Insper

LL.M. Direito dos Contratos

Paula de Castro Ferraz

Aplicabilidade da Lei n.º 13.709/2018 nos Contratos de Prestação de Serviços

São Paulo

2019

Paula de Castro Ferraz

Aplicabilidade da Lei n.º 13.709/2018 nos Contratos de Prestação de Serviços

Trabalho de Conclusão de Curso, apresentado ao programa LLM Direito dos Contratos como requisito parcial à obtenção do título de pós-graduada em Contratos.

Orientadora: Professora Mestre Maria Isabel Carvalho Sica Longhi

São Paulo

2019

Dedico o presente artigo acadêmico aos meus incansáveis incentivadores: Paulo A. Ferraz Filho e Mayra Cruz Domingues.

RESUMO

O presente trabalho acadêmico trata de um estudo a respeito aplicabilidade da Lei n.º 13.709/2018 nos Contratos de Prestação de Serviços. Abordando as especificidades da Lei Geral de Proteção de Dados brasileira nas relações comerciais entre Operador e Controlador no tratamento de dados pessoais e demonstra a responsabilização das partes dentro do âmbito dos contratos de prestação de serviços frente à Autoridade Nacional de Proteção de dados e os próprios titulares de dados, além das demais peculiaridades que envolvem a nova legislação e os direitos envolvidos. Utilizando o método de pesquisa dedutiva e comparativa, e concluindo que há possibilidade de realizar o tratamento de dados pessoais nas prestações de serviços desde que seja dentro dos limites estabelecidos na referida Lei, bem como, poderá ocorrer a responsabilidade solidária entre os agentes de tratamento, assim como a reparação dos danos aos titulares que eventualmente sejam lesionados devido à eventual conduta indevida dos agentes de tratamento.

Palavras-chave: Proteção de Dados, Lei Geral de Proteção de Dados; Privacidade; Responsabilização do Controlador e Operador sobre o tratamento de dados; Titulares de Dados; Responsabilidade Solidaria do Operador e Controlador.

ABSTRACT

This academic work deals with a study about the applicability of Law 13.709/2018 in Service Agreements. It addresses the specificities of the Brazilian General Data Protection Law in the commercial relations between Operator and Controller in the processing of personal data and demonstrates the responsibility of the parties within the scope of service contracts with the National Data Protection Authority and the owners of data, in addition to the other peculiarities that involve the new legislation and the rights involved. The work uses a deductive and comparative research method and concludes that it is possible to carry out the processing of personal data in Service Agreements provided it is within the limits established in the mentioned Law. Also, joint liability may occur between the treatment agents, as well as compensation for damage to holders who may be injured due to undue conduct of treatment agents.

Keywords: Protection of Data; Brazilian General Data Protection Law; Privacy, Liability of the controller and the processor under this regulation, Joint liability of controller and processor.

Lista de Siglas

ANPD – Autoridade Nacional de Proteção de Dados

GDPR – *General Data Protection Regulation*

LGPD – Lei Geral de Proteção de Dados

PL – Projeto de Lei

Sumário

1. INTRODUÇÃO AO TEMA

O presente trabalho abordará a respeito da recém sancionada Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados e a Medida Provisória 869/2018, que ainda está tramitando para aprovação e propõe 176 (cento e setenta e seis) emendas a Lei em comento, aplicadas aos Contratos de Prestação de Serviços celebrados entre Pessoas Jurídicas.

Antecipadamente é importante destacar que até o momento da conclusão do presente trabalho acadêmico, a referida Medida Provisória não havia sido aprovada e que a sua aprovação, modificação ou reprovação podem impactar de maneira significante o conteúdo ora exposto.

A Lei Geral de Proteção de Dados apenas passará a produzir efeitos no mês de agosto de 2020 e possui o intuito de regulamentar a forma como as organizações no Brasil deverão coletar e tratar os dados pessoais (assim definidos como informação relacionada à pessoa natural identificada ou identificável).

Acredita-se que a Lei geral de Proteção de dados tem a missão de corrigir a defasagem do país com relação ao tema e chega em um momento social crítico, no qual são frequentes as notícias envolvendo casos de vazamento de dados pessoais, tratamentos sem consentimento, coleta de dados feitas de formas excessivas e aleatórias, ameaçando a privacidade de forma discreta mas o suficiente para causar danos e expor indevidamente as pessoas.

A legislação nova terá o papel de regulamentar todo o fluxo de tratativas necessárias para a coleta e armazenamento de dados e assim garantir a privacidade de seus titulares.

Apesar de o Brasil ter tido outras Leis que protegem indiretamente os dados pessoais, como o Marco Civil da Internet (12.965/2011) e a Lei de Acesso a Informação (Lei 12.527/2011), o assunto é novo e a Lei 13.709/2018 veio com o intuito

de elucidar e preencher lacunas contidas na legislação brasileira a respeito do tema. A LGPD foi criada com base na legislação Europeia, que é a referência no que tange a privacidade de dados.

Com relação a aplicabilidade da referida Lei nas cláusulas contratuais dos contratos de prestação de serviços entre pessoas jurídicas, onde o foco presente trabalho acadêmico está direcionado, a problemática estará envolvida nas relação entre Controlador e Operador, nas obrigações entre as partes e nas cláusulas a serem incluídas para observância da referida Lei, bem como, a proteção das informações pessoais que possam vir a ser coletadas em decorrência da prestação de serviços.

Conforme exposto acima, apesar da amplitude trazida pela Lei Geral de Proteção de dados, o foco do trabalho acadêmico se dará nas relações contratuais de prestação e serviços entre empresas privadas. Sobre quais serão as formas de exigir contratualmente que a outra parte do Contrato possa adimplir com as obrigações legais e não expor os dados que venha a ter acesso em decorrência da relação comercial que será avençada. Como realizar o gerenciamento dessas informações pessoais expostas a prestação de serviços e inclusive responsabilizar por eventual falha na gestão das informações obtidas e por inadimplemento contratual.

2. A PROTEÇÃO DE DADOS

2.1 Privacidade e Dados Pessoais

A privacidade está diretamente relacionada ao campo mais íntimo do ser humano. Desde os próprios pensamentos, as atividades de seu cotidiano e escolhas que tenha feito pessoal e profissionalmente. O nome, a imagem a reputação são apenas a extensão de todo esse rol de itens que envolve o universo do ser humano.

Muito antes de qualquer Lei abordar a temática, sempre foi comum que os indivíduos se preocupassem com a sua privacidade, desde fotos, senhas de banco, números de documentos, histórico de doenças, etc.

A Privacidade passou a constar na Declaração Universal de Direitos Humanos de 1948.[1]

> Art XII – Ninguém será sujeito à interferência em sua vida privada, em sua família, em seu lar ou em sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da Lei contra tais interferências ou ataques.

A Constituição Federal de 1988 traz em seu Artigo 5º, inciso X, também menção a cerca da intimidade e vida privada, vejamos:

> C.F. Art. 5º, inciso X - São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação.2

Com o advento da internet, a privacidade tornou-se mais exposta. Se no passado para localizarmos o telefone de uma pessoa era necessário mexer em enormes listas telefônicas, atualmente basta pesquisar o nome e sobrenome nos sites de busca e os resultados já trazem informações o suficiente a respeito de um indivíduo, não só para localiza-lo, mas também que envolvem questões íntimas como fotos de família, “posts” em redes sociais, preferências políticas, etc.

É claro que grande parte dessas informações são divulgadas pelos próprios indivíduos, mas talvez muitas pessoas não tenham a dimensão da exposição de suas informações. Muito embora esse tipo de exposição se dê por conta da falta de conhecimento das pessoas ou mesmo da ausência de leitura dos termos de uso de como por exemplo os de sites e redes sociais, atualmente o que se tem constatado é a utilização desses dados para rastrear preferências de consumo dos usuários. Isso quer dizer, que as informações acabam sento utilizadas para que as empresas tracem perfis de consumo e também para que façam propagandas direcionadas a esse público em específico, o que não seria um problema, se as pessoas titulares dos dados de fato tivessem ciência de que seus dados estão sendo utilizados para tal finalidade.

---

[1] UNIC. **Declaração Universal de Direitos Humanos**. 2009, Disponível em: https://nacoesunidas.org/wp-content/uploads/2018/10/DUDH.pdf>. Acesso em: 07 mai.2019

A Lei Geral de Proteção de Dados veio com o intuito de trazer equilíbrio para a era da informatização, onde tudo se localiza a respeito de alguém. Uma legislação baseada na nova Lei Europeia, onde as questões de privacidade já são tratadas de forma mais madura que no Brasil, certamente irá contribuir para mudar a perspectiva das empresas ao tratarem os dados e dos titulares de dados a respeito de seus direitos.[3] [4]

A LGPD conceitua dado pessoal como Informação relacionada a pessoa natural identificada ou identificável. Sendo ainda, dado pessoal sensível aquele que está relacionado a personalidade do indivíduo.

Vejamos o texto da Lei:

> LGPD. Art. 5º Para os fins desta Lei, considera-se:
>
> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
>
> II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

A diferença no conceito dos dados pessoais é relevante para determinar as regras de tratamento de dados.

