A LEI GERAL DE PROTEÇÃO DE DADOS E A BANALIZAÇÃO NO USO DE DADOS PESSOAIS NO MEIO EMPRESARIAL

José Geraldo Alves Leal[1]

Recebido em 05/08/2021
Aceito em 11/09/2021

RESUMO
O presente artigo tem como objetivo analisar as implicações do uso indiscriminado de dados pessoais por empresas dos mais diversos ramos de atividade ante ao estabelecido pela Lei 13.709/2018 – Lei Geral de Proteção de Dados (LGPD), visando a proteção dos direitos fundamentais, em conformidade com o texto constitucional. Atualmente assistimos a uma incessante busca por informações pessoais dos consumidores, onde diversas organizações, visando diversos interesses, que vão desde o direcionamento de suas políticas comerciais, compartilhamento de dados, ou até mesmo a venda desse ativo para outras organizações. O titular dos dados pessoais sempre foi o responsável pela proteção de seus dados, definindo as situações que irá consentir ou não o seu compartilhamento com terceiros, é nesse contexto que foi promulgada a LGPD, que estabelece regras e procedimentos para a coleta, armazenamento e tratamento dos dados pessoais dos consumidores, proporcionando uma maior proteção e segurança ao titular destes dados.

PALAVRAS-CHAVE: Dados pessoais; empresas; lei geral de proteção de dados; tratamento de informações pessoais.

THE GENERAL DATA PROTECTION LAW AND BANALIZATION IN THE USE OF PERSONAL DATA IN THE BUSINESS ENVIRONMENT

ABSTRACT
This article aims to analyze the implications of the indiscriminate use of personal data by companies in the most diverse fields of activity, compared to what is established by Law 13.709/2018 - General Data Protection Law (LGPD), aiming at the protection of fundamental rights, in accordance with the constitutional text. Currently, we are witnessing an unprecedented race, where several organizations seek personal information from their consumers, aiming at different interests, ranging from directing their commercial policies, sharing data, or even selling this asset to other organizations. The holder of personal data has always been responsible for protecting their data, defining the situations in which they will or will not consent to its sharing with third parties. It is in this context that the LGPD was promulgated, which establishes rules and procedures for the collection, storage and processing personal data of consumers, providing greater protection and security to the holder of these data.
Keywords: Personal data; companies; general data protection law; handling of personal information.

[1] Bacharel em Ciências Contábeis formado pelo Instituto Cultural Newton de Paiva Ferreira, Pós-graduado em Auditoria Interna e Externa pela UFMG, Aluno do 8º período do Curso de Direito no Instituto Cultural Newton de Paiva

NORTH, C. Douglas. **Instituições, Mudança institucional e desempenho econômico**. São Paulo: Três Estrelas, 2018.

1 INTRODUÇÃO

A Lei Geral de Proteção de Dados, sancionada em agosto de 2018, teve sua vigência fracionada, conforme art. 65, inspirada no Regulamento Geral sobre a Proteção de Dados (General Data Protection Regulation – GDPR) implementada na União Europeia no ano de 2016, sendo reconhecida como a mais inovadora e eficiente legislação sobre a proteção de dados, servindo de modelo para muitos países implementares tais políticas, ou mesmo otimizando políticas já adotadas.

A LGPD, se aplica a qualquer pessoa, seja natural ou jurídica, de direito público ou privado, determina uma série de diretrizes na obtenção, no armazenamento e na exclusão de dados pessoais. A Constituição da República de 1988, no seu artigo 5º, incisos X e XII, trata da proteção à intimidade, a vida privada, a honra e a imagem das pessoas, assegurando direito à indenização face eventuais danos decorrentes de sua violação. Nesse sentido a LGPD, tem como objetivo proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, não podendo o Estado intervir na vida privada dos cidadãos, exceto nas hipóteses previstas em Lei.

Nesse sentido, explica DONEDA (2011, p. 94):

> a informação pessoal está, quase como ato reflexo, ligada à privacidade por uma equação simples e básica que associa um maior grau de privacidade a menor difusão de informações pessoais e vice-versa. Esta equação nem de longe encera toda a complexa problemática em torno dessa relação, porém pode servir como ponto de partida para ilustrar como a proteção das informações pessoais passou a encontrar guarida em nosso ordenamento jurídico: como um desdobramento da tutela do direito à privacidade.

