profissional não se confunde com a Lei Geral de Proteção de Dados, pois ambas determinações buscam regulamentar situações diversas. Os direitos do titular de dados, o papel de dono dos próprios dados, serão acompanhados pela LGPD, diferentemente do dever de confidencialidade sobre as informações conhecidas em razão do exercício profissional do advogado.

Os escritórios de advocacia, ou mesmo o advogado autônomo (que exerce atividade com fins econômicos), para iniciar sua adequação à Lei Geral de Proteção de Dados, deverão se atentar às sugestões primordiais para que a atividade advocatícia esteja a atender os requisitos legais da LGPD.

3.1 Tenha um encarregado de dados

O art. 41 da Lei 13.709/2018 (LGPD) traz a obrigação de existir o encarregado de dados (ou DPO – *Data Protection Officer*), nomeado exclusivamente pelo controlador, para fins de aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências, receber comunicações da autoridade nacional e adotar providências, orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais, executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

Saiba que a identidade e as informações de contato do encarregado de dados deverão ser divulgadas, publicamente, de for-

ma clara e objetiva. Os escritórios de advocacia que possuem site eletrônico deverão publicar a informação de seu encarregado de dados juntamente ao site que possuem, permitindo que o titular de dados possa contatá-lo sempre que necessário.

3.2 Tenha controle sobre os dados que possui em seu escritório

Uma das sugestões mais importantes é que você tenha controle e ciência dos documentos que estão sob sua responsabilidade. Nesta hipótese, você conhecerá e poderá identificar todos os dados e suas consequentes diferenças, dados pessoais, dados pessoais sensíveis ou dados anonimizados e, consequentemente, trabalhará sobre eles de acordo com a permissão legal, com a retenção correta e utilizando-se das bases legais que dizem respeito ao seu tratamento. Em casos de compartilhamento, o consentimento deve ser claro, com finalidade específica, granularizado e com as devidas informações de controlador, tempo de retenção, e principalmente, conter os direitos do titular.

Desta forma, será também possível identificar todo o ciclo de vida que os dados pessoais apresentam no seu escritório, inclusive as finalidades e utilização que lhe são destinados e se são ou não compartilhados com outras organizações. A partir deste conhecimento, o advogado passará e poderá classificar os dados que tem em posse e devolvê-los, excluí-los, ou mantê-los conforme a necessidade, finalidade do seu uso, e o grau de proteção que possui.

3.3 Crie políticas internas para proteção de dados

Se você trabalha sozinho ou em conjunto com outros advogados, bacharéis em direito ou estagiários, é importante saber que todos os integrantes da equipe precisam trabalhar em conjunto para a proteção integral dos dados pessoais que o escritório administra.

Como já mencionado anteriormente, nos casos em que seu escritório possua site eletrônico para a divulgação de informações, áreas de atuações ou notícias da sua área, a Política de Privacidade, assim como os termos de uso e informações pertinentes ao encarregado de dados, devem estar visíveis e claras ao titular. Porém, internamente é importante que também s e tenham políticas e métodos para a cultura de boas práticas e proteção de dados.

A forma de atuar na advocacia pressupõe ligação direta aos dados de seus clientes, estes que, muitas vezes, são indispensáveis ao andar processual. Cabe ressaltar que o escritório deva criar, atualizar e manter viva a Política Interna para com a Confidencialidade e Proteção dos Dados Pessoais a que se possui acesso. Ainda, cada advogado poderá utilizar-se de senhas de acesso para logar nos sistemas internos e/ou externos para a execução de suas atividades laborativas, bem como o escritório poderá criar limites de acesso a determinados dados pessoais, principalmente em casos de segredos de justiça.

3.4 Adeque seus contratos de honorários à LGPD

Outra situação muito utilizada no dia a dia dos advogados, imprescindível para a atuação com terceiros, são os contratos de honorários. Uma das bases principiológicas da LGPD, a transparência, demonstra e traz garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.

