PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS

ESCOLA DE DIREITO, NEGÓCIOS E COMUNICAÇÃO

NÚCLEO DE PRÁTICA JURÍDICA

COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO

MONOGRAFIA JURÍDICA

LEI GERAL DE PROTEÇÃO DE DADOS

ADAPTAÇÃO DAS EMPRESAS PARA PROTEÇÃO E PRIVACIDADE DOS DADOS DE SEUS CLIENTES, FORNECEDORES, COLABORADORES E OUTROS.

ORIENTANDO: BRENNO HENRIQUE DANTAS OLIVEIRA

ORIENTADOR: PROF. GIL CÉSAR COSTA DE PAULA

GOIÂNIA
2021

BRENNO HENRIQUE DANTAS OLIVEIRA

LEI GERAL DE PROTEÇÃO DE DADOS

ADAPTAÇÃO DAS EMPRESAS PARA PROTEÇÃO E PRIVACIDADE DOS DADOS DE SEUS CLIENTES, FORNECEDORES, COLABORADORES E OUTROS.

Monografia Jurídica apresentado à disciplina Trabalho de Curso II, da Escola de Direito e Relações Internacionais, Curso de Direito, da Pontifícia Universidade Católica de Goiás (PUC-GOIÁS).
Prof. Orientador: Gil César Costa de Paula

GOIÂNIA
2021

LEI GERAL DE PROTEÇÃO DE DADOS

ADAPTAÇÃO DAS EMPRESAS PARA PROTEÇÃO E PRIVACIDADE DOS DADOS DE SEUS CLIENTES, FORNECEDORES, COLABORADORES E OUTROS.

Data da Defesa: _____ de _____ de 2021

BANCA EXAMINADORA

_____ _____

Orientador: Prof. Gil César Costa de Paula Nota

_____ _____

Examinador Convidado: Prof. Roberto Rodrigues Nota

SUMÁRIO

LEI GERAL DE PROTEÇÃO DE DADOS

ADAPTAÇÃO DAS EMPRESAS PARA PROTEÇÃO E PRIVACIDADE DOS DADOS DE SEUS CLIENTES, FORNECEDORES, COLABORADORES E OUTROS.

Brenno Henrique

Dantas Oliveira[1]

RESUMO

O direito fundamental de proteção aos dados pessoais finalmente foi colocado em norma autônoma no Brasil, devido à sanção da Lei Geral de Proteção de Dados nº 13.709/2018 (LGPD), que entrou em vigor no país este ano. Tendo em vista o panorama atual da nossa sociedade, a LGPD carrega grandes expectativas para a defesa dos direitos dos indivíduos. Nesse sentido, o presente artigo almeja trazer uma análise do conceito de privacidade na sociedade informacional, assim como apresentar as principais características e conceitos trazidos pela referida lei. Não se pretende esgotar o assunto, mas apenas fazer um paralelo com alguns dos desafios a serem observados a fim de garantir a efetividade da norma.

Palavras-chave: Lei geral de proteção de dados; proteção de dados pessoais; banco de dados; sociedade informacional; privacidade.

1. Acadêmico do Curso de Direito da Pontifícia Universidade Católica de Goiás, brennodantas11@hotmail.com

INTRODUÇÃO

O tema deste trabalho, é um tema recente e que vem sendo muito debatido nos dias atuais, gerando ainda muitas dúvidas sobre o seu funcionamento, métodos de aplicação, dentre outros.

O fato de a Lei 13.709/2018 ainda não ter entrado vigor totalmente, vem trazendo várias indagações, como já descrito, os artigos da LGPD sobre sanções administrativas para quem desrespeitar as regras de tratamento de dados pessoais ainda não estão valendo. Por força da Lei 14.010/20, as sanções entram em vigor a partir de 1º de agosto de 2021.

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.

Os dados pessoais são manipulados com facilidade hoje em dia, e muitas vezes, ficam de certo modo vulneráveis, e as pessoas, sejam físicas ou jurídicas que detenham esses dados, tem a responsabilidade de fazer uso correto deles. Isso é aplicável em (dados de clientes, fornecedores, colaboradores etc.) devendo ser uma prioridade para qualquer empreendedor, empresa, entidade ou instituição.

A Lei Geral de Proteção de Dados Pessoais (LGPD) vem para proteger os direitos fundamentais de liberdade e de privacidade e a livre formação da personalidade de cada indivíduo. A lei dispõe sobre o tratamento de dados feito por pessoa física ou jurídica de direito público ou privado e engloba um amplo conjunto de operações efetuadas em meios manuais ou digitais.

Vale para: dados relacionados à pessoa (brasileira ou não) que esteja no Brasil, no momento da coleta; dados tratados dentro do território nacional, independentemente do meio aplicado, do país-sede do operador ou do país onde se localizam os dados; dados usados para fornecimento de bens ou serviços. Não se aplica para fins exclusivamente: jornalísticos e artísticos; de segurança pública; de

defesa nacional; de segurança do Estado; de investigação e repressão de infrações penais; particulares (ou seja, a lei só se aplica para pessoa física ou jurídica que gerencie bases com fins ditos econômicos). E não se aplica a dados de fora do Brasil e que não sejam objeto de transferência internacional.

Neste artigo científico, serão tratados os principais problemas que as empresas podem enfrentar caso não estejam com seu negócio adequado à LGPD, hipótese de adequação e informações contundentes sobre o assunto. Serão tratados também temas a respeito da efetividade de adequação da referida lei, sobre o sigilo, e a incidência da LGPD nas atividades do poder Judiciário.

1. LGPD VISTA PELAS EMPRESAS, ECONOMIA DIGITAL, PROTEÇÃO DE DADOS E COMPETITIVIDADE

1. EMOÇÕES INICIAIS DIANTE DA LGPD

Em 14 de agosto de 2018, nossa Lei Geral de proteção de Dados (LGPD), foi finalmente sancionada, depois de longas e intensas discussões na Câmera dos Deputados e no Senado Federal. As reações à notícia, contudo, variaram. Instituições representantes dos consumidores celebraram a aprovação da lei, chamando-a de uma “grande vitória”. Já as empresas, por outro lado, encararam a aprovação da LGPD como uma enorme desconfiança, reforçando o sentimento já vinha permeando a indústria desde as discussões dos projetos de lei que deram origem ao referido diploma, ainda no Congresso.