Hoje em dia, quer seja através das redes sociais, compras *on-line*, instituições financeiras, companhias de telemarketing, bancos, órgãos públicos, etc., há uma busca desenfreada pela busca de informações pessoais dos consumidores, por se tratar de um ativo de grande valor financeiro no meio empresarial. A utilização em massa da internet e outros meios digitais, elevou significativamente o nível de vulnerabilidade por parte dos consumidores, na medida em que estão expostos a riscos dos quais não tem conhecimento, ou que estão sendo ocultados, muitas vezes de maneira intencional. Os mais comuns são através da opção “Li e Aceito os Termos” em determinadas plataformas, onde o consumidor acaba concordando com

termos aos quais não tem conhecimento; ou através da utilização de *cookies*[2], realizadas para melhorar o desempenho de sites na web.

A Academia Brasileira de Direito do Estado (ABDET) fez a seguinte análise:

> Na sociedade atual mergulhada no âmbito digital, é possível considerar que a personalidade e cidadania da pessoa humana também são moldados pelo uso da internet: por esse meio a pessoa se expressa, busca informações, se relaciona. O ambiente virtual, tanto quanto o real, deve se submeter à proteção dos direitos humanos, de forma mais abrangente possível, respeitando o princípio do não retrocesso. (ABDET,2015, p.2)

A coleta e a armazenagem de informações acontecem de forma invisível, arbitrária e sem o consentimento do titular dos dados pessoais, visa obter o maior volume possível de dados com o objetivo de distribuir, vender e revender a outras instituições, criando uma verdadeira indústria de dados pessoais privados de terceiros. Um dos principais efeitos dos avanços da tecnologia da informação reflete diretamente nas relações de consumo, onde tanto empresas privadas quanto da administração pública, desenvolvem arquivos com informações pessoais dos cidadãos com o objetivo de segmentar produtos e serviços, aumentar a eficiência de seus processos produtivos, gerando maiores volumes de receitas e lucro. Há de se destacar que o próprio Estado atua de maneira indiscriminada na retenção de dados e informações pessoais dos cidadãos com o objetivo de melhor fiscalizar, vigiar e aumentar suas receitas tributárias.

São inúmeras as situações em que o consumidor tem a sua privacidade violada, nesse contexto, não há dúvida de que este é o sujeito vulnerável nessa relação de consumo, e que se faz necessário o desenvolvimento de política públicas para garantir a efetiva proteção de seus dados pessoais. Um exemplo clássico está no vazamento de informações pessoais dos aposentados e pensionistas do INSS, uma vez que têm sua privacidade violada, principalmente por instituições financeiras, oferecendo todo tipo de produtos e serviços, de seguros, a cartão de crédito, empréstimos consignados, sendo que em muitos casos, operações de créditos são realizadas sem o consentido destes.

Ainda tratando desse tema, destaca RAPÔSO (2019):

---

[2] Cookies são arquivos de texto enviados por sites aos usuários que navegam por eles, que contêm informações necessárias para identificá-lo na próxima visita. Dependendo do site eles podem armazenar preferências de idioma e outras coisas mais amenas até dados como seu endereço IP, o seu e-mail e senhas usadas no seu navegador. Tais arquivos ficam armazenados em seu computador ou celular e são usados quando você volta a visitar os sites, de modo a identificá-lo rapidamente. É por isso que você não precisa fazer login toda vez que acessa o Gmail ou uma loja recupera seu carrinho. O grande problema que envolve a segurança é justamente o fato deles serem extremamente flexíveis, podendo armazenar qualquer informação do usuário; se acessados por gente mal-intencionada, os estragos podem ser enormes.

> Com a globalização e o desenvolvimento de novas tecnologias desenvolve uma competição cada vez mais voraz entre as empresas, desenvolvendo questionamentos sobre a segurança das informações corporativas e de seus clientes. As empresas e até o estado estão cada vez mais vulneráveis à espionagem ou de ataques de Hackers como evidenciado as divulgações de áudios de empresas e dos principais poderes do Brasil.

Continua RAPÔSO (2019):

> Também é comum casos de empresas que fazem uso de forma incorreta dos dados de seus clientes, vendendo ou fornecendo os dados pessoais sem a conscientização e conhecimento deles.

Os constantes avanços tecnológicos, possibilita que empresas estejam sempre inovando as formas de obtenção dos dados pessoais, seja de forma direta ou indireta, daí a surge a necessidade de implementação da LGPD. A busca desenfreada de informações pessoais, e a complexidade dessas operações, resultou naquilo que podemos chamar de terceirização da comercialização. Segundo BIONI (2017, p. 27), atualmente existe uma rede publicidade (ad networkers):

> Elas conectam milhares de aplicações, como websites que exibem (publishers) publicidade aos fornecedores, que querem anunciar (advertisers) um bem de consumo. Os veiculadores (publishers) associam-se a tais redes, terceirizando a venda, total ou parcialmente, dos seus espaços publicitários. Assim, mediante tais acordos, um anunciante (advertisers) poderá capilarizar a promoção de seu produto por todos os publishers dessa rede, em vez de fazê-lo, isoladamente, apenas em uma determinada aplicação.

