A LEI GERAL DE PROTEÇÃO DE DADOS COMO FERRAMENTA DE PROTEÇÃO DOS DIREITOS FUNDAMENTAIS

Lucas Rabello Cartolari[1]
Danilo Pierote Silva[2]
Artigo Científico[3]

RESUMO

A Lei 13.709/2018, denominada Lei Geral de Proteção de Dados, é a Lei brasileira mais atual e com a maior importância em relação a proteção de dados, onde regularizará como os dados serão coletados e tratados. O objetivo da Lei é proteger principalmente os Direitos Fundamentais, como o direito de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural junto com o tratamento de dados. O presente trabalho busca expor e analisar a maneira de que a Lei 13.709/2018 servirá como uma ferramenta para resguardar os Direitos Fundamentais garantidos pela Constituição Federal de 1988, além de como vigorará a regulamentação de todos os processos envolvendo dados. O presente artigo, se baseia no método hipotético-dedutivo, com o procedimento embasado em pesquisa documental e bibliográfica. Seguindo o raciocínio, o trabalho vigente busca demonstrar como a Lei Geral de Proteção de Dados conseguirá proteger os Direitos Fundamentais e os métodos de tratamento de dados, devido aos critérios rígidos para a coleta e tratamento de dados, juntamente com as sanções devidamente aplicadas.

Palavras-chave: Lei Geral de Proteção de Dados. Direito Digital. Big Data.Internet.

SUMÁRIO: INTRODUÇÃO, 1 A IMPORTÂNCIA DA LEI GERAL DE PROTEÇÃO DE DADOS, 2 OBJETIVOS DA LEI GERAL DE PROTEÇ˜AO DE DADOS, 2.1 Princípio da Finalidade, 2.2 Princípio da Adequação, 2.3 Princípio da necessidade, 2.4 Princípio do livre acesso, 2.5 Princípio da qualidade dos dados, 2.6 Princípio da transparência, 2.7 Princípio da segurança, 2.8 Princípio da prevenção, 2.9 Princípio da não discriminação, 2.10 Princípio da responsabilização, 3 ABRANGÊNCIA DA LEI, 3.1 Exceções de inaplicabilidade, 4 DEFINIÇÕES LEGAIS, 4.1 Dados Pessoais, 4.2 Dados pessoais sensíveis, 4.3 Dado Anonimizado, 4.4 Banco de dados, 4.5 Titular, 4.6 Controlador, operador e encarregado, 4.7 Tratamento de Dados, 5 DIREITOS DO TITULAR, 5.1 Confirmação da existência de tratamento, 5.2 Acesso aos dados, 5.3 Correção de dados incompletos, inexatos ou desatualizados, 5.4 Anonimização, bloqueio ou eliminação de dados desnecessários, 5.5 Portabilidade dos dados, 5.6 Eliminação dos dados, 5.7 Informação das entidades públicas e privadas com as quais o controlador compartilhou os dados, 5.8 Informação sobre a possibilidade de não fornecer consentimento, 5.9 Revogação do consentimento, 6 RESPONSABILIDADE CIVIL, 7 FISCALIZAÇÃO, 8 SEGURANÇA E BOAS PRÁTICAS CONCLUSÃO, REFERÊNCIAS.

---

[1]Aluno do Curso de Direito da Fundação de Ensino Eurípides Soares da Rocha, Marília, São Paulo;
[2]Professor Ms/Dr. do Curso de Direito da Fundação de Ensino Eurípides Soares da Rocha, Marília, São Paulo;
[3] Trabalho de Conclusão de Curso em Direito apresentado à Fundação de Ensino Eurípides Soares da Rocha, Mantenedora do Centro universitário Eurípides de Marília, para obtenção do grau de bacharel em Direito.

INTRODUÇÃO

Com o avanço tecnológico a qual a sociedade vivencia, não há equívoco em falar que a distância entre as pessoas não existe mais, tudo em razão da Internet, na qual se possibilita uma constante e quase infinita troca de informações entre pessoas de diferentes partes do mundo e em tempo real. Esta nova realidade trouxe à tona a necessidade de uma inovação no mundo jurídico, com o intuito de garantir a segurança do ambiente virtual concomitantemente com o ambiente real, sendo assim criada a Lei 12.965/2014, oficialmente chamada de Marco Civil da Internet, para que a mesma, não se tornasse um ambiente sem leis.

Essa inovação foi de grande relevância dentro do Direito, em vista do aumento dos crimes cibernéticos, ferindo assim os Direitos Fundamentais garantidos pela Constituição Federal de 1988, entretanto, esta nova ferramenta trouxe benefícios como o aprimoramento constante dos métodos de investigação e produção de provas.

Para auxiliar a Lei 12.965/2014, também atuará na defesa dos usuários da Internet e fora dela, a nova Lei 13.709/2018, a Lei Geral de Proteção de Dados, onde visa proteger principalmente a privacidade, os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Com o imensurável aumento do uso da internet pela população brasileira e mundial, o número de coleta de dados aumentou sincronicamente com o número de usuários, tornando-se quase incalculável.

A Lei Geral de Proteção de Dados só entrará em vigor em agosto de 2020, porém é necessário conhece-la e a manejá-la como uma ferramenta para resguardar os Direitos Fundamentais, pois, ainda que no âmbito virtual, até então uma extensão do mundo real, já temos nossos Direitos protegidos pela Constituição Federal, entre outras leis de menor potencial, e eles estão sendo completamente violados, junto com o tratamento irregular de nossos dados.

