UNIVERSIDADE ESTADUAL DA PARAÍBA
CAMPUS I
CENTRO DE CIÊNCIAS JURÍDICAS
DEPARTAMENTO DE DIREITO PRIVADO
CURSO DE DIREITO

NATANY LETICIA DE OLIVEIRA FELIX

LEI N° 13.709/18: A PROTEÇÃO DE DADOS PESSOAIS E OS IMPACTOS NA SOCIEDADE BRASILEIRA

CAMPINA GRANDE - PB
2019

NATANY LETICIA DE OLIVEIRA FELIX

LEI 13.709/18: A PROTEÇÃO DE DADOS PESSOAIS E OS IMPACTOS NA SOCIEDADE BRASILEIRA

Trabalho de Conclusão de Curso da Universidade Estadual da Paraíba, como requisito parcial à obtenção do título de bacharel em direito.
Área de Concentração: Direitos Fundamentais

Orientador: Prof. Me. Paulo Esdras Marques Ramos

CAMPINA GRANDE – PB
2019

F316l Felix, Natany Leticia de Oliveira.
Lei n° 13.709/18 [manuscrito] : a proteção de dados pessoais e os impactos na sociedade brasileira / Natany Leticia de Oliveira Felix. - 2019.
23 p.
Digitado.
Trabalho de Conclusão de Curso (Graduação em Direito) - Universidade Estadual da Paraíba, Centro de Ciências Jurídicas , 2019.
"Orientação : Prof. Me. Paulo Esdras Marques Ramos , Coordenação do Curso de Direito - CCJ."
1. impactos na sociedade brasileira. 2. Lei n° 13. 3. 709/18. 4. Lei n° 13709/18. 5. Proteção de dados pessoais. I. Título
21. ed. CDD 347

Elaborada por Fernanda M. de A. Silva - CRB - 15/483 BSCCJ/UEPB

LEI N° 13.709/18: A PROTEÇÃO DE DADOS PESSOAIS E OS IMPACTOS NA SOCIEDADE BRASILEIRA

Trabalho de Conclusão de Curso da Universidade Estadual da Paraíba, como requisito parcial à obtenção do título de bacharel em direito.
Área de Concentração: Direitos Fundamentais e Direito Civil
Orientador: Prof. Me. Paulo Esdras Marques Ramos

Aprovada em: 04/06/2019

BANCA EXAMINADORA

Paulo Esdras M. Ramos.
Prof. Me. Paulo Esdras Marques Ramos
Universidade Estadual da Paraíba (UEPB)

Olindina Ioná da Costa Lo. Ramos
Prof. Dra. Olindina Ioná da Costa Lima Ramos
Universidade Federal de Campina Grande (UFCG)

Raïssa de Lima e Melo
Prof. Me. Raïssa de Lima e Melo
Universidade Estadual da Paraíba (UEPB)

Aos meus pais, por terem se sacrificado tanto para que eu chegasse até aqui, DEDICO.

“O direito à intimidade confere ao seu titular o poder de resguardar o indivíduo de uma publicidade não querida. Não se garante uma intimidade determinada, mas sim o direito a exercê-la, a ter uma vida privada, estabelecendo um poder de controle sobre a publicidade da informação relativa à pessoa.”

Marco Aurélio Rodrigues da Cunha

AGRADECIMENTOS

Aos meus pais, Nazareno e Maria José Felix, por terem sempre me apoiado e me dado todo o suporte possível para que eu chegasse aqui.

Ao meu irmão, Natan Felix, por estar sempre ali para me dar conselhos e me ajudar quando mais preciso.

As grandes amizades que fiz pela Universidade, em especial à Jaqueline e Saskia, que nos últimos períodos fizeram do CCJ um lugar mais aprazível.

Ao meu grande companheiro João Batista Caitano, que nunca me negou um abraço ou uma palavra de conforto, que se fez presente durante os quase 6 anos de curso, que me fazia rir das coisas mais improváveis e me fez enxergar pontos tão distintos do que eu considerava o certo.

Por fim, mas não menos importante, a Deus e ao Universo, que sempre conspiraram ao meu favor, fazendo com que tudo acontecesse na hora certa, mesmo que as vezes eu não entendesse o porquê.

LISTA DE ABREVIATURAS E SIGLAS

GDPR	Regulação Geral de Proteção de Dados da União Europeia
IBGE	Instituto Brasileiro de Geografia e Estatística
LGDP	Lei Geral de Proteção de Dados Pessoais
OECD	Organização para a Cooperação Econômica e Desenvolvimento

SUMÁRIO

LEI N° 13.709/18: A PROTEÇÃO DE DADOS PESSOAIS E OS IMPACTOS NA SOCIEDADE BRASILEIRA

Natany Leticia de Oliveira Felix

RESUMO

A Lei n° 13.709/18 trata da proteção e o tratamento de dados pessoais recolhidos e tratados aqui no Brasil. Tendo isto em vista, o presente artigo busca explanar o histórico da proteção de dados pelo mundo, analisar a lei em seus principais aspectos e ilustrar quais serão os principais impactos que a Sociedade Brasileira vai sofrer quando a lei começar a ser aplicada. A presente pesquisa terá finalidade explicativa e descritiva, tendo como objetivo geral estudar a lei destrinchando alguns de seus aspectos mais relevantes, especificamente, objetiva-se apontar quais os impactos imediatos de tal lei na sociedade brasileira. Ao final, observamos que a lei dá especial importância ao consentimento do titular para tratamento de seus dados pessoais para fins comerciais, e que as empresas deverão se adequar para sempre o requerer e especificar qual será o tratamento destinado a estes dados. Insta salientar que a lei se encontra em período de *vacatio legis,* pois foi dado um prazo de 2 anos para que a lei entrasse plenamente em vigor.