Em 2016, o Confederação Nacional das Indústrias (CNI), por exemplo, já manifestava preocupação quanto ao tema: ao propor uma agenda para o governo para o ano de 2017, indicou como prioridade a necessidade de conciliação da proteção de dados pessoais com o desenvolvimento e a inovação da indústria. De acordo com a referida confederação: “O excesso de proteção das informações pessoais por meio da privacidade pode levar a efeitos indesejados, como a criação de obstáculos ao desenvolvimento econômico e tecnológico, à livre concorrência”.

Em 2018, posteriormente à sanção da LGPD, a Mobile Markenting Association (MMA), também demonstrado ceticismo, citou a dificuldade que empresas de menor porte enfrentarão para cumprir as novas regras e o impacto que esta dificuldade poderá gerar sobre o mercado: “Regular esse mercado era mesmo necessário. Só que, ao fixar as mesmas exigências para companhias de diferentes portes, a lei levantou o sarrafo a uma altura que startups e empresas menores dificilmente conseguirão alcançar. Corre-se o risco de desestimular a inovação e prejudicar o desenvolvimento da economia digital.”

Neste espírito, houve aqueles que, diante da aprovação da LGPD, previram a catástrofe completa, outros, ainda que concordando com a possível desgraça, acalmavam os mais ansiosos.

1.1. PROCESSO DE ADEQUAÇÃO E AMEAÇA DE SANÇÕES

É certo que as críticas e preocupações com as novas regras de privacidade não são infundadas. O processo de adequação à LGPD exigirá tempo, pessoas e dinheiro.

Especialistas afirmam que projetos básicos de estruturação para o cumprimento com a LGPD, tanto sob o aspecto de TI quanto sob o aspecto jurídico, podem custar entre R$ 25 mil e R$ 3 milhões a depender do tamanho da empresa, isto, é claro, sem contar os custos de execução e manutenção, que são perenes.

Empresas que não tiverem os meios para ou por qualquer razão não estiverem dispostas a incorrer em tamanhos custos de adequação à LGPD estarão sujeitas a penalidades gravíssimas. A começar pela própria multa prevista na referida lei: 2% do faturamento da empresa no Brasil, limitada a R$ 50 milhões, por infração. Trata-se de um valor bastante significativo, que pode afetar profundamente uma empresa a depender de seu porte econômico e saúde financeira.

A pena de proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados pode ter efeitos ainda mais graves: dependendo da relevância da atividade de tratamento de dados para vida da empresa, sua proibição pode significar simplesmente a inviabilização de seu funcionamento, determinando o encerramento do negócio.

E, independentemente da imposição de penalidades propriamente ditas, não se pode ignorar o impacto que ocorrências envolvendo a violação da privacidade de titulares pode gerar sobre a reputação da empresa aos olhos de consumidores, clientes e fornecedores.

Nesse sentido, não há dúvidas de que, por um lado, os custos de adequação são inegavelmente altos, a não adequação às regras de privacidade também traz risco significativo às empresas, ameaçando desestabilizar o bom andamento de suas atividades no mercado ou até mesmo inviabilizá-las, dependendo da gravidade das penalidades impostas e do impacto da ocorrência sobre a reputação da empresa.

Conforme mencionado anteriormente, a adequação das empresas à nova lei demandará muito trabalho e será bastante dispendiosa.

Nas palavras de Araújo (p. 23, 2019):

> [...] adequar-se à LGPD envolve o desenvolvimento de projetos de revisão são dos processos de captação das informações pessoais, ou melhor, a releitura da comunicação e da transparência com os indivíduos acerca das informações captadas e as razões para tal. Avalia-se a natureza do tratamento, a finalidade e a utilização das informações em contexto e em concreto, conduzindo testes e proporcionalidade, adequação e necessidade.

Em outros termos, as empresas deverão repensar, avaliar, e adequar toda e qualquer captação e armazenamento de dados pessoais, começando com os dados solicitados em suas recepções, passando pelos dados de seus colaboradores alguns deles sensíveis, dados de seus fornecedores e, por fim e principalmente, de seus clientes.

1.2 A NOVA LEI GERAL DE PROTEÇÃO DE DADOS

A Lei n° 13.709/18 foi a resposta do legislador brasileiro para criar um marco abrangente de proteção aos dados pessoais dos brasileiros, não obstante já haver outras normas que conferiam alguma salvaguarda, com a Constituição Federal, o Código Civil Brasileiro, o Código de Proteção e da Defesa do Consumidor, A Lei do Cadastro Positivo, o Marco Civil da Internet e a Lei do Sigilo Bancário.

A LGPD foi inspirada, em boa parte, na regulação europeia de proteção de dados, conhecida como GDPR. Todavia, o legislador brasileiro foi além, pois a LGPD reconhece de forma inequívoca que está fundamentada não apenas nos direitos

básicos do cidadão, como o respeito à privacidade; a inviolabilidade da intimidade, honra e imagem; a liberdade de expressão, informação, comunicação e de opinião; a defesa do consumidor; mas também, esclarece que está alicerçada em pilares imprescindíveis para o exercício e o incremento das atividades econômicas, como o desenvolvimento econômico e tecnológico, a inovação, a livre iniciativa e a livre concorrência (Artigo 2° da LGPD).

Em verdade, a LGPD é um novo código ou um novo microssistema, possuindo 350 dispositivos, se considerados os artigos, incisos e parágrafos. Apenas para comparar, o CDC possui 367 dispositivos. A LGPD introduz no ordenamento jurídico brasileiro um sistema de regras abrangente e transversal, que incidirá sobre praticamente todos os setores da economia, afetando principalmente o relacionamento com o cliente.

É inegável que a LGPD consubstancia uma barreira de entrada para empresas que desejam tratar dados, uma vez que os requisitos da lei demandarão investimentos elevados em recursos humanos e materiais.

No entendo, o Brasil não está sendo sozinho. Segundo Graham Greenleaf, existiam no mundo, até o final de 2018, 132 países com as leis de proteção de dados pessoais, além de 28 outros países com projetos de lei tramitando.

Tendo-se em vista que a definição traçada no inciso X do Artigo 5° da LGPD, para tratamento de dados, é a mais abrangente possível, contendo nada menos do que treze ações que configurarão o tratamento, todo cuidado é pouco para o planejamento e a execução de compliance que serão exigidos das empresas.

Apenas para se ter uma ideia da envergadura das análises e providências que serão exigidas das empresas em geral, e das instituições financeiras em particular, em um estudo recente, verificou-se a existência de 162 leis ou decretos e 197 normas dos reguladores que exigem alguma forma de tratamento de dados pessoais pelos bancos brasileiros.

Os riscos também serão agravados. As possibilidades de erro ou de não conformidade com as centenas de dispositivos da lei serão enormes, o que poderá ocasionar o surgimento de uma nova indústria de indenizações e a imposição de sanções administrativas pela Autoridade Nacional de Proteção de Dados (ANPD).