Acrescente, altere e modifique as cláusulas contratuais presentes nos documentos particulares para que seu escritório possa demonstrar ao titular e, principalmente, informá-lo de seus direitos, do tratamento realizado para com seus dados pessoais e a transparência existente diante da relação contratual a ser pactuada. Caberá

ao escritório, no papel de controlador de dados, manifestar ao titular de dados a boa-fé existente para com a utilização necessária dos dados, bem como a relação de confiança a ser exercida entre as partes.

3.5 Adote práticas regulares para a mitigação de riscos

Além disso, se for possível, leve em consideração criar um comitê de ética multidisciplinar, se for possível, para instaurar as boas práticas de *compliance* e governança, buscando a melhor solução diante do tratamento de dados. O encarregado de dados, ou DPO, deverá auxiliar na mitigação de riscos favorecendo o auxílio dos demais membros a promover e executar o tratamento de dados corretos diante da legislação exigida e a cultura de proteção de dados para os clientes do seu escritório. Se faz necessário, também, manter as evidências necessárias que comprovem a boa atuação legal, através de políticas, conscientizações, treinamentos, termos, e documentos fundamentais para comprovação a atuação legal. Isso inclui a mudança de cláusulas contratuais no contrato de honorários realizado diretamente com o cliente. Atente-se a estas informações.

O Relatório de Impacto à Proteção de Dados (RIPD) servirá como uma base ao escritório para atentar-se a possíveis incidentes e, também, as possíveis formas de saná-los ou preveni-los. É importante que seu escritório possua um RIPD adequado.

O RIPD, sozinho, não vai eliminar todos os riscos presentes em seu escritório, mas é um processo importante porque identifica e minimiza os riscos relacionados ao processamento de dados pessoais, levando em consideração os benefícios que você deseja alcançar.

RAPHAEL DI TOMMASO
LUGARINHO DA FONSECA

4. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD)

De acordo com a LGPD, a Autoridade Nacional é o "órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta lei em todo o território nacional". Trata-se de uma definição que, por si só, não deixa muito clara a real importância desse órgão. Ao analisarmos o restante da lei, no entanto, começamos a perceber sua verdadeira dimensão.

Inicialmente, cabe mencionar que se trata de órgão ligado diretamente à Presidência da República. Em que pese se tratar de uma característica que mostra a importância da ANPD, esse fator tem sido alvo de críticas por parte da doutrina por poder comprometer a independência da autoridade. A própria lei, todavia, destaca a transitoriedade da natureza jurídica do órgão, permitindo sua transformação, pelo Poder Executivo, em entidade da administração pública indireta, submetida a regime autárquico especial. Essa avaliação deverá ocorrer em até dois anos da entrada em vigor da estrutura regimental da ANPD, ocorrida em 6 de novembro de 2020. Vale destacar que a principal crítica diz respeito à autonomia financeira da ANPD, uma vez que sua autonomia técnica e decisória é garantida pela própria lei (art. 55-B).

À época da nomeação dos primeiros diretores executivos do Conselho Diretor do órgão, também houve críticas de parte da imprensa a uma alegada "militarização" da ANPD, ante o fato de três de

seus diretores nomeados serem do Exército Brasileiro. A crítica é, no entanto, na melhor das hipóteses, exagerada e, na pior, mal intencionada.

A lei determina (art. 55-D, §§ 1º e 2º) que os membros do Conselho Diretor sejam escolhidos e nomeados pelo Presidente da República, exigindo que sejam brasileiros com "reputação ilibada, nível superior de educação e elevado conceito no campo de especialidade dos cargos para os quais serão nomeados". Há, ainda, outra limitação legal relevante: a ANPD é criada "sem aumento de despesa" (art. 55-A).