Podemos através dos exemplos abaixo, demonstrar a importância do correto de informações pessoais e dos riscos quanto ao armazenamento dessas informações:

Com o advento da pandemia do COVID-19, a discussão pertinente ao direito fundamental à proteção de dados, esteve em grande evidência, já que a coleta, armazenamento e processamento de dados da população brasileira se tornou de suma importância para que fossem fornecidas respostas rápidas e adequadas para a tomada de decisão por parte da comunidade científica e dos gestores do setor de saúde. Inclusive com a utilização de aplicativos que captam dados de geolocalização e circulação de pessoas, para se medir o índice de isolamento da população no enfretamento da pandemia.

Lado outro, no dia 22 de janeiro de 2021, veio a público a notícia de um vazamento de dados pessoais de proporções jamais vistas no país[3], o qual foi identificado pela empresa de

[3] Megavazamentos de dados expõem informações de 223 milhões de números de CPF. Dezenas de arquivos foram disponibilizados publicamente e colocados à venda por criminosos. Vazamento de Dados Serasa - Pesquisa Google.

segurança PSafe: mais de 220 milhões de pessoas tiveram informações relacionadas aos mais diversos aspectos de suas vidas publicizadas. A Serasa Experian, empresa que mantém cadastro de pessoas quanto a suas obrigações comerciais, é questionada por conta do vazamento que expôs dados, tais como: nome, CPF, foto de rosto, endereço, telefone, e-mail, score de crédito e salário.

No cenário internacional, temos um exemplo de grande relevância ocorrido na eleição presidencial americana, onde a empresa britânica Cambridge Analytica, através da manipulação de dados algoritmos do Facebook direcionou informações com vistas a beneficiar o então candidato Donald Trump.

Em julho de 2018, o Centro Hospitalar Barreiro Montijo, em Portugal, foi multado em EUR 400.000 euros por violar o Regulamento Geral de Proteção de Dados[4].

A autoridade de supervisão do país, a Comissão Nacional de Proteção de Dados, constatou que houve três violações do GDPR.

(a) Violação ao princípio de minimização, ao permitir acesso indiscriminado a um número excessivo de usuários, e a um dos princípios básicos de processamento de dados;

(b) Violação da integridade e da confidencialidade em resultado da não aplicação de medidas técnicas e organizacionais para impedir o acesso ilícito a dados pessoais, também um dos princípios básicos de processamento.

(c) Finalmente, foi aplicada multa pela incapacidade do réu para garantir a continuação da confidencialidade, integridade, disponibilidade e resiliência dos sistemas e serviços de tratamento, bem como a não implementação das medidas técnicas e organizacionais para garantir um nível de segurança adequado ao risco.

Podemos citar ainda, aplicativos de entretenimento gratuitos, como o “Faceapp”, que através de uma atuação dissimulada, coletava diversas informações dos usuários, fato esse objeto de notificação do PROCON-SP junto à empresa responsável.

2 A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS - LGPD

[4] Hospital do Barreiro multado em 400 mil euros por não proteger dados clínicos dos doentes - Saúde - Jornal de Negócios (jornaldenegocios.pt)

A declaração Universal dos Direitos Humanos de 1948, posteriormente adotada pela Assembleia Geral das Organização das Nações Unidas, já reconhecia o direito à proteção da vida privada, reconhecendo a necessidade de proteção da privacidade individual e familiar, e a liberdade de informação, opinião e expressão:

> Artigo 12º - Ninguém será sujeito à interferência na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques.
> Artigo 19º - Todo ser humano tem direito à liberdade de opinião e expressão; esse direito inclui a liberdade de, sem interferência, ter opiniões e de procurar, receber e transmitir informações e ideias por quaisquer meios e independentemente de fronteiras.

A Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais de 1950, dispõe sobre a proteção dos indivíduos acerca da sua correspondência, da sua vida privada e familiar, exceto se em virtude da lei.

> Artigo 8.º (Direito ao respeito pela vida privada e familiar)
> 1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência.
> 2. Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar económico do país, a defesa da ordem e a prevenção das infracções penais, a protecção da saúde ou da moral, ou a protecção dos direitos e das liberdades de terceiros.

