

A BUSCA INCESSANTE PELA PROTEÇÃO DE DADOS PESSOAIS NA SOCIEDADE ATUAL SOB A ÓTICA DA LEI 13.709/18

Raiana Caberlon Duarte
Andressa Maria Dias Neumann

Resumo

O presente artigo versa sobre a Lei Geral de Proteção de Dados (Lei 13.709/18 - LGPD) e como utilizá-la. Considerando a imensa circulação de dados pessoais na atualidade e a possibilidade de vazamento dos mesmos, é necessária uma análise minuciosa do referido texto legal. Com base neste estudo, em conjunto com a doutrina nacional e estrangeira já existente, é possível compreender o impacto que a LGPD está causando no Brasil. Na era da informação, é imprescindível um controle sobre os dados e sua segurança. As empresas, neste ponto, sofrem inúmeros percalços, a exemplo de como aplicar a LGPD, adequando os sistemas a ela, a fim de não suportarem as sanções em caso de vazamento de dados. Sendo assim, busca-se expor conceitos, analisar requisitos e alternativas que conduzam à exploração adequada do Big Data, um sistema de armazenamento de dados pessoais que será estudado no desenvolvimento do artigo.

Assim sendo, é possível dizer que o estudo busca verificar qual a solução correta para empresas brasileiras adequarem-se à LGPD, destacando que o investimento em tecnologias no sentido de possuir maior controle sobre os dados pessoais é o caminho, minimizando-se a possibilidade de vazamento.

Palavras-chave: Big Data. Proteção de dados. Era da informação. Dados pessoais. Tecnologia.

1 INTRODUÇÃO

Na era da sociedade da informação e com o avanço digital, em que todos estão cada vez mais conectados e os negócios mais e mais

informatizados, o trânsito de dados pessoais ampliou de forma avassaladora, estando por toda parte. Com isso, surgiu a necessidade de proteção dos dados relativos às pessoas naturais em razão do crescente risco de manipulação e utilização destes contra seus detentores.

Neste novo cenário mundial, as empresas - através da tecnologia - desempenham um papel central nas interações sociais. A rede social que sugere uma amizade, o site que apresenta uma oportunidade de trabalho, e o aplicativo que aponta o melhor caminho para casa, todos eles têm em comum o mesmo combustível: nossos dados pessoais. O incremento da tecnologia da informação permitiu às empresas monitorar o comportamento atual e as tendências futuras de seus clientes a partir do tratamento de seus dados pessoais.

Tornou-se necessário, então, enquadrar juridicamente a proteção de dados pessoais como um direito fundamental global. Em outras palavras, direito humano, cujo âmbito de proteção tende a se expandir com o crescimento desenfreado da utilização de dados pessoais, tanto pelo setor privado como pelos órgãos públicos. Assim, surgiram no mundo várias legislações visando à tutela da proteção de dados pessoais.

O Brasil já possuía uma série de normas setoriais sobre o assunto, com dispositivos que podem ser aplicados à proteção de dados espalhados pela Constituição Federal, Código de Defesa do Consumidor, Código Civil, Lei de Acesso à Informação, Lei do Cadastro Positivo e Marco Civil da Internet. Todavia, nosso acervo legislativo sofreu um considerável incremento em 14 de agosto de 2018, com a sanção da Lei n. 13.709/2018, conhecida como Lei Geral de Proteção de Dados Pessoais - LGPD, que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou jurídica (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.

Em suma, a Lei n. 13.709/2018 inaugura uma nova cultura de privacidade e proteção de dados no país, o que demanda a conscientização de toda a sociedade acerca da importância dos dados pessoais e os seus

reflexos no tocante aos direitos e garantias fundamentais, mais especificamente a liberdade, a privacidade e o livre desenvolvimento da personalidade da pessoa natural.