1 A IMPORTÂNCIA DA LEI GERAL DE PROTEÇÃO DE DADOS

A proteção de direitos fundamentais está evidente no artigo 2º da Lei Geral de Proteção de Dados, onde se correlaciona com o texto da Constituição Federal brasileira, principalmente no artigo 5º, incisos X e XII, que versam sobre a privacidade, a honra, a imagem das pessoas e o sigilo na comunicação.

O direito à privacidade nos tempos modernos se tornou quase uma raridade, pois a maioria das pessoas expõe as suas vidas particulares em diversas redes sociais, onde milhares de outras pessoas podem ver e acompanhar o que cada uma delas está fazendo.

Há também uma violação no sigilo da comunicação, pois a plataforma que a conversa está sendo realizada está sendo monitorada 24 horas e todos os dados da conversa são armazenados nos servidores das empresas.

Não só as empresas que armazenam, coletam, tratam ou utilizam os dados pessoais que violam tais dispositivos, mas também os hackers, que por algum meio ilegal ou fraudulento acabam conseguindo tais informações, cuja as mesmas podem ser vendidas por valores inimagináveis, dependendo de quem for, e qual a importância do dado.

Ainda no mundo físico, fora da internet, os direitos podem ser violados, tendo em vista que, por meio de documentos escritos, ou até mesmo em uma conversa tais dados podem ser coletados, colocando em risco à privacidade e a honra de quem pertencem as informações.

Vale ressaltar que da mesma forma, a Lei Geral de Proteção de Dados se aplica aos dados decorridos da relação de consumo que forem violados pelo fornecedor, quer sejam pessoas físicas ou jurídicas.

2 OBJETIVOS DA LEI GERAL DE PROTEÇÃO DE DADOS

A LGPD tem por seu objetivo já apresentado no art. 1º, onde dispõe sobre o tratamento de dados pessoais, sendo eles por meio digital ou não, seja por pessoa natural ou pessoa jurídica de direito público ou privado, visando proteger os direitos fundamentais de liberdade e privacidade, garantidos pela Constituição Federal, como anteriormente citado.

A Lei, em seu art. 2º nos apresenta os fundamentos gerais adotados como critério para proteger os direitos fundamentais abordados previamente, fundamentos esses, o respeito à privacidade, a autodeterminação afirmativa, a liberdade de expressão, informação, comunicação e a opinião, a inviolabilidade da intimidade, da honra e da imagem, o desenvolvimento econômico, tecnológico e a inovação, a livre-iniciativa, livre concorrência e defesa do consumidor, os direitos humanos, livre desenvolvimento da personalidade, dignidade e exercício da cidadania pelas pessoas naturais.

Ainda é acrescentado, em seu art. 6º, um rol de dez princípios que devem orientar o tratamento de dados. Esses princípios são:

2.1 Princípio da finalidade

Como o próprio nome já diz, o princípio da finalidade é acrescentado a Lei para exigir a finalidade do tratamento de dados pessoas, sejam eles legítimos, específicos, explícitos e informados ao titular do dado, tornando qualquer tratamento ilegal quando incompatível com qualquer uma das finalidades.

Consequentemente, não bastará ao controlador do dado apenas o consentimento do titular, devendo ainda respeitar o princípio da finalidade, e informar com clareza todas as atividades do procedimento.

2.2 Princípio da adequação

Este princípio foi adicionado à Lei visando amparar e acrescentar o princípio da finalidade, pois ele determina que o tratamento dos dados seja compatível com a finalidade apresentada pelo controlador. Isto é, além de comunicar ao titular o propósito do tratamento, ainda deverá garantir que os limites estipulados pelo titular sejam efetivamente cumpridos.

2.3 Princípio da necessidade

O princípio da necessidade, assim como o princípio da adequação, também vem ao auxílio para complementar o princípio da finalidade, pois define que o tratamento de dados deva ter um limite, sendo este um mínimo necessário para o cumprimento de sua finalidade. Deste modo, essa trindade de princípios determina que o tratamento deva ser pertinente, proporcional e não excessivo.

Vale ressaltar o entendimento que, este princípio, veda o tratamento de dados que possam ultrapassar os limites necessários, impedindo assim, coletas de dados desnecessárias que não possuem relação com a finalidade.

2.4 Princípio do livre Acesso

Este princípio garante ao titular do dado, a consulta gratuita e facilitada, sobre qualquer atividade envolvendo o tratamento de seus dados, podendo ser feita a qualquer momento, pois esses dados deverão estar armazenados de uma maneira que favoreça o exercício do direito do livre acesso.

O art. 9º da LGPD é bem claro quanto a maneira sobre as informações que o titular poderá requerer, sendo essas informações disponibilizadas com a finalidade específica do tratamento, a forma e duração do tratamento, a identificação e informações de contato do controlador, informações acerca do uso compartilhado de dados pelo controlador,

responsabilidades dos agentes que realizarão o tratamento e por fim, os direitos do titular, este último abordado pelo art. 18 da Lei, que será abordado futuramente.

2.5 Princípio da qualidade dos dados

Por este princípio, os agentes de tratamento proporcionarão aos titulares a garantia de exatidão, relevância, clareza e atualização de seus dados tratados, sempre em conformidade com a finalidade e necessidade do tratamento.

A Lei também garante ao titular o direito de solicitar uma revisão das decisões tomadas quando o tratamento de dados pessoas forem automatizados e afetarem os seus interesses.