Palavras-chave: Lei n° 13.709; Proteção aos dados pessoais; Impactos na sociedade.

ABSTRACT

The Act n° 13.709/18 deals with the protection and processing of personal data collected and processed here in Brazil. With this in mind, this article seeks to explain the history of data protection in the world, to analyze the law in its main aspects and to illustrate what will be the major impacts that the Brazilian Society will suffer when the law begins to be applied. The present research will have an explanatory and descriptive purpose, having as general objective to study the law by unraveling some of its most relevant aspects, specifically, it aims to indicate which are the immediate impacts of such law in Brazilian society. In the end, we note that the law gives special importance to the consent of the holder to the processing of his personal data for commercial purposes, and that the companies should suit for ever to request and specify what the treatment will be for these data. It urges to emphasize that the law is in the period of vacatio legis, since a period of two years was given for the law to enter fully into force.

Keywords: Act n° 13.709; Protection of personal data; Impacts on Society.

1. INTRODUÇÃO

Com o crescimento da internet e a utilização cada vez mais ampla de dados pessoais para identificação, classificação e autorização faz com que eles se tornem elementos essenciais para que seus titulares possam viver com liberdade no que hoje chamamos de Sociedade da Informação. Atualmente, abrimos mão de certa privacidade em prol de facilidades que nos são concedidas.

Ocorre que lidar com dados pessoais e a automatização de seu tratamento é uma atividade de risco que merece atenção e a proteção devida do Estado, para que se evite uma exposição exagerada ou a utilização indevida ou abusiva de dados que facilmente caracterizam um indivíduo.

Há muito tempo as empresas recolhem dados pessoais de seus clientes e os tratam a fim de melhorar o alcance de suas vendas. Desde 1980 existe uma preocupação com a forma que se dá esse tratamento, a fim de se resguardar a intimidade dos cidadãos. Os países membros da Organização para Cooperação Econômica e Desenvolvimento já determinavam que esses deveriam providenciar legislação que protegesse seus cidadãos.

Em 1995, a União Europeia tratou de estabelecer diretrizes para uniformização do tratamento de dados pessoais. Tal diretiva foi seguida não só por países membros da União Europeia, como também pelos Estados Unidos, que mantinham estreita relação com a Europa e precisava seguir a Diretriz a fim de continuar tratando com seus clientes europeus.

Com relação à proteção de dados pessoais e da intimidade, a Constituição Brasileira tem como fundamento, descrito no art. 1°, inciso III, a dignidade da pessoa humana. Tal fundamento/princípio é extremamente amplo e guia todo o ordenamento jurídico pátrio a respeitar o ser humano como um todo, bem como seus direitos fundamentais. O art. 5°, inciso X, do mesmo diploma legal, preceitua que "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação".

O art. 21, do Código Civil, também tutela a intimidade e a vida privada das pessoas, dispondo que a vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma.

Agrupando conceitos trazidos pelo Marco Civil da Internet, pelo Código de Defesa do Consumidor e a Lei de Acesso à Informação, a Lei n° 13.709, ou Lei Geral de Proteção aos Dados Pessoais (LGPD) é a primeira legislação brasileira específica a tratar sobre o tema do tratamento de dados pessoais pelo Setor Público e o Privado, disciplinando o modo como poderá se dar este tratamento e os direitos e deveres dos envolvidos, ela segue a tendência mundial de fortalecer a proteção aos dados pessoais, garantindo direitos aos titulares e restringindo o uso injustificado e indiscriminado dessas informações.

A Lei Geral de Proteção aos Dados Pessoais objetiva disciplinar proteção dessa intimidade de informações pessoais no âmbito comercial e privado, com relação ao tratamento de dados pessoais pelas pessoas naturais e jurídicas de direito público e privado.

A LGPD, que tem forte influência das legislações Europeias sobre o tema, traz conceito do que é o dado pessoal, e como se dá o tratamento a ele. Ela especifica que, para que seja feito o tratamento, é necessário que o titular dê expresso consentimento para aquilo. Ademais, traz em seu corpo quem se enquadra na lei, como se dará a fiscalização e quais as punições para quem não a cumprir.

2. HISTÓRICO

Desde a propagação da internet, dados pessoais dos internautas têm sido compartilhados entre empresas a fim de direcionar melhor as estratégias de marketing. Tais dados podem ser recolhidos por meio de inscrições e documentos recebidos pela empresa, mas a maior parte é obtido pela internet, por meio de sites, e-mails e redes sociais, que os recolhe e mantém armazenados em seus bancos de dados.

Segundo o *Breach Level Index*, site que trata sobre o estado da segurança de dados no mundo, ao longo de 2017, 55 dados pessoais foram perdidos ou roubados por segundo, somando o total de 4,7 milhões de dados perdidos ou roubados por dia.

Esta insegurança na coleta e tratamento de dados pessoais por meio da Internet fez com que diversos países tomassem atitudes e inovasse em suas legislações para prever medidas de proteção a estes dados e evitar vazamentos que possam gerar dano aos seus titulares.

Desde 1980 os países membros da Organização para Cooperação Econômica e Desenvolvimento estabeleceram diretivas que indicavam que os Estados membros deveriam prover legislação interna para a proteção da privacidade e dos direitos individuais no gerenciamento de dados pessoais, a qual deveria ser aplicada aos setores públicos e privados.