> Os dados sensíveis são aqueles que podem gerar discriminação caso se tornem públicos. Trata-se, por exemplo, de dados que informem a orientação sexual, ideológica, política, religiosa ou a raça de um indivíduo. Dados relativos à saúde, vida sexual, assim como dados genéticos ou biométricos, também são considerados sensíveis. Uma lei de proteção de dados pessoais deve criar um regime de tratamento diferenciado a esses dados, requerendo o consentimento expresso para o seu tratamento, pois seu vazamento pode gerar graves consequências aos titulares e pessoas próximas, podendo, inclusive, causar restrições ao exercício da liberdade de expressão (um exemplo seria quando alguém não declara sua religião ou orientação sexual com medo de sofrer represálias). [5]

---

[3] GISELE TRUZZI. **Privacidade e Proteção de Dados Pessoais**. 2017, Disponível em: <https://www.academia.edu/34223006/PRIVACIDADE_E_PROTEÇÃO_DE_DADOS_PESSOAIS>. Acesso em: 09 mai. 2019.

[4] FREDERICO MEINBERG CEROY. **Dados pessoais sensíveis**: Três projetos de lei que tramitam no Congresso Nacional abordam o tema. 2017, Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/dados-pessoais-sensiveis-29112017> Acesso em: 11 mai. 2019.

[5] ARTIGO 19. **Proteção de dados pessoais no Brasil**: Análise dos projetos de lei em tramitação no Congresso Nacional. 2016, Disponível em: < https://artigo19.org/wp-content/blogs.dir/24/files/2017/01/Proteção-de-Dados-Pessoais-no-Brasil-ARTIGO-19.pdf >. Acesso em: 13 mai. 2019.

A Lei Geral de Proteção de Dados visa proteger quaisquer informações (dados) relacionadas aos indivíduos, especificadamente pessoas físicas, de modo que essas informações de forma isolada ou em conjunto possam identificá-lo. Fazer a distinção entre Dados Pessoais e Dados Pessoais Sensíveis foi um ponto muito relevante da nova legislação e torna possível demarcar o limite de atuação do Controlador, pois sem essa divisão, o conceito de Dado pessoal tornar-se-ia amplo e difícil de controlar pela ANPD.

2.2 Breve Histórico de Proteção de dados no Brasil

No Brasil, antes da Lei n.º 13.709/2018, a atual Lei Geral de Proteção de Dados, houve três projetos de Lei que versavam de certa forma a respeito do tem a que a antecederam, quais sejam:

O Projeto de Lei n.º 4060/2012, Projeto de Lei 330/2013 e o Projeto de Lei 5276/2016.

Em análise comparativa dos três projetos, especificamente a respeito dos tópicos “Proteção de Dados Sensíveis”, “Graus de Consentimento” e “Adoção de Medidas de Segurança Pública para manuseio de dados”, verifica-se que, no primeiro Projeto de Lei (PL 4060/2012) o Conceito de Proteção de Dados Sensíveis era incompleto, fazendo apenas duas menções em seu Artigo 11, parágrafo único, que prevê da seguinte forma: "proporcionais ao atual estado da tecnologia, à natureza dos dados e às características específicas do tratamento, em particular no caso do tratamento de dados sensíveis.”[6] [7]

Sem aprofundar no que de fato seria a natureza dos dados e as referidas características específicas de tratamento.

Com relação aos Graus de Consentimento pode-se considerar como um tema ausente, embora em seu artigo 12, o mesmo Projeto de Lei refere-se ao tratamento

---

[6] Idem ao 5

[7] RENATO LEITE MONTEIRO. **A (i)legalidade de sites que divulgam dados pessoais**. 2015. Disponível em: < https://renatoleitemonteiro.jusbrasil.com.br/artigos/191596216/a-i-legalidade-de-sites-que-divulgam-dados-pessoais>. Acesso em: 13 mai.2019.

de dados sensíveis, mencionando ainda que a autorização do titular para esse tipo de tratamento se dê por qualquer meio que permita a manifestação de sua vontade, não se aprofundou em explanar a respeito.

A respeito da Adoção de Medidas de Segurança Pública para manuseio de Dados Pessoais o texto do Projeto de Lei é incompleto pois não possui seção específica para tratar o tema de segurança dos dados. Se limitando somente a instruir que sejam adotadas medidas tecnológicas para reduzir ao máximo o risco da destruição, perda e o acesso não autorizado ou tratamento não permitido pelo titular. Não é mencionado a prevenção e as possibilidades de verificações periódicas dos tratamentos de dados ou mesmo as garantias de acesso.

Com relação ao Projeto de Lei PLS 330/2013, os itens de "Proteção de Dados Sensíveis", "Graus de Consentimento" e "Adoção de medidas de Segurança Pública para Manuseio de Dados Pessoais" começaram a tomar forma e se assemelharem com o que hoje é a Nova Lei Geral de Proteção de Dados.

A respeito da Proteção de Dados Sensíveis o Projeto em questão (PLS 330/2013) proíbe o tratamento de dados pessoais sensíveis e estabelece sete exceções possíveis para a referida regra.

> O projeto 330/2013, em seu artigo 4, inciso V, prevê que um dos princípios para o tratamento de dados é o consentimento livre, específico, inequívoco e informado do titular dos dados — em se tratando de dados sensíveis, o consentimento deve ser ainda mais prévio e expresso. O artigo 6, inciso IV, reforça esse princípio e requer que a concordância deva se dar de maneira destacada. [8]

Posteriormente, houve o Projeto de Lei n.º 53/2018 que originou a nova Lei Geral de Proteção de Dados, qual seja: Lei 13.709 de 14 de agosto de 2018.

[8] ARTIGO 19. **Proteção de dados pessoais no Brasil**: Análise dos projetos de lei em tramitação no Congresso Nacional. 2016, Disponível em: < https://artigo19.org/wp-content/blogs.dir/24/files/2017/01/Proteção-de-Dados-Pessoais-no-Brasil-ARTIGO-19.pdf >. Acesso em: 13 mai. 2019.

2.3 Breve Comparativo da Lei Geral de Proteção de Dados vs *General Data Protection Regulation*

A *General Data Protection Regulation* (GDPR) é uma regulamentação que se consolidou para reunir privacidade e proteção de dados em vinte e oito países (união europeia), aplicada ao processamento de dados no contexto de um estabelecimento da Europa, independentemente do local de processamento (podendo ser proveniente de outros países).

Visa proteger os dados de indivíduos localizados na União Europeia, especialmente quando se oferece serviços e produtos a indivíduos da mesma região. Assim como, tem por objetivo monitorar o comportamento de indivíduos situados em um dos países da União Europeia. Não se aplicando a questões relativas a segurança pública, para uso pessoal das informações ou para casos relativos a investigação criminal.

Enquanto a Lei Geral de Proteção de Dados (LGPD) é aplicada apenas ao Brasil e referente a coleta e tratamento de dados pessoais dos indivíduos localizados no território nacional e se refere aos serviços e bens ofertados para indivíduos no Brasil.

A LGPD não se aplica aos dados vindos ou destinados a outros países que passem pelo Brasil apenas em estado transitório, também não é objeto da referida Lei o uso pessoal dos dados ou sua utilização para fins não comerciais, fins jornalísticos, artísticos, acadêmicos e relativos a segurança pública.[9]

A GDPR em seu Artigo 1º normatiza a respeito dos direitos e liberdades fundamentais das pessoas singulares e de seu respectivo direito a proteção dos dados pessoais.

Já a LGPD em seus artigos 1º e 2º indica que protege os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa

[9] JOSÉ BELO. **GDPR E LGPD:** Comparativo Parte I. Arquivo recebido por mensagem de e-mail por belsica@gmail.com em 16 abri 2019. Informação pessoal.

natural. E tem como princípio o respeito à privacidade, a autoderminação informativa, liberdade de expressão, informação, comunicação e opinião, inviolabilidade da intimidade, da honra e da imagem.[10]

No que tange a sua aplicação, a GDPR em seu Artigo 3º se refere ao tratamento de dados pessoais realizado na circunstância das atividades comerciais de um responsável pelo tratamento ou de um subcontratante que esteja situado no território da União Europeia, tendo como requisito que os bens ou serviços tenham sido ofertados aos titulares dos dados dentro de um dos países que integram a União e independentemente de o tratamento vier a ocorrer dentro ou fora de um desses 28 países.[11] [12]

Na LGPD, também em seu artigo 3º indica que a aplicação será a qualquer operação de tratamento de dados que tenha sido realizada por pessoa natural ou jurídica (de direito privado ou público), sendo irrelevante qual o país que fica sediada ou onde os dados estejam localizados, desde que a coleta ou operação de tratamento de dados seja realizada no território brasileiro, que a atividade de tratamento tenha por objetivo ofertar ou fornecer bens ou serviços ou que o tratamento de dados seja de indivíduos localizados no território nacional.[13] [14]

O Artigo 3º da LGPD prescreve nesse sentido:

> Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:
>
> I - a operação de tratamento seja realizada no território nacional;

---

[10] CAIO CESAR CARVALHO LIMA e RONY VAINZOF. **Sancionada a Lei Geral Brasileira de Proteção de Dados (LGPD): e agora?:** Autoridade (ANPD) será criada por meio de Projeto de Lei de iniciativa do Executivo, diante do veto parcial apresentado por Temer. 2018, Disponível em: <https://www.jota.info/paywall?redirect_to=//www.jota.info/opiniao-e-analise/colunas/direito-digital/sancionada-a-lei-geral-brasileira-de-protecao-de-dados-lgpd-e-agora-14082018>.Acesso em: 15 mai.2019.