2.6 Princípio da transparência

O foco principal do princípio da transparência é, como o próprio nome já afirma, garantir ao titular do dado, todas as informações de forma precisas e claras, bem como um acesso facilitado sobre como está sendo realizado o tratamento. Ou seja, o titular ganhará um acesso livre e irrestrito sobre todos os seus dados.

Cabe ainda lembrar que a própria Lei limita o princípio da transparência em casos de segredos industriais e comerciais que impeçam a divulgação das informações sobre o tratamento dos dados.

2.7 Princípio da segurança

Basicamente os agentes de tratamento deverão utilizar todos os meios técnicos e administrativos mais atuais e eficazes para proteger os dados pessoais, sejam eles digitais ou não, evitando qualquer tipo de acesso não autorizado, perda, vazamento, alteração ou à destruição dos mesmos. Isto é, o agente disporá de todas as medidas possíveis e razoáveis ao seu alcance para assegurar os dados.

2.8 Princípio da prevenção

Por sua vez, o princípio da prevenção foi introduzido para amparar o princípio da segurança citado anteriormente, pois impõe ao agente a obrigação de utilizar medidas preventivas contra qualquer tipo de dano aos dados.

Uma recomendação da própria Lei, é a criação de boas práticas e de governança, onde serão estabelecidas todas e qualquer tipo de norma de segurança, padrões técnicos e as obrigações específicas para os envolvidos no tratamento do dado.

2.9 Princípio da não discriminação

Este princípio tem a finalidade de impedir que o tratamento de dados seja usado para qualquer tipo de discriminação, ato ilícito ou abusivo. Assim, é garantido ao titular do dado a possibilidade de conferir a qualquer momento como seus dados estão sendo usados.

No caso de não fornecidas as informações devido ao fato dessegredo comercial ou industrial, a Autoridade Nacional poderá realizar uma auditoria para verificar qualquer atitude discriminatória em relação aos dados.

2.10 Princípio da responsabilização

Por fim, segundo este último princípio, o agente de tratamento deverá atestar que está utilizando todas as medidas capazes e eficazes de cumprir as normas de proteção de dados pessoais, sob pena de uma responsabilização individual ou até mesmo solidária do controlador ou do operador em caso de violação.

O art. 42 da Lei estabelece as sanções administrativas sofridas por quem realizar o tratamento irregular dos dados, sendo elas desde uma "simples" advertência, até uma multa por infração de até 2% do faturamento da empresa, com limite de R$ 50.000.000,00.

3 ABRANGÊNCIA DA LEI

O art. 3º da Lei, em seu *caput*, deixa bem claro que a LGPD poderá ser válida "independente do meio", ou seja, visa proteger o tratamento dos dados tanto "offline" quanto dos dados "online", diferente do antecessor "Marco Civil da Internet", onde só abrange os métodos online. Porém, não haverá a revogação tácita do Marco Civil da Internet, pois trata de outros temas, não só da proteção dos dados.

A Lei nos apresenta três hipóteses de sua aplicabilidade, sendo a primeira quando o tratamento for realizado no território nacional, onde nesse caso, basta ocorrer o tratamento de dados no Brasil, pouco importando o local em que se encontre a sede ou domicílio do agente de tratamento, ainda que no exterior. Cabe ressaltar que a lei também é válida para estrangeiros que tiverem seus dados tratados no Brasil, ainda que o estrangeiro esteja no exterior.

A segunda hipótese é quando o tratamento tenho por objetivo a oferta ou o fornecimento de bens ou serviços, ou o tratamento de dados de indivíduos localizados no território nacional, ou seja, o fato gerador nesse caso é a localização geográfica do fornecimento dos bens ou serviços do titular, com a certeza de que quando o tratamento for

realizado no Brasil, a LGPD deverá ser aplicada, independente se o agente estiver em território nacional ou fora dele.

Já a terceira e última hipótese, acontecerá quando os dados pessoais objetos do tratamento tenham sido coletados no território nacional, tendo em vista que quando os dados forem coletados o titular se encontre no Brasil.

3.1 Exceções de inaplicabilidade

O art. 4º da LGPD nos apresenta seis hipóteses de não incidência da Lei, onde o agente de tratamento não será penalizado pelo tratamento de dados. A primeira delas, é o tratamento de dados com fins exclusivamente particulares e não econômicos, sendo ela a mais comum e cotidiana das hipóteses, sendo nada mais, nada menos, que armazenar o contato telefônico ou e-mail de um colega, fotos, alguma carta, elementos que contenham dados de terceiros, porém são frutos de uma vida comum, e não serão utilizados com relações econômicas.

Já a segunda hipótese, é o tratamento de dados com fins exclusivamente jornalísticos, pois a Constituição garante o direito de liberdade de expressão, desde que a matéria jornalística tenha finalidade apenas de informação com o dado utilizado, descaracterizando a exceção de inaplicabilidade da LGPD se junto com a informação o agente pretende obter alguma vantagem econômica. No caso de sites de jornalismo, só serão válidos aqueles que não contenham a venda de anúncios publicitários de serviços ou produtos relacionados ao dado coletado.

A terceira hipótese é a de fins exclusivamente artísticos, esta hipótese correlacionada com o direito à liberdade artística, assegurada pelo art. 5º, IX da Constituição Federal de 1988. Ou seja, o agente não poderá ser penalizado pela LGPD caso venha a utilizar os dados em obras artísticas de cunho literário, musical, cinematográfico, escultural, etc. Um conceito de obras intelectuais pode ser facilmente explicado pelo rol contido no art. 7º da Lei 9.610/98.