2 DESENVOLVIMENTO

2.1 ENTENDENDO A LEI 13.709/2018

Baseando-se no próprio site da Lei Geral de Proteção de Dados (endereço eletrônico <<https://www.lgpdbrasil.com.br/>>), a Lei 13.709/18 foi aprovada em agosto de 2018 e terá suas sanções aplicadas a partir de agosto de 2021. No seu artigo primeiro já menciona a disposição sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou 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.

Conforme Mario Bruno Aliste (2019), a construção da LGPD surgiu pela demanda da proteção de dados pessoais mediante inúmeros vazamentos e ataques cibernéticos ocorridos recentemente. Um bom exemplo de tais ataques foi o vazamento de dados de milhões de usuários do Facebook para a empresa britânica de marketing político Cambridge Analytica.

Segundo consta no site do Governo do Brasil (endereço eletrônico <<https://www.serpro.gov.br/lgpd/menu/a-lgpd/o-que-muda-com-a-lgpd>>), evitando confusão, a lei define o que são dados pessoais em seu artigo 5º. Inclusive, estabelece que existem alguns desses dados que estão sujeitos a cuidados ainda mais específicos, como os sensíveis e os sobre crianças e adolescentes, e que dados tratados tanto nos meios físicos como nos digitais estão vinculados à regulação. Nesse mesmo artigo, no inciso XII, há um elemento essencial que é o consentir; ele é extremamente importante tendo em vista que, atualmente, grande parcela da economia gira em torno da coleta, tratamento e comercialização de dados pessoais. Dessa forma, o consentimento é a base para que dados pessoais possam ser tratados. Isso significa que a pessoa autoriza o tratamento de determinados dados após ter recebido informações suficientes para formar sua opinião.

Contudo, o site mencionado anteriormente, traz que o tratamento de dados pessoais poderá ser realizado nas seguintes hipóteses: cumprir uma obrigação legal; executar política pública prevista em lei; realizar estudos via órgão de pesquisa; executar contratos; defender direitos em processo; preservar a vida e a integridade física de uma pessoa; tutelar ações feitas por profissionais das áreas da saúde ou sanitária; prevenir fraudes contra o titular; proteger o crédito; ou atender a um interesse legítimo, que não fira direitos fundamentais do cidadão.

Resumidamente, as principais funções da lei são assegurar o direito à privacidade e à proteção de dados pessoais dos usuários, por meio de práticas transparentes e seguras, garantindo direitos fundamentais e fortalecer a segurança das relações jurídicas e a confiabilidade do titular no tratamento de dados pessoais, garantindo a livre iniciativa, a livre concorrência e a defesa das relações comerciais e de consumo, bem como, estabelecer regras claras sobre tratamento de dados pessoais, impulsionar o desenvolvimento, promover a concorrência e padronizar normas.

No entanto, 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 (art. 8º, §5º).

2.1.2 Abrangência da aplicação da LGPD

O Art. 3º da Lei 13.709, afirma que a LGPD regulamentará qualquer atividade que envolva utilização de dados pessoais, no território nacional ou em países onde estejam localizados os dados. Irá aplicar-se extraterritorialmente nos seguintes casos: a operação de tratamento dos dados seja realizada no território nacional; a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; os dados pessoais, objeto do tratamento, tenham sido coletados no território nacional.

2.1.3 Direito do titular dos dados

Neste ponto, importante mencionar e estar atento ao que estabelece o art. 18 da Lei 13.709/18: "O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição".