1.3 A RESPONSABILIDADE E O RASSARCIMENTO DE DANOS

Os Artigos 42 a 45 da LGPD, que abordam sobre a responsabilidade e o ressarcimento de danos, enquadram-se, talvez, entre aqueles que mais preocupam as empresas que tratam dados.

O Artigo 42 prescreve que o controlador e o operador que causarem qualquer dano (material, moral, individual ou coletivo) a outrem serão obrigados a repará-lo.

No inciso I do § 1° do mesmo artigo, há previsão de que o operador responderá solidariamente com o controlador, quando descumprir a lei ou não seguir as instruções lícitas do controlador, o que nos parece bastante razoável, pois o operador será um contratado do controlador, que agirá por conta e risco deste.

Já o inciso II subsequente trouxe uma regra insólita: a responsabilidade solidária entre duas ou mais empresas controladoras, sem que haja algum vínculo ou negócio entre elas. Basta que estejam diretamente envolvidas no tratamento que venha a causar dano. Em outras palavras, de acordo com a nova lei, poderá haver responsabilidade solidária entre duas ou mais empresas que tratam dados, mesmo que não haja nenhum vínculo societário, contratual ou negocial entre elas.

Tal responsabilidade nos parece exagerada e descabida, haja vista que existirão casos em que diversos controladores poderão o mesmo dado, com graus distintos de conformidade com a lei, em atividades de maior ou menor risco de vazamento, alguns por obrigação legal, outros como fornecedores de serviços e outros como compradores ou menos consulentes de dados para utilizá-los em suas atividades empresariais.

Como exemplo, podemos citar o caso das empresas que consolidam dados bancários. Essas empresas obtêm autorizações dados e senhas bancárias de seus clientes, acessam seus extratos de contas, cartões de crédito, investimentos e operações de crédito em diversos bancos, consolidam esses dados e oferecem consultoria e soluções financeiras para os clientes.

No exemplo supra, na hipótese de ocorrer um dano em razão de um vazamento ou de um acesso indevido aos dados do cliente ocorrido nos sistemas da empresa consolidadora de dados, o banco será responsável solidário.

O Artigo 43 prevê que os agentes de tratamento só não serão responsabilizados quando provarem que: não realizaram o tratamento que lhes é atribuído; embora tenham realizado o tratamento de dados que lhes é atribuído; o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiros.

Diante de tal previsão, parece ser despiciendo o comando do § 2° do Artigo 42, que estabelece a possibilidade de o juiz, no processo civil, inverter o ônus da prova a favor do titular de dados, em três hipótese específicas.

É o que se depreende do disposto no Artigo 43, pois se o agente de tratamento não comprovar uma das três situações ali previstas será, automaticamente, responsável pelo dano causado ao titular de dados.

A grande questão que se coloca é: e se o agente de tratamento não comprovar que não realizou o tratamento ou que o dano é de decorrente de culpa exclusiva de titular ou de terceiro?

Apesar de não haver previsão de responsabilidade objetiva do agente de tratamento de dados pessoais na LGPD, a obrigação imposta pelo comando do seu Artigo 43 torna a responsabilidade do agente próxima do regime da responsabilidade objetiva.

2. PRIMEIROS DESAFIOS QUANTO A EFETIVIDADE, COMUNICAÇÃO DE DADOS, PROTEÇÃO E SIGILO

2 PRIMEIROS DESAFIOS DE EFETIVIDADE

Com a aprovação, sanção e apreciação dos vetos da Lei n° 13.709, de 14/08/2018, deu-se como concluída a etapa legislativa, com a formatação da ANPD, Autoridade Nacional de Proteção de Dados, do Conselho Nacional de Proteção de Dados pessoais e da Privacidade e outras alterações de mérito e de forma.

A *vacatio legis* foi estendida para 03/05/2021, conforme MP 959/2020, o que, teoricamente, possibilitaria aos agentes de tratamento de dados um tempo razoável para aprender adequações visando a conformidade com o novo diploma regente da proteção de dados.

Com efeito, o país tem muito que comemorar pelo que logrou. Todavia, há que não se perder de vista os próximos desafios que nos habilitarão auferir as oportunidades. A LGPD será exitosa se inserindo o Brasil nos mercados globais, e lograr alto de conformidade por parte das empresas e da administração pública.

De acordo com o relatório Global Concern about Internet Privacy risk vs. Convenience (STATISTA, 2019):

> [..] 89% dos brasileiros têm preocupação com a privacidade na Internet, e 49% aceitam correr o risco da privacidade em troca por conveniência. 55% dos brasileiros creem que seus dados estão sendo impropriamente utilizados, um percentual elevado perante a média global de 42%.

Tendo em conta da propensão que nosso povo tem para aderir a novas tecnologias e conveniências, é de suma importância que a ANPD lidere e estimule campanhas informativas e educativas sobre o uso seguro da internet e de aplicações que envolvem tratamento de dados pessoais, ressaltando que o uso de dados pessoais redunda em utilidade.

Semelhantemente, a ANPD deve trabalhar com todas as esferas governamentais no sentido se garantir transparência, quanto à abertura de dados públicos, e respeito à titularidade dos dados. O fortalecimento da confiança social quanto ao tratamento de dados pessoais é fator crítico para introdução da economia

intensiva em dados. Tais desafios estão em linha com a competência disposta no Art. 55-J, IV.

Sob o argumento de que muitas empresas não estavam preparadas e que a autoridade nacional de proteção de dados (ANPD) não havia sido criada, projetos de lei adiaram a entrada em vigor da LGPD, que, na versão original, seria em fevereiro de 2020. Após diversas discussões na Câmara e no Senado, a LGPD enfim entrará em vigor em setembro. O primeiro desafio foi vencido. A população já amadureceu o debate e não tolera mais que seus dados sejam coletados, processados e compartilhados sem o seu consentimento.

O segundo desafio reside exatamente na elaboração do projeto de adequação das empresas, que deve ser moldado à realidade e às necessidades específicas de cada uma. Em linhas gerais, o projeto de conformidade à LGPD compreende três fases principais: (I) mapeamento, (II) desenho de soluções e (III) implementação. A execução dessas etapas vai demandar comprometimento e trabalho árduo de profissionais de diversas áreas das empresas, incluindo também advogados (internos ou terceirizados) e profissionais da área de tecnologia e informação especializados em proteção de dados.