A quarta hipótese é relativa ao fim exclusivamente acadêmico, onde o legislador praticamente deu uma “carta branca” ao agente que utilizar o tratamento de dados para qualquer atividade acadêmica, colocando assim, todo o âmbito acadêmico completamente fora da aplicação da LGPD.

No tocante a quinta hipótese, muito provável a mais sensível, é o tratamento de dados com fins exclusivos de segurança pública, defesa nacional, segurança do Estado e atividades de investigação e repressão de infrações penais, sendo todas estas finalidades de competência exclusiva do Poder Público. Portanto, quando o Poder Público necessitar de um tratamento

envolvendo qualquer uma das finalidades apresentadas, não terá a aplicabilidade da LGPD, pois o tratamento de dados nessas situações só acontecerá para garantir assuntos de segurança para a coletividade.

A sexta e última hipótese é o simples fato de dados provenientes do exterior, hipótese esta que beneficia as empresas brasileiras, pois poderão oferecer serviços de hospedagem de dados do exterior no Brasil, pois com os mesmos hospedados em território nacional, seria uma maneira de se aplicar a LGPD.

4 DEFINIÇÕES LEGAIS

As definições legais auxiliam no entendimento e aplicabilidade da Lei, pois torna mais exato, lógico e intuitivo todos os termos presentes na LGPD, assim excluindo possíveis dúvidas quanto a maioria da interpretação da mesma.

A seguir, vejamos detalhadamente cada termo presente no art. 5º, justamente para tornar mais claro o entendimento dos mesmos:

4.1 Dados pessoais

O art. 5º da Lei, em seu inciso I, exemplifica o que são dados pessoais, podendo estes serem definidos como a informação que possa, imediatamente, identificar uma pessoa natural, como o nome, número do RG, fotos etc. Pode ser considerado como um dado pessoal "objetivo", pois a identificação ocorre de imediato.

Para um entendimento melhor e mais claro, basta imaginarmos um auditório com 50 pessoas e o palestrante vendado, onde um assistente lhe passa informações, até que ele adivinhe a pessoa sentada em uma cadeira x. Informações essas como, se a pessoa é homem ou mulher, já eliminando 50% das possibilidades, se o nome da pessoa começa com uma letra Y e, após cada resposta, as possibilidades se afunilarão, até que o palestrante identifique a pessoa.

A pessoa que estava sentada na cadeira x não estava identificada, porém é identificável mediante as informações que foram passadas pelo assistente.

Vale ressaltar o Decreto 8.771/2016, que altera o Marco Civil da Internet (Lei 12.965/2014) onde, em seu artigo 14, inciso I, nos apresenta uma definição de dado pessoal:

> Art. 14. Para os fins do disposto neste Decreto, considera-se:
> I – Dado pessoal – dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou

> identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa.

O decreto utilizou-se de um critério adotado por Bruno Bioni, onde afirma ser um critério expansionista, não sendo só pessoal os dados que identifiquem imediatamente uma pessoa natural, como algumas informações certas, como o próprio nome ou identificação de documentos como previamente dito.

4.2 Dados pessoais sensíveis

Já os dados pessoais sensíveis, são aqueles que podem ser considerados “subjetivos”, pois somente a pessoa natural consegue identificá-los, pois tais dados podem ser sobre origem étnica, ideologia religiosa, opinião política, orientação sexual, todos vinculados ao pensamento de uma pessoa natural. Resumidamente, um dado pessoal sensível é um dado pessoal, porém pode acarretar algum tipo de discriminação com o dado coletado.

Devido ao fato de que os dados pessoais sensíveis possam causar maiores danos ao seu titular, já que estão atrelados à sua privacidade, a LGPD apresenta um diferencial para o tratamento dos mesmos, tornando ainda mais rígidas as hipóteses de tratamento, como abordaremos futuramente.

Voltemos ao exemplo anterior, onde o palestrante tentava adivinhar a pessoa na cadeira x, e as informações passadas a ele são que a pessoa é asiática, judia, torce para o Corinthians e sua cor favorita é a azul. É muito mais fácil descobrir a identidade da pessoa, pois como dito anteriormente, essas informações são de cunho pessoal e subjetivo, onde muitas vezes, somente a própria pessoa tem conhecimento desse dado.

Porém, para um entendimento maior da gravidade de um possível vazamento ou até mesmo um tratamento incorreto de um dado pessoal sensível, podemos imaginar um site de compras que não aparece para quem for negro, assim, acarretando em uma discriminação racial por conta de um dado pessoal sensível, ou até mesmo recentemente na época de eleições, onde sites de informações políticas de cunho “esquerdista” ou da “direita conservadora”, só apareciam para aqueles que apoiavam seus respectivos partidos.

4.3 Dado anonimizado

Como o próprio nome já o define, consiste em um dado “anônimo”, pois o seu titular não pode ser identificado somente com este dado, assim, protegendo ainda mais o titular de um possível dano. O dado pode ser anônimo da origem da coleta, ou pode passar por um

processo de anonimização, onde é desassociado o dado de seu titular, sendo findo o processo quando este dado não puder mais identificar este titular.

Para entendermos melhor, um dado anônimo presente no cotidiano são as pesquisas de rua, onde são coletados apenas os dados interessantes e com finalidade de responder o questionário. Ou seja, voltando ao tema de eleições, se pegarmos uma pesquisa onde X% das pessoas votaram no partido A e Y% das pessoas votaram no partido B, esses dados são considerados anônimos, pois não se pode identificar o titular apenas com esse dado coletado.