[11] JOSÉ BELO. **GDPR E LGPD:** Comparativo Parte I. Arquivo recebido por mensagem de e-mail por belsica@gmail.com em 16 abri 2019. Informação pessoal.

[12] RAFAEL ALMEIDA DE OLIVEIRA REIS. **O QUE MUDA COM A NOVA LEI GERAL DE PROTEÇÃO DE DADOS?** 2018, Disponível em: < https://novojurista.com/2018/08/19/o-que-muda-com-a-nova-lei-geral-de-protecao-de-dados/>.Acesso em: 15 mai.2019

[13] Idem ao 8

> II - 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; ou (Redação dada pela Medida Provisória nº 869, de 2018)
>
> III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.
>
> § 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.
>
> § 2º Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do caput do art. 4º desta Lei.

Dessa forma, pode-se concluir que a diferença relativa a aplicação do tratamento de dados ter ocorrido ou não dentro do território é um fator de divergência entre as duas legislações, já que para a GDPR é indiferente o local de tratamento (desde que ofertados na União Europeia) e na LGPD o local de tratamento deve ser no território nacional ou que esteja vinculado a oferta ou fornecimento de bens ou serviços no país e ainda, caso o tratamento de dados seja de indivíduos localizados no território brasileiro.

Com relação as Bases Legais para tratamento de Dados pessoais existem semelhanças entre as bases legais da LGPD e da GDPR, as semelhantes são: Consentimento, execução de Contrato, cumprimento de obrigação, interesse legítimo, processos (judiciais, administrativos e arbitrais), saúde (sendo que para esse caso a Lei brasileira é mais abrangente), Pesquisas e Estudo, Interesse público, Pela Autoridade pública ou em seu benefício (sendo que para a LGPD determina que deve ser feito pela Administração publica para execução de políticas públicas previstas em Leis) e para proteção de Crédito.[15] [16]

Com relação aos Dados pessoais sensíveis as bases em comum para ambas as legislações são: Consentimento, Cumprimento de Obrigação Legal, Processo

---

[15] MACHADO, MEYER, SENDACZ E OPICE ADVOGADOS. **LEI 13.709/2018:** Lei Geral de Proteção de Dados
2018, Disponível em: <https://www.machadomeyer.com.br/images/publicacoes/PDFs/Lei_Protecao_de_Dados_ebook_18.pdf>. Acesso em: 29 mai. 2019.

[16] RONALDO LEMOS, DANIEL DOUEK, NATALIA LANGENEGGER, OLIVIA BONAN COSTA, PHILIPPE SUNDFELD e RAMON ALBERTO DOS SANTOS. **GDPR: a nova legislação de proteção de dados pessoais da Europa:**
O que mudará no ambiente de negócios internacional? E quais os efeitos sobre cidadãos e entidades brasileiras? 2018, Disponível em: < https://www.jota.info/opiniao-e-analise/artigos/gdpr-dados-pessoais-europa-25052018>. Acesso em: 30 mai. 2019.

judicial ou administrativo, Saúde, pesquisa e estudo, interesse público, pela autoridade pública.

Para fins de execução de Contrato e Prevenção a fraude, a GDPR não menciona a respeito, apenas a LGPD consta previsão direta.

Já para associações de cunho político, filosófico, religioso ou sindicatos e dados manifestamente colocados em público, apenas a GDPR possui previsão em suas bases legais.

Tanto a LGPD quanto a GDPR não possuem Proteção ao crédito como uma base legal para tratamento de dados pessoais sensíveis.[17]

3. COLETA E TRATAMENTO DE DADOS NA PRESTAÇÃO DE SERVIÇOS

3.1 A Coleta de dados de forma proporcional: Necessidade e Finalidade.

No Brasil é muito comum os dados pessoais serem solicitados em situações cotidianas que não apresentam necessidade.

Muitas vezes ao efetuar uma simples compra em uma loja já é solicitado um cadastro, onde o Cliente pessoa física informa além de nome e CPF, dados como endereço, profissão, dentre outros. É nítido que o endereço residencial e profissão por exemplo, não são itens necessários para a compra de uma peça de roupa, mas ainda assim, com frequência são solicitados.

Onde serão armazenados esses dados posteriormente? Quem terá acesso? São perguntas que se os consumidores (titulares de dados) ao questionarem a loja no momento do cadastro, certamente não terão a resposta.

Ainda que no exemplo supramencionado tenha ocorrido o consentimento do consumidor ao informar seus dados, é visível que em uma estrutura menor não seria

[17] Idem ao 13

possível trazer a rastreabilidade necessária com relação a consultas e exclusões futuras dos dados pessoais coletados.

No entanto, o ponto aqui não se trata especificamente do consentimento por ora, mas sim dos fatores necessidade e finalidade. Ao realizar compras simples não são necessários tantos dados, assim como a depender da atividade realizada pelo Controlador e da interação com o titular de dados talvez não seja necessário coletar dado algum. Transpondo a questão para uma estrutura maior e complexa, pode-se perceber que até mesmo dentro de grandes empresas os dados coletados de seus consumidores são quase sempre maior do que o necessário.

É muito comum o tipo de fraude de dados em cartões de créditos vinculados à lojas de departamento, onde alguém mal intencionado coletou os dados básicos de cadastro de uma pessoa e de forma fraudulenta, passou-se por essa pessoa utilizando seus dados para obter um cartão, e o titular dos dados é surpreendido com a chegada da fatura em seu endereço residencial sem que sequer tenha feito qualquer compra. Isso é um exemplo comum do vazamento de dados pessoais. Sem mencionar o despreparo da financeira responsável pelo cartão que não fez a checagem correta e é inegável sua responsabilidade pelo ocorrido, mas centrando no fato de que a pessoa que cometeu a fraude, teria tido maior dificuldade em fazê-la caso não tivesse os dados pessoais da vítima. E isso é apenas um dos milhares de exemplos possíveis de fraudes que ocorrem com os vazamentos de dados.

Maximizando a questão e pensando nas atividades econômicas de outras empresas, é comum o pensamento de armazenar o máximo de dados possíveis, para caso seja necessário, mas sem pensar no que de fato é necessário e para qual finalidade.

A LGPD traz princípios para o tratamento de dados pessoais em seu Artigo 6º e em seus incisos I, II e III traz a conceituação de Finalidade e Necessidade perante a Lei:

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
>
> I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

> II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
>
> III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

No Projeto de Lei (PL 53/2018) que precede a Lei Geral de Proteção de Dados, constava em seu artigo 9, §3º de forma mais expressa "É vedada a exigência de dados pessoais que não decorra de propósitos legítimos do controlador e que não seja estritamente necessária ao cumprimento das obrigações estabelecidas em relação ao Titular".

Dessa forma, percebemos que a LGPD vira a trazer uma mudança estrutural e que até mesmo fornecedores que não tratam dados diretamente, como lojas de shopping, por exemplo, necessitarão adequar-se e atentar-se a finalidade da coleta de dados que pretendem realizar de forma que não excedam a necessidade e façam o tratamento somente dos dados que forem de fato necessário, obedecendo à LGPD em especial com relação as bases legais para tratamento de dados.

3.2 Bases legais para tratamento de dados na prestação de serviços

A Lei Geral de Proteção de Dados estabelece dez requisitos taxativos para que seja realizado o tratamento de dados pessoais no Brasil. Requisitos esses elencados no Artigo 7º.

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
>
> I - mediante o fornecimento de consentimento pelo titular;
>
> II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
>
> III - 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, observadas as disposições do Capítulo IV desta Lei;
>
> IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

> V - 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;
>
> VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;
>
> VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;
>
> VIII - para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;
>
> IX - 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; ou
>
> X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

A razão de uma empresa realizar a coleta ou o tratamento de dados pessoais necessita estar relacionada com ao menos um dos critérios (bases legais) supracitados.

Dessas dez bases, cinco delas possuem relação com as atividades realizadas pelas Pessoas Jurídicas de Direito Privados e, portanto, são aplicáveis à Prestação de Serviços. São elas: O consentimento (Inciso I); o cumprimento de obrigação legal ou regulatória (Inciso II); execução de contrato (Inciso V), o legítimo interesse (Inciso IX) e a proteção do crédito (Inciso X).

a) Consentimento

A respeito da primeira base legal, qual seja, o consentimento, sem dúvida é a base legal que mais traz polêmica, isso porque está diretamente relacionada ao portador dos dados pessoais e porque traz a ele possibilidades de agir mediante as atividades empresariais que estejam sendo realizadas com seus dados, desde que seja cabível.

A LGPD traz em seu Artigo 5º, inciso XII a definição de consentimento como a “manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.".

Dessa forma, a própria Lei já determina o que é necessário para considerar o Consentimento como válido. E deve ser de fato manifestado pelo Titular de dados, no sentido de não haver vício, ou seja, que não tenha sido compelido a consentir a coleta

de seus dados. Que seja informado, no sentido de expressamente ter comunicado a sua vontade e inequívoco no sentido de não conter vícios e ser passível de obter provas a respeito de sua ação em consentir. (Ainda não publicado)[18]

A Lei Geral de Proteção de Dados, em seu Artigo 8º menciona especificamente a respeito do Consentimento.

> Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.
>
> § 1º Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais.
>
> § 2º Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei.
>
> § 3º É vedado o tratamento de dados pessoais mediante vício de consentimento.
>
> § 4º O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas.
>
> § 5º O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei.

b) Cumprimento de obrigação legal ou regulatória pelo controlador

A segunda base legal prevista no Artigo 7º da Lei 13.709/2018 trata a respeito do cumprimento de obrigação legal ou regulatória pelo controlador.

Dessa forma, quando a coleta de dados for justificada nessa base legal, será necessário comprovar que de fato há uma obrigação legal ou regulatória da qual o controlador deva cumprir e que esteja associada a coleta de dados pessoais que eventualmente esteja realizando.

No entanto, a coleta deve estar limitada ao que a regulação exige, não podendo ultrapassar seus limites, é o que explica o Professor Marcel Leonardi (Ainda não publicado):

---

[18] MARCEL LEONARDI. **Artigo Principais bases legais de tratamento de dados pessoais no setor privado a ser publicado no livro Direito e Internet IV.** Mensagem recebida por marcel.leonardi@gmail.com em 07 mai. 2019 (Ainda não publicado)

> Isso porque o tratamento de diversos dados pessoais realizado por certos setores da economia é imposto por leis ou regulamentos, particularmente em setores regulados como o financeiro, de saúde suplementar.
>
> Evidentemente, cada controlador deve conhecer as obrigações legais ou regulatórias aplicáveis à sua atividade que exigem o tratamento de dados pessoais. Nesses casos, as normas dessa natureza consistem em obrigações legais e regulatórias que justificam o tratamento de dados pessoais com base no artigo 7º, inciso II, da Lei 13.709/18, observado que o tratamento, nessa hipótese, é limitado à finalidade dessas normas.
>
> Ou seja: ainda que o tratamento de dados pessoais baseado em obrigação legal ou regulatória não exija que leis ou regulamentos imponham diretamente uma atividade específica de tratamento, a finalidade do tratamento realizado nessa hipótese é justamente o cumprimento da obrigação legal ou regulatória prevista nessas normas, não podendo exceder essa finalidade.[19]

Trazendo esse contexto para o foco do presente trabalho, que é a tratativa dos dados pessoais no cenário da contratação de serviços, é importante destacar que caso o fornecedor pretendido seja integrante de um setor regulado, que esteja sujeito ao atendimento de Leis ou regulamentos específicos ou ainda, caso o Controlador quem seja parte integrante desse cenário, as informações devem ter como base legal esse dispositivo.

Situações como contratação de serviços bancários ou de terceirização de etapas de departamento pessoal de uma empresa, são questões que devem atender a legislações específicas e que determinam o armazenamento de um rol de informações já definido e que não poderiam o Controlador ou o Operador omitir-se em relação a essas determinações.

c) Execução de contrato ou de procedimentos preliminares

A Lei Geral de Proteção de dados, em seu Artigo 7º, inciso V determina como uma base legal para o tratamento de dados a execução de contrato ou de procedimentos preliminares relativos ao contrato.

Isso significa que dentro da cadeia de prestação de serviços para o atendimento de uma contratação realizada, o Controlador possa a vir compartilhar os dados para a correta execução dos serviços. O professor Marcel Leonardi menciona

---

[19] MARCEL LEONARDI. **Artigo Principais bases legais de tratamento de dados pessoais no setor privado a ser publicado no livro Direito e Internet IV**. Mensagem recebida por marcel.leonardi@gmail.com em 07 mai. 2019 (Ainda não publicado)

(Ainda não publicado) como exemplo as Contratações de serviços de uma agência de viagem, vejamos:

> Imagine-se, por exemplo, o titular de dados pessoais que adquire um pacote turístico em um website de agência de turismo. Para poder executar os serviços contratados, essa agência de turismo precisará compartilhar os dados pessoais do titular com a companhia aérea, o hotel e eventuais prestadores de serviços complementares e, para tanto, poderá utilizar como base legal de tratamento a execução de contrato.[20]

Desde que assim como nas outras bases legais, a tratativa dos dados seja em conformidade com a necessidade aplicada a necessidade de executar o objeto contratual e sua finalidade.

d) Legítimo Interesse

O inciso IX, do Art. 7º da LGPD prescreve como uma das bases legais para tratamento de dados o seguinte o Legítimo Interesse:

> Art. 7. Inciso IX - 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

No entanto a questão “legítimo interesse” soa subjetiva, pois não está relacionado a finalidade específica. Muito embora o Artigo 10 da Lei Geral de Proteção de Dados seja uma tentativa de especificar quando seria possível a utilização dessa base legal, mas ainda assim, a subjetividade permanece:

> Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:
>
> I - apoio e promoção de atividades do controlador; e
>
> II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.
>
> § 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.

[20] MARCEL LEONARDI. **Artigo Principais bases legais de tratamento de dados pessoais no setor privado a ser publicado no livro Direito e Internet IV**. Mensagem recebida por marcel.leonardi@gmail.com em 07 mai. 2019 (Ainda não publicado)

> § 2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.
>
> § 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.

A utilização do Legítimo interesse pode apresentar um risco devido a sua subjetividade, é o que explica o Professor Marcel Leonardi

> O tratamento de dados pessoais com base no legítimo interesse é, normalmente, a base legal mais flexível entre as dez disponíveis, já que não está atrelado a uma finalidade específica. Nem sempre, porém, é a base legal mais apropriada para todas as situações. A utilização do legítimo interesse sempre representa um risco jurídico, na medida em que a avaliação de seus elementos deve ser documentada em relatório de impacto à
>
> proteção de dados pessoais e está sujeita à revisão, e possível discordância, por parte da Autoridade Nacional de Proteção de Dados.
>
> Ao decidir utilizar o legítimo interesse como base legal de tratamento, o controlador deve efetuar um teste com três etapas:
>
> (i) teste da finalidade: identificação de qual é o interesse legítimo e se esse interesse legítimo é próprio ou de terceiros;
>
> (ii) teste da necessidade: demonstração de que o tratamento dos dados pessoas é necessário para alcançar esse interesse legítimo; e
>
> (iii) teste da proporcionalidade: balanceamento desse interesse legítimo com os direitos e as liberdades fundamentais do titular que exijam a proteção dos dados pessoais.[21]

Provavelmente após a efetiva criação da Autoridade Nacional de Proteção de Dados, o ponto referente a essa base legal poderá ser melhor esclarecido.

e) Proteção do Crédito

A LGPD não trouxe a conceituação de Proteção do Crédito. No entanto, por ser uma questão inerente a atividade comercial, é considerada como uma das bases legais a serem utilizadas na prestação de serviços, visto que são informações necessárias para contratações de empréstimos, cartões e crediários de lojas e demais situações corriqueiras da relação com o consumidor. [22]

---

[21] MARCEL LEONARDI. **Artigo Principais bases legais de tratamento de dados pessoais no setor privado a ser publicado no livro Direito e Internet IV.** Mensagem recebida por marcel.leonardi@gmail.com em 07 mai. 2019 (Ainda não publicado)

[22] Idem

São essas as bases legais que de fato relacionam-se diretamente com a prestação de serviços entre pessoas jurídicas de direito privado, especificamente. O que não quer dizer que essas mesmas bases não possam ser aplicadas para outras situações.

Além disso, há de se ressaltar que é possível que mais de uma base legal esteja sendo aplicada, já que não há nenhum impeditivo de serem aplicadas concomitantemente, é o que explica o Professor Marcel Leonardi:

> É extremamente importante compreender que não há hierarquia entre bases legais: todas são igualmente importantes e podem ser utilizadas, sem que qualquer delas se sobreponha ou prevaleça em relação às demais. Cabe a cada controlador definir qual base legal é a mais apropriada em cada caso, sempre de acordo com as finalidades de tratamento.
>
> Assim, é importante compreender como essas bases legais podem ser utilizadas para o tratamento de dados pessoais realizado no curso das atividades empresariais.[23]

Dessa forma ao relacionar a suas atividades de coleta e tratamento de dados a uma das bases legais descritas na legislação a empresa estará resguardada e atuará em conformidade. Deve-se exigir que seus prestadores se serviço (Operadores) atuem no mesmo sentido.

3.3 Diretrizes preventivas

Os dados coletados possuem um ciclo de vida que passa pelas seguintes fases: Criação, Manuseio, Processamento, Armazenamento, Transporte, Transmissão e Destruição.[24]

As diretrizes preventivas são mecanismos internos utilizados para a supervisão e mitigação de riscos e precisam operar em todos os meios possíveis de coleta e tratamento de dados.

---

[23] idem

[24] VIVIANE MALDONADO, RONY VAINZOF, CAIO OLIVEIRA, LUIS FERNANDO PRADO CHAVES, CAIO LIMA E CAMILLA JIMENE. **CURSO ON LINE DE PROTEÇÃO DE DADOS LEC NEWS.** Informação pessoal. 09 mai 2019.

Para traçar diretrizes preventivas é necessário ter estratégias para cada uma dessas fases do ciclo de vida dos dados, bem como, exigir que o fornecedor ou o prestador de serviços, uma vez que estejam figurando como Operadores sigam as mesmas estratégias.

É importante que toda a estrutura relativa ao tratamento de dados seja passível de ser rigorosamente mapeada pois quanto mais se puder mapear e controlar, consequentemente mais os riscos poderão ser mitigados.

Nesse sentido, os registros de processamento de dados devem ser implementados desde sua concepção.

