ETIC 2018 - Encontro de Iniciação Científica
ISSN 21-76-8498

A IMPORTÂNCIA DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS NO AMBIENTE ONLINE

Joice AGOSTINELLI[1]

RESUMO: O presente estudo intitulado – "A importância da Lei Geral de Proteção de Dados Pessoais no ambiente online" - tem por objetivo identificar a relevância de uma legislação específica para conduzir a forma de tratamento de dados pessoais por pessoas jurídicas de direito público e privado dentro da esfera virtual, chamada de a rede das redes, a internet. Por meio de método dedutivo e levantamento bibliográfico analisa-se os direitos da personalidade, mais especificamente a privacidade, como a base principiológica de uma lei que visa trazer transparência e liberdade nas relações entre titular e agente de tratamento de dados. A partir das alterações trazidas pela Lei Geral de Proteção de Dados Pessoais (LGPD), não só no Marco Civil da internet, mas também em todo o ordenamento jurídico competente desta matéria, busca analisar as consequências da violação da lei, a responsabilidade das empresas e órgãos enquanto controladores de dados, as mudanças e os avanços acarretados com a aprovação da lei e acima de tudo a segurança jurídica em igual proporção aos demais países do Mercosul em relação ao tratamento e armazenamento de dados sensíveis, que demanda maior responsabilidade em razão dos potenciais danos e prejuízos causados por um possível vazamento de dados ou um tratamento irresponsável destes.

Palavras-chave: Dados Pessoais, Legislação, Direito Digital, Privacidade.

1. INTRODUÇÃO

Este artigo teve por objetivo discorrer sobre a importância de uma legislação específica sobre o armazenamento e proteção de dados pessoais na internet, visando garantir o direito à privacidade, que é assegurado pela Constituição Federal, também no ambiente virtual.

A pesquisa buscou mostrar através de levantamento bibliográfico, os reais benefícios que a Lei Geral de Proteção de Dados Pessoais (LGPD), recentemente sancionada no Brasil, deve trazer as empresas e consumidores, bem como suas consequências e o avanço que essas novas medidas proporcionam ao país.

O presente tema não somente possibilitou mensurar a segurança jurídica nas relações comerciais na internet, como também fazer um exercício de

[1] Discente do 1º ano do curso de Direito pelo Centro Universitário "Antônio Eufrásio de Toledo" de Presidente Prudente

comparação com a legislação já existente no exterior e as mudanças que as novas medidas protetivas devem ocasionar no Brasil.

O presente estudo procurou abordar a importância da responsabilidade das pessoas jurídicas de direito público e privado na hora de coletar dados pessoais, para que não seja ferido um dos braços dos direitos da personalidade que visa assegurar a dignidade da pessoa humana, sendo assim cada vez mais comum pensar em medidas que garantam a privacidade também em âmbito digital.

2. INTERNET

Para dar início ao estudo é necessário entender o que de fato é a internet, sua abrangência e seus aspectos reais, para enfim poder definir o que é um ambiente digital e delimitar o espaço virtual.

Segundo Paesani (2003) a internet pode ser encarada como um meio de comunicação que une mundialmente milhões de computadores, possibilitando acesso praticamente ilimitado de informações a qualquer tempo e local. “Sob o ponto de vista técnico, a *Internet* é uma imensa rede que liga elevado número de computadores em todo o planeta. As ligações surgem de várias maneiras: redes telefônicas, cabos e satélites.” (PAESANI, 2003, p. 27)

De acordo com os pesquisadores Evaristo e Cesar (2014), a internet apareceu pela primeira vez com a Guerra fria, na tentativa de o governo americano obter troca de informações. Isso entre as décadas de 1960 e 1970.

Naquele contexto já havia a intenção de armazenamento de dados. Conforme relata Evaristo e Cesar (2014), o governo norte americano ansiava por uma tecnologia capaz de preservar os dados ainda que sofressem um ataque nuclear.

Gonçalves (2017) explica acerca da natureza da internet, diferenciando-a das coisas imutáveis, pelo fato de ser construída por seres humanos.