No âmbito da União Europeia, em 24 de outubro de 1995, se formalizou a Diretiva n° 95/46/EC, do Parlamento Europeu e do Conselho da União Europeia, que estabelece diretrizes para uniformização do tratamento de proteção de dados pessoais pelos Estados-membros. Ela busca regular as relações das empresas nas operações que visem o tratamento dos dados pessoais, e considera como direito fundamental a proteção dos dados de caráter pessoal e o direito à privacidade. Seu artigo primeiro estabelece o seguinte:

> Os Estados-membros assegurarão, em conformidade com a presente diretiva, a proteção das liberdades e dos direitos fundamentais das pessoas singulares, nomeadamente do direito à vida privada, no que diz respeito ao tratamento de dados pessoais.

A referida diretiva criou e estruturou o conceito de *Safe Harbor,* que se baseia em sete princípios fundamentais, quais sejam: aviso, escolha, acesso, transferência progressiva, segurança, integridade de dados e execução.

O primeiro, aviso, informa que as empresas devem informar seus clientes sobre a finalidade da coleta de suas informações e as opções e meios que a organização oferece aos indivíduos para limitarem suas utilizações e divulgação. Eles também devem informar com quem essas informações são compartilhadas e como contatar a organização em caso de dúvidas ou reclamações.

O segundo, escolha, determina que a empresa forneça uma forma clara e acessível para os usuários escolherem como as informações prestadas serão divulgadas a terceiros.

Com relação a segurança, antes de compartilhar qualquer informação com terceiros, a organização deve seguir os dois princípios referidos acima. Devem também se assegurar de que os terceiros também sigam os Princípios do Safe Harbor.

Organizações envolvidas na coleta, processamento e manutenção dos dados pessoais dos usuários devem protegê-los do mau uso, da perda, da alteração e do acesso não autorizado.

A integridade indica que uma organização deve usar as informações apenas para os fins pelos quais as coletou, e deve ser responsável por mantê-las atualizadas e atuais.

Os indivíduos devem também ter acesso à informação que fornecem à empresa até certo ponto. O acesso pode depender da natureza e da sensibilidade das informações coletadas.

Com o objetivo de permitir o fluxo de dados pessoais entre a União Europeia e os Estados Unidos (que já seguia a diretiva 95/46/EC), a comunidade europeia adotou o *Privacy Shield* (Escudo de Privacidade), a fim de garantir um nível adequado de proteção de dados dos cidadãos europeus, bem como mecanismos e recursos para uma efetiva segurança jurídica.

A União Europeia, que já seguia a diretiva 95/46/CE, adotou o *General Data Protection Regulation* (GDPR), por meio do qual foram estabelecidas diversas regras com relação à coleta e ao tratamento de dados pessoais de titulares europeus. O regulamento já está em vigor desde 25/05/18 e atinge não só as empresas europeias, como também pessoas físicas ou jurídicas situadas no Brasil que, de alguma forma, utilizem dados pessoais de europeus para o desenvolvimento de suas atividades econômicas.

Como bem pontua Ericson M. Scorsim, "atualmente, os bancos de dados pessoais são fonte de valor econômico para as empresas privadas. Para o setor público, é fundamental para a realização de políticas públicas, em diversas áreas, como, por exemplo, saúde pública". Ante a grande importância dessas informações, cada vez mais se torna imprescindível que as empresas que as recolhe sejam compelidas a protegê-los, a fim de evitar que informações personalíssimas como orientação sexual e política caiam em mãos erradas.

No Brasil, a vida privada, a intimidade e os dados pessoais já eram protegidos de forma genérica pela Constituição Federal, em seu art. 5°, X, e no Código Civil, em seu art. 21. O Código de Defesa do Consumidor trouxe a primeira proteção de forma mais específica, em seu art. 43, que dispõe que o consumidor terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes, o pedido deveria ser feito administrativamente, ou por Habeas Data, em caso de negativa pela autoridade responsável.

Em sequência, entrou em vigor o Marco Civil da Internet, lei n° 12.965/14, que tratou timidamente do assunto em seu art. 11 sobre a questão dos dados pessoais, vejamos:

> Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.
> § 1º O disposto no caput aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil.
> § 2º O disposto no caput aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil.

> § 3º Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações.
> § 4º Decreto regulamentará o procedimento para apuração de infrações ao disposto neste artigo.

É possível observarmos que a proteção de dados foi tratada de forma muito superficial no presente artigo, deixando em aberto a possibilidade de regulamentação posterior. A LGPD buscou justamente regulamentar esse tratamento, buscando detalhar melhor o assunto.

3. DOS PRINCÍPIOS E FUNDAMENTOS DA LEI N° 13.709 DE 2018

Redes sociais são espaços virtuais onde grupos de pessoas ou empresas se relacionam partilhando conteúdo. Com o crescimento da internet, e sua democratização, a maioria da população pode se integralizar com essa nova realidade e passou a utilizá-las indiscriminadamente, expondo lá informações personalíssimas. Ao utilizarmos redes sociais como Facebook e Instagram, curtimos e compartilhamos postagens que definem nosso perfil para essas empresas. Lá, sem notar, acabamos expondo para o mercado não só nosso nome e data de nascimento, mas também nossos gostos, tendências políticas e religiosas, círculo de amizades e interesses no geral. Com tais informações em mãos, as empresas traçam nosso perfil de consumo e a melhor forma de nos influenciar a comprar algo ou alguma ideia. Tal influência não se restringe a compra de mercadorias. Ela é exercida a ponto de mudar nossa opinião pessoal sobre determinados assuntos, como política e comportamentos.