Duas das diretrizes preventivas principais para os sistemas de tecnologia são as chamadas de *Privacy by desing* e *Privacy by default.*

Privacy by desing é o termo utilizado para sistemas que foram criados e compostos desde seu início com o intuito de garantir a privacidade na coleta de dados. Não foi adaptado e sim, já foi desenvolvido de forma estrutural para que todo o ciclo de vida dos dados que sejam coletados em função de aplicações, produtos e serviços estejam em linha com o ideal para a preservação da privacidade, garantindo quando possível, que o titular tenha acesso ao sistema e possa gerenciar a coleta de seus dados pessoais.

Privacy by default é um termo que significa dizer que as configurações de privacidade sejam consideradas como Configurações padrão, de forma que garantirá maior interação com o titular dos dados, coletando seu consentimento durante o uso do sistema ou aplicação.[25]

Os termos supracitados acompanham o que a Lei Geral de Proteção de dados prescreve, já que em seu Artigo 46, parágrafo 2º a referida Lei menciona que as medidas (relativas à proteção de dados) devem ser aplicadas desde a fase de concepção do produto até a sua execução.

---

[25] FIESP. **LGPD: Lei Geral de Proteção de Dados,** 2018. Disponível em: <https://www.google.com.br/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKEwiXgcP3ivLiAhVxIbkGHVLDBcQQFjABegQIBBAC&url=https%3A%2F%2Fwww.fiesp.com.br%2Farquivo-download%2F%3Fid%3D252615&usg=AOvVaw21uwfDTmhSPxP6EfPlDII7.> Acesso em 15 mai. 2019.

Assim como o Art. 49 da LGPD prescreve no mesmo sentido:

> Art. 49. Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares.

Ocorre que a Lei não se aplica só a meios digitais de coleta de dados, mas sim sobre qualquer forma de coleta e tratamento, ainda que de modo físico ou analógico.

Por isso, possuir padrões técnicos como o *Privacy by design* e o *Privacy by default* mencionados acima é importante, mas é necessário ir além e atingir também a coleta feita de modo físico.

Antecipadamente se deve definir quais tipos de Dados serão coletados em razão da prestação de serviços celebrada entre Controlador e Operador. Ou seja, qual o objeto contratual e para a sua consecução quais dados pessoais serão necessários coletar. E depois disso, em segundo passo, verificar qual é a base legal para coleta de cada dado.

Caso seja a base legal seja a de consentimento, averiguar qual seria a melhor forma de obter e registrar o consentimento do titular de titular de dados.

Outro ponto importante, independente da base legal que autorize a coleta e o tratamento de dados, deve ser respeitado os direitos dos Titulares, uma vez que a Lei determina que o Controlador deve observa-los, prestando as devidas informações que vierem a ser solicitadas e dando a possibilidade de edição de informações incorretas ou exclusão se for o caso.

Desse modo, ao contratar um prestador de serviços que atuará como Operador, deve pactuar que os serviços sejam realizados de modo que facilite as consultas futuras e que seja registrado a origem da coleta, a data e a razão da manutenção do dado (base legal). Isso deve ocorrer ainda que a base legal não seja a de Consentimento, pois a Lei determina que o Titular de dados tenha no mínimo, o direito ao acesso de seus dados. É o que prescreve o parágrafo 6º do Artigo 7º da Lei 13.709/2018: “A eventual dispensa da exigência do consentimento não desobriga os agentes de tratamento das demais obrigações previstas nesta Lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular.”

Uma outra diretriz relevante é o programa de governança como todo. Um programa de governança deve contemplar todo o ciclo de vida dos dados, definindo padrões técnicos para cada fase.

Isso quer dizer que, que o programa de governança bem estruturado deve determinar que a criação dos dados, ou seja, a coleta inicial, seja feita de forma lícita, assim como o manuseio e o processamento seja feito por pessoas treinadas e capacitada a respeitarem a privacidade das informações; que o armazenamento sempre que possível seja realizado de forma segura e se utilizando a criptografia quando aplicável. [26]

Além disso, deve determinar que caso o ocorra a transmissão de dados somente ocorra quando houver cláusulas contratuais específicas e atenda as demais determinações da Lei Geral de Proteção a respeito do tema.

Por fim, o programa de governança deve abranger ainda, a respeito da destruição dos dados coletados.

A LGPD dedica uma Seção para falar a respeito do tema, nos seus Artigos 15 e 16 da referida Lei, encontramos diretrizes a respeito do término e da eliminação dos dados:

> Art. 15. O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:
>
> I - verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;
>
> II - fim do período de tratamento;
>
> III - comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º desta Lei, resguardado o interesse público; ou
>
> IV - determinação da autoridade nacional, quando houver violação ao disposto nesta Lei.

[26] DANILO DONEDA, **O QUE É A GOVERNANÇA DE ALGORITMOS?.** 2016, disponível em: <https://politics.org.br/edicoes/o-que-é-governança-de-algoritmos>. Acesso em 30 mai. 2019.

> Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:
>
> I - cumprimento de obrigação legal ou regulatória pelo controlador;
>
> II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
>
> III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou
>
> IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

Ou seja, independente da coleta de dados e o tratamento tenham sido realizados de forma física ou digital, sempre quando os dados não forem mais uteis, não deve o Controlador ou o Operador, manter informações arquivadas sem que haja a real necessidade. Devendo descartá-las de um modo que reduza ao máximo o risco de vazamento dessas informações.

Além das diretrizes mencionadas acima, existem outras inúmeras que podem ser aplicadas conforme cada caso. Como as alterações de políticas e procedimentos, códigos de conduta e relatórios de acompanhamento.

Tanto o Controlador quanto o Operador, que no caso presente seria o fornecedor prestador de serviços devem seguir diretrizes preventivas.

4. ADOÇÃO DE MEDIDAS PARA PROTEÇÃO DE DADOS EM CONTRATAÇÕES

4.1 Alterações necessárias nos procedimentos de Due Diligence para contratação de fornecedores

Atualmente a grande maioria das empresas no Brasil, principalmente as multinacionais, realizam o procedimento de *Due Diligence* de fornecedores, que é um processo de avaliação prévia sobre as informações da empresa que prestará serviços.

Essa avaliação consiste em verificar se o objeto social da empresa condiz com o serviço que prestará, se o capital social é compatível com a complexidade dos serviços ofertados, se existem alvarás ou licenças necessárias para a execução dos serviços e se o fornecedor as possui. Se constam protestos em seu nome ou processos cíveis e criminais, se está regular do ponto de vista fiscal, enfim, todo histórico possível e acessível do ponto de vista Legal.

Porém, muitas vezes durante um processo de Due Diligence acaba-se por encontrar dados pertinentes a pessoa física responsável pela Pessoa Jurídica em questão. Fato esse que, para alguns especialistas, pode vir a colidir com a Lei Geral de Proteção de Dados, já que seriam detectadas informações a respeito de Pessoas físicas, a quem a referida Lei protege.[27]

No entanto, compreende-se que os dados a serem buscados a respeito das pessoas jurídicas seriam dados públicos, e que por sua vez, se for necessário a busca de informações a respeito dos sócios ou responsáveis legais das empresas que estão sendo objeto de análise, deve ser buscado dados públicos também, de forma idônea, sem que tenha sido feito nenhum trâmite a ser considerado invasivo para a obtenção dessas informações.

Outro ponto relevante ao falar dos procedimentos de Due Diligence, é olhar pelo prisma de responsável subsidiário pelos serviços prestados pelo fornecedor. Uma vez que o procedimento de Due Diligence tenha sido feito e o fornecedor validado, deve se exigir que o mesmo exerça suas atividades em conformidade com a Lei Geral de Proteção de Dados.

Uma das formas de estar em conformidade é que se reportar ao órgão regulador pedindo autorização para coletar dados pessoais. Vejamos a explicação de Maria Maximina Cartaxo a respeito:

> Na prática, qualquer empresa que faça uso de dados pessoais terá de se submeter à LGPD. Ou seja, terá que pedir prévia autorização e esclarecer

[27] LEC EDITORA E ORGANIZAÇÃO DE EVENTOS LTDA (Maria Maximina Cartaxo). **Impactos da LGPD EM DUE DILIGENCE DE TERCEIROS**. 2018, Disponível em: < http://www.lecnews.com.br/blog/impactos-da-lgpd-em-due-diligence-de-terceiros/ >. Acesso em: 15 mai. 2019.

> o porquê de estar coletando tais dados, o modo e a finalidade da coleta, bem como a forma que estes dados ficarão armazenados, por quanto tempo, e com quem serão compartilhados, se for o caso.
>
> Empresas com Sistemas de *Due Diligence* e as consultorias de *background check* terão que se submeter e se adaptar para utilizar os dados recolhidos de forma correta.[28]

Dessa forma, entende-se que a ANPD deverá regular melhor a respeito da *due diligence* de terceiros, e independente disso, poderá a ter que pedir autorização prévia para coletar determinados dados.

4.2 Cláusulas pertinentes a serem exigidas aos fornecedores na prestação de serviços (relativas ao tratamento de dados pessoais).

Uma empresa ao ser contratada para prestar serviços e agir em nome de outra determinada empresa, poderá coletar dados em razão dessa contratação. E com isso, passará a ser responsável por esses determinados atos.