Importante, todavia, abrir um parêntese para destacar que os diretores são altamente qualificados tecnicamente para os cargos para os quais foram nomeados. O diretor-presidente, Waldemar Gonçalves Ortunho Júnior, é formado em engenharia eletrônica pelo Instituto Militar de Engenharia – IME, uma das mais respeitadas instituições de ensino superior do país, além de ter pós-graduação em engenharia elétrica pela Universidade de Brasília – UnB, e ter atuado como engenheiro na Diretoria de Telecomunicações do Ministério da Defesa e chefe do Centro de Telecomunicações do Exército. Arthur Pereira Sabbat, por sua vez, além da formação militar, possui, dentre suas pós-graduações, uma em Gestão da Segurança da Informação pelo IESB e uma em Crimes Cibernéticos pela UNISUL, além de dezenas de cursos realizados em instituições nacionais e internacionais, incluindo certificação pela Exin, uma das certificadoras mais respeitadas do mundo. Em sua vasta atuação profissional, destacam-se os cargos de coordenador-geral do Centro de Tratamento e Resposta a Incidentes do Governo e de Diretor do Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República. Por fim, Joacil Basilio Rael é engenheiro de computação, também formado pelo Instituto Militar de Engenharia – IME, onde fez mestrado em sistemas e computação, e doutor em ciências da informação pela Universidade de Brasília – UnB. Tem vasto conhecimento nas áreas

de criptografia, segurança da informação e proteção de dados.

Duas diretoras civis completam o quadro: Miriam Wimmer, que é doutora em políticas de comunicação e cultura pela UnB, mestre em direito público e graduada em direito pela Universidade do Estado do Rio de Janeiro – UERJ, além de contar com certificação intitulada Certified Information Privacy Professional/Europe – CIPP-E pela International Association of Privacy Professionals – IAPP, a mais respeitada instituição do mundo no segmento; e Nairane Farias Rabelo Leitão, advogada atuante na área, autora de diversos artigos e também certificada pela Exin.

Esse parêntese se faz necessário para deixar claro que o conselho diretor da ANPD nasceu altamente qualificado, com profissionais com alto nível de conhecimento na área – o que, diga-se, não é a regra em outros órgãos fiscalizadores, muitas vezes aparelhados pelas próprias empresas que deveriam fiscalizar. Essa qualidade fica clara, inclusive, já nas primeiras ações da ANPD, que vem publicando materiais orientativos de excelente nível técnico e didático. As críticas feitas inicialmente por uma parcela da imprensa, portanto, não se sustentam.

Além do supramencionado Conselho Diretor, também compõem a ANPD o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade – CNPD, em fase de composição enquanto escrevo este texto, a corregedoria, a ouvidoria, um órgão de assessoramento jurídico próprio e unidades administrativas e unidades especializadas necessárias.

Das estruturas mencionadas, o CNPD merece atenção especial, ante sua importância e suas características. Trata-se de um conselho plural, com 23 representantes do poder público e de instituições e entidades da sociedade civil. Seu papel está definido no art. 58-B: propor diretrizes estratégicas e fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da

Privacidade e para a atuação da ANPD (I); elaborar relatórios anuais de avaliação da execução das ações da Política Nacional de Proteção de Dados Pessoais e da Privacidade (II); sugerir ações a serem realizadas pela ANPD (III); elaborar estudos e realizar debates e audiências públicas sobre a proteção de dados pessoais e da privacidade (IV); e disseminar o conhecimento sobre a proteção de dados pessoais e da privacidade à população (V).

Na data em que esse texto foi escrito, ainda não haviam sido nomeados os 13 representantes da sociedade civil, cujo processo de escolha é regulado por meio de editais, embora já tenham sido compostas listas tríplices por vaga, faltando apenas o Presidente da República escolher um titular e um suplente de cada lista.

4.1 Atribuições da ANPD

A competência da ANPD está positivada, principalmente, no art. 55-J da LGPD. Em linhas gerais, pode-se dizer que suas atribuições são, nas palavras do legislador, "zelar, implementar e fiscalizar o cumprimento" da Lei. Vale destacar, de pronto, que seu papel é zelar não apenas pela proteção dos dados pessoais, mas, também, pela observância dos segredos comercial e industrial.