> A natureza da internet é uma série de protocolos e procedimentos que foram e estão sendo criados por estudiosos, usuários, empresas e governos. Ou seja, por seres humanos. Não há lei física, química ou biológica que determinam os rumos do que é ou será a internet. Tudo é dado e construído pelos humanos. Então, nesse ponto, a natureza da internet se confunde com práticas sociais, culturais, econômicas e históricas dos seres humanos. Assim, diferentemente das regras imutáveis da Natureza, [...] a internet possui protocolos e procedimentos que se alteram constantemente, ao sabor das relações de poder existentes nas redes da internet. (GONÇALVES, 2017, p. 51)

Paesani (2003) ressalta que “[...]a rede telemática é uma oportunidade de encontro, de confronto, de troca de opiniões, de crescimento de relações interpessoais (global village), com todas as vantagens e os riscos das relações sociais.” (PAESANI, 2003, p. 27)

2.1. INTERNET NO BRASIL E SUAS CARACTERÍSTICAS

A internet chegou ao Brasil muito mais tarde e se popularizou gradativamente quando já havia sido liberada para fins comerciais.

> Inicialmente, a internet era exclusividade de grandes empresas e órgãos governamentais e interligava tão-somente universidades e centros de pesquisa. Contudo, em 1987 ocorreu sua liberação para uso comercial (o que no Brasil deu-se apenas em 1995) e a partir de 1992, com o surgimento das primeiras empresas provedoras de acesso nos Estados unidos, a internet começou a se popularizar. (SOUZA apud. ROVER, 2004, p. 22)

Com tal popularização, a internet passa a sediar praticamente todos os ramos das relações humanas. Segundo Souza (2004), a rede disponibiliza inúmeros serviços, dentre eles, o correio eletrônico (e-mails), a transferência de arquivos, bem como o acesso a base de dados.

A internet faz parte do cotidiano de milhares de pessoas e por isso fica cada vez mais difícil imaginar a vida sem ela. Como ressalta Evaristo e Cesar (2014), ela facilita a pesquisa, proporciona rapidez e menor consumo de recursos no acesso a informação.

Evaristo e Cesar (2014) destacam também a praticidade em transações financeiras e relações comerciais, quando se pretende adquirir um produto importado sem precisar fazer nenhum esforço. “Toda essa movimentação de produto, serviço e dinheiro cibernético gera facilidade na compra, pois há a praticidade de não precisar sair de casa.” (EVARISTO; CÉSAR, 2014, p. 1)

Dentre as várias funções da rede, Paesani (2003) também destaca o comércio eletrônico: “Trata-se da aplicação da internet nas atividades econômicas em contínuo crescimento.” (PAESANI, 2003, p. 28)

2.2. DADOS PESSOAIS NA INTERNET

Segundo Raminelli e Rodegheri (2016), a informática possibilitou que as informações fossem digitalizadas e armazenadas.

“As TIC permitem que uma infinidade de informações e dados sejam lançados e difundidos na web, [...] qualquer pessoa pode, [...] nela expressar opiniões, comentários, críticas e, também, inserir dados pessoais.” (RAMINELLI; RODEGHERI, 2016, p. 91)

Raminelli e Rodegheri (2016) destacam a vasta observação no ambiente online:

> [...] o grande desafio que se coloca à frente dos cidadãos é o controle dos dados pessoais que pode ser feito por empresas ou, até mesmo, pelos governos. Há possibilidade de verificação, por meio de um monitoramento online, de preferências artísticas, musicais, hábitos de vida, de viagens, operações financeiras, orientação sexual, crenças religiosas, entre outros. (RAMINELLI; RODEGHERI, 2016 p. 92)

Para obter uma melhor compreensão sobre o conceito de dados, é preciso, segundo Veiga e Rover (2004), separar em dois grandes grupos: dados públicos e privados.

De acordo com Veiga e Rover (2004), são dados públicos aqueles que não estão sob sigilo, “que são do conhecimento geral [...] como os que constam de cadastros à disposição do público e os dados registrados em cartórios e repartições públicas”. (VEIGA; ROVER, 2004, p. 32)

Já os dados privados referem-se a vida privada do indivíduo. Segundo Veiga e Rover (2004) “as informações confidenciais, sigilosas, as estritamente pessoais e que não devam cair no conhecimento público.” (VEIGA; ROVER, 2004, p.32)

> Como exemplos podemos citar os atos da vida pessoal do cidadão, hábitos de consumo, preferências no lazer, a correspondência recebida e a expedida, as ligações telefônicas, o conteúdo das mensagens eletrônicas (e-mails) recebidas e expedidas, as páginas da internet com restrição de acesso. (VEIGA; ROVER, 2004, p.32)

O art. 5º, inciso I da Lei Geral de Proteção aos Dados Pessoais (LGPD) traz a seguinte definição:

“I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável” (BRASIL, 2018)

O inciso II especifica ainda mais:

> II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. (BRASIL, 2018)

De acordo com Raminelli e Rodegheri (2016) é importante entender as classificações. "Por dados sensíveis, entende-se como os referentes à ideologia, religião ou crença, origem racial, saúde ou vida sexual." (RAMINELLI; RODEGHERI, 2016, p. 93)