Porém, há de ter um cuidado, pois se junto com a resposta da opinião política, for coletado algum outro dado pessoal como nome, telefone, e-mail, etc. O dado é considerado pessoal sensível por se tratar de um pensamento da pessoa, devendo este então, passar pelo processo de anonimização antes mencionado para se tornar um dado anônimo.

4.4 Banco de dados

O banco de dados é simplesmente onde estão sendo armazenados e tratados os dados, podendo ser de meios físicos ou digitais, devido a abrangência da Lei em proteger os dados tanto offline quanto online.

Um exemplo de banco de dados físico é um cofre ou gaveta, onde dentro contém uma folha de papel que está preenchida com dados pessoais e dados sensíveis. Já um banco de dado digital poderá ser um servidor ou software em nuvem, onde também estarão presentes os dados.

4.5 Titular

O titular é unicamente a pessoa natural, a quem os dados pessoais objetos do tratamento se referem e, pode ser considerado a essência da Lei, pois a mesma visa proteger os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade, estes vinculados à pessoa natural.

Conforme o art. 2º do Código Civil, onde é adotado a teoria natalista, a personalidade civil da pessoa natural se dá com o nascimento com vida, assim, automaticamente já conta com os direitos tutelados pela LGPD.

Porém, há recentes discussões tanto no STJ, quanto no STF acerca dos dados coletados no ultrassom do nascituro, onde afirmam que, sua imagem, peso, tamanho, sexo, entre outros, o feto tenha no mínimo, uma expectativa de direito sobre seus dados pessoas, dada a sua personalidade jurídica formal, constituída desde a concepção, até sua

personalidade jurídica material, adquirida o seu nascimento com vida. Assim sendo, há essa exceção para que os dados do feto sejam resguardados pela LGPD.

4.6 Controlador, Operador e Encarregado

O controlador pode ser uma pessoa natural ou jurídica, de direito público ou privado, sendo ele a quem competem as decisões sobre o tratamento de dados pessoais.

A Lei fixa o maior peso jurídico no controlador pois ele é o responsável por qualquer decisão envolvendo o tratamento de dados pessoais, sendo indispensável a definição de quem realmente é o controlador em cada caso, para a melhor aplicabilidade da LGPD.

Já o operador, também poderá ser uma pessoa natural ou jurídica, de direito público ou privado, porém, ele apenas realiza o tratamento em nome do controlador, esse sendo mais um motivo para a Lei ser mais rígida quando se trata do controlador. Portanto, o operador apenas realizará o tratamento dos dados dentro do que for determinado pelo controlador, ou previsão.

Vale ressaltar que a Lei também se refere aos controladores e operadores apenas como agentes de tratamento.

Por fim, o encarregado é a pessoa indicada pelo controlador para atuar diretamente com a comunicação entre o próprio controlador, os titulares e a Autoridade Nacional de Proteção de Dados, porém, além da comunicação, o encarregado será responsável por receber as reclamações do titular, prestar esclarecimentos e tomar certas providências de menor potencial, além é claro de outras atribuições requisitadas pelo controlador, ou de uma possível norma complementar.

4.7 Tratamento dos Dados

O art. 5º da LGPD, em seu inciso X, traz o conceito de tratamento, que é toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Como visto anteriormente, os dados podem ser divididos em pessoais e pessoais sensíveis, e a LGPD em seus artigos 7º e 11, versam, respectivamente, sobre o tratamento dos mesmos.

O art. 7º, em seus incisos, apresenta um rol taxativo, indicando quando o tratamento de dados pessoais ocorrerá, hipóteses essas que podem ser, mediante consentimento expresso do titular, para cumprimento de obrigação legal ou regulatória pelo controlador, 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 da LGPD, para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais, 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, para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307/96, para a proteção da vida ou da incolumidade física do titular ou de terceiro, para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária, 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 para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

Já os dados pessoais sensíveis, possuem um rol taxativo menor em comparação ao anterior, pois estão profundamente ligados a privacidade do usuário, alcançando a sua intimidade, e um possível vazamento destes dados, seria de uma gravidade maior.

O tratamento de dados pessoais sensíveis só ocorrerá somente se o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas ou sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para o cumprimento de obrigação legal ou regulatória pelo controlador, para o tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos, para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis, para o exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307/96, para a proteção da vida ou da incolumidade física do titular ou de terceiro, para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária ou para a 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.

A LGPD ainda apresenta um rol taxativo exclusivo para os dados de crianças e adolescentes, previsto no art. 14, onde afirma que os dados só poderão ser tratados se obtiver

o consentimento específico e em destaque, dado por pelo menos um dos pais ou pelo responsável legal, sendo que os controladores deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos, e sem o consentimento dos responsáveis, os dados só poderão ser coletados se for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiros.

Além disso, as informações sobre o tratamento de dados de crianças e adolescentes deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança.

5 DIREITOS DO TITULAR

O art. 17 da LGPD, afirma que à pessoa natural, é assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, intimidade e de privacidade, ou seja, os dados sempre serão da pessoa natural, não podendo ser objeto de cessão ou transferência, amparados pelo art. 11 do Código Civil, onde afirma que os direitos da personalidade são intransmissíveis e irrenunciáveis, devendo assim, qualquer negócio jurídico, de cessão ou transferência de dados pessoais, ser considerado nulo.