No âmbito da regulamentação, do planejamento e da promoção da cultura da proteção de dados, cabe à ANPD elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade; promover, na população, o conhecimento das normas, políticas públicas e medidas de segurança afeitas ao tema; promover e elaborar estudos sobre as práticas de proteção de dados e privacidade; estimular a adoção de padrões com vistas a facilitar o controle dos titulares sobre seus dados pessoais; dispor sobre as formas de publicidade das operações de tratamento de dados; elaborar relatórios de gestão periódicos; editar regulamentos e procedimen-

tos sobre proteção de dados pessoais e temas conexos; editar normas, orientações e procedimentos simplificados e diferenciados para microempresas, empresas de pequeno porte e startups; regulamentar o acesso a dados pessoais utilizados para estudos em saúde pública (art. 13, § 3º); regulamentar o processo de portabilidade de dados pessoais a outros fornecedores (art. 18, V); regulamentar o processo de atendimento aos direitos do titular (arts. 18, §§ 3º e 5º e 19, §3º); regulamentar a informação acerca da comunicação ou uso compartilhado de dados de pessoa jurídica de direito público a pessoa de direito privado (art. 27, *caput* e parágrafo único); regulamentar e avaliar, para fins de transferência internacional, se o nível de proteção de dados de país estrangeiro ou organismo internacional é adequado às exigências da LGPD (art. 34, *caput* e IV); definir cláusulas-padrão contratuais, verificar cláusulas específicas para uma determinada transferência e a regulamentação da aplicação de sanções administrativas.

Especificamente no que tange à regulamentação das sanções administrativas, foi aberta, em 28 de maio de 2021, consulta pública para avaliação da Resolução de Fiscalização, que dispõe sobre a fiscalização e a aplicação de sanção pela ANPD. Embora o documento ainda não tenha sido validado até a data em que esse texto foi concluído, ele deixa claros os caminhos que a ANPD pretende seguir. Inicialmente, dispõe que a fiscalização se subdividirá nas atividades de monitoramento, orientação e atuação preventiva, além de estabelecer que a finalidade da Resolução é prevenir e reprimir as infrações à LGPD.

Não cabe, aqui, discorrer profundamente acerca do documento, até porque ele ainda deve sofrer alterações, mas alguns aspectos são dignos de menção. Um dos pontos mais relevantes, por óbvio, é a regulamentação do processo administrativo, que não traz grandes novidades em relação ao que já ocorre em outros órgãos.

No que tange à atividade de fiscalização, a Resolução traz questões interessantes. Inicialmente, determina que a ANPD "adota-

rá procedimentos de monitoramento, orientação e atuação preventiva na sua atividade de fiscalização". O monitoramento tem o intuito de levantar informações relevantes que venham a subsidiar as competências regulatória, fiscalizatória e sancionadora. A orientação visa a promover a conscientização e educação dos titulares e agentes de tratamento.

A atividade preventiva pretende auxiliar na condução do agente de tratamento à "plena conformidade", além de evitar ou remediar situações que possam causar riscos ou danos aos titulares. Quem trabalha na área, no entanto, sabe que a conformidade plena é uma meta que se situa em algum ponto entre o ousado e o utópico, notadamente em um país como o Brasil, em que a insegurança jurídica vem se tornando regra.

A atividade repressiva, que vem sendo utilizada como argumento de venda por parte do mercado de consultoria, está voltada à interrupção de situações de dano ou risco, à reparação de danos, à recondução à "plena conformidade" e à tão temida punição aos responsáveis por meio do já referido processo administrativo.

Vale salientar que, como esperado, o foco da atividade da ANPD não será punir, mas prevenir e educar. A proposta de Resolução deixa isso claro. Pelo que se aduz do documento, o agente de tratamento que agir de boa-fé terá todas as chances para corrigir suas inconformidades antes de sofrer uma sanção pecuniária.