Conceito confirmado na seguinte afirmação:

> A utilização de dados pessoais pelos bancos de dados, em especial os chamados "dados sensíveis", que envolvem histórico de saúde, orientação religiosa, opção sexual, histórico policial, etc., possibilita a descoberta de aspectos relevantes da intimidade dos cidadãos. (TEPEDINO, 2001; apud TOMIZAWA, 2008 p. 107)

Raminelli e Rodegheri explicam ainda que os dados não sensíveis são aqueles que não violam diretamente o princípio da igualdade. "A proteção dos dados pessoais, públicos ou privados, sensíveis ou não, está diretamente relacionada à tutela da intimidade e da vida privada dos indivíduos." (RAMINELLI; RODEGHERI, 2016, p. 94)

Segundo Pereira (2006), por ser imensurável o número de informações armazenadas na rede, é comum que dentre elas encontremos informações pessoais, que se referem a vida privada do indivíduo, que ao navegar pela internet deixará rastros. " A problemática centra-se em que tipo de informações o usuário deixou na Rede das redes, bem como onde estão e quais as condições de armazenamento delas." (PEREIRA, 2006, p. 241)

Pereira (2006) afirma que na rede não estão devidamente protegidas e resguardadas as informações pessoais de seus usuários:

> Ainda que uma empresa que possua seu sistema informático interconectado à Rede possa estar mais propensa a sofrer um ataque hacking, indiretamente, a privacidade das pessoas, vale dizer, dos internautas, encontra-se em perigo. (PEREIRA, 2006, p. 241)

Evaristo e Cesar (2014) são enfáticos ao afirmar que o controle dentro de toda essa tecnologia ainda é algo a ser buscado “principalmente para a matéria do Direito, por isso cabe a tal matéria o desafio de a regular.” (EVARISTO; CESAR, 2014, p. 2)

3. INTIMIDADE E PRIVACIDADE

A constituição Federal é clara ao tutelar a intimidade e privacidade humana, como consta no artigo 5º.

Art. 5º - X diz “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurando o direito a indenização pelo dano material ou moral decorrente de sua violação”. (BRASIL, 1988)

A privacidade é um dos direitos da personalidade também assegurada pelo código civil no artigo 21. “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.” (Código Civil, 2002)

Paesani (2003) ressalta que o direito à privacidade está fundamentado na defesa da personalidade humana. “Esse direito vem assumindo, aos poucos, maior relevo, com a expansão das novas técnicas de comunicação, que colocam o homem numa exposição permanente.” (PAESANI, 2003, p. 49)

Segundo Peck (2002) cabe ao direito equilibrar as relações de interesse comercial e privacidade que os novos veículos de comunicação geram.

> “Se por um lado cresce a cada dia o número de empresas que disputam os consumidores da internet [...] com preenchimento de formulários e cadastros, por outro lado cresce também o nível de conscientização dos consumidores quanto à possibilidade de aplicação do atual código do consumidor, que trata da matéria de utilização de informações de consumidores para fins comerciais, trazendo uma série de penalidades para quem a pratica.” (PECK, 2002, p. 37)

Para conceituar o real significado de privacidade Pereira (2006) se utiliza de uma definição lógica. “Pensamos que devemos partir do conceito que lhe dá o dicionário RAE. [...] esse dicionário a define como: “ámbito de la vida privada que se tiene derecho de proteger de cualquier intromisión” (PEREIRA, 2006, p. 125)

4. A IMPORTÂNCIA DA PROTEÇÂO DE DADOS PESSOAIS NA INTERNET

É assegurado pela constituição a confidencialidade das comunicações e isso também vale no ambiente virtual.

O artigo 5º, inciso XII da Constituição Federal diz:

> -É inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal. (BRASIL, 1988)

Partindo do princípio de que informações privadas não podem se tornar públicas, Tomizawa (2008) afirma que o setor cibernético, por ser público dificulta a obtenção de proteção jurídica e sigilo das informações.