No ano de 1995, a União Europeia promulgou a Diretiva Europeia de Proteção de Dados Pessoais, aplicando-se a mesma legislação a todos os países integrantes do bloco econômico, sendo posteriormente substituída no ano de 2018, pelo Regulamento Geral sobre a Proteção de Dados – GDPR, que influenciou de forma significativa a Lei Geral de Proteção de Dados Pessoais – LGPD, no Brasil.

O Brasil como signatário de alguns acordos internacionais, dentre eles a Convenção de Berna de 1986 e o Acordo sobre Aspectos dos Direitos de Propriedade Intelectual relacionados ao Comércio (TRIPS), já possuía ainda que de forma precária, algumas ações voltadas para a proteção de dados pessoais. Já no âmbito interno, podemos destacar as seguintes Leis:

(a) Lei nº 8.078/1990 – Código de Defesa do Consumidor;
(b) Decreto Federal nº 7.962/2013 e nº 7.963/2013 – Lei do E-commerce e Plano Nacional de Consumo e Cidadania;
(c) Lei nº 12.965/2014 – Marco Civil da Internet;

(d) Lei nº 13.709/2018 e Medida Provisória nº 869/2018 – Lei Geral de Proteção de Dados e Autoridade Nacional de Proteção de Dados.

Até a promulgação da LGPD, o titular dos dados era o responsável pela proteção de seus próprios dados, decidindo a todo momento se consentia ou não o uso deles, não tendo nenhuma segurança de como seria sua utilização, com edição da lei, atribui-se responsabilidade pelo coletor dos dados pessoais, definindo atribuições específicas para a sua coleta, armazenamento e processamento.

A LGPD, disciplina sobre o tratamento dos dados pessoais, inclusive nos meios digitais, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, estabelece regras e limites na coleta, armazenamento, tratamento e compartilhamento de dados, dentre os benefícios advindos da lei, destaca-se:

(a) Fomentar o desenvolvimento econômico e tecnológico;
(b) Padronização de normas, estabelecendo regras únicas e gerais sobre o tratamento de dados pessoais;
(c) Segurança jurídica, garantindo a livre iniciativa, a livre concorrência e a defesa das relações comerciais e de consumo;
(d) Estimular a concorrência e a liberdade econômica, possibilitando inclusive a portabilidade de dados.

O Brasil, há longa data, deseja ingressar na Organização para a Cooperação e Desenvolvimento Econômico (OCDE), com o objetivo de estabelecer uma cooperação internacional, visando a ampliação de parceiros comerciais e a obtenção de investimentos. Isto, explica a tramitação e promulgação da Lei de forma tão célere, uma vez que um dos requisitos para se ingressar como membro da OCDE, é a existência de uma lei específica de proteção de dados pessoais.

A LGPD, em seu artigo 6º, caput, dispõe sobre a boa-fé nas atividades de tratamento de dados pessoais, e elenca outros 10 (dez) princípios a serem observados:

> "I – Finalidade; II – Adequação; III - Necessidade; IV – Livre acesso; V – Qualidade dos dados; VI – Transparência; VII – Segurança; VIII – Prevenção; IX – Não discriminação; X – Responsabilidade e prestação de contas."

O princípio da boa-fé deve ser considerado concomitantemente com os demais princípios. O princípio da finalidade, impõe que o dado coletado deve ter sua destinação em conformidade com o objetivo inicialmente proposto, sem possibilidade de tratamento posterior

de forma incompatível com esses objetivos, e com as normas que regulamentam o tratamento de dados. Delimita a transmissão de dados a terceiros, define demais critérios, tais como: propósitos legítimos, específicos, explícitos e informados ao usuário, impedindo sua utilização de forma genérica e indeterminada.

O art. 2º da LGPD apresenta um rol de fundamentos, incluindo:

> "I - o respeito à privacidade; II - a autodeterminação informativa; III - a liberdade de expressão, de informação, de comunicação e de opinião; IV - a inviolabilidade da intimidade, da honra e da imagem; V - o desenvolvimento econômico e tecnológico e a inovação; VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais."

Estes fundamentos guardam relação direta com os direitos fundamentais previstos na Constituição da República/88, e servem como uma base ampla e geral, para a interpretação de todos os dispositivos da lei.