Mas não é só nas redes sociais que nossos interesses são coletados. Praticamente todos os serviços disponíveis na internet recolhem dados pessoais de seus usuários sem que eles notem, e tais informações são valiosíssimas, pois direcionam as empresas que as possuem para atingir o consumidor de forma mais certeira.

A importância de tais informações tornou-se ainda mais evidente quando se tornou conhecido pela mídia o vazamento de dados de 87 milhões de usuários do Facebook para a empresa de marketing político Cambrige Analytica, que atuou na campanha presidencial de Donald Trump.

Diante de tal panorama, surgiu a necessidade de se regulamentar o comércio de dados pessoais dos internautas, a fim de se impedir que tais dados sejam utilizados de forma indevida, a fim de evitar abusos que levem à violação de direitos fundamentais dos usuários, dentre eles a privacidade, a intimidade e a liberdade de pensamento.

Inicialmente, é importante ressaltar o conceito de dado pessoal. O Conselho Europeu, por meio da Convenção de Strasbourg, de 1981, ofereceu a seguinte definição: “dado pessoal é qualquer informação relativa a uma pessoa singular identificada ou susceptível de identificação.”.

A Regulação Geral de Proteção de Dados da União Europeia (GDRP em inglês) inspirou o legislativo brasileiro a publicar a Lei Geral de Proteção de Dados (LGDP) que tem por objetivo conferir aos usuários maior controle sobre seus dados, mas não só isso, ela visa regulamentar e fomentar um ambiente de desenvolvimento econômico e tecnológico, através de regras flexíveis que podem se adequar aos mais inovadores modelos de negócio baseados no uso de dados pessoais. Tais regras,

apesar de flexíveis, buscam evitar e reprimir abusos no uso de dados pessoais, a fim de evitar que direitos fundamentais sejam atingidos.

A lei n° 13.709 foi publicada no dia 15 de agosto de 2018 e visa regulamentar e proteger os dados pessoais. Milene Regina Amoriello Spolador Ribeiros, em seu artigo sobre a LGPD sintetiza bem o obtivo da lei:

> Da análise da nova lei podemos dizer que o objetivo da LGPD é garantir que a pessoa física saiba quem tem seus dados, quais informações estão em posse seja de pessoa física ou jurídica e o que estas pessoas estão fazendo com as informações que possuem, ou seja, existe uma preocupação com a transparência, o acesso à informação e a garantia de que a pessoa física terá controle sobre seus dados e sobre a forma com que estas informações são tratadas.

Como acima descrito, a LGPD dispõe sobre como deve se dar o tratamento dos dados pessoais dos indivíduos, e a forma como eles podem ser armazenados e utilizados por empresas e pessoas físicas. Ela tem como objetivo principal proteger os direitos fundamentais de liberdade e de privacidade, bem como o livre desenvolvimento da personalidade da pessoa natural, assim dispõe o caput de seu art. 1°.

O inciso I, do artigo quinto da lei n° 13.709 informa que, para efeitos da referida lei, considera-se dado pessoal toda informação relacionada a pessoa natural identificada ou identificável. Ou seja, nome, CPF, RG, profissão, estado civil, grau de escolaridade etc., tudo isso é considerado dado pessoal para fins da lei.

Mas não só esses dados são protegidos, o art. 5°, inciso II, determina que também são resguardados os dados pessoais sensíveis, que são aqueles que informam a origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou à organização de caráter religioso, filosófico ou político, dados referentes a saúde e a vida sexual, bem como dados genéticos ou biométricos quando vinculados a uma pessoa natural.

O tratamento dado às informações de caráter pessoal pode ser definido como toda a operação realizada com os dados pessoais, seja o armazenamento, a análise, processamento, eliminação, avaliação, controle, enfim, tudo que for feito com os dados pessoais pode ser definido desta forma, assim está descrito no art. 5°, inciso X, da LGPD.

A lei em análise tem seus fundamentos descritos no art. 2°, quais sejam:

> Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
> I - o respeito à privacidade;
> II - a autodeterminação informativa;
> III - a liberdade de expressão, de informação, de comunicação e de opinião;
> IV - a inviolabilidade da intimidade, da honra e da imagem;
> V - o desenvolvimento econômico e tecnológico e a inovação;
> VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
> VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Além dos fundamentos acima citados, a lei também explicita quais os princípios que a regem, eles estão descritos no art. 6° e o primeiro inciso apresenta o princípio da finalidade, e informa que o tratamento dos dados pessoais deve obedecer a propósitos legítimos, específicos, explícitos e informados ao titular. O inciso “VI” do aludido artigo completa tal perspectiva ao determinar que é garantido ao usuário a

transparência, de forma que o tratamento dado as suas informações pessoais devem ser encontradas de maneira clara, precisa e facilmente acessível ao titular.

O inciso segundo do art. 6° determina que deve haver compatibilidade do tratamento com as finalidades informadas ao titular, ou seja, se o titular foi informado que sua informação seria utilizada para determinado fim, ela não pode ser utilizada de modo diverso sem a autorização do usuário, exceto se houver um novo consentimento do usuário para este fim diverso. Ademais, o princípio do livre acesso garante aos titulares a consulta facilitada e gratuita sobre a integralidade de seus dados, bem como sobre a forma e a duração do tratamento que está sendo dado a eles.

É garantido ao usuário também a segurança de que suas informações não serão vazadas, que serão utilizados meios de proteção às informações do usuário de modo a prevenir que tais informações não sejam roubadas. Ademais, a lei determina que terá como princípio a não discriminação, de modo que as informações não poderão ser utilizadas com fins discriminatórios ou ilícitos.