De forma acertada, as medidas preventivas adotadas pela ANPD não serão consideradas sanções. As medidas previstas são a divulgação de informações, o aviso, a solicitação de regularização e o plano de conformidade, conforme o caso concreto. Caso o agente de tratamento descumpra o que acordar com a Autoridade ou aja reiteradamente em inconformidade com a lei, poderá responder processo administrativo sancionador, que pode ter início de ofício pela ANPD, em decorrência de processo de monitoramento ou diante de requerimento. Importante mencionar a previsão, no texto atual, pra

arquivamento do processo em caso de suspensão comprovada da conduta investigada e, se cabível, reparação dos danos dela decorrentes. O arrependimento é cabível até a intimação da decisão de primeira instância.
A Resolução também prevê a possibilidade de celebração de termo de ajustamento de conduta (TAC) por iniciativa do autuado, que acarreta a suspensão do processo, caso aceito pela ANPD.

Na possibilidade de condenação, o autuado poderá recorrer administrativamente da decisão, sendo necessária a intimação do recorrente nos casos em que sua situação puder se agravar. Por fim, sempre que surgirem fatos novos e relevantes, os processos que resultarem em sanção poderão ser revistos, a pedido ou de ofício, sendo que, a sanção do autuado não poderá ser agravada nos casos de revisão.

Nota-se, portanto, que a proposta de Resolução apresentada vai ao encontro do que tem sido dito pelos diretores da ANPD e pela melhor doutrina desde o começo: a prioridade não é punir, mas orientar, educar e incentivar a adequação.

Além do exposto, também cabe à ANPD promover ações de cooperação com autoridades de proteção de dados estrangeiras e articular-se com autoridades reguladoras públicas. Suas atividades também devem ser coordenadas com os demais órgãos e entidades públicos responsáveis pela regulação de setores específicos, inclusive por meio de fórum de comunicação. Quanto a esse ponto, vale mencionar os acordos de cooperação técnica já firmados com a Secretaria Nacional do Consumidor (Senacon) e com o Conselho Administrativo de Defesa Econômica (Cade).

4.2 Guias orientativos e operacionais

Outra atividade da ANPD, que merece destaque e reconhecimento, é a publicação de diversos guias, que vem ocorrendo desde sua constituição. Os guias oferecem excelentes subsídios para as

empresas e órgãos que desejam se adequar à lei, além de auxiliarem na compreensão de alguns conceitos da LGPD.

O Guia de Boas Práticas, elaborado em agosto de 2020, apesar de voltado para a implementação na administração pública, tem material muito rico. Aborda os direitos fundamentais do titular, explica o tratamento de dados, seus requisitos e seu ciclo de vida, apresenta boas práticas em segurança da informação e discorre sobre as principais normas concernentes ao tema, a exemplo das ISO 27001 (sistemas de gestão da segurança da informação) e 31000 (gestão de riscos).

O Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado também é muito útil para auxiliar na compreensão dos papéis do encarregado (vulgo DPO) e da diferença entre controlador e operador. Trata-se de importante documento que pôs fim à dúvida suscitada por pessoas de fora da área quanto a quem pode ser controlador ou operador (houve quem defendesse que poderia ser alguém de dentro da organização, e não a organização em si, em decorrência da interpretação equivocada do art. 5º, incisos VI e VII de forma isolada do restante da lei). O documento também traz dicas valiosas para os agentes de tratamento se adequarem à lei.

O Guia de Elaboração de Programa de Governança em Privacidade, por sua vez, define o que é um programa de governança em privacidade, explicando como estruturá-lo e trazendo um "passo a passo" desde a iniciação e planejamento até a fase de monitoramento.

Há, ainda, outros materiais interessantes disponíveis, como guias para elaboração de inventário de dados pessoais, de termo de uso, de avaliação de riscos, de elaboração de relatório de impacto à proteção de dados, de segurança em aplicações web e de framework de segurança.

Além dos guias em formado pdf, o site da ANPD disponi-

biliza aulas em vídeo, templates, estudos de caso e outros materiais muito ricos, não só para quem está "engatinhando" no tema, mas também para profissionais da área.