Em resumo, o desenvolvimento da parte jurídica do projeto requer a revisão minuciosa de todos os processos, documentos, contratos e políticas internas e comerciais, políticas de cookies, de privacidade, termos de uso do website e, é claro, investir pesado no treinamento dos colaboradores. Já, com relação à parte de Tecnologia da Informação envolve diversas providências relativas à observância ao ISO 27.001 e normas técnicas correlatas, tais como desenvolvimento de política de segurança de dados e adaptação de aplicações, ferramentas de controle de privacidade em sistemas e em dispositivos móveis, soluções para criptografar e para anonimizar o banco de dados, dentre outras medidas.

O terceiro desafio, e talvez o mais significativo, consiste no monitoramento do projeto de proteção de dados no cenário pós-implementação. A manutenção da conformidade à LGPD deve ser contínua e permanente, com avaliações periódicas

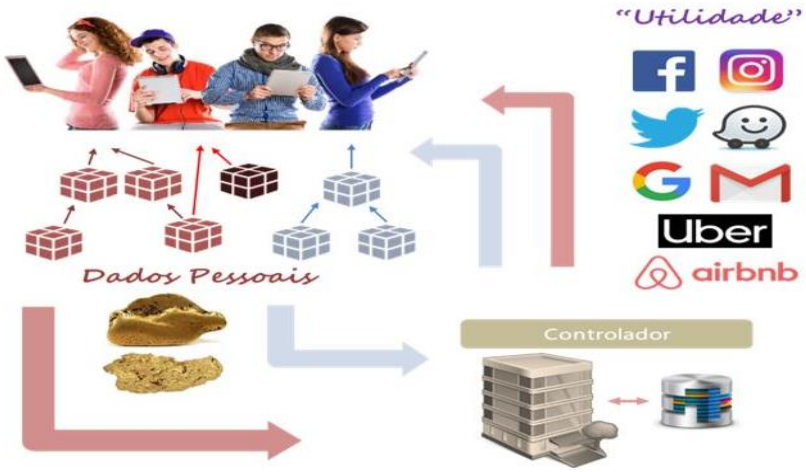
sobre o seu funcionamento e efetividade. Além disso, é de extrema importância a realização de treinamentos periódicos e a criação de procedimentos técnicos para a promoção de uma cultura organizacional que privilegie a proteção de dados como elemento intrínseco do trabalho realizado por todos os colaboradores, bem como do feixe de relações contratuais que compõem a empresa (fornecedores, distribuidores, colaboradores, clientes, etc.). Caso isso não seja feito, os prejuízos ao negócio podem ser significativos, tanto no âmbito financeiro, em razão das pesadas multas previstas na legislação (ainda que as punições começaram apenas em agosto de 2021), quanto no âmbito reputacional.

2.1 CONSENTIMENTO E NEGÓCIO JURÍDICO

A LGPD, no seu artigo 7°, estabelece hipótese autorizativas para realização de tratamento de dados pessoais, entre as quais destacamos o consentimento, inciso I, que é definido na léxicon, artigo 5°, XII, como a “manifestação livre, informada e inequívoca” do titular concordando “com o tratamento de seus dados pessoas para uma finalidade determinada”.

Tal definição emergiu de acalorado debate legislativo sobre a necessidade de impor ou não o consentimento expresso em matéria de dados pessoais. A dicção adotada, meritosa na medida em que abarca, de forma suscinta, as características essenciais do ato do titular, não esgotava, todavia, a questão das múltiplas facetas. Com efeito, as operações envolvendo dados pessoais, que são típicas da economia intensiva em dados, se caracterizam por serem sinalagmáticas.

A figura abaixo ilustra a situação:



2.2 VIRTUDES DA LGPD

Emergida de longa tramitação, a partir de iniciativas por parte das duas casas legislativas e da Presidência da República e que contou com ampla participação de membros da academia e de organizações representativas da sociedade civil e do empresariado, a Lei n° 13.709, de 14/08/2018, Lei Geral de Proteção de Dados Pessoais (LGPD), nasce como uma lei moderna e com amplo potencial perante a oportunidade de desenvolver a economia intensiva em dados no Brasil.

Inicialmente, destaca-se tratar de uma lei principiológica. Em seu art. 2°, estão elencados fundamentos lastreados em uma pluralidade de fontes do direito, como paradigmas distintos e teleologias diversas, que podem, por vezes, demonstrarem-se conflitantes.

A Lei a um só turno garante o respeito à privacidade ao lado da liberdade de expressão. Contrapõe a autodeterminação informativa com a liberdade de

informação, de comunicação e de opinião. Reafirma o primado da livre-iniciativa e da livre concorrência ao mesmo tempo a defesa do consumidor.

Dispõe a inviolabilidade da intimidade no mesmo patamar que almeja o desenvolvimento econômico e tecnológico e a inovação.

A Lei Geral de Proteção de Dados coloca o Brasil como referência em segurança de informações sensíveis. Ainda que estar em conformidade com a nova legislação signifique um investimento extra para as empresas, a verdade é que há vantagens também.

A geração de dados cresce em ritmo frenético, ao estabelecer responsabilidades e garantias às empresas, as novas regulamentações de dados causam profundo impacto aos negócios. Estima-se que 90% dos dados gerados em todo o planeta, foram produzidos só nos dois últimos anos! Esse é um claro indício de que, cada vez mais, as empresas devem atuar em suas atividades com responsabilidade, segurança e respeito à privacidade.

A adequação necessária para atender a nova regulamentação – que já está em vigor, apesar do prazo para as sanções em relação ao seu descumprimento ser agosto de 2021– pode ser considerada sinônimo de grandes custos às empresas.

Entretanto, é possível entender a legislação como algo positivo.

Melhora no relacionamento com o cliente através da confiabilidade e respeito à privacidade, pela necessidade do consentimento para captação e tratamento de dados pessoais, além de deixar clara a finalidade da coleta de dados, o cliente terá conhecimento integral sobre o uso de suas informações de forma transparente, o que contribui para uma maior credibilidade social e alcance positivo do público-alvo.

Além disso, a navegação nos sites deverá ser mais prazerosa devido à redução de publicidade e anúncios não solicitados.

Assim, um dos benefícios da LGPD é aumentar consideravelmente a probabilidade de proximidade dos clientes com as organizações que sejam do seu real interesse. Com abordagens menos invasivas, e melhorando a experiência do cliente, o interesse do consumidor tende a crescer naturalmente para determinada marca ou produto.

Aumento da segurança jurídica para atuar através de dados pessoais, a LGPD determina regras para o tratamento de dados pessoais, onde garante a privacidade e segurança dessas informações em qualquer país que seja coletado, devido sua aplicação extraterritorial.