De acordo com Tomizawa (2008), “Estão em risco os nichos mais preciosos da privacidade. Contas correntes, declarações do Imposto de Renda, números e operações dos cartões de crédito, dados do passaporte, nomes e endereços de contatos comerciais e pessoais [...]”. (TOMIZAWA, 2008, p. 107)

Acerca da importância da proteção dos dados, Dominguez (2013), afirma:

> Além da mera classificação como “informações”, deve-se lembrar de que a combinação de dados pessoais permite a obtenção de um perfil muito preciso dos interesses e atividades de um indivíduo, sendo que estes dados podem ser utilizados para fins diversos, principalmente comerciais e publicitários. Ademais, surgem outros riscos, mais preocupantes, como é o caso de roubo de identidade, para fins criminosos, ou até mesmo perda de um possível emprego, devido a buscas prévias acerca do candidato pela empresa que deseja contratar (DOMÍNGUEZ, 2013; apud RAMINELLI; RODEGHERI, 2016, p. 98)

Doneda (2014) explica que os dados pessoais, por serem utilizados em diversas atividades, como para identificar, classificar, autorizar, dentre outras, acabaram se tornando essenciais para a obtenção de autonomia e liberdade na atual Sociedade da informação.

Sobre os dados pessoais acrescenta: “[...] acabam por identificar ou mesmo representar a pessoa em uma série de circunstâncias nas quais a sua presença física não é possível [...]. São elementos centrais, portanto, da construção da identidade em nossa sociedade.” (DONEDA apud MARTINS, 2014, p. 61)

Segundo Doneda (2014), os riscos apresentados pelos processos automatizados no tocante ao tratamento de dados pessoais, são cada vez mais

perceptíveis. “Risco que se concretiza na possibilidade de exposição e utilização indevida ou abusiva de dados pessoais [...]” (DONEDA apud MARTINS, 2014, p. 61)

Doneda (2014) atenta para a necessidade de existir mecanismos que propiciem ao indivíduo um maior controle dos seus próprios dados.

> As tecnologias da informação contribuíram para que a informação pessoal se tornasse algo capaz de extrapolar a própria pessoa. A facilidade de sua coleta, ar- mazenamento e a sua utilidade para diversos fins tornou-a um bem em si, ligado à pessoa, mas capaz de ser objetivado e tratado longe e mesmo a despeito dela – não é por outro motivo que a informação pessoal é o elemento fundamental em uma série de novos modelos de negócios típicos da Sociedade da Informação. Por esse motivo a proteção de dados pessoais é tida em diversos ordenamentos jurídicos como um instrumento essencial para a proteção da pessoa humana e é considerada como um direito fundamental. (DONEDA apud MARTINS, 2014, p. 62)

Sobre tal problemática, Castro (2002) alerta para a banalização deste processo de coleta e tratamento de dados, a partir da facilidade tecnológica e por isso demanda proteção jurídica, visto a demasiada exposição desde o nascimento.

“Desde o nascimento, uma pessoa já tem seus dados inseridos em arquivos informatizados de registo civil, [...] até que, na idade adulta, seus dados passem a constar dos cadastros da receita federal [...] e muitos outros.” (CASTRO, 2002, p. 41)

Para Castro (2002) ainda é importante frisar que os dados armazenados ao decorrer das relações privadas podem ser ainda mais atrativos, pois revelam informações de consumo e comportamento que podem ser utilizados para fins nem sempre éticos e nem sempre de forma transparente, fazendo assim com que pessoas corram o risco de serem até mesmo, discriminadas devido a um fato isolado de sua vida particular.

“[..] a prática comum e crescente de coleta e tratamento de informações de caráter pessoal [...] não pode colocar em risco um direito maior de respeito a vida privada.” (CASTRO, 2002, p. 41)

Eis então o motivo da preocupação constante e a necessidade de tutela judicial:

> Por tal razão, já há algum tempo, não apenas os juristas, mas a própria sociedade, por meio de representantes lúcidos do que se costumou chamar “sociedade civil”, deram-se conta do risco representado pelo potencial maléfico dos bancos de dados de caráter pessoal, a ponto de criticar seu uso indiscriminado e pugnar pelo controle de seu funcionamento, com a

> imposição de regras claras para o seu uso transparente. (CASTRO, 2002, p. 41)

Sob a observância da necessidade real de proteção aos dados, apresenta-se no capítulo seguinte a importância da lei.

5. LEGISLAÇÂO INTERNACIONAL E AS DESVANTAGENS DA FALTA DE LEGISLAÇÃO ESPECÍFICA NO BRASIL

Segundo Castro (2002) a proteção dos dados pessoais é uma preocupação antiga tanto na américa do norte e quanto na Europa, onde se discutia e se preocupava com a transparência primeiramente do Estado e também das instituições privadas em relação ao tratamento dos dados pessoais.

"[...] em 28/1/1981, foi aprovada, pelo conselho da Europa, a Convenção n. 108, que firmou as bases principiológicas e a terminologia das atuais legislações de proteção a dados pessoais. " (CASTRO, 2002, p. 42)

Castro (2002) ainda explica que em 1995, foi aprovada uma diretiva pelo parlamento europeu para harmonizar as legislações europeias, que em seu texto inicial não consideravam o advento da internet.