Dado isso, o art. 18 apresenta ao titular dos dados, os seus direitos a serem pleiteados mediante requisição ao controlador. A LGPD admite que para o titular tenha a total aptidão para controlar o fluxo de seus dados pessoais, é indispensável que lhe seja concedido alguns direitos subjetivos em face dos agentes de tratamento, direitos esses que são:

5.1 Confirmação da existência de tratamento

Como o próprio nome já afirma, este direito é garantido ao titular a possibilidade de simplesmente confirmar se os seus dados pessoais estão sendo tratados, tendo consonância com o princípio da transparência visto anteriormente. Ainda que fora informado, no momento da coleta do dado que os mesmos seriam tratados, o titular ainda tem o direito de requerer esta confirmação.

5.2 Acesso aos dados

Assim que obtiver a confirmação da existência do tratamento de dados, seja pelo direito apresentado previamente ou se o titular abertamente já tinha conhecimento do

tratamento, o mesmo terá o direito de acessá-los, além de obter as informações sobre a finalidade, prazos, origem, e tudo o que desejar saber durante o tratamento.

Cabe ressaltar que o titular deva ter o acesso facilitado e da forma mais clara possível, observando os princípios do livre acesso e o princípio da qualidade dos dados.

5.3 Correção de dados incompletos, inexatos ou desatualizados

Após conferir todos os dados, o titular tem o direito de exigir a modificação dos mesmos, caso eles estejam incompletos, inexatos ou desatualizados, devendo o controlador alterar imediatamente.

Deve-se apontar também, que é aconselhável ao controlador registrar todo o histórico de mudanças do dado, para que, futuramente, possam ter variadas utilidades tanto por parte do titular, quanto por parte do controlador.

5.4 Anonimização, bloqueio ou eliminação de dados desnecessários

Como já exposto anteriormente, dados anônimos são os dados que não possibilitam a identificação do titular, e, devido a esta questão, é garantido este direito que visa garantir a segurança do dado, podendo o titular requerer a anonimização do mesmo a qualquer tempo.

O direito ao bloqueio de dados é meramente uma medida temporária, como uma suspensão, e a eliminação, uma medida concreta e, ambas podem ser exigidas tanto no decorrer do tratamento, quanto no final.

Esses três direitos estão correlacionados entre si, pois eles têm em comum a utilização de dados desnecessários ou excessivos, ultrajando assim, o princípio da necessidade.

5.5 Portabilidade dos dados

Assim como no cotidiano, é garantido ao titular dos dados, a portabilidade dos mesmos, caso queira, mediante requisição expressa, exigir a transferência de seus dados pessoais a outro fornecedor de serviço ou produto.

Cabe ressaltar que se o dado já tiver sido anonimizado pelo controlador, o direito à portabilidade não poderá ser aplicado, pois para a Lei, é mais benéfico ao titular que o dado permaneça anônimo do que transferido a um outro controlador.

5.6 Eliminação de dados

Diferente do que visto anteriormente, o titular também poderá pleitear a eliminação de dados, ainda que eles não forem desnecessários, pois envolve o seu consentimento. Como um

requisito para o tratamento de dados é o consentimento do titular, o mesmo tem o direito de retirá-lo, assim, sem o consentimento, o tratamento acaba se tornando irregular, por isso o titular poderá requerer a eliminação desses dados.

Porém, o art. 16 aponta uma exceção para a eliminação dos dados, fenômeno esse que acontece quando é prevista a autorização da conservação dos dados após o término de sua finalidade, se fortuitamente houver obrigações legais ou regulatória a serem cumpridas pelo controlador, no caso de estudo por órgão de pesquisa ou ainda se ocorrerá uma transferência a terceiro e uso exclusivo do controlador após a anonimização.

5.7 Informação das entidades públicas e privadas com as quais o controlador compartilhou os dados

Derivado diretamente do princípio da transparência, esse direito visa atender à necessidade do titular, onde após permitir o compartilhamento nos termos da lei, em se informar pra quais entidades, sejam elas públicas ou privadas, o controlador realizou este compartilhamento, não sendo facultativo ao controlador a omissão dos entes ao qual foram compartilhados os dados. Vale salientar os casos de segredos comerciais e industriais, hipóteses essas que excluem este direito.

5.8 Informação sobre a possibilidade de não fornecer consentimento

Este direito também é atribuído ao princípio da transparência, pois é garantido ao titular a alternativa de saber, que poderá fornecer ou não, o consentimento para o tratamento de dados, e derivado disso, quais as possíveis consequências deste consentimento ou de sua recusa.

Desta forma, caso essa informação não tenha sido demonstrada, o titular possui o direito de solicitar ao controlador o esclarecimento, de uma maneira expressa, explicita e clara.

5.9 Revogação do consentimento

Enfim, o último direito do art. 18 assegura ao titular que, a qualquer momento, o consentimento poderá ser revogado, mediante sua manifestação de maneira expressa, sendo este requerimento gratuito e facilitado.

Como dito anteriormente, o consentimento é um dos fatores primordiais para o início e continuação do tratamento de dados, tendo em vista que com sua recusa, o tratamento poderá se tornar irregular se o consentimento for o único requisito para a finalidade do tratamento.

O fator interessante deste direito, é a questão temporal irrelevante, ou seja, o consentimento poderá ser revogado até mesmo no instante seguinte ao fornecimento mesmo, estabelecendo assim, que o tratamento dos dados deve cessar imediatamente, salvo se outra base legal fosse cumulada com o consentimento à finalidade do tratamento.