4. REQUISITOS PARA TRATAMENTO DE DADOS PESSOAIS E OS IMPACTOS NA SOCIEDADE BRASILEIRA

O art. 3° da LGPD determina que a referida lei se aplica a qualquer operação de tratamento realizada por pessoa natural ou jurídica, seja ela de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que preencha alguns requisitos.

O primeiro requisito determina que a operação de tratamento deve ser realizada no território nacional, entendendo-se, neste caso, os dados pessoais cujo titular se encontre no Brasil no momento da coleta. Os dados pessoais objeto do tratamento também deve ter sido coletado no território nacional, e a atividade de tratamento deve ter por objetivo a oferta ou fornecimento de bens ou serviços, ou mesmo o tratamento de dados de indivíduos localizados no território nacional.

Trocando em miúdos, só se aplicará a lei aos dados coletados no Brasil, de pessoas que estejam aqui, e tais dados devem ter sido coletados com objetivos comerciais.

O parágrafo quarto, do referido artigo 3° determina que não se aplica a lei quando o tratamento de dados pessoais for realizado por pessoa natural para fins exclusivamente particulares e não econômicos, bem como os realizados para fins jornalísticos, artísticos, acadêmicos, de segurança pública ou defesa nacional, e por fim, em atividades de investigação e repressão de infrações penais.

Insta salientar que o tratamento de dados para fins de segurança pública ou defesa nacional feito por pessoa jurídica de direito privado só será admitido em procedimentos sob a tutela de pessoa jurídica de direito público. Nesta senda, foi inserida uma limitação legal para que tais pessoas jurídicas de direito privado não possam deter total controle sobre os dados recolhidos. Tais informações deverão ter sempre a tutela de uma pessoa jurídica de direito público.

Por fim, o inciso “IV”, do parágrafo 3°, do art. 3°, nos informa que dados provenientes de fora do território nacional que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamentos brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência (desde que o país de proveniência proporcione grau de proteção de dados pessoais), também não serão objeto da LGPD.

De modo resumido, toda informação recolhida, aqui no Brasil, para fins comerciais deve ser enquadrada nos ditames da lei n° 13.709/201. Informações

recolhidas para fins investigativos, pessoais, acadêmicos e de segurança não precisam deste tratamento.

O art. 7° da LGPD define as hipóteses em que será realizado o tratamento de dados pessoais. O primeiro inciso afirma que para que haja o tratamento, é necessário o consentimento do titular.

Tal regra é, à primeira vista, bem simples, e determina que alguém só poderá coletar ou tratar de qualquer dado pessoal se for dado o consentimento pelo seu titular. Sendo assim, as empresas não podem mais coletar dados dos seus usuários sem que eles tenham dado sua anuência expressamente. Tal manifestação deve ser dada de forma inequívoca: o usuário tem que saber que está concordando com o tratamento de seus dados pessoais, bem como que lhe será dada uma finalidade determinada.

Tal cláusula pode ser por escrito (caso em que deverá vir destacada das demais), ou por outro meio que demonstre a manifestação de vontade do titular. Insta salientar que, cabe ao controlador[1] o ônus da prova de que o consentimento foi obtido em conformidade com a Lei.

Caso a anuência tenha sido dada de forma viciada, esta será considerada nula se as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo, ou mesmo não tenha sido apresentada previamente com transparência, de forma clara e inequívoca.

Na hipótese de mudanças significativas na finalidade do tratamento que já foi aceito, o controlador tem obrigação de informar previamente ao titular sobre elas, e este pode revogar o consentimento, caso discorde destas alterações. Por fim, insta salientar que o titular pode revogar a qualquer momento o consentimento dado para que houvesse tratamento de seus dados pessoais, o procedimento deve ser gratuito e facilitado.

Em razão do princípio do livre acesso, o art. 9° da LGDP dispõe que o titular tem direito de acessar as informações sobre o tratamento de seus dados, tais como, a finalidade específica dele, sua forma e duração, quem é o controlador e como contatá-lo, informações acerca do uso compartilhado de dados pelo controlador e sua finalidade, a responsabilidade dos agentes que realizarão o tratamento e os direitos do titular.

Como a LGPD inverteu o ônus de provar o consentimento para o controlador dos dados, as empresas agora precisam adequar seus sites para que seja requerido o consentimento do titular em todas as ações necessárias; ademais, para que não haja dúvida com relação ao consentimento, devem ser instaurados protocolos de confirmação. Nos cadastros rápidos, como os de compra na internet, é preciso que o cliente não só aceite que seus dados serão processados, mas também que eles sejam armazenados após a operação comercial.

Para as empresas que negociam com pessoas jurídicas, é preciso ficar atento de requerer o consentimento não só da pessoa jurídica em si, com quem está se negociando, mas da pessoa natural que ali está lhe representando, pois, na grande maioria dos casos, seus dados também ficarão armazenados e, sem o devido consentimento, poderá gerar um processo judicial posterior.

Importante ressaltar também que, no âmbito das relações trabalhistas, a lei trará modificações pois, ao armazenar dados dos seus empregados, ou mesmo os currículos enviados pelos candidatos, as empresas deverão requerer o consentimento expresso para tal tratamento, caso seja feito contrato de trabalho, deverá conter nele

---

[1] Lei n° 13.709, Art. 5°, VI. CONTROLADOR: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

cláusula requerendo o consentimento e especificando qual o destino será dado aos dados do trabalhador.