De acordo com Raminelli e Rodegheri (2016), a Argentina foi o primeiro país da América Latina a editar uma lei de proteção de dados, recebendo certificação europeia em relação a segurança no tratamento das informações. "Em linhas gerais, a Lei de nº 25.326/00 estabelece direitos e deveres, cria os órgãos de supervisão de proteção de dados e estabelece sanções em caso de descumprimento." (RAMINELLI; RODEGHERI, 2016, p. 97)

Raminelli e Rodegheri (2016) salientam a necessidade de se criar uma lei específica para tutelar o direito à privacidade, que já é protegido de forma genérica pelas constituições. "A Lei nº 25.326, sancionada e promulgada no mês de outubro do ano 2000, possui o intuito de regrar o direito à privacidade no pertinente aos dados pessoais do usuário. Este direito, que se encontra inserido entre os direitos de personalidade [...]" (RAMINELLI; RODEGHERI, 2016, p. 98)

Raminelli e Rodegheri (2016) apontam para a classificação dos dados na lei argentina: "Os dados pessoais estão caracterizados na legislação argentina como "informação de qualquer tipo referida a pessoas físicas ou de existência ideal

determinadas ou determináveis" (ARGENTINA, 2000)." (RAMINELLI; RODEGHERI, 2016, p. 98)

> Por fim, em outubro de 2000, foi sancionada a Lei 25.326, conhecida por Lei de Proteção de Dados Pessoais, sendo seu decreto promulgado em novembro de 2001. Possui como objetivo fundamental a proteção total de dados pessoais de bancos públicos ou privados destinados a fornecer informação16, com o fim de garantir o direito à honra e à intimidade das pessoas, consoante o art. 43 da Constituição Nacional da República Argentina (DELPECH, 2004, apud RAMINELLI: RODEGHERI, 2016, p.99).

O senador Ricardo Ferraço, relator da Comissão de Assuntos econômicos (CAE) que fez alguns ajustes de redação no projeto de Lei que regulamenta o tratamento de dados no Brasil, diz que: "Até mesmo na América do sul e no Mercosul todos os países já contavam com lei que protege a intimidade [...], estabelecendo regras, limites, diretrizes, responsabilidades e penalidades objetivas e solidárias." (SENADO, 2018)

Segundo Ferraço (2018) a implementação dessa lei vai colocar o individuo efetivamente no controle de seus dados e retirar o Brasil de uma desvantagem. "O Brasil perde oportunidades de investimento financeiro internacional em razão do "isolamento jurídico" por não dispor de uma lei geral de proteção de dados pessoais." (SENADO, 2018)

6. MATÉRIA DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Visando fortalecer a proteção das informações pessoais e a transparência na forma de tratamento e armazenamento de dados, foi sancionada parcialmente, isto é, com alguns vetos, pelo Presidente da República Michel Temer, no dia 14 de agosto de 2018, a lei Nº 13.709, Lei Geral de Proteção de Dados Pessoais (LGPD).

A nova legislação contém ao todo 65 artigos. Em seu primeiro artigo, a lei dispõe seu objetivo geral:

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. (BRASIL, 2018)

Logo em seguida em seu segundo artigo, traz os fundamentos a respeito da proteção de dados, sendo a privacidade, o primeiro deles.

> 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. (BRASIL, 2018)

Em seu artigo terceiro e quarto, a matéria trata de informar a quem e quando a lei deve ser aplicada e suas exceções.

> Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:
> I - a operação de tratamento seja realizada no território nacional;
> II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional;
> III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional. (BRASIL, 2018)

É em seu artigo 4º que a lei expõe as exceções, deixando claro que não é aplicável para fins exclusivamente particulares e não econômicos, nem para fins jornalísticos, artísticos ou acadêmicos, sendo este último, tratado nos artigos 7º e 11º.

O inciso III também traz hipóteses onde esta lei não se aplica, ficando sobre o tratamento de lei específica em casos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais, como é explicado no parágrafo 1º do inciso IV.

> § 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei. (BRASIL, 2018)

O artigo 5º da presente lei estudada traz as definições de termos importantes da matéria. Tendo sido o inciso I e II já mencionados no capítulo 2.2 deste estudo. Os outros termos se apresentam nos incisos seguintes. É importante destacar

os incisos X e XII, cuja, as definições expostas traz mais compreensão sobre o tema abordado. A respeito do tratamento dos dados a lei define:

> X - tratamento: 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; (BRASIL, 2018)

Sobre a autorização, essencial para a transparência tão almejada, o inciso XII explica:

"XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;" (BRASIL, 2018)

A finalidade, portanto, é o primeiro princípio a ser exposto no artigo seguinte da lei.

Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

"I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;" (BRASIL, 2018)

Os incisos seguintes do artigo 6º trazem as definições de adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas, todos estes, princípios norteados pela boa fé do titular dos dados.

No capítulo II da atual legislação é abordado o tratamento dos dados, sendo que para isso, o controlador ou operador dos dados deve seguir alguns requisitos expostos no artigo 7º, sendo o primeiro deles, o consentimento que vem em conformidade com a liberdade do titular de fornecer ou não.

"Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

I - mediante o fornecimento de consentimento pelo titular;" (BRASIL, 2018)

Consentimento este, que deve ser documentado de forma clara e explícita como aborda o artigo seguinte.

"Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular." (BRASIL, 2018)

O parágrafo 5º ainda expõe a possibilidade do titular revogar o consentimento:

> § 5º O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei. (BRASIL, 2018)

Os artigos 9º e 10º trazem respectivamente os direitos do titular e os limites do controlador. O primeiro baseando-se no princípio do livre acesso, garantindo assim ao titular o direito de conhecer a:

> I - finalidade específica do tratamento;
> II - forma e duração do tratamento, observados os segredos comercial e industrial;
> III - identificação do controlador;
> IV - informações de contato do controlador;
> V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade;
> VI - responsabilidades dos agentes que realizarão o tratamento; e
> VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei. (BRASIL, 2018)

Os parágrafos 1º e 2º do artigo 9º, explicam sobre o requerimento de consentimento ao titular, na primeira hipótese, se as informações fornecidas ao titular forem abusivas ou enganosas, o consentimento pode ser considerado nulo, e na segunda hipótese, se houver mudanças na finalidade dos tratamentos dos dados, o titular deve ser informado e este pode revogar o consentimento caso não aprove a alteração.

> § 1º Na hipótese em que o consentimento é requerido, esse será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca.
> § 2º Na hipótese em que o consentimento é requerido, se houver mudanças da finalidade para o tratamento de dados pessoais não compatíveis com o consentimento original, o controlador deverá informar previamente o titular sobre as mudanças de finalidade, podendo o titular revogar o consentimento, caso discorde das alterações. (BRASIL, 2018)

A legislação preocupou-se em delimitar o uso dos dados pessoais sensíveis possibilitando apenas quando houver autorização expressa do titular ou em casos específicos quando for indispensável, como explica o artigo 11.

> 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; (BRASIL, 2018)

O inciso II trata das hipóteses sem o fornecimento de autorização, indispensáveis como, obrigação legal, proteção a vida, tutela da saúde, etc. E o parágrafo 1º reforça:

"§ 1º Aplica-se o disposto neste artigo a qualquer tratamento de dados pessoais que revele dados pessoais sensíveis e que possa causar dano ao titular, ressalvado o disposto em legislação específica." (BRASIL, 2018)

Os artigos 12 e 13 explanam sobre os dados anonimizados e os utilizados em pesquisas de saúde pública, que também devem incluir anonimização ou pseudonimização dos dados. O inciso III do artigo 5º traz o conceito:

"III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;" (BRASIL, 2018)

O tratamento dos dados pessoais de crianças e adolescentes também estão especificados na lei, nos seis parágrafos do artigo 14.

"§ 1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal." (BRASIL, 2018)

Já o parágrafo 4º é claro ao proibir o condicionamento desses dados a menos que seja extremamente necessário.

> § 4º Os controladores não deverão condicionar a participação dos titulares de que trata o § 1º deste artigo em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade. (BRASIL, 2018)

O tratamento de dados deve ocorrer por um período específico, sendo assim, o legislador determina nos artigos 15 e 16 quando é chegado ao fim este processo e a necessidade de eliminar os dados após o término de seu tratamento.

No capítulo III, os artigos 17 até o 22 tratam dos direitos dos titulares.

"Art. 17. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei." (BRASIL, 2018)

São nos artigos 21 e 22 que percebemos com clareza a proteção dos dados com tutela jurídica em defesa de possíveis prejuízos ao seu titular.

> Art. 21. Os dados pessoais referentes ao exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo.
> Art. 22. A defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual ou coletivamente, na forma do disposto na legislação pertinente, acerca dos instrumentos de tutela individual e coletiva. (BRASIL, 2018)

O capítulo IV é destinado ao tratamento de dados pessoais pelo poder público. Utilizando-se dos artigos 23 até o 30 para explanar sob que forma deve ser conduzido o tratamento de dados por pessoas jurídicas de direito público, estando estes também sob o domínio desta lei, como expõe o artigo 26.