COÊLHO (2020) traz importante recorte acerca do tema:

> Os dados são o ativo e o legado do século 21, da "Era da Informação". Esse novo giro histórico requer do Estado a adequada e efetiva proteção dos cidadãos, da sua privacidade e da autodeterminação em relação aos seus dados pessoais. Constitui dever de um Estado Social e Democrático de Direito, garantidor da dignidade humana e de sua autodeterminação no campo informacional, livrar-nos de horizontes distópicos como aqueles imaginadas pelo escritor George Orwell, em sua obra "1984" ou na série televisiva "Black Mirror". (...) Novos dados de realidade exigem o reconhecimento de novos direitos e o alargamento das garantias jurídicas com vistas a tutelar, com a máxima efetividade, a autodeterminação das pessoas e, ao fim e ao cabo, o direito à dignidade humana. Na Era da Informação, inegável que o direito ao sigilo dos dados pessoais e à autodeterminação sobre eles seja constitutivo de um direito mais amplo da dignidade e da personalidade humanas.

Portanto, as informações pessoais, na era da informação, como disse Coêlho, é o patrimônio mais precioso e íntimo a ser preservado, onde deu lugar ao nascimento de leis que protege tal ativo em face da dignidade da pessoa humana.

2.1 DOS AGENTES DE TRATAMENTO DE DADOS PESSOAIS

Conforme disposto na LGPD, no art. 5º, temos 4 sujeitos envolvidos no tratamento de dados.

(a) Titular: é a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

(b) b. Controlador: pessoa natural ou jurídica, de direito público ou privado, que realiza a coleta os dados pessoais e toma as decisões quanto a forma do tratamento a ser realizado;

(c) Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento dos dados pessoais, conforme determinado pelo controlador;

(d) Encarregado: pessoa natural, indicada pelo controlador e operador atuando como um canal de comunicação entre os titulares dos dados e a Autoridade Nacional de Proteção de Dados – ANPD. Também conhecido como DPO (Data Protection Officer).

O controlador e o operador também são chamados de agentes de tratamento, e devem manter registro das operações de tratamento de dados pessoais que realizarem. Poderá ainda, a autoridade nacional determinar a elaboração de relatório de impacto à proteção de dados pessoais, avaliando os riscos às liberdades civis e aos direitos fundamentais, bem como medidas preventivas para salvaguarda e mitigação de riscos.

O encarregado pelo tratamento de dados pessoais deverá ter sua identidade e informações de contato divulgadas publicamente de forma clara e objetiva, de preferência no sítio eletrônico do controlador. Dentre outras, suas atribuições consistem em aceitar reclamações e comunicações dos titulares; prestar esclarecimentos e adotar providências, atender e tomar as providências necessárias às requisições emanadas da autoridade nacional, realizar treinamento aos funcionários e contratados da entidade.

2.2 DEFINIÇÕES RELEVANTES

Um dos principais requisitos para o tratamento de dados pessoais, é o consentimento do titular dos dados, que se trata da manifestação livre e inequívoca de que autoriza o tratamento dos dados pessoais para uma finalidade específica. São nulas as autorizações genéricas, ou seja, aquelas que não apresentam uma finalidade específica, explícita e informada. O consentimento deverá ser obtido de forma escrita, ter caráter temporário, uma vez que pode ser revogado a qualquer momento pelo titular dos dados. Caso haja a mudança de finalidade para o tratamento dos dados pessoais, e esta não seja compatível com a finalidade originária, deverá o controlador

informar previamente o titular dos dados. Uma vez atingida a finalidade para qual os dados foram coletados, deverá haver a imediata exclusão destes.

Além do consentimento do titular dos dados, a lei traz um rol de mais 9 situações nas quais é possível tratar dados pessoais sem o consentimento do titular. São elas:

(a) Cumprimento de obrigação legal ou regulatória pelo controlador;
(b) Pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres;
(c) Para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
(d) Quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
(e) Para o exercício regular de direitos em processo judicial, administrativo ou arbitral, este último nos termos da Lei da Arbitragem;
(f) Para a proteção da vida ou da incolumidade física do titular ou de terceiro;
(g) Para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
(h) Quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, e;
(i) Para a proteção do crédito.

Entende como Dado Pessoal aqueles relacionados com a pessoa natural, identificada ou identificável, que especifica uma pessoa de forma individualizada, podendo através destes monitorar o comportamento e o perfil da pessoa titular dos dados. São exemplos de dados pessoais: Nome, Carteira de Identidade, CPF, Título de Eleitor, CNH, endereço, geolocalização de dispositivo móvel, endereços de IP, etc.