Convém memorar que uma possível alteração das finalidades do tratamento sempre deverá ser comunicada ao titular, que por sua vez, tem a escolha de manter o consentimento ou revoga-lo.

6 RESPONSABILIDADE CIVIL

A responsabilidade civil manifesta-se quando há uma violação de uma norma jurídica preexistente, podendo ela ser contratual (violação de normas pré-acordadas, nos termos dos arts. 389 e seguintes do Código Civil) ou extracontratual (ato ilícito ou abuso de um direito, nos termos do art. 186 e seguintes do Código Civil).

Com um direito violado, o ofendido poderá requerer uma indenização por parte do infrator que violou o direito, seja ela ocorrendo de cunho patrimonial ou moral.

O art. 42 da LGPD trata sobre a responsabilidade civil, onde o controlador ou o operador, em razão do tratamento de dados pessoais, causar dano patrimonial, moral, individual ou coletivo é obrigado a repará-lo.

Observamos que o *caput* do artigo em questão, não menciona a necessidade de comprovação de culpa, configurando responsabilidade civil objetiva, devendo assim o ofendido comprovar apenas o nexo causal entre o dano e o ato ilícito, além da inexistência de alguma das causas excludentes de ilicitudes previstas no art. 43.

As causas excludentes de ilicitudes ocorrerão quando os agentes de tratamento provarem que não realizaram o tratamento de dados pessoais que fora atribuído, que embora tenham realizado o tratamento de dados pessoais que lhe fora atribuído, não houve violação à LGPD ou que o dano seja decorrente de culpa exclusiva do titular do dado ou de terceiros.

A LGPD apresenta duas hipóteses de responsabilidade solidária, estas previstas nos incisos I e II do §1º do art. 42, onde afirmam que o operador responderá solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da própria LGPD ou quando não tiver seguidos as instruções licitas do controlador, salvo nos casos de exclusão de ilicitude previstos no art. 43, e a outra hipótese é de que os controladores que estiverem

diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados, responderão solidariamente, salvo também, os casos do art. 43 mencionados anteriormente.

No tocante à inversão do ônus da prova, o legislador considera que o titular se encontra em desvantagem diante dos controladores e operadores, motivo esse que levou a LGDP prever a inversão do ônus da prova no tocante ao tratamento de dados pessoais, desde que a alegação do titular possua indícios de verdade e de que haja hipossuficiência para a produção da prova, ou na onerosidade da mesma.

Cabe ainda ressaltar que, em seu art. 45, a LGDP prevê que qualquer hipótese de violação de direito do titular, no âmbito das relações de consumo, as regras de responsabilidade permanecem sujeitas ao Código de Defesa do Consumidor.

7 FISCALIZAÇÃO

Nos textos finais da LGPD, adicionada pela lei 13.853/2019, há a criação da ANPD (Autoridade Nacional de Proteção de Dados), autoridade esta que, resumidamente deverá zelar, implementar e fiscalizar o cumprimento da LGPD.

A ANPD é vinculada à Presidência da República, ou seja, trata-se de um órgão da Administração direta, não possuindo autonomia administrativa nem personalidade jurídica própria, devendo observar as diretrizes da União. Cabe ainda ressaltar que, a ANPD será sujeita a obedecer ao art. 37 da Constituição Federal de 1988, devendo respeitar os princípios da legalidade, impessoalidade, moralidade, publicidade e eficiência.

As competências da ANPD estão previstas nos incisos do art. 55-J, onde podemos destacar as atribuições de maior notoriedade que são, zelar pela proteção de dados pessoais, editar normas e procedimentos sobre a proteção de dados pessoais, deliberar na esfera administrativa sobre a interpretação da LGPD, suas competências e casos omissos, e fiscalizar e aplicar as sanções, na hipótese de tratamentos de dados que descumpram a legislação.

As sanções administrativas estão previstas no art. 52, e podem variar entre uma simples advertência, exclusão de dados e multas.

A sanção de advertência é a mais branda, pois funciona apenas como um aviso ao infrator, ganhando o mesmo uma oportunidade de corrigir a irregularidade, devendo a autoridade indicar o prazo para a regularização. A advertência poderá ser via oral ou escrita.

A multa simples é a sanção administrativa pecuniária onde será arbitrada até o limite de 2% do faturamento da pessoa jurídica infratora, tendo como base seu ultimo exercício financeiro, não excedendo a quantia de R$50.000.000,00 por infração, ou seja, se houver mais

de uma infração, será aplicada a multa individualmente para cada uma delas, podendo assim, se somadas superar a quantia de R$50.000.000,00.

A multa diária é a sanção administrativa pecuniária a ser determinada por dia, enquanto durar a infração, devendo ser respeitado os valores e base de cálculo da multa simples anteriormente citados.

A publicização da obrigação é a divulgação da infração cometida ao público, tanto para fins de sanção ao infrator, tanto quanto para informar os interessados do ocorrido. Há uma falha na LGPD, pois a mesma não regulou quem deverá fazer o anúncio. Vale ressaltar que, tal medida deverá ocorrer somente após a confirmação da autoria e materialidade da infração.

Poderá também como sanção o bloqueio e exclusão de dados, onde, respectivamente há uma suspensão temporária do tratamento de dados mediante guarda do dado pessoal ou banco de dados sobre o dado pessoal relacionado com a infração e, a eliminação em caráter definitivo, incidente apenas também, nos dados relacionados com a infração.