A questão da responsabilidade será tratada mais adiante, no entanto, é imprescindível que sejam pactuadas cláusulas claras e determinantes para a limitação da responsabilidade de cada parte, bem como, cláusulas que tornem possível a exigibilidade em juízo em casos de ilícitos.

Para que venha a fazer sentido todas as políticas internas que serão alteradas e criadas pelo Controlador, assim como o programa de governança que deve ser implementado, é necessário exigir que os Prestadores de Serviço estejam alinhados com os parâmetros da empresa contratante e que executem suas atividades em conformidade com a Lei.

Por mais obvio que seja simplesmente “estar em conformidade com a Lei” sabe-se que para que se possa exigir de fato e aplicar penalidades de forma ágil, o meio mais seguro é a formalização por meio de um contrato, que é título executivo entre as Partes.

---

[28] Idem ao 27

Antes de tratar a respeito das Cláusulas propriamente ditas, é importante delimitar o escopo de atuação do prestador de serviços e averiguar quais atividades serão outorgadas ao mesmo.

Posteriormente, ao iniciar a redação contratual, deve-se ter como premissa os esclarecimentos dos conceitos de dados pessoais e dados pessoais sensíveis. Separando um campo específico no início do contrato como “Definições” para que esses e outros termos peculiares tenham suas respectivas descrições ou em outro formato que for melhor convier no contexto entre as partes.

Em seguida, a descrição do objeto contratual deve ser o mais detalhada possível, de forma que fique nítida a atuação do prestador de serviços. Na maioria dos casos, a coleta de informações pessoais é decorrente da prestação e serviços e não o objeto contratual em si. No entanto, para que se possa individualizar as condutas em um momento futuro, é importante que seja detalhado o escopo de atuação da empresa prestadora de serviços.

Se possível, deve-se dedicar Cláusula exclusiva para tratativa da Proteção de Dados, indicando que a atuação do fornecedor deverá ser feita em linha com a legislação aplicável, em especial a Lei 13.709/2018 e quaisquer outras legislações aplicáveis e que se referem à Proteção de Dados. Isso porque a depender da atuação do fornecedor, poderá estar sujeito a demais legislações, como o GDPR. Nessa mesma Cláusula, caso as Partes optem por seguir o Código de Conduta de uma das partes relativo a proteção de dados ou outra documentação referente a programa de governança com o intuito de incluir questões relativas a proteção de dados, caso as Partes concordem, é um bom momento para que seja incluído. Isso quer dizer, que seja mencionado em cláusula e incluso o documento como Anexo contratual.

Exemplo de Cláusula contratual para esse caso:

“A CONTRATADA declara que prestará os serviços objeto desse Contrato em conformidade com a Legislação aplicável incluindo, mas não se limitando a Lei 13.709/2018, bem como, atenderá o Guia de Conduta relativo a Proteção de Dados da CONTRATANTE, que consta no Anexo I do presente instrumento.”

A transferência internacional de dados é outro item que merece uma cláusula em contratos como esse, isso porque a Lei Geral de Proteção de Dados, em seu Artigo 33 autoriza que a transferência seja realizada mediante o atendimento de critérios pelo Controlador. Ainda que se possa discutir a equiparação do Operador (prestador de serviços), com o Controlador, o mais adequado seria a vedação. Nesse sentido a sugestão de cláusula seria não só aplicando a vedação da transferência internacional de dados, mas também aproveitando o ensejo e aplicaria a vedação de modo amplo: "É vedada a transferência dos dados pessoais que venham a ser coletados em razão dessa Contratação a quaisquer Partes alheias ao presente Contrato."

Como todos os contratos, existem cláusulas obrigacionais destinadas as duas Partes. É importante que dentro desse contexto existam cláusulas obrigacionais que abordem a operação do tratamento de dados relativa à prestação de serviços. Isso quer dizer, cláusulas que especifiquem as ferramentas a serem utilizadas pelo prestador de serviços como a troca de informações entre Contratada e Contratante. Definições entre as Partes de como se dará a coleta e o armazenamento, se as partes utilizarão ou não a criptografia como recurso de armazenamento seguro das informações, dentre outras questões próprias do tratamento de dados e que podem ser delimitadas pela Contratante. Muitas vezes questões tão operacionais como essa podem exigir um texto grande e com quantidade maior de informações técnicas, nesse caso, é possível que as partes alternativamente façam uma cláusula que direcione o tema a um anexo contratual, que poderá conter detalhes exclusivamente técnicos da operação.

Outro item significativo para que seja acordado entre as partes no contrato, é a respeito da eliminação dos dados em caso de os dados coletados não serem mais uteis a função contratual ou como a Lei prescreve em seu Artigo 15, inciso I "Verificação de que a finalidade foi alcançada ou que os dados deixaram se der necessários ou pertinentes ao alcance da finalidade específica almejada". Muito embora a Lei mencione a respeito, assim como também cita outras hipóteses de término de tratamento de dados, é válido inserir cláusula nesse sentido.

Mais uma cláusula necessária seria a que garante os direitos dos titulares, pois, independentemente da base legal aplicada, o titular dos dados tem como um de seus direitos a informação a respeito de seus dados estarem sendo tratados ou não, bem

como consultar quais dados a empresa detém. Dessa forma, as Partes podem convencionar que o prestador de serviços atuará de modo a facilitar a prestação dessas informações em caso de solicitações e por se tratar de obrigação legal do Controlador, informará imediatamente ao Controlador a despeito do requerimento feito pelo titular de dados, para que esse o faça diretamente.

Ainda a respeito dos direitos dos titulares, a Lei não determina qual é o prazo razoável para o atendimento dessa solicitação. No entanto, é importante que a parte contratante e o prestador de serviços alinhem entre si e descrevam em Contrato cláusula que estabeleça um prazo palpável para o envio dessa comunicação para que o Controlador tenha meios de cumprir com a sua obrigação e as expectativas de atendimento estejam alinhadas.

Em atendimento a Legislação, pode-se inserir cláusula que determine que o prestador de serviços irá contribuir da melhor forma possível para esclarecer os fatos em caso de processos administrativos perante a Autoridade Nacional de Dados e que caso eventualmente a contratante venha a ser responsabilizada por fatos que tenham sido praticados pelo prestador de serviços, que esse irá fazer tudo o quanto for possível para excluir a empresa Contratante do processo administrativo, e caso não seja possível, que arcará com os custos da defesa, bem como, com os custos eventuais com indenizações.

Por fim, para que todas as cláusulas anteriores possam ter um peso maior, o ideal é que se tenha uma cláusula penal, ou seja, cláusula que determine o pagamento de percentual relativo a multa em caso de descumprimento das cláusulas anteriores. É evidente que se pode ter uma cláusula penal para quaisquer casos de descumprimento contratual e para ambas as Partes, independente de o referido descumprimento estar ou não relacionado a Lei Geral de Proteção de Dados e as cláusulas a ela relacionadas. Mas no caso em tela, será feita uma sugestão de cláusula para descumprimento no âmbito da LGPD.

“Em caso de descumprimento das cláusulas relativas à Lei 13.709/2019, a CONTRATADA deverá pagar à CONTRATANTE o valor de 20% (vinte por cento) do valor total do Contrato além de responsabilização e pagamento por perdas e danos relativas ao descumprimento.”

Para responsabilização contundente da empresa contratada, é possível incluir ainda, cláusula que determine que o descumprimento da LGPD é uma das razões para a resilição contratual.

4.3 Auditoria e Monitoramento dos Prestadores de Serviço com finalidade em garantir a proteção dos dados pessoais.

Quando uma pessoa jurídica contrata uma empresa para que essa preste serviços sendo que a referida prestação de serviços implica em atuação com os dados pessoais de terceiros atuando em seu nome, o prestador de serviços passa a ser o que a Lei chama de Operador, conforme veremos mais adiante na parte de penalização.

No entanto, tal relação contratual, traz responsabilidades as duas partes perante a Autoridade Nacional de Proteção de Dados, o que torna necessário por parte da empresa contratante (que a Lei o intitula como “controlador”) auditar e monitorar a prestação de serviços com a finalidade de garantir a proteção dos dados pessoais envolvidos na relação contratual.

O Artigo 37 da Lei 13.709/2018, a Lei Geral de Proteção de Dados, prescreve que: “O Controlador e o Operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especificamente quando baseado no legítimo interesse.”

A Lei conforme visto acima, traz a determinação de que independente da base legal aplicada para o tratamento de dados, tanto o Controlador quanto o Operador devem manter os registros relativos as suas atividades.

Desse modo, é importante pactuar o padrão de relatório de registro a ser feito pelo prestador de serviços (Operador), e validar o referido relatório com periodicidade pertinente ao volume de dados a serem tratados. Isso porque, embora o Artigo seguinte, qual seja, o Artigo 38 traz a possibilidade de a Autoridade Nacional de Proteção de Dados determinar ao Controlador a elaboração de relatório e impacto à proteção de dados pessoais referente a suas atividades, certamente, ao ter esse

relatório prévio e validado com o prestador de serviços que atuará em seu nome, traz celeridade para que seja atendido em caso de solicitação da referida autoridade.

A Lei determina ainda, em seu Artigo 39 que “O operador deverá realizar o tratamento de segundo as instruções fornecidas pelo Controlador, que verificará a observância das próprias instruções e das normas sobre a matéria.” Ou seja, o legislador traz nesse artigo a responsabilidade de o Controlador, empresa que contratará os serviços, a obrigação de checar se as suas instruções estão sendo observadas no tratamento de dados feito pelo Operador, bem como, a obrigação do Operador em seguir as referidas instruções. O que justifica a necessidade de auditar e monitorar as atividades do prestador de serviços, não só pela responsabilidade solidária aplicada entre as Partes, mas também por determinação legal.