Conforme o próprio site da LGPD dispõe, dentre os principais direitos estão:

1. Confirmar a existência de tratamento de seus dados pessoais.
2. Acessar seus dados pessoais.
3. Corrigir dados pessoais incompletos, inexatos ou desatualizados.
4. Anonimização, bloqueio ou eliminação de dados pessoais desnecessários, excessivos ou tratados em desconformidade com a LGPD.
5. Portabilidade de dados pessoais a outro fornecedor de produto ou serviço.
6. Eliminação de dados tratados com o seu consentimento.
7. Obtenção de informações sobre as entidades públicas e privadas com as quais o controlador realizou o compartilhamento de dados pessoais.
8. Obtenção de informações sobre a possibilidade de não consentir com o tratamento de dados pessoais e sobre as consequências da negativa.
9. Revogação do consentimento dado para o tratamento de dados pessoais.
10. Portabilidade dos dados (artigo 18, V), que, similar ao o que pode ser feito entre diferentes empresas de telefonia e bancos, permite ao titular não só requisitar uma cópia da integralidade dos seus dados, mas também que estes sejam fornecidos em um formato interoperável, que facilite a transferência destes para outros serviços, mesmo para concorrentes. Devido a sua natureza, este novo direito tem sido encarado como um forte elemento de competição entre diferentes empresas que oferecem serviços similares baseados no uso de dados pessoais.

2.1.4 Controlador e operador

Controlador e operador são os agentes de tratamento de dados pessoais. O art. 37 da LGPD dispõe que “o controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse”.

O operador deve realizar o tratamento de dados de acordo com as instruções fornecidas pelo controlador (art. 39 da LGPD). O controlador deve indicar o encarregado (DPO – Data Protection Officer) pelo tratamento de dados pessoais (art. 41 da LGPD).

Entretanto, a lei traz responsabilidades para aqueles que de alguma forma descumprirem os ditames legais ou vasarem dados pessoais e, de alguma forma, causarem prejuízos a terceiros. Assim, surge a possibilidade de ressarcimento de danos, onde o controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, será obrigado a repará-lo.

2.1.5 Tratamento de dados para cumprimento de obrigação legal ou regulatória

De acordo com o art. 7º da LGPD, o tratamento de dados para cumprimento de obrigação legal ou regulatória dar-se-á nos seguintes casos:

1. Pelo controlador (art. 7º, II);
2. Pela administração pública (art. 7º, III);
3. Para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais (art. 7º, IV);
4. 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 (art. 7º, V);
5. Para o exercício regular de direitos em processo judicial, administrativo ou arbitral (art. 7º, VI);

6. Para a proteção da vida ou da incolumidade física do titular ou de terceiro (art. 7º, VII);

7. Para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias (art. 7º, VIII).

Entretanto, existem exceções dispostas nos incisos IX e X, os quais mencionam que o tratamento de dados pessoais poderá ser realizado, quando necessário, para atender aos interesses legítimos do controlador ou de terceiros, salvo no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, ou para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

Além disso, o Estado detém enormes bancos de dados pessoais, muitos deles formados a partir de informações fornecidas obrigatoriamente pelos cidadãos. A LGPD não faz menção à expressão "dados públicos", mas sim a "dados pessoais cujo acesso é público", ou seja, dados cuja divulgação pública é obrigatória por lei, como por exemplo, o fato de alguém ser proprietário de um imóvel (art. 7º, §3º da lei 13.709/18)

Levando tudo isso em consideração, diante da inovação digital dos últimos anos, o universo dos negócios consegue ter disponível um grande volume de informações, que cresce exponencialmente. Tais informações, necessitam, por óbvio, de um gigantesco "banco de dados", capaz de armazenar em tempo real toda essa gama de conteúdo; aí surge o denominado "Big Data".

2.2 BIG DATA

O "Big Data" representa uma revolução de dados relativamente recente, que tem sua grandeza confirmada pelos números que a acompanham. Ele é de rápido crescimento (exponencial, diga-se de passagem) em todo o mundo, com imensas consequências para a sociedade, independentemente de classe social, e que é caracterizado pela coleta e processamento de um grande volume e variedade de dados e obtenção de informações a uma velocidade quase impossível de se imaginar (BAGNOLI, 2016). É, de fato, uma avalanche informacional.