4.3 Próximos passos?

A ANPD tem se mostrado bastante ativa, mas ainda há muito trabalho pela frente nos próximos meses – quiçá anos. De acordo com a agenda regulatória publicada, os próximos passos devem ser a regulamentação diferenciada para pequenas e médias empresas, startups e pessoas físicas que tratam dados pessoais com fins econômicos, a aprovação da Resolução de Fiscalização, a regulamentação dos pontos pendentes para comunicação de incidentes e a regulamentação para a confecção do relatório de impacto à proteção de dados pessoais (RIPD ou DPIA). Posteriormente, o estabelecimento de normas complementares acerca da definição e das atribuições do encarregado pela proteção de dados pessoais (DPO) e a regulamentação das transferências internacionais de dados pessoais. Por fim, a regulamentação de pontos pendentes concernentes aos direitos dos titulares e a publicação de documento orientativo em relação às hipóteses (ou bases) legais de tratamento de dados pessoais.

Certamente tem muito mais a ser feito, mas essas questões são as que estão elencadas na agenda regulatória e certamente são prioritárias. Há outros pontos listados no documento que já estão prontos, como a publicação do primeiro regimento interno da ANPD e a divulgação do planejamento estratégico 2021-2023 da Autoridade. Outros, como a regulamentação do processo sancionatório e a regulamentação diferenciada para as empresas de pequeno porte (EPPs) e startups, já estão bem adiantados. Há, entretanto, alguns pontos que devem demorar um pouco mais, especialmente em razão da exigência legal de realização de audiências públicas, consultas públicas e análises de impacto regulatório. O que se pode dizer desde já é que, mesmo com uma estrutura muito

aquém da necessária, a Autoridade Nacional vem mostrando um excelente trabalho, tanto do ponto de vista técnico quanto de produtividade.

Mônica Tais Medeiros
Lopes Scariot

5. GLOSSÁRIO LGPD

AGENTES DE TRATAMENTO DE DADOS: São aqueles que tratam, operam etc. os dados pessoais. Na LGPD são o controlador e o operador (vide mais adiante conceito mais específico dos agentes).

ANONIMIZAÇÃO: 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;

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD): Órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da Lei Geral de Proteção de Dados em todo o território nacional.

BANCO DE DADOS: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

DADO ANONIMIZADO: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

DADO PESSOAL: informação relacionada a pessoa natural identificada ou identificável. Ou seja, são dados tais como NOME, CPF, RG,

data de nascimento, e-mail, etc. Identificável quer dizer que somado a outras informações, é possível identificar o titular, por exemplo: apelido, placa de carro etc.

DADO PESSOAL SENSÍVEL: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou à organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
Ou seja, são informações sensíveis, que podem gerar algum tipo de discriminação ou exposição.
Exemplo: religião, exame médico (resultado de HIV positivo ou informação de doença).

CONSENTIMENTO: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada; também conhecido como autorização.

CONTROLADOR: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.
Exemplo: uma loja ou site que coleta e armazena dados de um consumidor.

COOKIES (RASTREADORES): arquivos enviados por servidores de sites e/ou plataformas para o computador ou celular do usuário, que ficam armazenados no seu equipamento, com o objetivo de identificá-lo e obter dados de acesso (como, por exemplo, o IP, histórico de navegação, etc.), que são considerados dados pessoais. Esses dados permitem identificar o perfil do usuário e podem ser usados para garantir maior segurança e personalizar sua experiência nos sites e plataformas. São divididos em necessários (técnicos

para navegação) e opcionais (relacionados a publicidade, preferências etc.).

ELIMINAÇÃO: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado.

ENCARREGADO: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).
Observação: em inglês, essa pessoa é normalmente chamada de Data Protection Officer (DPO). Por isso, ainda que nomenclatura da lei brasileira seja encarregado, é comum ver essa figura nominada também como DPO.

INCIDENTE DE SEGURANÇA: violação de segurança que provoca, de modo acidental ou ilícito, a distribuição, perda, alteração, divulgação de dados ou o acesso não autorizado a dados pessoais sujeitos a qualquer tipo de tratamento.

OPERADOR: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.
Exemplo: um escritório de contabilidade que recebe os dados dos funcionários de uma empresa para cumprimento das obrigações legais.