> Art. 26. O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei. (BRASIL, 2018)

A transferência internacional de dados também é controlada no capítulo V, artigos 33 ao 36, exigindo garantia por parte do controlador do devido cumprimento dos princípios desta lei para proteção de dados previsto.

> Art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos:
> I - para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei;
> II - quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei [...] (BRASIL, 2018)

O capítulo VI foi dividido em três seções, a primeira delas aponta os deveres do controlador e do operador no manuseio dos dados, as funções do encarregado pelo tratamento de dados estão especificadas na seção II, enquanto a

seção III traz os deveres de responsabilidade e ressarcimento de danos, como explicita o artigo 42.

> Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo. (BRASIL, 2018)

O operador e o controlador que estiverem diretamente envolvidos no tratamento de dados devem responder pelos danos causados para assegurar a efetiva indenização do titular prejudicado. Salvo as exceções dispostas na lei.

> Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem:
> I - que não realizaram o tratamento de dados pessoais que lhes é atribuído;
> II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou
> III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro. (BRASIL, 2018)

Neste artigo percebe-se que o ônus da prova foi invertido como previsto no parágrafo 2º do art. 42.

> § 2º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa. (BRASIL, 2018)

É no capítulo VII que são abordadas as medidas de segurança que devem ser tomadas e as boas práticas para manter o sigilo e a proteção almejada. Assim explicam os seguintes artigos:

> Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.
> Art. 47. Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término.
> Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. (BRASIL, 2018)

Essa comunicação deve ser feita dentro de um prazo razoável e conter a natureza dos dados, informações dos titulares envolvidos, as medidas de segurança utilizadas, os riscos relacionados ao incidente, motivos da demora, se houver, e os procedimentos adotados para reverter os efeitos e prejuízos, conforme prevê o parágrafo 1º do art. 48.

Já o artigo 50 cuida das boas práticas e da governança.

> Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais. (BRASIL, 2018)

O parágrafo 3º do art. 50 ainda traz a necessidade de publicação e atualização periódica das boas práticas.

"§ 3º As regras de boas práticas e de governança deverão ser publicadas e atualizadas periodicamente e poderão ser reconhecidas e divulgadas pela autoridade nacional." (BRASIL, 2018)

A atual legislação apresenta a existência de estímulo por parte da autoridade nacional para que os titulares adotem padrões que facilitem o controle de seus dados, assim disposto no artigo 50.

"Art. 51. A autoridade nacional estimulará a adoção de padrões técnicos que facilitem o controle pelos titulares dos seus dados pessoais." (BRASIL, 2018)

Para a efetiva funcionalidade de uma lei que tem por objetivo tutelar judicialmente o tratamento dos dados pessoais, é sem dúvida necessário a aplicação de sanções administrativas, que são identificadas no capítulo VIII que trata da fiscalização.

> 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; (BRASIL, 2018)

Para a aplicação das sanções serão analisados critérios como a gravidade, a boa fé ou a vantagem pretendida pelo infrator, a condição econômica deste, a reincidência, o grau do dano, entre outros dispostos nos 11 incisos do parágrafo 1º.

Para o cálculo do valor da multa serão disponibilizadas as metodologias definidas pala autoridade nacional.

> Art. 53. A autoridade nacional definirá, por meio de regulamento próprio sobre sanções administrativas a infrações a esta Lei, que deverá ser objeto de consulta pública, as metodologias que orientarão o cálculo do valor-base das sanções de multa. (BRASIL, 2018)

O capítulo IX teve seus artigos vetados e o capítulo X trouxe então as disposições finais e transitórias. A lei 13.709 altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet) e seu artigo 60 traz a matéria alterada.

Art. 60. A Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet), passa a vigorar com as seguintes alterações:

> Art. 7º
> X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei e na que dispõe sobre a proteção de dados pessoais;" (NR)
> Art. 16.
> II - de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular, exceto nas hipóteses previstas na Lei que dispõe sobre a proteção de dados pessoais." (NR). (BRASIL, 2018)

A lei sancionada deve entrar em vigor 18 meses após a data de sua publicação, sendo assim, a adequação dos bancos de dados devera acontecer gradualmente. Assim prevendo o seguinte artigo:

> Art. 63. A autoridade nacional estabelecerá normas sobre a adequação progressiva de bancos de dados constituídos até a data de entrada em vigor desta Lei, consideradas a complexidade das operações de tratamento e a natureza dos dados. (BRASIL, 2018)

Nada do que foi exposto nesta lei, será objeto de exclusão de outros direitos garantidos pelo ordenamento jurídico.