Dados Pessoais Sensíveis, são dados que quando vinculados a uma pessoa natural, merecem uma proteção mais rigorosa por parte da LGPD, exigindo um termo de consentimento mais específico e de forma destacada. Não se permitindo o tratamento de dados pessoais sensíveis para atender interesse legítimo do controlador ou de terceiros ou de proteção do

crédito. Lado outro, permanece inalterada a possibilidade de tratamento quando necessário para o cumprimento de obrigação legal ou regulatória pelo controlador dos dados, para o exercício legal de direitos em processo judicial, administrativo ou arbitral, e também nas situações em que se torna necessário para a execução de contratos. São exemplos de dados pessoais sensíveis: convicção religiosa, origem racial ou étnica, dados referentes à saúde, à vida sexual, opinião política, dado genético, etc.

Dados Anonimizados, dado relativo a titular que não permite ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis quando de ser tratamento. Situação em que o dado perde a possiblidade de associação, direta ou indireta, a uma pessoa natural individualizada. Esses dados não contam com a proteção da Lei Geral de Proteção de Dados Pessoais.

Dados Pseudo-anonimizados, situação semelhante ao dado anonimizado, em que o dado perde a possibilidade de associação, direta ou indireta, a uma pessoa natural individualizada, porém pode ser tratado através de informação adicional, mantida separadamente pelo controlador em ambiente controlado e seguro. Este tipo de dado não só conta com a proteção da LGPD, como também há um incentivo à adoção dessa prática, com vistas a minimizar os riscos, resultando em maior segurança no tratamento dos dados pessoais.

Tratamento de Dados Pessoais de Crianças e de Adolescentes deverá ser realizado em atendimento ao seu melhor interesse, e somente poderá ser realizado com o consentimento específico dado por pelo menos um dos pais ou pelo responsável legal. Sendo permitida a sua coleta sem o consentimento de pais ou responsável legal, quando tiver por objetivo contatar os pais ou representante legal, podendo ser utilizados apenas uma vez, sem armazenamento e não podem ser repassados a terceiros.

A lei garante ao titular dos dados pessoais, os direitos fundamentais de liberdade, intimidade e de privacidade, lhe assegurando o direito de obter junto ao controlador, a qualquer momento e mediante requisição, informações a respeito de seus dados, podendo exigir a imediata correção de dados incompletos, inexatos ou desatualizados. Verificado o descumprimento de algum dispositivo da lei, poderá o titular dos dados se opor ao tratamento de seus dados pessoais, mesmo se este for realizado em uma das hipóteses de dispensa de consentimento. Poderá mediante requisição expressa, solicitar a transferência de seus dados pessoais a outro fornecedor de produtos ou serviços, assim como revogar o consentimento realizado anteriormente.

O titular dos dados pessoais tem direito de forma gratuita e mediante requisição expressa ao controlador, das seguintes informações:

(a) Confirmação da existência de tratamento e acesso aos seus dados pessoais;
(b) Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou contrários ao disposto na lei;
(c) Informações a respeito do uso compartilhado de dados pessoais,
(d) Eliminação dos dados pessoais, exceto nos casos judiciais ou regulatórios.

O titular dos dados pessoais tem direito se ter acesso facilitado às informações a respeito do tratamento de seus dados pessoais, dentre eles: finalidade específica do tratamento; forma e duração do tratamento; responsabilidade dos agentes de tratamento, identificação e contato do controlador, e outros conforme disposto na LGPD.

2.3 AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

Se o texto original da LGPD, aprovado em agosto de 2018, previa a criação de uma entidade, com natureza autárquica e, portanto, pertencente à Administração Pública indireta no plano federal, a MP 869/2018 andou em sentido diametralmente oposto, criando-a como órgão vinculado à Presidência da República, conforme PFEIFFER (2019). Por fim, na consolidação do texto final da reforma, por ocasião da conversão da medida provisória na Lei nº 13.853, de 08 de julho de 2019, notou-se certa intenção de equacionar esta controvérsia, com a criação da ANPD como órgão, mas de natureza transitória, sendo possivelmente transformada em entidade (autarquia) a posteriori, FERRAZ (2020). Naturalmente, a inserção do verbo "poderá" no §1º do artigo 55-A causou imediato receio, uma vez que deixou em aberto certo grau de discricionariedade para a efetiva conversão do novo órgão em entidade, embora o §2º delimite um prazo de até 2 (dois) anos para que esta decisão seja tomada, MARTINS (2021).

Com a promulgação de LGPD, foi criada a Autoridade Nacional de proteção de Dados (ANPD), através da Lei nº 13.853/2019, tendo suas competências estabelecidas pelo artigo 55-J, sendo suas principais atribuições:

(a) Zelar pela proteção dos dados pessoais, nos termos da legislação;
(b) Apreciar as petições de titular contra controlador, após comprovada a apresentação de reclamação e não solucionada no prazo estabelecido;
(c) Solicitar, a qualquer momento, às entidades do poder público relatórios sobre as operações de tratamento de dados realizadas, e emitir parecer técnico quanto a sua adequação a LGPD;

(d) Editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais.
(e) Realizar auditorias ou determinar a sua realização;
(f) Comunicar às autoridades competentes as infrações penais da quais tiver conhecimento;
(g) Fiscalizar e aplicar sanções em caso de tratamento de dados em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso.