POLÍTICA DE PRIVACIDADE: documento que contém informações acerca do uso dos dados (informações sobre coleta, armazenamento, compartilhamento, descarte etc.) de forma transparente e clara. Pode conter conceitos, direitos dos titulares, bem como pode ser externa (direcionada normalmente para o público geral) e também interna (relativa ao tratamento dos dados dos funcionários, parceiros etc.).

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS (RIPD): documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

SUBOPERADOR: é aquele contratado pelo operador para auxiliá-lo a realizar o tratamento de dados pessoais em nome do controlador.

TERMOS DE USO/TERMOS DE SERVIÇO: documento que contém regras e diretrizes relacionadas a determinado serviço.
Exemplo: termos de uso de aplicativo (normas para utilização, que conterão diretrizes sobre cobrança ou gratuidade, etc.).

TITULAR: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento. O titular dos dados pode ser comparado ao consumidor na relação de consumo.

TRATAMENTO DE DADOS: toda operação realizada com dados pessoais (tudo o que pode ser feito com os dados pessoais), como, por exemplo: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

TRANSFERÊNCIA INTERNACIONAL DE DADOS: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro.

USO COMPARTILHADO DE DADOS: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.

Mônica Tais Medeiros
Lopes Scariot

6. DICAS PRÁTICAS

• Se você é controlador ou operador de dados pessoais, lembre-se de solicitar somente os dados necessários para finalidade indicada, evitando, dessa forma, o acúmulo de dados desnecessários.

• O consentimento deve ser solicitado para cada finalidade específica, logo, se houver modificação na finalidade inicial do tratamento de dados, deve-se obter um novo consentimento.

• Na qualidade de titular dos dados, você tem uma série de direitos, previstos no art. 18 da LGPD. Dentre eles, você pode solicitar de imediato a confirmação de acesso aos seus dados pessoais. O controlador dos dados deverá fornecer imediatamente informações sobre os dados que possui, bem como, no prazo de 15 dias, deverá fornecer um relatório completo, contendo, além dos dados que possui, o fluxo dos referidos dados (se são ou não compartilhados e com quem, por exemplo) dentre outras informações que foram obtidas a partir do mapeamento dos dados, conforme previsto no art. 19 da LGPD.

O formato desse arquivo (se impresso ou digital) é o titular que escolhe, conforme previsão do artigo 19, II, §2 da LGPD.

• CUIDADO com seus dados pessoais! Evite divulgá-los (cuidado com postagens de fotos com certificados, carteira de vacina-

ção etc.). Muitas vezes não percebemos, mas dando um zoom na imagem, é possível identificar uma série de dados pessoais, o que é um prato cheio para fraudadores.

• Uma das formas de vazamentos de dados pessoais ocorre por meio de cibercrimes. Por isso, utilize senhas fortes, conforme sugestão que segue: Crie uma senha longa (8 caracteres ou mais), contendo letras maiúsculas e minúsculas, números e símbolos (*@#:/.). Não use palavras nem datas pessoais, o que dificultará os algoritmos que são utilizados para descobrir suas senhas e invadir seus dispositivos.

Ainda, mantenha o antivírus atualizado e faça as devidas atualizações do sistema operacional. Se você utiliza compartilhamento de documentos, realize a configuração de rede corporativa, com hierarquia de pastas, política de restrições/permissões de acesso e firewall corporativo. Coloque senha de usuário para acesso ao sistema operacional (ou acesso ao computador). As medidas de segurança da informação não impedirão que possa ocorrer algum crime cibernético, contudo, atuarão na prevenção e mitigação dos riscos.

• Apesar de ter sido promulgada em 2018, a LGPD ainda é uma lei nova e possui algumas questões que serão regulamentadas pelas ANPD. Fique por dentro dessas atualizações no site oficial da Autoridade Nacional de Proteção de Dados (https://www.gov.br/anpd/pt-br), bem como nas suas mídias sociais: @anpdgov @ANPD - Linkedin e Canal do Youtube: Autoridade Nacional de Proteção de Dados - ANPD.