O §1º do art. 52 define os parâmetros e critérios para nortear a aplicação das sanções, fatores estes que são, gravidade do ocorrido, ausência de boa-fé, vantagem auferida ou pretendida, condição econômica do infrator, reincidência, nível de cooperação do infrator e a proporcionalidade.

8 SEGURANÇA E BOAS PRÁTICAS

A LGPD estabelece em seus arts. 46 a 49 parâmetros mínimos de segurança e boas práticas relacionadas às atividades de tratamento de dado, enaltecendo os princípios da segurança e da prevenção.

Os agentes de tratamento ou qualquer outra pessoa que participar de qualquer fase do tratamento, são obrigados a adotar as mais atuais e eficientes medidas de segurança, técnicas e administrativas existentes no mercado, para proteger os dados pessoais, sejam eles de acessos não autorizados ou até mesmos de situações onde possa ocorrer uma eventual destruição, perda ou alteração do dado. A ANPD poderá dispor sobre os padrões técnicos mínimos para melhorar a aplicabilidade da segurança.

Caso aconteça um incidente de segurança que possa provocar risco ou dano relevante ao titular aconteça, o controlador imediatamente terá de comunicar a ANPD e o titular sobre o fato, informando no mínimo a descrição da natureza dos dados pessoais afetados, os titulares envolvidos, a indicação das medidas técnicas e de segurança utilizadas na proteção de dados,

os riscos relacionados ao acidente, os motivos da demora na comunicação (se houver) e as medidas que já foram ou que serão adotadas para reverter ou tranquilizar o prejuízo.

O art. 50 garante aos agentes que, individualmente ou por meio de associações poderão formular regras de boas práticas e governanças, a fim de se estabelecer toda a questão de segurança (prevenção e precaução) até a uma possível mitigação do prejuízo, relacionados com o tratamento de dados pessoais.

Cabe ainda ressaltar, que de acordo com o art. 51, a ANPD incentivará a adoção de padrões técnicos para facilitar o controle pelos titulares sobre seus dados.

CONCLUSÃO

Avaliando todo o exposto, chega-se a uma conclusão de que nós e os nossos dados estão expostos, tanto no mundo digital, e muitas das vezes nós acabamos por no expor, quanto fora dele. Parece que, vivendo nessa era digital, o cotidiano das redes sociais acabou por afrontar diretamente os direitos fundamentais contidos no art. 5º, X da Constituição Federal de 1988, como o da intimidade, privacidade e imagem das pessoas.

Esses dados expostos na rede e fora dela, estavam literalmente vagando de mão em mão, sem nenhuma regulamentação, afetando assim, muitas pessoas que estavam sendo prejudicadas pelo tratamento irregular de seus dados pessoais.

Contudo, com a criação da Lei 13.709/2018, a Lei Geral de Proteção de Dados, os direitos fundamentais podem ser novamente protegidos por esta nova ferramenta, devido a ampla abrangência da Lei, tal como os critérios para o a coleta e início do tratamento de dados, quanto as sanções de valores intensos estabelecidas.

Por fim, cabe ainda ressaltar que, mesmo com a vinda da Lei para garantir a eficácia dos direitos fundamentais, nós devemos nos salvaguardar aderindo às normas de segurança e boas práticas, pois, mesmo que o causador e o culpado pelo possível dano causado por um incidente sejam responsabilizados, a extensão do dano poderá ser minimizada caso parta do titular a utilização de todos os meios possíveis para a segurança dos dados, além de as atitudes estabelecidas para também resguardá-los. Portanto ponderemos, vale mais a inexistência de um dano para o titular, e multa alguma para os agentes, do que um dano grave ou até gravíssimo para o titular, e uma multa para os agentes.

Portanto, como ensina Rony Vainzof,

> A LGPD trará um equilíbrio entre interesses sociais e econômicos, entre o público e o privado, entre liberdade, proteção e segurança, buscando tutelar ao mesmo tempo, a proteção de dados pessoais, a dignidade da pessoa humana, a privacidade, a honra e a imagem das pessoas, assim como a livre

> iniciativa e o uso econômico dos dados, de forma legítima, séria, responsável e razoável.
> (VAINZOF, 2018).

REFERÊNCIAS

BIONI, B. R. Proteção de dados pessoais: a função e os limites do consentimento. 1 ed. Rio de Janeiro: Forense, 2019.

COTS,M.; OLIVEIRA, R. Lei geral de Proteção de dados pessoais comentada. 2 ed. São Paulo: Editora Revista dos Tribunais, 2019.

FEIGELSON, B.; SIQUEIRA, A. H. A. Comentários à Lei Geral de Proteção de Dados Lei 13.709/2018. 1 ed. São Paulo: Editora Revista dos Tribunais, 2019.

LEMOS, R. et al. Marco civil da internet jurisprudência comentada. 1 ed. São Paulo: Editora Revista dos Tribunais, 2017.

LEONARDI, M. Fundamentos de Direito Digital. 1 ed. São Paulo: Editora Revista dos Tribunais, 2019.

NETTO, Felipe Braga. Novo Manual de Responsabilidade Civil. 1 ed. Salvador: Editora JusPodivm, 2019.

OPICE BLUM, R. et al. LGPD Lei Geral de Proteção de Dados. 1 ed. São Paulo: Editora Revista dos Tribunais, 2019.

PINHEIRO, Patricia Peck. Proteção de dados pessoais comentários à LGPD: 1.ed. São Paulo: Saraiva Educação,2018.