Caso os dados pessoais forem tornados públicos pelo próprio titular (como aqueles disponibilizados nas redes sociais), é dispensada a exigência do consentimento, mas se mantém resguardados os demais direitos do titular previstos da LGPD.

O parágrafo 5° do referido artigo informa que, caso o controlador necessite comunicar ou compartilhar dados que já foram consentidos com outros controladores, ele deverá obter novo consentimento do titular, com esse fim específico, exceto se for fato que dispensa de consentimento, como é o caso dos dados manifestamente públicos.

Outra hipótese é para o cumprimento de obrigação legal ou regulatória pelo controlador. Por exemplo, caso o controlador precise de dados como nome e CPF por exigência legal, ele deverá requerê-los ao titular, assim como avisar que será dado o tratamento por exigência legal.

O inciso terceiro, do art. 7°, informa que a administração pública pode fazer o tratamento e o uso compartilhado de dados pessoais necessários à execução de políticas públicas previstas em leis e regulamentos, ou respaldadas em contratos e convênios. Ainda que seja recolhida pela administração pública, o titular deverá ser avisado que terá seus dados tratados.

O inciso quarto do referido artigo anuncia que poderá ser realizada análise de dados para a concretização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados.

O art. 5°, inciso XI da referida lei define anonimização como a utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, ou seja, se faz com que a informação não possa ser ligada ao titular do dado.

O órgão de pesquisa aqui citado não pode ser generalizado como empresa de pesquisa. Segundo o art. 5°, inciso XVIII, é assim entendido o órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no país, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico. Como maior exemplo, temos o IBGE, Instituto Brasileiro de Geografia e Estatística.

O art. 7° traz também as seguintes hipóteses de tratamento:

> [...]
> 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.

No inciso IX, entende-se por interesse legítimo do controlador o tratamento de dados pessoais para finalidades legitimamente consideradas a partir de situações concretas como o apoio e promoção de atividades do controlador, bem como a proteção do exercício regular de direitos do titular. Neste caso, apenas os dados estritamente necessários para o fim pretendido poderão ser tratados, no mais, o controlador deverá adotar medidas para garantir a transparência deste tratamento de dados baseado no legítimo interesse.

Um exemplo claro do inciso X do referido artigo é o sistema nacional de proteção ao crédito (SERASA e SPC), utilizado amplamente no comércio e no setor bancário.

A LGPD deu especial atenção ao tratamento de dados pessoais sensíveis, abrindo capítulo próprio para o tema. O art. 11, dispõe:

> Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
> I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;
> II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
> a) cumprimento de obrigação legal ou regulatória pelo controlador;
> b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
> c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
> d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;
> e) proteção da vida ou da incolumidade física do titular ou de terceiro;
> f) tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; ou
> g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

O parágrafo 3° do art. 11 dispõe que “A comunicação ou o uso compartilhado de dados pessoais sensíveis entre controladores com objetivo de obter vantagem econômica poderá ser objeto de vedação ou regulamentação por parte de autoridade nacional, ouvidos os órgãos setoriais do Poder Público, no âmbito de suas competências”. Aqui, observa-se que poderá ser vedada a venda de dados pelo poder público.

Ademais, poderá também ser restringido o compartilhamento de tais dados sensíveis a fim de se evitar que sejam utilizados como dificultadores para obtenção de planos de saúde, pois estes utilizam-se de bancos de dados públicos para analisar o histórico clínico de seus clientes, e assim definir o preço de seu plano.

Insta salientar que dados anonimizados não serão considerados sensíveis, justamente por não ter como ligar as informações ao seu titular.

Com relação aos dados de crianças e adolescentes, o parágrafo 1°, do artigo acima citado, determina que o tratamento desses dados pessoais somente poderá ocorrer com o consentimento específico de um dos pais ou responsável legal. Tal dispositivo é de extrema importância, pois evitará que, sem o consentimento dos pais, as empresas influenciem os jovens com propagandas direcionadas, sendo capaz de

formar completamente um pensamento ou desejo que não lhes pertence. Ademais, plataformas como Youtube deverão requerer o consentimento dos pais para que seja liberado o uso pelas crianças e adolescentes.

É interessante destacar que os dados pessoais de crianças poderão ser coletados sem o consentimento dos pais unicamente quando a coleta for necessária para contatar os pais ou o responsável legal.

Quanto ao Poder público, o art. 23 da LGPD determina que este deverá fazer o tratamento para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público. Para tal execução, deve ser expressamente indicada a previsão legal, a finalidade, os procedimentos e as práticas utilizadas.

O art. 25 traz à baila importante determinação que facilitará a comunicação de dados dos usuários entre os órgãos da administração pública, ao dizer que os dados deverão ser estruturados para o uso compartilhado, visando à execução de políticas e serviços públicos e à descentralização da atividade pública. Deste modo, entidades do poder público terão acesso a todas as informações de seus usuários sem necessitar fazer requisições.

É vedado ao Poder Público transferir para entidades privadas dados pessoais constantes de base de dados a que tenha acesso, exceto se for hipótese de delegação de função pública a particular, sendo possível o compartilhamento de dados pessoais, conforme prevê art. 26, §1º, I. Também, é autorizado o compartilhamento na hipótese de previsão legal e se a transferência de dados pessoais estiver fundamentada em contratos, convênios ou instrumentos similares.