Além disso, a legislação coloca o Brasil em alinho com outras regulamentações através do globo, garantindo-nos a reputação de ambiente seguro para o pleno tratamento e uso de dados pessoais.

Estando em conformidade com a GDPR (Regulamento Geral de Proteção de Dados), a lei permite que empresas nacionais possam tratar dados pessoais eventualmente coletados no território da União Europeia, sem complicações e transtornos à empresa ou aos titulares dos dados. É ou não é um dos grandes benefícios da LGPD?

Segurança cibernética aprimorada para usos determinados, ao tratar com seriedade a privacidade e o uso de dados pessoais, as empresas vão gerar a tendência de criar fluxos de trabalhos mais conscientes dessas informações e por consequência, mais seguros também.

Devido às altas sanções, a preocupação com a infraestrutura de dados pessoais passará a vir em primeiro lugar, trazendo consideráveis mudanças no processo de proteção cibernética.

É importante que estas alterações entrem em vigor para trazer políticas de segurança claras, e que reduzem os riscos de uso inadequado de informações pessoais, invasões, violações ou vazamentos de dados.

Valorização do marketing e aumento de sua produtividade, continuando a lista de benefícios da LGPD para sua empresa, lembramos que eliminar informações pessoais irrelevantes ao negócio (minimização), propiciará aumento na qualidade das informações realmente decisivas e necessárias às empresas, com bancos de dados alimentados com informações de clientes verdadeiros e relevantes.

O uso de dados reais e atualizados possibilitará uma comunicação clara com a sociedade, com mensagens coerentes de acordo com as necessidades e desejos do público a ser impactado, onde os investimentos serão utilizados de forma assertiva e inteligente, evidenciando aumento na credibilidade das campanhas.

2.3. REPERCUSSÃO JURÍDICA

A LGPD mal entrou em vigor e já temos condenações crescentes em demandas judiciais e administrativas, em que nem a ausência de sanções ou de uma Autoridade Nacional de Proteção de Dados está sendo capaz de coibir tais ocorrências.

Recente decisão ocorrida no Processo de nº 1080233-94.2019.8.26.0100 do Tribunal de Justiça do Estado de São Paulo não deixou por menos: uma construtora foi condenada por compartilhar, ilegalmente, sem qualquer consentimento dos titulares, dados pessoais de compradores de suas unidades autônomas com diversas outras empresas, em flagrante violação a lei, ainda mais quando esse

compartilhamento é realizado junto a empresas estranhas à relação contratual, como foi o caso, o que causou sérios danos a esses titulares ocasionando, por consequência, a condenação por danos morais.

Ou seja, em relação a construção civil, de maneira geral, a adequação à lei deverá ser alinhada em diferentes frentes. Isso porque objetiva-se a construção de grandes empreendimentos e, para tanto, diversas são as atividades que se inter-relacionam.

Para quem já está acostumado com todo esse processo, sabe que ele tem início com os procedimentos preliminares à uma incorporação imobiliária e que finda na construção do empreendimento, com a respectiva venda/locação de suas unidades. Essas etapas levam em consideração desde a relação com o proprietário do terreno, que é o cedente do espaço, até a atuação da construtora e incorporadora, as quais realizam a construção e a parceria relacionada a venda das unidades, respectivamente. Associados a tudo isso, e não menos importante, também devem ser considerados os compradores, clientes, que são as pessoas físicas ou jurídicas interessadas no imóvel.

Em todo esse processo há um atrelado de relações contratuais e, por conseguinte, tratamento de dados pessoais que deverão ser considerados no contexto de todos os participantes desta relação jurídica: desde os dados dos sócios, até aqueles relacionados aos colaboradores das empresas contratadas, fornecedores e clientes.

Isso sem citar as empresas que igualmente participam de estudos técnicos e de viabilidade econômica na execução do projeto, assim como o eventual compartilhamento de dados dos sócios das empresas junto aos órgãos públicos, para auxiliar na realização do processo. Em obediência às leis do setor, desde leis específicas, como a Lei nº 4.195/1964, que trata da incorporação imobiliária, até as leis mais gerais, como o Código Civil e o Código de Defesa do Consumidor, por exemplo, todas as normas que deverão estar presentes e obrigatórias relacionadas ao setor devem ser igualmente obedecidas.

Ou seja, considerando que desde um planejamento de obra estruturado e detalhado até a entrega de uma unidade diversos fatores devem ser considerados, a responsabilidade das construtoras em relação aos dados pessoais que controlam deve ser ainda maior, visto que seu papel diante de todo esse processo será de decisão sobre o tratamento deles e consequente definição de bases legais adequadas.

Não obstante, é necessário que se conheça todas as relações jurídicas as quais essas organizações estão atreladas, considerando o fluxo e o ciclo de vida dos dados desde sua coleta, até os necessários compartilhamentos realizados em razão da natureza de suas atividades negociais, seu período de retenção e posterior descarte.

A título de exemplo, podemos citar alguns dados que usualmente são coletados:

— Provenientes de clientes, compradores das unidades: nome, RG, CPF, estado civil, sexo, telefone, e-mail, endereço, dados bancários, entre outros dados constantes de um contrato de adesão;

— Dados pessoais dos colaboradores, cujo conteúdo também abarca dados sensíveis, e que ficam alocados em áreas como Departamento Pessoal, Financeiro, RH;

— Dados pessoais de fornecedores, parceiros de negócios e terceiros;

— Dados coletados de processos judiciais ajuizados;

— Dados compartilhados dos funcionários terceirizados e advindos de outras empresas contratadas para prestar serviços a construtora, como vigilância, limpeza, obra, projetos, pintura etc.

Em relação aos dados pessoais dos funcionários de empresas terceirizadas: a construtora, como tomadora dos serviços, pode vir a ser responsabilizada, mormente na seara trabalhista, e, por tal motivo, justificável a retenção deles face a fazer defesa desde o período da contratação até o prazo prescricional previsto na lei, ou o que for definido internamente.

As políticas de retenção, nesse caso, devem ser diferenciadas. Durante o período em que a obra se encontra em andamento, a construtora deve manter esses dados sob seu controle. Após o término da obra, a base legal pode ser modificada, visto que a obra já acabou, não se justificando a manutenção das informações do colaborador da empresa terceirizada, exceto pelas situações em que demandas trabalhistas podem surgir, situação que deve ser discutida caso a caso. Existem doenças ocupacionais que podem surgir anos após a prescrição prevista nas legislações trabalhistas e a organização deve ficar atenta à natureza dos serviços que são por ela prestados.