O objeto de auditoria deve ter como principal finalidade verificar se os dados estão sendo coletados de maneira proporcional, que é o ponto focal da legislação. Entende-se que a definição da base legal que justifica a coleta e tratamento de dados fica a cargo do Controlador, mas é sua função averiguar se o prestador de serviços não está excedendo o limite ao coletar e tratar os dados.

Outro ponto importante a ser auditado são os sistemas de tecnologia utilizados pelo prestador de serviços. Devem estar em linha com o que se exige para garantir a proteção de dados e conforme mencionado anteriormente no presente trabalho, se possível devem ter sido elaborados para garantir a proteção de dados desde sua concepção, garantindo os requisitos de segurança e as boas práticas de governança.

O Artigo 46 já mencionado anteriormente, prescreve o seguinte:

> Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

A Lei determina a obrigação às duas partes, ou seja, os agentes de tratamento, devem adotar as medidas necessárias para a proteção de dados.

5. RESPONSABILIZAÇÃO

5.1 Penalidades

A Lei Geral de Proteção de Dados chegou ao Brasil com o mesmo viés que a Lei Anticorrupção, com um caráter reputacional, isso quer dizer, não estar cumprindo a Lei fere a imagem da empresa e pode impactar nos negócios e parcerias.

Seguindo exemplo do impacto da Lei anticorrupção no Brasil, as empresas que atualmente não seguem a legislação ou não possuem código de conduta a respeito, já estão saindo da lista de fornecedores. E acredita-se que a expectativa da Lei geral de Proteção de Dados impacte as relações comerciais da mesma maneira.

Especificamente sobre a Lei e suas penalidades propriamente ditas, o Artigo 52 traz as sanções a serem aplicadas em caso de descumprimento:

> Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:
>
> I - advertência, com indicação de prazo para adoção de medidas corretivas;
>
> II - multa simples, de até 2% (dois por cento) 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;
>
> III - multa diária, observado o limite total a que se refere o inciso II;
>
> IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;
>
> V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
>
> VI - eliminação dos dados pessoais a que se refere a infração.

O inciso II especifica que o valor de multa será aplicado por infração, ou seja, em caso de infração múltipla, a multa poderá ser cumulativa, o que é de fato um valor impactante, ainda mais considerando a estrutura econômica atual do país.

Além disso, o parágrafo 4º do mesmo Artigo, informa que para cálculo da multa que trata o inciso II poderá ser considerada o faturamento total das empresas em

situações a serem definidas em conformidade com a Autoridade Nacional de Proteção de Dados. Ou seja, o valor da multa pode ser o suficiente para assustar investidores estrangeiros em caso de descumprimento ou despreparo de empresas brasileiras perante a nova legislação.

A publicização, que significa de fato trazer ao público o ocorrido, é uma forma de sanção moral, da qual o legislador pretende de fato usar o erro de exemplo. É o que foi mencionado acima, sanção de cunho reputacional, que muitas vezes pode ter um impacto financeiro equiparado à multa, já que pode afastar parcerias de negócios e afetar o prestígio dos consumidores e clientes.

O bloqueio dos dados até a regularização, vem trazer sentido a sanção imposta pela Lei, visto que nada adiantaria o pagamento de multas com valores significativos se a raiz do problema não fosse ajustada. A lei é coesa ao trazer esse aspecto, assim como a eliminação dos dados em questão. Se a empresa não soube lidar adequadamente com o tratamento de dados, a sua atividade no que se refere especificamente a esses dados, deve ser interrompida, com a finalidade de evitar que cause maiores danos.

Com tudo, a Lei 13.709/2018 acompanha o princípio do Devido Processo Legal, pois traz no parágrafo 1º do Artigo 52 o seguinte: “As sanções serão aplicadas após o procedimento administrativo que possibilite a oportunidade de ampla defesa de forma gradativa, isolada ou cumulativa...”. O que traz a chance de a parte infratora se defender e comprovar sua inocência caso não tenha cometido nenhum ilícito ou ainda, transferir a responsabilidade caso prove que o dano na verdade tenha ocorrido devido a conduta de terceiro.

A Lei determina ainda, que o prestador de serviços que figura como agente de tratamento de dados na qualidade de operador, poderá solidariamente pelos dados causados pelo tratamento de dados, bem como, a depender da situação, poderá ser equiparado a Controlador e ter seu âmbito de responsabilidade no mesmo nível que o mesmo.

Além das penalidades administrativas descritas acima a serem aplicadas pela Autoridade Nacional de Proteção de Dados, fica a responsabilidade civil a ser apurada em processo judicial, o qual os titulares que forem lesionados pelas condutas do

Controlador e Operador podem pleitear na justiça a indenização e reparação dos danos.

5.2 Prestação de Contas e responsabilização do fornecedor por descumprimento contratual

Conforme visto anteriormente o Controlador exigirá do prestador de serviços, o operador, que siga todas as instruções e atue dentro das práticas de governança e segurança estabelecidas entre eles. No entanto, como qualquer outra relação de prestação de serviços, em algum momento a atuação pode desviar do esperado.

Como o objeto contratual dessa relação é sensível e tem uma Lei específica que trata sobre o assunto, é certo que a atuação do prestador de serviços será assistida detalhadamente pela empresa que o Contratar, isso porque a responsabilidade pelo tratamento dos dados será solidária entre o Controlador e Operador. Vejamos entendimento da Professora Ana Frazão a respeito do da responsabilidade solidaria:

> Para que não haja dúvida da amplitude da sua aplicação, a LGPD, já no seu art. 5º, define como controlador toda "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais" (inciso VI) e como operador toda "pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador" (VII), agrupando-os conjuntamente na categoria de agentes de tratamento (inciso IX).
>
> Como se pode ver, qualquer pessoa, natural ou jurídica, de direito público ou privado, pode ser considerada controladora ou operadora desde que, respectivamente, tenha poder decisório sobre tratamento de dados ou realize o referido tratamento em nome do controlador, independentemente da finalidade para a qual os dados estejam sendo utilizados. Embora a atuação de cada agente tenha peculiaridades para efeitos da definição do regime jurídico, há várias hipóteses de deveres comuns, assim como de responsabilidade solidária entre os dois, além da possibilidade de o próprio operador ser equiparado ao controlador (LGPD, art. 42).[29]

O operador deve responder por seus atos e pelas atuações que excedam o limite determinado contratualmente e pela LGPD.

---

[29] ANA FRAZÃO. **O alcance da LGPD e repercussões para a atividade empresarial**: 2018, Disponível em: < https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/o-alcance-da-lgpd-e-repercussoes-para-a-atividade-empresarial-05092018 >. Acesso em: 01 jun. 2019

> Art. 42. 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, é obrigado a repará-lo.
>
> § 1º A fim de assegurar a efetiva indenização ao titular dos dados:
>
> I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou **quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador,** salvo nos casos de exclusão previstos no art. 43 desta Lei;
>
> II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.

Conforme grifado acima, a Lei traz a equiparação do Operador a Controlador em caso de não cumprimento das orientações lícitas do Controlador, ou seja, considerando que todas as obrigações e diretrizes sejam contratualmente estabelecidas, o inadimplemento contratual por parte do Operador pode trazer maiores responsabiliza-lo por todos os danos que causar no tratamento de dados, como se Controlador fosse, conforme a determinação da própria LGPD. Devendo, portanto, reparar os titulares de dados pelos danos causados.

Caso o dano tenha sido comprovadamente causado pelo Operador de dados e o Operador, parte que contratou os serviços, venha a reparar os dados aos titulares, a Lei prevê o direito de regresso, em seu Artigo 42, inciso II, parágrafo 4º “ aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso.”

Além da previsão legal a respeito da responsabilidade, é cabível a cobrança de multa que eventualmente for estabelecida em Cláusula Penal entre as Partes, além de apuração das perdas e danos que o Operador pode ter causado ao Controlador, essa que deverá ser comprovada e exigida mediante processo judicial cível.

6. CONCLUSÃO

A Lei 13.709/18, conhecida como Lei Geral de Proteção de Dados (LGPD) veio com a função de regulamentar a coleta e o tratamento de dados no Brasil.

Apesar da LGPD ter sido baseada na legislação europeia foi adaptada as necessidades brasileiras e veio em um momento oportuno onde o assunto tem se tornado cada vez mais global e o Brasil carecia de legislação a respeito que pudesse lhe colocar no mesmo patamar que estão as grandes potências comerciais com relação ao tema, facilitando principalmente os negócios entre os países.

Assim como a Lei anticorrupção, o tema de proteção de dados também chegou ao Brasil após outros países terem criado leis no mesmo sentido, dessa forma, empresas multinacionais geralmente estão tendo contato com o tema de proteção de dados antes da LGPD, pois a exemplo temos a GDPR que já trazia questões com as quais as multinacionais brasileiras precisaram se adaptar para cumpri-la e por isso o mercado recebeu com alta expectativa a Lei de Proteção de Dados no Brasil. Inclusive é fato que a LGPD foi criada baseada na GDPR e ambas possuem muitas semelhanças entre si, ficando a principal diferença a respeito do limite de aplicabilidade.