O termo “Big Data” refere-se aos conjuntos de dados cujo tamanho está além da capacidade de uma ferramenta tradicional de base de dados capturar, armazenar, gerenciar e analisar, representando a próxima fronteira para inovação, concorrência e produtividade. O volume, a velocidade, a variedade, o valor, a veracidade e a validação, ou os “6V’s”, são virtuosas características atreladas ao Big Data (BAGNOLI, 2017).

2.2.1 Desafios à exploração do Big Data

A primeira característica fundamental, e que traz grandes desafios à sua legítima exploração, se deve ao fato de que a análise de Big Data frequentemente revela a possibilidade de se utilizar os dados coletados para uma finalidade diversa daquela proposta inicialmente. A segunda está relacionada ao volume de dados coletados, que não raramente se mostram amplamente melhores e mais valiosos do que aqueles encontrados tradicionalmente em bases de dados estruturados (KALYVAS; OVERLY, 2015). Dessa maneira, decorrem, obviamente, impactos econômicos e sociais, o que fortalece o poder daqueles que detêm as informações. Em outras palavras: informação é poder.

De acordo com Vinicius Cervantes e David Fernando Rodrigues, autores do artigo “Big data e proteção de dados: o desafio está lançado”, tais características desafiam princípios a serem observados no tratamento de dados pessoais e o direito à privacidade, que acabam impondo limites à exploração de Big Data considerando sua capacidade de interferir na efetivação de direitos individuais fundamentais.

No Brasil, um dos grandes desafios a serem enfrentados, tratando-se de Big Data, é a própria LGPD. Dentre seus princípios, ela elenca os seguintes: adequação; necessidade; livre acesso; qualidade dos dados; transparência; segurança; prevenção; não discriminação; responsabilização e prestação de contas. Contudo, a observância de tais princípios torna-se uma tarefa bastante difícil de ser completada, o que talvez reflita uma controvérsia à própria essência de Big Data.

2.2.2 Sanções em caso de vazamento

Quando ocorre o vazamento de informações pessoais sigilosas, obviamente devemos seguir um roteiro a fim de mitigar os prejuízos advindos de tal fato. Assim sendo, as etapas de comunicação a seguir são as seguintes:

1. A descrição da natureza dos dados pessoais afetados
2. As informações sobre os titulares envolvidos
3. A indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial
4. Os riscos relacionados ao incidente
5. Os motivos da demora, no caso de a comunicação não ter sido imediata
6. As medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

Uma vez vazados os dados e feita a comunicação, a Lei 13.709/2018 estabelece parâmetros e critérios para aplicação das sanções aos responsáveis, as quais, obviamente, devem ser proporcionais à gravidade da infração. Em caso de descumprimento da lei, a Autoridade Nacional poderá aplicar:

1. Advertência, com indicação de prazo para adoção de medidas corretivas
2. Multa simples, de até 2% do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R\$ 50.000.000,00 (cinquenta milhões de reais) por infração
3. Multa diária, observado o limite total a que se refere o inciso II
4. Publicização da infração após devidamente apurada e confirmada a sua ocorrência
5. Bloqueio dos dados pessoais a que se refere a infração até a sua regularização
6. Eliminação dos dados pessoais a que se refere a infração

Dito isso, não há dúvidas quanto às vantagens proporcionadas pelo Big Data aos agentes econômicos para melhor atuação no mercado e ao Estado

para o melhor desenvolvimento de políticas públicas. Certamente, a regulamentação das atividades de tratamento de dados pessoais no Brasil trouxe maior segurança não apenas para o mercado, mas também aos indivíduos, consumidores e titulares dos dados pessoais.

2.3 IMPLEMENTAÇÃO DA LGPD NAS EMPRESAS

A lei brasileira tem como inspiração a General Data Protection Regulation (GDPR), assinada na União Europeia em 2016 e, como o modelo estrangeiro, objetiva ampliar a segurança no tratamento de dados pessoais de usuários online.