Além desses motivos, é urgente a adequação da LGPD nessas organizações: em todo o processo de implementação, em que não só os documentos são considerados, mas as medidas técnicas, organizativas e operacionais que garantam a segurança dessas informações.

No mais, adequações nos contratos com a definição dos papéis são motivo de grande importância para avaliar em quais situações a construtora age como controladora, como controladora conjunta ou, quem sabe, podendo até atuar como operadora. Tudo vai depender das suas atividades exercidas e da natureza operacional.

Atentos a tudo isso, de certo que um grande passo para a conformidade será tomado, visto que muito ainda deverá ser definido pela Autoridade Nacional de Proteção de Dados Pessoais. No entanto, antes mesmo que sejam definidas novas diretrizes acerca do tratamento de dados pessoais a ser realizado em setores econômicos específicos, é fundamental que as determinações normativas mais abrangentes sobre o tema sejam colocadas em prática em respeito ao Estado democrático de Direito, através da tutela fundamental dos direitos de privacidade.

3. LGPD NAS ATIVIDADES DO PODER JUDICIÁRIO

3. DA EFETIVA APLICAÇÃO DA LGPG

Entrou em vigor em 01/08/2021 a aplicação de sanções para quem descumprir a Lei Geral de Proteção de Dados Pessoais (LGPD), Lei n° 13.709. As instituições serão obrigadas a justificar a coleta de dados pessoais e solicitar autorização para o proprietário das informações. Segundo a norma, qualquer pessoa pode requerer a consulta dos dados, assim como a sua retirada do sistema.

A Lei Geral de Proteção de Dados Pessoais (LGPD) busca estabelecer regras de coleta, uso, armazenamento e compartilhamento de dados de um cidadão por outra pessoa natural ou jurídica. A advogada Deborah Toni, sócia da Deborah Toni Advocacia, especialista em Direito Digital e Proteção de Dados pela PUC-SP e CEO do CEAPD (Centro de Estudos Avançados em Tecnologia, Privacidade e Proteção de Dados) explicou que, o número de empresas em conformidade com a lei ainda é baixo.

“Pesquisas realizadas entre novembro/2020 e fevereiro/2021 apontam que somente 11% das instituições estão em conformidade com a lei. Como se vê, a adesão ainda é muito baixa. Falta conscientização a respeito da importância do novo regramento, o que naturalmente aconteceria com a aplicação das sanções administrativas pela Autoridade Nacional”, ressaltou.

Para Toni é imprescindível que as organizações se preparem não só para compreenderem o novo regramento, mas para que possam atuar preventiva e relativamente no caso de eventuais incidentes. “Aqueles que demonstrem boa-fé, a adoção ‘reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados’, bem como a pronta adoção de medidas corretivas serão menos impactados pelas sanções.”

Será necessário que as empresas se adequem para não serem punidas, é o que defende a advogada especialista em direito digital e sócia do TozziniFreire Advogados, Isabela Pompilio. “O número de empresas que já se adequou ainda é muito pequeno, as sanções entrarão em vigor e muitas empresas poderão ser surpreendidas. Não por falta de aviso. Imagina-se, portanto, que após o início da aplicação das diversas sanções previstas na lei, haverá uma corrida das demais empresas que ainda não se adequaram”, explicou.

Pompilio afirmou que as sanções aplicadas poderão variar de acordo com o ato praticado, com possibilidade de aplicação de multa com um teto de 50 milhões. “As sanções, bem como os valores, variam de acordo com o ato praticado: desde advertências e multas, até a suspensão ou proibição, parcial ou total, do exercício de atividades relacionadas ao tratamento de dados – o que, para algumas empresas, pode significar, inclusive, o encerramento da própria atividade empresarial”, destacou.

Segundo o advogado especialista em proteção de dados, Enrique Tello Hadad, as empresas deverão passar por mudança cultural e operacional radical. As organizações precisarão implementar uma nova governança e gestão de dados pessoais e prestar contínuo treinamento a todos os colaboradores.

“As penalidades administrativas são aplicadas pela ANPD, podendo variar de acordo com o grau do impacto e a gravidade da infração à LGPD, desde uma advertência a multas simples de até 2% do faturamento das empresas (limitadas a R$ 50 milhões por infração), multas diárias, publicização da infração, bloqueio ou eliminação de dados pessoais, suspensão e até a proibição parcial ou total das atividades das empresas”, disse.

A LGPD trouxe mais segurança aos titulares dos dados, como maior transparência, obrigação das empresas em ter o consentimento do proprietário dos dados, as informações só podem ser usadas nos casos previstos por lei etc. Segundo o advogado William Teidy Oka Inoue, especialista do Zilveti Advogados, os proprietários podem recusar o fornecimento dos dados.

“A princípio, as pessoas poderão sim se recusar a fornecer os dados para as empresas, mas é necessário entender que determinados serviços dependem do fornecimento de dados e também a empresa pode encaixar a necessidade de tratar os dados em uma das hipóteses autorizadas na LGPD. Posso citar como exemplo: a) proteção do crédito; b) cumprimento de obrigação legal; c) decisão judicial; d) legítimo interesse; e as demais hipóteses previstas na LGPD”, acrescentou.

A advogada Andreia Mendes, do escritório Mauro Menezes & Advogados, contou que os maiores desafios das pequenas e médias empresas têm sido a falta de conhecimento do assunto e, quando há conhecimento, os custos de adequação. "O processo de adequação à LGPD é de extrema importância e complexo, pois envolve uma análise jurídica dos tratamentos realizados por cada setor da empresa, bem como análises realizadas por profissionais de tecnologia da informação e pode levar à necessidade de mudanças e/ou aquisição de sistemas".

"As empresas precisam estar preparadas e precavidas contra ataques de hackers ou uso indevido de dados, pois o titular de dados que se sinta prejudicado pelo uso indevido pode buscar a proteção de seus direitos junto ao Poder Judiciário", comentou.

Já para o advogado, Lucas Anjos, do escritório CerveiraTech, o principal risco que as empresas passam a ter com a lei já em vigência é a possibilidade de serem alvos de fiscalização pela Autoridade Nacional de Proteção de Dados (ANPD), na medida em que as sanções administrativas já poderão ser aplicadas. "As penalidades vão de simples advertências a multas de até 2% do faturamento bruto anual da empresa, limitada a R$ 50 milhões", afirmou.

De acordo com Lucas, outro risco que se tornou mais evidente nos últimos meses é a crescente judicialização do tema. "Até o momento o número de decisões em que os consumidores e empregados questionam a conformidade das empresas vêm crescendo abruptamente", declarou.