REFERÊNCIAS

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados.

MALLMANN, Felipe Pereira e Sulzbach, Cesar Emílio. Coord. Lei Geral de Proteção de Dados – Estudo direcionado e comentado da Lei Geral de Proteção de Dados – Artigo a Artigo. Comissão de Direito da Tecnologia e Inovação da OAB/RS.

MENKE, Fabiano. A possibilidade de cumulação de bases legais nas operações de tratamento de dados pessoais. Disponível em https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/340890/cumulacao-de-bases-legais-nas-operacoes-de-tratamento-de-dados. Acesso em: 25/06/2021.

SIMÃO FILHO, Adalberto e Rodrigues, Janaína de Souza Cunha. O Gambito da Rainha e as estratégias para a tomada de decisão na governança de dados em LGPD. Disponível em https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/340576/o-gambito-da-rainha-e-as-estrategias-para-a-tomada-de-decisao-na-lgpd. Acesso em 25/06/2021.

FUNDAÇÃO UNIVERSIDADE DE CAXIAS DO SUL

UCS UNIVERSIDADE DE CAXIAS DO SUL

EDUCS COLEÇÕES COMUNIDADE ENSINO INFANTOJUVENIL LITERÁRIO PESQUISA TRADUÇÕES 45 anos

A Universidade de Caxias do Sul é uma Instituição Comunitária de Educação Superior (ICES), com atuação direta na região nordeste do estado do Rio Grande do Sul. Tem como mantenedora a Fundação Universidade de Caxias do Sul, entidade jurídica de Direito Privado. É afiliada ao Consórcio das Universidades Comunitárias Gaúchas - COMUNG; à Associação Brasileira das Universidades Comunitárias - ABRUC; ao Conselho de Reitores das Universidades Brasileiras - CRUB; e ao Fórum das Instituições de Ensino Superior Gaúchas.

Criada em 1967, a UCS é a mais antiga Instituição de Ensino Superior da região e foi construída pelo esforço coletivo da comunidade.

Uma história de tradição

Em meio século de atividades, a UCS marcou a vida de mais de 100 mil pessoas, que contribuem com o seu conhecimento para o progresso da região e do país.

A universidade de hoje

A atuação da Universidade na atualidade também pode ser traduzida em números que ratificam uma trajetória comprometida com o desenvolvimento social.

Localizada na região nordeste do Rio Grande do Sul, a Universidade de Caxias do Sul faz parte da vida de uma região com mais de 1,2 milhão de pessoas.

Com ênfase no ensino de graduação e pós-graduação, a UCS responde pela formação de milhares de profissionais, que têm a possibilidade de aperfeiçoar sua formação nos programas de Pós-Graduação, Especializações, MBAs, Mestrados e Doutorados. Comprometida com excelência acadêmica, a UCS é uma instituição sintonizada com o seu tempo e projetada para além dele.

Como agente de promoção do desenvolvimento a UCS procura fomentar a cultura da inovação científica e tecnológica e do empreendedorismo, articulando as ações entre a academia e a sociedade.

A Editora da Universidade de Caxias do Sul

O papel da EDUCS, por tratar-se de uma editora acadêmica, é o compromisso com a produção e a difusão do conhecimento oriundo da pesquisa, do ensino e da extensão. Nos mais de 1000 títulos publicados é possível verificar a qualidade do conhecimento produzido e sua relevância para o desenvolvimento regional.

Conheça as possibilidades de formação e aperfeiçoamento vinculadas às àreas de conhecimento desta publicação acessando o QR Code:

EDUCS 45 anos

ISBN 978-65-5807-098-6

OAB RIO GRANDE DO SUL Subseção Caxias do Sul

EDUCS

OAB RIO GRANDE DO SUL CDDNT Comissão Direito Digital e Novas Tecnologias

ISBN 978-65-5807-098-6

OAB RIO GRANDE DO SUL Subseção Caxias do Sul

EDUCS

OAB RIO GRANDE DO SUL CDDNT Comissão Direito Digital e Novas Tecnologias