Outra importante regulamentação é a transferência internacional de dados. Com o advento da lei e sua futura aplicação, a transferência internacional só será permitida para países ou organismos internacionais que garantam o mesmo grau de proteção proporcionado pela LGPD. Ademais, é permitida a transferência quando for necessária para cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, ou para assegurar a proteção da vida ou integridade física do titular ou de terceiros. Por fim, é igualmente permitida a transferência internacional quando o responsável oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos na lei, conforme cláusulas contratuais específicas para a transferência. Tais possibilidades estão previstas no art. 33 da lei em estudo.

Podemos observar então, que a aplicação da lei cria demanda de contratação de profissionais responsáveis pela gestão do banco de dados, mas não só os ligados a tecnologia, como a consultoria jurídica que deve ser reforçada para dar apoio a gestão de tais dados.

5. DOS DIREITOS DO TITULAR E DA FISCALIZAÇÃO

Os direitos do titular dos dados pessoais estão previstos entre os artigos 17 e 22 da LGPD. O art. 17 assegura que toda pessoa natural terá a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade.

O art. 18 descreve os descreve os direitos do titular, vejamos:

> Art. 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:
> I - confirmação da existência de tratamento;

> II - acesso aos dados;
> III - correção de dados incompletos, inexatos ou desatualizados;
> IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
> V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa e observados os segredos comercial e industrial, de acordo com a regulamentação do órgão controlador;
> VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;
> VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
> VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
> IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.

Apesar de informações pessoais notadamente públicas não exigirem o consentimento de seu titular para serem tratadas, como dispõe o art. 7°, §4°, ele pode opor-se a este tratamento, caso ele esteja violando algum dispositivo da LGPD, assim dispõe o art. 18, §2°.

Insta salientar que para o exercício desses direitos, necessário se faz um requerimento expresso de seu titular, ou seu representante legal, ao agente do tratamento. O §5° do artigo acima citado determina que tal requerimento será atendido sem custos para o titular.

O requerimento de correção, anonimização, bloqueio ou eliminação de dados deverá se comunicado aos agentes de tratamento com os quais tenha havido o uso compartilhado dos dados. Ademais, a portabilidade de dados pessoais, referido no inciso V, não inclui dados que já tenham sido anonimizados pelo controlador

É rotina comum em bancos e comércios o uso de programas que tomam decisões automatizadas, com base em banco de dados, para deferir ou não financiamentos, empréstimos e operações afins. O art. 20 garante ao titular dos dados o direito de solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizados de dados pessoais que afetem seus interesses, incluídas decisões destinadas a definir o seu perfil pessoal, profissional, de consumo, e de crédito, ou aspectos de sua personalidade. Caso esses dados não sejam fornecidos com base em segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.

Para garantir que tais direitos serão resguardados, a lei definiu como se dará a fiscalização destes tratamentos, bem como as sanções impostas em caso de descumprimento da lei.

O art. 55-A, editado por meio de medida provisória, criou a Agência Nacional de Proteção de Dados (ANPD) que tem suas competências descritas no art. 55-J, e entre as principais, encontra-se fiscalizar e aplicar sanções na hipótese de descumprimento da lei (inciso VI) e editar normas e procedimentos sobre proteção de dados pessoais.

As sanções previstas para o caso de descumprimento variam de advertência a multas que podem chegar a R$ 50.000.000,00 (cinquenta milhões de reais). Vejamos:

> 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;
> VII - (VETADO);
> VIII - (VETADO);
> IX - (VETADO).

O presidente da República vetou as sanções de suspensão parcial ou total do funcionamento do banco e de dados, bem como da sanção de suspensão do exercício de atividade de tratamento de dados pessoais e a proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados. Segundo o veto, estas sanções administrativas de suspensão ou proibição do funcionamento/exercício de atividade relacionada ao tratamento de dados podem ensejar "insegurança aos responsáveis por estas informações, bem como impossibilitar a utilização e tratamento de banco de dados essenciais a diversas atividades, a exemplo das aproveitadas pelas instituições financeiras, dentre outras, podendo acarretar prejuízo à estabilidade do sistema financeiro nacional".

É garantido que as sanções só serão aplicadas após procedimento administrativo sendo assegurada a ampla defesa. Elas serão aplicadas seguindo parâmetros como gravidade e natureza da infração, boa-fé do infrator, sua condição econômica, grau do dano, reincidência e vantagem auferida (ou pretendida) por ele.

Por fim, terminará o tratamento de dados quando for verificado que a finalidade foi alcançada, ou que aqueles dados deixaram de ser necessários para seu alcance. Caso termine o período consentido pelo titular, ou que ele peça sua eliminação ou ainda retire seu consentimento, além da possibilidade de ser terminado o tratamento por determinação da autoridade nacional, em caso de violação da lei.

6. CONCLUSÃO

Nesta senda, será protegido por esta lei todo aquele que tiver seus dados tratados por empresas ou mesmo pessoas naturais com fim comercial, de modo que tais empresas deverão requerer consentimento expresso dos titulares de tais dados, bem como deverá explicitar como se dará tal tratamento e por quanto tempo.

Caso tais dados sejam compartilhados com outras empresas, dever-se-á requerer novamente o consentimento do usuário para tal fim.

Tais determinações impactarão frontalmente o funcionamento dos sites das mais diversas empresas, pois só em armazenar os dados de uma simples inscrição ou venda, já deverá se pedir o consentimento expresso do usuário para tal fim, ademais, a venda de dados pessoais só será permitida se o titular de tais dados assim o consentir.

Com relação aos direitos dos titulares dos dados, a lei buscou facilitar ao máximo o acesso deles aos dados que as empresas possuem sobre eles, dando margem, inclusive, para contestação de dados já armazenados e retificação deles.