“Art. 64. Os direitos e princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte.” (BRASIL, 2018)

E para concluir a matéria é estipulado o período de vacância como já mencionado. “Art. 65. Esta Lei entra em vigor após decorridos 18 (dezoito) meses de sua publicação oficial.” (BRASIL, 2018)

7. CONCLUSÃO

Visto o quanto o controle dos dados pessoais, principalmente os dados sensíveis são preciosos para o seu titular, tendo este, o direito de poupar que suas informações sejam utilizadas de maneira que possa lhe causar danos ou prejuízo, baseado no princípio da dignidade da pessoa humana, é possível constatar que o tratamento destes dados por pessoas jurídicas de direito público e privado merecem regulamentação específica que norteie e limite a atuação de controladores e operadores.

Por ser ampla e vasta a dimensão do ambiente virtual, se configura ainda mais difícil o controle dos dados na internet, onde muitas vezes, são vazadas informações de bancos de dados, o que traz bastante insegurança ao titular em relação ao rumo que será destinado a essas informações de caráter pessoal, íntimo e privado.

Sendo assim, após sancionada a Lei Geral de Proteção de Dados Pessoais (LGPD), foi possível observar a dinâmica adotada pelo legislador em prol da transparência, liberdade e tutela jurídica em relação aos direitos fundamentais da personalidade. Trazendo dispositivos que tornam a relação do titular com os agentes de tratamento ainda mais transparentes devendo ser esta relação revestida de boa fé.

A regulamentação do tratamento de dados coloca o Brasil em igualdade com outros países do Mercosul que já gozavam de legislação própria e elimina o problema de falta de jurisdição em determinadas circunstâncias em que dados são solicitados e não são obtidos sob o argumento de não obter lei específica.

ISSN 21-76-8498

Isso é um grande avanço para as relações não só jurídicas, mas também comercias em nosso país. A lei possibilita atribuir responsabilidade a quem realmente lhe compete e em casos de violação do cumprimento legal, são atribuídas sanções administrativas e exigência de ressarcimento e reparação do dano. Trazendo maior segurança jurídica não só ao titular dos dados mas também aos agentes controladores.

REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. **Código Civil.** - 1. ed. São Paulo: Revista dos Tribunais, 2002.

BRASIL, Constituição (1988). **Constituição da República Federativa do Brasil.** – 7. ed. – Barueri: Manole, 2015.

BRASIL. **Lei nº. 13.709, de 14 de agosto de 2018.** Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm Acesso em 19 ago 2018.

EVARISTO, Silvana Aparecida Cardoso; CESAR, Claudio Evaristo. **Direito x internet.** In: Âmbito Jurídico, Rio Grande, XVII, n. 127, ago 2014. Disponível em: <http://ambitojuridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=14255>. Acesso em 19 ago 2018.

FEDERAL, Senado. **Senado Notícias.** Disponível em: https://www12.senado.leg.br/noticias/materias/2018/07/10/projeto-de-lei-geral-de-protecao-de-dados-pessoais-e-aprovado-no-senado Acesso em 01 Set 2018.

GONÇALVES, Vitor Hugo Pereira. **Marco Civil da Internet Comentado.** São Paulo: Atlas, 2017.

MARTINS, Guilherme Magalhães. **Direito Privado e Internet.** São Paulo: Atlas, 2014.

PAESANI, Liliana Minardi. **Direito e Internet.** São Paulo: Atlas, 2003.

PECK, Patrícia. **Direito Digital.** São Paulo: Saraiva, 2002.

PEREIRA, Marcelo Cardoso. **Direito à Intimidade na Internet**. Curitiba: Juruá Editora, 2006.

RAMINELLI, Francieli Puntel; RODEGHERI, Letícia Bodanese. **A Proteção de Dados Pessoais na Internet no Brasil:** Análise de decisões proferidas pelo Supremo tribunal Federal. In: Revista Cadernos do Programa de Pós-Graduação em Direito PPGDir./UFRGS. Disponível em: http://seer.ufrgs.br/ppgdir/article/view/61960/39936 Acesso em 22 ago 2018

ISSN 21-76-8498

ROVER, Aires José. **Direito e Informática.** São Paulo: Manole, 2004.

TOMIZAWA, Guilherme. **A invasão de Privacidade Através da Internet**. Curitiba: J.M. livraria jurídica, 2008.