Desta forma, ambas as legislações preveem a implementação de medidas de segurança em empresas privadas e públicas que façam uso de informações pessoais para comercializar produtos e serviços. A partir da vigência da LGPD, passa a ser obrigatório que todas as empresas que lidem com dados particulares - desde os mais simples, como nome, endereço, telefone, aos mais complexos, como informações bancárias - os protejam por meio de políticas internas, com o prazo para adequação até agosto de 2021, sob pena de sofrer as penalidades.

Na prática, há cinco principais pontos básicos que as empresas devem cumprir para estarem de acordo com a Lei Geral de Proteção de Dados.

2.3.1 Treinamento de equipe na LGPD

O primeiro deles é determinar uma equipe que deve ser treinada para responder pelo tratamento de dados. Eleger quem terá acesso às informações auxilia na prevenção de falhas internas e treinamento de planos em casos de risco de vazamento de informações. Outra vantagem é garantir agilidade na apuração de possíveis erros e na correção deles.

Desta forma, estes profissionais devem ter conhecimento sobre as normas e entender de compliance (o conjunto de disciplinas a fim de cumprir e se fazer cumprir as normas legais e regulamentares, da proteção de dados).

2.3.2 Implementação de medidas de segurança

Outra medida de segurança é adotar a emissão de certificados digitais corporativos para a identificação das pessoas que tratam os dados.

Este time atuará de forma a garantir a integridade dos dados, além de ser um canal de comunicação direto para atender demandas dos titulares das informações e da Agência Nacional de Proteção de Dados (ANPD). Será ainda o time responsável por justificar possíveis erros e irregularidades.

2.3.3 Transparência online

O Site oficial da LGPD (endereço eletrônico <https://www.lgpdbrasil.com.br/>) informa: “Seja transparente com o titular das informações”. A Lei 13.709/2018 proíbe o uso indiscriminado de dados por meio de cadastros. Assim, é necessário que a empresa informe ao titular sobre as razões do uso das informações e peça seu consentimento para isso. Esse processo garante transparência, pois o usuário ficará sabendo qual será o destino dos dados.

Desta forma, a empresa deve publicar no site um aviso informando ao visitante que as informações coletadas podem ser usadas e de que maneira isso pode ocorrer. Além disso, a autorização deve ser confirmada com uma solução mais confiável do que um botão de “ok” ou de “Aceito”.

Algumas soluções que usam criptografia garantem o sigilo de quem é o titular dos dados, como a assinatura digital, que tem valor jurídico, ou o carimbo do tempo, que deixa registrado o momento exato que o usuário permitiu o uso dos dados.

2.3.4 Configuração de sistemas internos

Todos os sistemas internos devem ser configurados para a proteção das informações evitando ataques externos de hackers. Um banco de dados com acesso restrito e com medidas para reforçar sua inviolabilidade é essencial. E, caso ocorra algum vazamento, mecanismos de segurança devem impedir a leitura destas informações, evitando o uso indevido delas.

2.3.5 LGPD deve ser levada a sério

Se utilizado de maneira correta as tecnologias e as medidas de segurança, ainda sim é necessário que toda a organização trate como prioridade a proteção dos dados dos usuários. Deve fazer parte da cultura da empresa o respeito às políticas de segurança para evitar que o mau uso de informações prejudique todo o negócio.

A lei, se implementada e executada de maneira correta pelas empresas, traz benefícios ímpares, os quais é possível destacar: organização e otimização dos dados coletados e armazenados; construção de relações mais transparentes com o cliente; valorização da segurança cibernética, entre outros.

Segundo Fabiana Rosa (2021), “a melhor forma para a empresa verificar se o tratamento está adequado tanto às exigências da LGPD quanto do GDPR, é através da análise de conformidade com os princípios norteadores” já citados anteriormente.