Em caso de incidente de segurança deverão ser comunicados, em prazo razoável, à autoridade nacional de proteção de dados e o titular dos dados. A autoridade poderá determinar a adoção de outras medidas e eventual comunicação a outros órgãos reguladores, como CVM e BACEN.

A LGPD prevê a aplicação de severas sanções para as entidades que descumprirem seus requisitos, sendo imperativo a adequação das empresas ao disposto na lei. A Autoridade Nacional de Proteção de Dados deverá observar diversos aspectos no caso de aplicação de uma sanção: o dano causado, mecanismos e procedimentos internos adotados pela empresa para mitigar os danos, implementação de boas práticas de governança, segurança e prevenção.

A legislação prevê diversas sanções administrativas aplicáveis pela autoridade nacional, que vão desde a advertência, com indicação de prazo para adoção de medidas corretivas, até multa que pode chegar até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, limitada a R$ 50.000,000,00 (cinquenta milhões de reais) por infração. Várias outras sanções podem ser impostas, tais como: multa diária; publicização da infração; bloqueio ou eliminação dos dados pessoais, suspensão parcial ou definitiva da atividade de tratamento dos dados pessoais.

O controlador ou o operador, que em função da atividade de tratamento de dados, causar danos a terceiros, é obrigado a repará-lo, o operador responde solidariamente quando descumprir as obrigações da legislação de proteção de dados, ou quando não seguir as instruções lícitas do controlador.

3 CONSIDERAÇÕES FINAIS

O princípio fundamental da LGPD é a proteção de dados pessoais, configurando-se como um direito fundamental da personalidade do indivíduo, inclusive de sua dignidade humana, destaca-se a forma comercial de como os dados pessoais são tratados atualmente no Brasil que, nesse sentido busca-se prevenir a violação e o uso abusivo de dados, como a forma abusiva de publicidade direcionada, estabelecendo critérios objetivos quanto à adequação e a necessidade para a coleta e tratamento de dados.

A LGPD permite ao cidadão que tiver seus direitos violados, tenha amparo no poder judiciário, buscando impedir que empresas detentoras dos dados continue a realizar manipulação dos dados de forma irregular. A lei provoca um grande impacto na atividade empresarial, passando a exigir adequações operacionais na obtenção e tratamento de dados pessoais, sempre preservando o binômio transparência e privacidade. Quanto maior a transparência com relação ao tratamento de dados, menos abusiva e desonesta será a conduta das empresas, tornando mais segura e confiável a privacidade dos usuários.

Nesse sentido, a nova legislação traz grandes desafios de natureza cultural, organizacional e principalmente para as pequenas e médias empresas, no que diz respeito aos elevados custos para implementação desses novos mecanismos de controle, em um ambiente já particularmente agravado em virtude da pandemia do COVID-19. Porém, obrigatória sua implantação e o modelo deve ser aplicado de forma peculiar, personalizada a necessidade do empresário.

Destaca-se, ainda, que a LGPD prevê a aplicação de severas sanções às organizações que não se adequarem ao novo marco regulador, que vão desde a advertência, com a indicação de prazo para adoção de medidas corretivas, até a aplicação de multa que pode chegar até 2, (dois por cento) do faturamento da pessoa jurídica de direito privado, limitada a R$ 50.000.000,00 (cinquenta milhões de reais) por infração. Contudo, a Autoridade Nacional de Proteção de Dados deverá levar em consideração diversos requisitos na aplicação de uma sanção: (i) o dano causado; (ii) mecanismos e procedimentos internos adotados pela empresa para mitigar os danos; (iii) implementação de boas práticas; (iv) segurança e (v) prevenção.Por fim, deve se destacar que a lei veio para proteger os dados, sobretudo em um mundo globalizado e muito virtual como o que estamos vivendo, onde os dados pessoais e o cruzamento das informações que eles carregam é um elemento importantíssimo para efeito de controle, comércio e respeito, não podendo ser banalizado.