Por fim, o advogado observou que, em consequência, empresas dos mais diversos segmentos enfrentam o mesmo desafio: dar o primeiro passo rumo à gestão dos seus processos e atividades que coletam, armazenam, compartilham e eliminam dados pessoais. "Registrar, rever e aplicar medidas de privacidade e segurança de algumas das atividades do dia a dia pode significar demonstração de boa-fé por parte

dos gestores, indicativo que sem dúvidas irá afastar ou minimizar penalidades. A lei obriga as empresas a entender que dados pessoal, além de ser um valioso ativo econômico, passou a ser um ativo de risco".

3.2. INTERPRETAÇÃO DA LGPD PELO PODER JUDICIÁRIO E PELA ANPD

A Lei Geral de Proteção de Dados Pessoais agora está totalmente operante. No âmbito judiciário, desde setembro de 2020, e na esfera administrativa, desde o último dia 1º, com a possibilidade de aplicação das sanções administrativas previstas no artigo 52 da lei pela Autoridade Nacional de Proteção de Dados Pessoais (ANPD).

A expectativa de estudiosos do assunto é que os órgãos se aprofundem no tema de proteção de dados pessoais e privacidade para garantir a interpretação adequada da lei e não submeta a sociedade a um verdadeiro retrocesso no sistema democrático de Direito.

A LGPD, considerada por Danilo Doneda como elemento estruturante do modelo brasileiro de proteção de dados, traz os elementos para a instrumentalização desse sistema protetivo, os quais devem ser associados a outros recursos, como o engajamento em políticas públicas e a aplicação eficiente pela ANPD e pelo Poder Judiciário.

No Judiciário decisões já analisam questões como ônus da prova do titular de pessoais, responsabilidade civil do controlador por ausência de consentimento do titular, litigância de má-fé do titular por ausência de provas do tratamento ilícito e relevância dos dados vazados para a responsabilização do controlador. A comunidade jurídica está atenta à interpretação da lei pelos órgãos que serão responsáveis por formar os primeiros precedentes sobre o tema de proteção de dados pessoais no Brasil.

Vejamos alguns exemplos jurisprudenciais:

> AGRAVO DE INSTRUMENTO. AÇÃO DE DISSOLUÇÃO DE SOCIEDADE. ACESSO DO EX-SÓCIO A DOCUMENTOS DA EMPRESA. FASE DE APURAÇÃO DE HAVERES. SOCIEDADE DE ADVOGADOS. LGPD. DECISÃO MANTIDA. 1. Havendo acordo de dissolução da sociedade homologado pelo juízo, o feito passou para a segunda fase e, a fim de que se possa liquidar os haveres, é necessário verificar se existem ou não, conforme defende cada parte dentro de seu interesse. 2. O fato do agravado não mais integrar a sociedade não lhe retira o direito de ter acesso aos contratos firmados durante sua atuação como sócio, tampouco aos documentos produzidos no mesmo período, posto que indispensáveis para a segunda fase da demanda (apuração de haveres), inclusive para eventual compensação de eventuais valores retirados a mais pelo sócio retirante. 3. No que tange ao tratamento de dados pessoais, sob a ótica da Lei Geral de Proteção de Dados (LGPD), é induvidoso que as sociedades de advogados também devem se adaptar ao normativo. Contudo, não constar dos autos que a sociedade tenha implementado a gestão do escritório nos termos da lei, tais como elaboração de normativos internos, fluxo de dados pessoais, forma e tempo de guarda do consentimento, dentre outros, dificulta a análise de qualquer inconveniente ou ilegalidade que o acesso aos contratos possa gerar. 4. Recurso desprovido.

> (TJ-DF 07483102920208070000 DF 0748310-29.2020.8.07.0000, Relator: JOSAPHA FRANCISCO DOS SANTOS, Data de Julgamento: 22/04/2021, 5ª Turma Cível, Data de Publicação: Publicado no DJE : 04/05/2021 . Pág.: Sem Página Cadastrada.)

Apesar de se tratar de uma lei contemporânea, o tema já é muito estudado pela doutrina brasileira, influenciada pelos sistemas jurídicos europeus, que desde 1977 possuem leis federais sobre o tema de proteção de dados pessoais, chamada *Bundesdatenchutzgesetz* [2]. Portanto, ouvir essas "vozes" que têm intimidade com o assunto significa nutrir a nossa jurisprudência com o que há de mais orgânico no universo de privacidade e proteção de dados.

Consequências decorrentes da vigilância dos cidadãos e da intrusão nas liberdades individuais através do uso de tecnologias de informação devem ser levadas em consideração nas decisões judiciais e administrativas. Na verdade, houve um consenso quase universal para formular políticas rígidas para minimizar as ameaças representadas pelo uso livre e não regulamentado e a manipulação de informações pessoais.

Trata-se de uma nova disciplina que se desconecta do componente isolamento, fruto de um longo processo de transformação do conceito de privacidade que evoluiu para a prevalência da autonomia e controle dos dados pessoais. A proteção de dados é mais ampla porque não visa apenas a tornar a proteção da privacidade concreta, mas também tende a proteger outros direitos e interesses como a liberdade de expressão, liberdade de religião e consciência, o livre fluxo de informação e o princípio da não discriminação.

No caso concreto, decisões que não interpretarem dados pessoais em congruência ao conceito legal, prejudicarão a amplitude da LGPD. Todos os dados pessoais são relevantes, ainda que coletados em bancos de dados públicos. O contrário desarticularia o conceito de que o titular é o senhor dos dados e tem o direito de controlá-los, ainda que diante de um tratamento lícito.

A decisão judicial ou administrativa deve assimilar que dados pessoais também podem estar implícitos na forma de dados comportamentais, por exemplo, de redes sociais, que podem ser vinculados a indivíduos. Por esse motivo, não é razoável medir o nível de proteção de dados pessoais em razão da pouca relevância que se mostrar para terceiros que o acessarem. Dados públicos ou de fácil acesso podem ser contrastados com dados considerados confidenciais, valiosos ou importantes por outros motivos, como receitas secretas, dados financeiros ou inteligência militar. Nesse sentido, é temerário interpretar que um vazamento de dados pessoais, com a qualificação comum de um indivíduo (nome, RG, CPF), fornecidos para acesso em portarias, aplicativos e sites de compras não estejam protegidos pela LGPD, com a ampla garantia dos direitos dos titulares previstos em seu artigo 18.

O que se pretende com a boa aplicação da LGPD é elevar a proteção de dados pessoais para um novo status, em que se possa equilibrar o estado de vulnerabilidade do cidadão diante do monopólio de informações pessoais na nova economia de dados.