Diante todo o exposto, chegamos à conclusão de que a Lei de Proteção aos Dados Pessoais terá o condão de modificar extensamente o modo como se dá as interações entre empresas e titulares de dados pessoais. A partir de agosto de 2020, mês que a lei começará a ser aplicada, observaremos uma mudança de postura na

hora de recolherem os dados dos usuários, pois as empresas deverão tomar o devido cuidado para só recolher o que é de extrema necessidade, bem como de requerer o consentimento expresso do titular do dado.

Haverá mais transparência nas relações e o usuário ficará mais ciente que seus dados não só serão recolhidos para um simples cadastro, mas que eles serão tratados e que a qualquer momento ele poderá mudar de ideia quanto a disponibilização deles. É importante notar que várias empresas já estão se adequando à norma e requerendo, em sua página inicial, o consentimento do usuário para uso, compartilhamento e tratamento de modo geral dos dados, porém, como ainda falta mais de um ano para que a lei seja realmente aplicada, ainda não podemos mensurar os reais impactos que ela trará, bem como quais as modificações foram feitas para se adequarem a ela, apenas conjecturar quais serão as atitudes a serem tomadas.

Mas, uma coisa é certa, sendo corretamente aplicada, a lei trará grandes benefícios para população, ao garantir direito a transparência nas relações e que seus dados não sejam levianamente utilizados, e a esperança de que empresas que não cumprirem o determinado serão devidamente punidas, nos ditames da lei.

REFERÊNCIAS

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília, DF, Senado, 1998.

_____. Lei n° 10.406, de 10 de janeiro de 2002. **Código Civil.** Brasília, DF, 2002. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm> Acesso em: 22/04/2019.

_____. Lei n° 12.965, de 23 de abri de 2014. **Marco Civil da Internet.** Brasília, DF, 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em 22/04/2019.

_____. Lei n° 8.078, de 11 de setembro de 1990. **Código de Defesa do Consumidor.** Brasília, DF, 1990. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8078.htm>. Acesso em: 25/04/2019.

_____. Lei n° 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais.** Brasília, DF, 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acessado em 10/10/2018.

CONSELHO DA EUROPA. **Convenção para a Protecção das Pessoas relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal**. European Treaty Series - No. 108, Estrasburgo, 28.1.1981.

DA CUNHA, Marco Aurélio Rodrigues et al. A disciplina normativa brasileira sobre a intimidade e os bancos de dados. **Araucaria. Revista Iberoamericana de Filosofía, Política y Humanidades**, v. 9, n. 18, p. 56-84, 2007.

DONEDA, Danilo. **A proteção dos dados pessoais como um direito fundamental.** Joaçaba, Santa Catarina. 2011.

FRANÇA. **Carta dos Direitos Fundamentais da União Europeia**. Nice, França, 2000.

VALENTE, Jonas. **Lei de Proteção de Dados Vai Mudar Cotidiano de Cidadãos e Empresas.** Disponível em: <http://agenciabrasil.ebc.com.br/geral/noticia/2018-07/lei-de-protecao-de-dados-vai-mudar-cotidiano-de-cidadaos-e-empresas> Acesso em: 30/10/2018.

_____. **Lei de proteção de dados trará impactos a pessoas, empresas e governo.** Disponível em: <http://agenciabrasil.ebc.com.br/geral/noticia/2018-08/lei-de-protecao-de-dados-trara-impactos-pessoas-empresas-e-governos>. Acesso em: 30/10/2018

LEI GERAL DE PROTEÇÃO DE DADOS. Migalhas. 2018. Disponível em: < https://www.dizerodireito.com.br/2018/08/lei-137092018-lei-geral-de-protecao-de.html >. Acesso em: 22/04/2019

FAUSTINO, André. **A proteção de dados pessoais no Brasil: Breve histórico do direito comparado até a atual realidade brasileira.** In: **Âmbito Jurídico**, Rio Grande, XIX, n. 154, nov 2016. Disponível em: <http://www.ambito-juridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=18241&revista_caderno=17>. Acesso em 01/11/2018.

REANI, Valéria. **O impacto da lei de proteção de dados brasileira nas relações de trabalho.** In: **Consultor Jurídico.** Setembro de 2018. Disponível em: < https://www.conjur.com.br/2018-set-21/valeria-reani-alei-protecao-dados-relacoes-trabalho>. Acesso em: 22/05/2019.

RIBEIROS, Milene Regina Amoriello Spolador. **Lei Geral de Proteção de Dados: Parte II – Os Princípios e requisitos para a realização do tratamento de dados.** Setembro de 2018. Disponível em: <https://jus.com.br/artigos/68846/lei-geral-de-protecao-de-dados-parte-ii-os-principios-e-os-requisitos-para-a-realizacao-do-tratamento-de-dados >. Acesso em 12/06/2019.

SANTIAGO, Fernando. **Lei de Proteção de Dados Muda Funcionamento de Empresas Brasileiras.** Disponível em: <https://www.conjur.com.br/2018-ago-20/fernando-santiago-lei-protecao-dados-muda-atuacao-empresas>. Acesso em: 31/10/2018.

SCORSIM, Ericson M. **Lei brasileira de proteção de dados pessoais: análise de seu impacto para os titulares de dados pessoais, empresas responsáveis pelo tratamento de dados pessoais e setor público.** Disponível em: <https://www.migalhas.com.br/dePeso/16,MI286453,21048-Lei+brasileira+de+protecao+de+dados+pessoais+analise+de+seu+impacto>. Acesso em: 30/10/2018.