REFERÊNCIAS

A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS E OS DESAFIOS DAS INSTITUIÇÕES DE ENSINO SUPERIOR PARA A ADEQUAÇÃO. Disponível em: https://repositorio.ufsc.br/bitstream/handle/123456789/201939/103_00090.pdf?sequence=1&isAllowed=y.ufsc.br/bitstream/handle/123456789/201939/103_00090.pdf?sequence=1&isAllowed=y. Último acesso em: 20 nov. 2021.

BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

BRASIL. Constituição da República Federativa do Brasil. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 5 out. 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Último acesso em: 20 nov. 2021.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, 2018. Disponível em: www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Último acesso em: 20 nov.2021.

BRASIL. Presidência da República. Casa Civil. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Último acesso em: 20 nov. 2021.

BRASIL. Presidência da República. Casa Civil. Lei nº 13.853, de 8 de julho de 2019. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm. Último acesso em: 20 nov. 2021.

COÊLHO, Marcus Vinicius Furtado. O direito à proteção de dados e a tutela da autodeterminação informativa. Consultor Jurídico, 2020. Disponível em: https://www.conjur.com.br/2020-jun-28/constituicao-direito-protecao-dados-tutela-autodeterminacao-informativa. Último acesso em: 20 nov. 2021.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. Espaço Jurídico, Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011.

FERRAZ, Pedro da Cunha. Autoridade Nacional de Proteção de Dados (ANPD): apontamentos sobre sua natureza e regime jurídico. In: DAL POZZO, Augusto; MARTINS, Ricardo Marcondes (Coords.). LGPD & Administração Pública: uma análise ampla dos impactos. São Paulo: Thomson Reuters Brasil, 2020, p. 621 et seq.

FIESP – CIESP: Lei Geral de Proteção de Dados. file-20181212135037-lei-geral-de-protecao-livreto-a5-web.pdf. Último acesso em: 20 nov. 2021.

GARCEL, Adriane; MORO, Sergio Fernando; SOUZA NETTO, José Laurindo de; HIPPERTT, Karen Paiva. Lei geral de proteção de dados: diretrizes e implicações para uma sociedade pandêmica. Coletâneas de artigos jurídicos: em homenagem ao Professor José Laurindo de Souza Netto. Viviane C. de S. K., Adriane G., José L. de S. N. 1.ed., Curitiba: Clássica Editora, 2020. ISBN 978-65-87965-03-1. p. 319-344

Guia para a Lei Geral de Proteção de Dados – Mattos Filho.
https://www.mattosfilho.com.br/EscritorioMidia/LGPD_MattosFilho.pdf. Último acesso em: 20 nov. 2021.

LGPD – Lei Geral de Proteção de Dados. Disponível em: https://www.sebrae.com.br/Sebrae/PortalSebrae/UFs/RJ/Click Empreendedor/LGPD-Sebrae-Nacional.pdf. Último acesso em: 20 nov. 2021.

MAIA, Adriane. Os impactos da LGPD para os negócios. E-commerce brasil, 2019. Disponível em: Os impactos da LGPD para os negócios | E-Commerce Brasil (ecommercebrasil.com.br) https://www.ecommercebrasil.com.br/artigos/os-impactos-da-lgpd-para-os-negocios/. Último acesso em: 20 nov. 2021.

MARTINS, Guilherme Magalhães; BASAN, Arthur Pinheiro; FALEIROS JÚNIOR, José Luiz de Moura. O direito fundamental à proteção de dados pessoais e a pandemia da covid-19. Revista Eletrônica de Direito do Centro Universitário Newton Paiva, Belo Horizonte, n.43, p.232-255, jan./abr. 2021. Disponível em: https://revistas.newtonpaiva.br/redcunp/n-43-o-direito-fundamental-a-protecao-de-dados-pessoais-e-a-pandemia-da-covid-19/. Último acesso em: 20 nov. 2021.

PARLAMENTO EUROPEU; CONSELHO EUROPEU. Regulamento (UE) 2016/679 de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE. Bruxelas: Jornal Oficial da União Europeia, 2016. Disponível em: < https://eur- 14 lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT>. Último acesso em: 20 nov. 2021.

PFEIFFER, Roberto Augusto Castellanos. ANPD em busca de sua autonomia: é preciso aperfeiçoar a MP 869/2018. Consultor Jurídico, 1º de maio de 2019. Disponível em: https://www.conjur.com.br/2019-mai-01/garantias-consumo-anpd-busca-autonomia-preciso-aperfeicoar-mp. Último acesso em: 20 nov. 2021.

Revista Processando o Saber (eISSN: 21795150) é publicada pela FATEC Praia Grande Multidisciplinar - Acesso aberto - www.fatecpg.edu.br/revista - revista@fatecpg.edu.br. Último acesso em: 20 nov. 2021.