O titular dos dados pessoais, na maioria dos casos, não possui consciência tecnológica e não compreende os potenciais riscos do tratamento de dados pessoais, seja em razão da complexidade da arquitetura tecnológica empregada em um sistema, seja em razão da opacidade encontrada nos dados coletados e suas combinações. Por essas questões, é dever do Estado, seja através do Poder Judiciário ou da ANPD, concretizar a proteção ao tratamento de dados pessoais como um direito básico, em razão da posição desigual do titular, frente ao controlador dos dados pessoais, seja na esfera pública ou privada.

Confrontar os direitos de proteção de dados com as medidas preventivas e boas práticas adotadas pelas organizações é o início do processo para garantir a proteção dos novos direitos fundamentais na sociedade da informação. Cabe indagar em cada caso a ser analisado pelos órgãos competentes o propósito da proteção de dados e em que medida se coaduna com o imperativo do controle sobre os dados pessoais.

CONCLUSÃO

O desenvolvimento deste trabalho se deu a partir da adequação de uma nova Lei que deu efetividade ao tratamento de dados pessoais no Brasil, desta forma, foram abordados os métodos de adequação, as sanções previstas e como as empresas devem agir para estarem de acordo com a referida Lei.

O artigo 5º, inciso X da Lei nº 13.709, a LGPD, prevê que tratamento é toda operação realizada com dados pessoais. Assim, inclui-se como tratamento: a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Como a Lei prevê um protagonismo do titular de dados em todas as etapas do tratamento, é de extrema importância ter o consentimento do titular desde a coleta até a eliminação dos dados. Tal consentimento deve ocorrer, preferencialmente, por escrito, de maneira que as empresas devem adequar seus termos de privacidade – no meio virtual – para constar a previsão de consentimento de forma clara e expressa, assim como devem formular termos de consentimentos impressos, quando a relação ocorrer presencialmente.

Assim, como a LGPD prevê ao longo de seu texto autonomia e participação ativa do titular dos dados durante todo o procedimento, todas essas alterações significam que as empresas terão muito o que fazer para se adequar à nova realidade, o que também vale para as startups já concebidas e em processo de criação.

A governança do tratamento de dados, isto é, a criação de regras relacionadas às normas que visam a segurança dos dados e a preservação da privacidade do titular é, como dissemos, fundamental para a adequação à LGPD. Contudo, sem o treinamento adequado, o fator humano pode representar um risco à segurança e aos mecanismos implementados.

Para evitar tal problema é necessário ter uma rotina de segurança de dados bem definida e auditorias internas para avaliar, fiscalizar e atualizar as medidas adotadas pela empresa, bem como uma resposta rápida à eventuais violações.

Além de cumprir com todas as determinações exigidas pela Lei, é necessário ainda que as empresas saibam como comprovar que estão adequadas à LGPD.

No entanto, é importante se adequar às disposições contidas na nova Lei porque o seu descumprimento, além de outras penalidades cabíveis no âmbito cível e penal, pode gerar desde advertências a multas de até R$ 50.000.000,00 (cinquenta milhões de reais) por infração cometida.

REFERÊNCIAS

ABNT NBR ISO/IEC 27002:2013: Tecnologia da Informação – Técnicas de segurança – Código de prática para controles de segurança da informação. Rio de Janeiro, 2013;

BIONI, Bruno. Proteção de Dados Pessoais: a função e os limites do consentimento – Rio de Janeiro: Editora Forense, 2019, p. 135/136;

BIONI, Bruno. Regulação de dados é uma janela de oportunidades. Mar. 2019. Disponível em: https://valor.globo.com/opiniao/coluna/regulacao-dedados-e-uma-janela-de-oportunidade.ghtml;

Lei 13.709 de 14 de agosto de 2018, disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm;

Lei Geral de Proteção de Dados – a caminho da efetividade: contribuições para a implementação da LGPD – REVISTA DOS TRIBUNAIS – 2019;

Proteção de Dados Pessoais: Comentários à Lei n. 13.709/2018 –LGPD - Por Pinheiro, Patricia Peck · 2020;

Roberto Gonsalves, especialista em Logística e Gestão de Processos gerenciais, comentários disponíveis em: https://www.eboxdigital.com.br/blog/lei-geral-de-protecao-de-dados-ja-estavalendo-sua-empresa-esta-preparada?gclid=CjwKCAjw6qqDBhBEiwACBs6x11qFYJ3ZN7b9D8cdjnAyguvEpvvoq13nitqqVgfQS3Gzq2d9445WR oCZUMQAvD_BwE;

PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
PRÓ-REITORIA DE DESENVOLVIMENTO INSTITUCIONAL
Av. Universitária, 1069 I Setor Universitário
Caixa Postal 86 I CEP 74605-010
Goiânia I Goiás I Brasil
Fone: (62) 3946.3081 ou 3089 I Fax: (62) 3946.3080
www.pucgoias.edu.br I prodin@pucgoias.edu.br

RESOLUÇÃO n°038/2020 – CEPE

ANEXO I

APÊNDICE ao TCC

Termo de autorização de publicação de produção acadêmica

O(A) estudante Brenno Henrique Dantas Oliveira
do Curso de Direito, matrícula 2017100011361 6,
telefone: (62) 98470-2331 e-mail brenno.dantas11@hotmail.com, na qualidade de titular dos direitos autorais, em consonância com a Lei nº 9.610/98 (Lei dos Direitos do autor), autoriza a Pontifícia Universidade Católica de Goiás (PUC Goiás) a disponibilizar o Trabalho de Conclusão de Curso intitulado Lei Geral de Proteção de Dados - Adoptação das empresas para proteção de dados de seus clientes, fornecedores, colaboradores e outros., gratuitamente, sem ressarcimento dos direitos autorais, por 5 (cinco) anos, conforme permissões do documento, em meio eletrônico, na rede mundial de computadores, no formato especificado (Texto (PDF); Imagem (GIF ou JPEG); Som (WAVE, MPEG, AIFF, SND); Vídeo (MPEG, MWV, AVI, QT); outros, específicos da área; para fins de leitura e/ou impressão pela internet, a título de divulgação da produção científica gerada nos cursos de graduação da PUC Goiás.

Goiânia, 16 de novembro de 2021.

Assinatura do(s) autor(es): Brenno Henrique D. Oliveira

Nome completo do autor: Brenno Henrique Dantas Oliveira

Assinatura do professor-orientador: Gil César Paula

Nome completo do professor-orientador: Dr. Gil César Costa de Paula