Podemos compreender que esses princípios significam que o tratamento de dados está de acordo com às finalidades exigidas, devendo ser coletados somente os dados minimamente necessários para o alcance da finalidade a que se destinam, em estrita adequação com a informação e consentimento do titular, a quem é conferido o livre acesso aos seus dados, que deverão ser atualizados para manutenção da qualidade e exatidão, devendo a empresa que trata os dados tomar as medidas adequadas e suficientes para garantir a segurança desses dados.

Assim, verificamos que o consentimento da pessoa natural titular do dado é um ponto central da lei. Portanto, as empresas somente estarão autorizadas a utilizar os dados de seus clientes, por exemplo, para envio de promoção, divulgação de produtos e outros contatos, se tiverem o consentimento prévio do titular.

2.3.6 Incidente com dados pessoais e plano de resposta a incidentes

Ao ter ciência sobre qualquer incidente com dados, é preciso comunicar imediatamente o Comitê de Privacidade (ou qualquer outra equipe correspondente) e o Encarregado pelo Tratamento de Dados Pessoais (DPO), que deverão acionar o Departamento de Tecnologia da Informação e o Departamento Jurídico. O colaborador deve seguir as orientações dos responsáveis, pois a adoção de medidas por conta própria pode agravar o problema ou danificar evidências do Incidente com Dados Pessoais.

Em caso de descumprimento da LGPD e de infrações comprovadas, com dados pessoais ou dados pessoais sensíveis, podem ocorrer as sanções administrativas já citadas anteriormente. Por esses motivos é primordial ter uma equipe multidisciplinar, com objetivos e prazos bem definidos, a fim de realizar a adequação à lei e evitar prejuízos futuros e vazamento de dados.

O processo não é simples e as multas por não atendimento à regulamentação são milionárias, demandando uma enorme responsabilidade para os envolvidos. Por outro lado, a implementação da nova lei, embora de difícil concretude, pode gerar grandes frutos para as organizações e a sociedade como um todo.

3 CONCLUSÃO

Ante o exposto, fica claro que a lei 13.709/18 é de extrema necessidade na Era digital, a mesma uniu diversas normas que fiscalizavam e determinavam as práticas que empresas públicas e privadas deveriam seguir na coleta, utilização e armazenamento de dados em uma só, se tornando a principal legislação sobre o assunto atualmente.

Sendo o sigilo dos dados pessoais matéria prima valiosa, a LGPD atende, também, aos direitos constitucionais de privacidade, intimidade, honra e imagem, e somente pode ser quebrado mediante ordem judicial. O ideal é que as empresas invistam em uma tecnologia que atenda aos requisitos da nova lei, e as organizações que capturarem dados sem base legal, protegendo de forma inadequada as informações de seus clientes e levando

ao possível vazamento das mesmas devam sofrer a aplicação de uma sanção por descumprimento pela ANPD prevista por lei.

Dito isso, é importante lembrar que a Autoridade Nacional poderá aplicar: advertência, com prazo determinado para correção de possíveis erros; multa simples, limitada no total de R\$ 50.000.000,00 (cinquenta milhões de reais) por infração; multa diária, entre outras.

Por fim, a LGPD mostra sua importância no dia a dia de maneira sutil e ímpar, desde a criação de um sistema complexo a confirmação de informação do titular. As empresas devem buscar se adequar as exigências estabelecidas até o prazo determinado, a fim de se ajustarem o quanto antes, pois no caminho do conhecimento e da informação, não há lacunas ou brechas quando se trata de dados pessoais.

REFERÊNCIAS

ALISTE, Mario Bruno. GOVERNO DO BRASIL. Big Data e LGPD: do impacto negativo ao positivo. Disponível em: <<https://www.serpro.gov.br/lgpd/noticias/2019/lgpd-bid-data-grande-volume-dados-impactos>>. Acesso em: 30 abr. 2021.

BAGNOLI, Vicente. Direito econômico e concorrencial. 7. ed.rev., atual e ampli. São Paulo: Editora Revista dos Tribunais, 2017.