No Brasil houve outras leis anteriores que abordaram a respeito da proteção de dados, mas de maneira mais genérica e superficial, sendo a LGPD a Lei mais completa e enfática a respeito do assunto em nosso país.

É importante destacar que está em votação a medida provisória 869/2018 que propõe 176 emendas à LGPD e sua aprovação poderá alterar significativamente o conteúdo do presente trabalho.

A LGPD passará a produzir efeitos em agosto de 2020, no entanto, a preparação das empresas deverá ser a partir de agora, pois são diversas mudanças e adaptações a serem feitas para atender a nova legislação, o que virá a sobrecarregar principalmente as empresas menores, que não tinham contato com a GDPR anteriormente.

A Lei Geral de Proteção de Dados traz a figura dos agentes e dentro do âmbito de prestação de serviços, dentre eles, destaca-se a figura do Controlador que pode ser pessoa física ou jurídica e toma decisões a respeito do tratamento de dados e a figura do Operador que executa o tratamento de dados em nome do Controlador. As ações em conjunto trazem peculiaridades a respeito da responsabilidade de cada um.

As alterações nos procedimentos relativos a prestação de serviços em especial, serão estruturais e afetarão desde o procedimento de *due diligence* do fornecedor, controle das atividades e descarte das informações coletadas e tratadas. Sendo que a coleta de dados deverá estar sempre relacionada a necessidade e finalidade, devendo o Controlador cuidar para que não ocorram excessos na coleta de informações, bem como garantir que todo o ciclo de tratamento de dados seja executado da maneira mais segura possível. Para isso, é importante delimitar o escopo de atuação do Prestador de Serviços (Operador). Além disso, para garantir a segurança no tratamento de dados deverão ser aplicadas medidas preventivas e inclusive, exigir que o Operador (prestador de serviços) as cumpra também, como por exemplo políticas, registros de coletas, programas de governança relativos à Proteção de Dados, dentre outros.

Para que a coleta de dados possa ser realizada, a LGPD determina dez bases legais, sendo que as que são interessantes às relações de prestação de serviços de pessoas jurídicas são: consentimento; cumprimento de obrigação legal ou regulatória pelo controlador; execução de contrato ou de procedimento preliminar; legítimo interesse e proteção do crédito.

É importante que o Controlador faça a auditoria e monitoramento das atividades do Operador relacionadas ao Contrato de Prestação de Serviços entre eles avençado. Não só porque poderá recair sobre o Controlador a responsabilidade de seus atos perante os titulares de dados, mas também porque haverá uma Autoridade regulatória, criada pela LGPD, qual seja Autoridade Nacional de Proteção de Dados e que regulamentará a respeito, bem como, aplicará sanções em caso de descumprimento da Lei. Até o presente momento a autoridade em questão não foi criada.

Por fim, entende-se que dentro do âmbito dos Contratos de Prestação de Serviços, a LGPD determina a responsabilização tanto do Controlador quanto do Operador pelos dados coletados e tratados. E por isso, além de pactuar cláusulas robustas, treinar, compartilhar modelos de governança, auditar e realizar demais medidas, cabe principalmente, por parte do Controlador envolver-se diretamente nos serviços a serem executados pelo Operador, acompanhando todo o processo e

garantindo que os direitos dos titulares de dados estejam sendo preservados, bem como que a sua conduta esteja em linha com as exigências legais e contratuais.

REFERÊNCIAS BIBLIOGRÁFICAS

ANA FRAZÃO. O alcance da LGPD e repercussões para a atividade empresarial. 2018, Disponível em: < https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/o-alcance-da-lgpd-e-repercussoes-para-a-atividade-empresarial-05092018 >.

ARTIGO 19. Proteção de dados pessoais no Brasil: Análise dos projetos de lei em tramitação no Congresso Nacional. 2016, Disponível em: < https://artigo19.org/wp-content/blogs.dir/24/files/2017/01/Proteção-de-Dados-Pessoais-no-Brasil-ARTIGO-19.pdf >.

CAIO CESAR CARVALHO LIMA e RONY VAINZOF. Sancionada a Lei Geral Brasileira de Proteção de Dados (LGPD): e agora?: Autoridade (ANPD) será criada por meio de Projeto de Lei de iniciativa do Executivo, diante do veto parcial apresentado por Temer. 2018, Disponível em: <https://www.jota.info/paywall?redirect_to=//www.jota.info/opiniao-e-analise/colunas/direito-digital/sancionada-a-lei-geral-brasileira-de-protecao-de-dados-lgpd-e-agora-14082018>

DANILO DONEDA, O QUE É A GOVERNANÇA DE ALGORITMOS?. 2016, disponível em: https://politics.org.br/edicoes/o-que-é-governança-de-algoritmos

FIESP. LGPD: Lei Geral de Proteção de Dados, 2018. Disponível em: <https://www.google.com.br/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKEwiXgcP3ivLiAhVxIbkGHVLDBcQQFjABegQIBBAC&url=https%3A%2F%2Fwww.fiesp.com.br%2Farquivo-download%2F%3Fid%3D252615&usg=AOvVaw21uwfDTmhSPxP6EfPlDIl7.>

FREDERICO MEINBERG CEROY. Dados pessoais sensíveis: Três projetos de lei que tramitam no Congresso Nacional abordam o tema. 2017, Disponível em: https://www.jota.info/opiniao-e-analise/artigos/dados-pessoais-sensiveis-29112017

JOSÉ BELO. *GDPR E LGPD*: Comparativo Parte I. Arquivo recebido por mensagem de e-mail por belsica@gmail.com em 16 abri 2019. Informação pessoal.

GISELE TRUZZI. Privacidade e Proteção de Dados Pessoais. 2017, Disponível em: <https://www.academia.edu/34223006/PRIVACIDADE_E_PROTEÇÃO_DE_DADOS_PESSOAIS>

LEC EDITORA E ORGANIZAÇÃO DE EVENTOS LTDA (Maria Maximina Cartaxo). IMPACTOS DA LGPD EM DUE DILIGENCE DE TERCEIROS. 2018, Disponível em: < http://www.lecnews.com.br/blog/impactos-da-lgpd-em-due-diligence-de-terceiros/ >.

MACHADO, MEYER, SENDACZ E OPICE ADVOGADOS. LEI 13.709/2018: Lei Geral de Proteção de Dados. 2018, Disponível em: <https://www.machadomeyer.com.br/images/publicacoes/PDFs/Lei_Protecao_de_Dados_ebook_18.pdf>

MARCEL LEONARDI. Artigo Principais bases legais de tratamento de dados pessoais no setor privado a ser publicado no livro Direito e Internet IV. Mensagem recebida por marcel.leonardi@gmail.com

RAFAEL ALMEIDA DE OLIVEIRA REIS. O QUE MUDA COM A NOVA LEI GERAL DE PROTEÇÃO DE DADOS? 2018, Disponível em: <https://novojurista.com/2018/08/19/o-que-muda-com-a-nova-lei-geral-de-protecao-de-dados/>.

RENATO LEITE MONTEIRO. A (i)legalidade de sites que divulgam dados pessoais. 2015. Disponível em: <https://renatoleitemonteiro.jusbrasil.com.br/artigos/191596216/a-i-legalidade-de-sites-que-divulgam-dados-pessoais>.

RONALDO LEMOS, DANIEL DOUEK, NATALIA LANGENEGGER, OLIVIA BONAN COSTA, PHILIPPE SUNDFELD e RAMON ALBERTO DOS SANTOS. GDPR: a nova legislação de proteção de dados pessoais da Europa:O que mudará no ambiente de negócios internacional? E quais os efeitos sobre cidadãos e entidades brasileiras? 2018, Disponível em: < https://www.jota.info/opiniao-e-analise/artigos/gdpr-dados-pessoais-europa-25052018>

UNIC. Declaração Universal de Direitos Humanos. 2009, Disponível em: https://nacoesunidas.org/wp-content/uploads/2018/10/DUDH.pdf>.

VIVIANE MALDONADO, RONY VAINZOF, CAIO OLIVEIRA, LUIS FERNANDO PRADO CHAVES, CAIO LIMA E CAMILLA JIMENE. CURSO ON LINE DE PROTEÇÃO DE DADOS LEC NEWS. Informação pessoal.

OBRAS COMPLEMENTARES

ABREU, Jacqueline. O compartilhamento de dados pessoais no Decreto n. 8.789/16: um Frankenstein de dados brasileiro? VARON, Joana et all. Bilhete Único: concentração de dados e dinheiro no transporte público do Rio.

BIONI, Bruno R. MACHADO, Jorge. A proteção de dados pessoais nos programas de Nota Fiscal: um estudo de caso do “Nota Fiscal paulista” BIONI, Bruno R. Expansão do Wi-fi "às custas" dos dados pessoais. Portal Jota, 2017

Data Protection Officers (WP 243): Guidelines on Data Protection Officers (‘DPOs’) (wp243rev.01)

Information Commissioner´s Office - ICO – Guide to Privacy by Design WP 29 Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679

PITA, Mariana. São Paulo Digital e Inteligente? Só se for com a proteção de seus Dados. Carta Capital

LEGISLAÇÃO:

Constituição da República Federativa do Brasil de 1988.

LEI No 10.406, de 10 de janeiro de 2002.

Lei 13.709, de 14 de agosto de 2018.