BAGNOLI, Vicente. The big data relevant market. Concorrenza e Mercato. Vol. 23/2016. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3064792>. Acesso em 05 maio. 2021.

BRASIL. Lei 13.709, de 14 de agosto de 2018. Diário oficial da União: seção 1, Brasília, DF, edição 157, p. 59, 15 set. 2018,

CERVANTES, Vinicius; RODRIGUES, David Fernando. Big Data e proteção de dados: o desafio está lançado, 2019. Disponível em: <<http://www.direitorp.usp.br/wp-content/uploads/2019/06/Inovacao-BigData-Cervantes-Rodrigues.pdf>>. Acesso em 30 abr. 2021.

GOVERNO DO BRASIL. O que é a Lei Geral de Proteção de Dados Pessoais? Dê um "giro" pela lei e conheça desde já as principais transformações que ela traz para o país. Disponível em:

<<https://www.serpro.gov.br/lgpd/menu/a-lgpd/o-que-muda-com-a-lgpd>>. Acesso em: 19 abr. 2021.

INSIGHT. A LGPD (Lei Geral de Proteção de Dados) e seu impacto no Big Data, 2020. Disponível em: [https://insightlab.ufc.br/a-lgpd-lei-geral-de-protecao-de-dados-e-seu-impacto-no-big-data/#:~:text=Dados%20LGPD%20Seguran%C3%A7a-,A%20LGPD%20\(Lei%20Geral%20de%20Prote%C3%A7%C3%A3o%20de%20Dados\)%20e,seu%20impacto%20no%20Big%20Data&text=No%20%C3%BAltimo%20dia%2018%20de,dados%20dos%20usu%C3%A1rios%20pelas%20corporac%C3%A7%C3%B5es..](https://insightlab.ufc.br/a-lgpd-lei-geral-de-protecao-de-dados-e-seu-impacto-no-big-data/#:~:text=Dados%20LGPD%20Seguran%C3%A7a-,A%20LGPD%20(Lei%20Geral%20de%20Prote%C3%A7%C3%A3o%20de%20Dados)%20e,seu%20impacto%20no%20Big%20Data&text=No%20%C3%BAltimo%20dia%2018%20de,dados%20dos%20usu%C3%A1rios%20pelas%20corporac%C3%A7%C3%B5es..) Acesso em: 30 abr. 2021.

KALYVAS, James R.; OVERLY, Michael R. Big data: a business and legal guide. Nova Iorque: 2015.

LGPD. O que a empresa deve fazer? Disponível em: <<https://www.lgpdbrasil.com.br/o-que-a-empresa-deve-fazer/>>. Acesso em 21 abr. 2021.

LGPD. O que muda com a nova lei de dados pessoais. Disponível em: <<https://www.lgpdbrasil.com.br/o-que-a-empresa-deve-fazer/>>. Acesso em: 21 abr. 2021.

NONES, Fernanda. Resultados Digitais. LGPD: o que diz a nova lei brasileira de proteção de dados e como ela pode impactar a estratégia de marketing de sua empresa, 2020. Disponível em: <<https://resultadosdigitais.com.br/blog/o-que-e-lgpd/>>. Acesso em 29 abr. 2021.

ROSA, Fabiana. Diário do Comércio. O que sua empresa precisa saber sobre a LGPD, 2021. Disponível em: <<https://diariodocomercio.com.br/opinia/o-que-sua-empresa-precisa-saber-sobre-a-lgpd>>. Acesso em 30 abr. 2021.

Sobre o(s) autor(es)

Andressa Maria Neumann Dias. Formanda em direito pela Universidade do Oeste de Santa Catarina - UNOESC, campus São Miguel do Oeste. Email: andressamneumann@gmail.com

Raiana Caberlon Duarte. Formanda em direito pela Universidade do Oeste de Santa Catarina - UNOESC, campus São Miguel do Oeste. Email: raicaberlon@hotmail.com