

UNILEÃO  
CENTRO UNIVERSITÁRIO DOUTOR LEÃO SAMPAIO  
CURSO DE GRADUAÇÃO EM DIREITO

MYLENA GOMES RODRIGUES

**A PROTEÇÃO DE DADOS PESSOAIS E OS INCENTIVOS REGULATÓRIOS  
NO BRASIL COM ENFOQUE NO DIREITO À PRIVACIDADE**

JUAZEIRO DO NORTE-CE

2021

MYLENA GOMES RODRIGUES

**A PROTEÇÃO DE DADOS PESSOAIS E OS INCENTIVOS REGULATÓRIOS  
NO BRASIL COM ENFOQUE NO DIREITO À PRIVACIDADE**

Trabalho de Conclusão de Curso – *Artigo Científico*,  
apresentado à Coordenação do Curso de Graduação em  
Direito do Centro Universitário Doutor Leão Sampaio, em  
cumprimento às exigências para a obtenção do grau de  
Bacharel.

**Orientador:** Christiano Siebra Felício Calou

JUAZEIRO DO NORTE-CE

2021

MYLENA GOMES RODRIGUES

**A PROTEÇÃO DE DADOS PESSOAIS E OS INCENTIVOS REGULATÓRIOS  
NO BRASIL COM ENFOQUE NO DIREITO À PRIVACIDADE**

Este exemplar corresponde à redação final aprovada do Trabalho de Conclusão de Curso de Mylena Gomes Rodrigues.

Data da Apresentação \_\_\_\_/\_\_\_\_/\_\_\_\_

**BANCA EXAMINADORA**

Orientador: Me. Christiano Siebra Felício Calou

Membro: Esp. Alyne Andrelyna Lima Rocha Calou

Membro: Me. Otto Rodrigo Cruz

**JUAZEIRO DO NORTE-CE**

2021

# A PROTEÇÃO DE DADOS PESSOAIS E OS INCENTIVOS REGULATÓRIOS NO BRASIL COM ENFOQUE NO DIREITO À PRIVACIDADE

Mylena Gomes Rodrigues<sup>1</sup>  
Christiano Siebra Felício Calou<sup>2</sup>

## RESUMO

A presente pesquisa se dedica ao estudo sobre a proteção de dados pessoais e os incentivos regulatórios no Brasil com enfoque no direito à privacidade. O objetivo geral da pesquisa é: estudar o sistema jurídico normativo do processo de regulação da proteção de dados no Brasil como elemento fundamental ao alcance da privacidade. Os objetivos específicos são: Investigar o contexto histórico e constitucional da privacidade e sua proteção jurídica no Brasil; avaliar o nível de *enforcement* da LGPD para efetividade do controle sobre os dados sensíveis com vistas à proteção da privacidade; discutir os requisitos necessários para o processo de implementação de um programa de governança em privacidade. A metodologia utilizada é do tipo básica, qualitativa, de caráter exploratório-explicativa e bibliográfica-documental. Como resultados obtidos constata-se que embora seja de grande utilidade a proteção de dados no âmbito do interesse do consumidor, vem sendo uma grande mudança de caráter burocrático em face das adaptações que as empresas precisam realizar para se adequarem à nova realidade.

**Palavras Chave:** Lei Geral de Proteção de dados. Privacidade. Empresas

## ABSTRACT

This research is dedicated to the study of personal data protection and regulatory incentives in Brazil with a focus on the right to privacy. The general objective of the research is: to study the normative legal system of the data protection regulation process in Brazil as a fundamental element to achieve privacy. The specific objectives are: Investigate the historical and constitutional context of privacy and its legal protection in Brazil; evaluate the level of enforcement of the LGPD for effectiveness of control over sensitive data with a view to privacy protection; discuss the requirements necessary for the process of implementing a privacy governance program. The methodology used is basic, qualitative, exploratory-exploratory and bibliographic-documentary. The results obtained show that although data protection is very useful in the consumer's interest, it has been a great bureaucratic change due to the adaptations that companies need to make in order to adapt to the new reality.

**Keywords:** General Data Protection Law. Privacy. Companies

## 1 INTRODUÇÃO

---

<sup>1</sup> Graduanda do Curso de Direito do Centro Universitário Dr. Leão Sampaio/Unileão/  
mylenagrodriques44@gmail.com

<sup>2</sup> Professor Orientador do Centro Universitário Dr. Leão Sampaio/Unileão

A presente proposta de pesquisa tem como problema: “Quais os incentivos regulatórios advindos da lei geral de proteção de dados capazes de estimular as empresas a assegurarem a efetiva proteção dos dados pessoais?”.

Na atual economia digital, as informações pessoais estão progressivamente mais vulneráveis a ataques, principalmente no cadastro de redes sociais e organizações operacionais virtuais. As restrições de terceiros no acesso a dados pessoais geralmente dependem dos usuários, mas as empresas que possuem redes sociais têm um impacto considerável na manutenção da segurança dos detentores de informações. Em outros termos, perante da nova era digital e das preocupações com a proteção de dados pessoais, é essencial que as empresas se adaptem às disposições legais da Lei Geral de Proteção de Dados e tomem medidas para proteger o processamento de dados pessoais.

É importante frisar que, são poucas as contribuições no ambiente acadêmico sobre a necessidade de que as empresas se adaptem à Lei Geral de Proteção de Dados, tal qual os meios por quais elas consigam executar na prática essa adaptação. Destarte, além da explanação teórica, é essencial que haja incentivos regulatórios provenientes da LGPD, que sejam capazes de estimular as empresas a assegurarem a efetiva proteção dos dados pessoais.

Para o desenrolamento da pesquisa foram escolhidos os objetivos de pesquisa subsequentes: o geral que é estudar o sistema jurídico normativo do processo de regulação da proteção de dados no Brasil como elemento fundamental ao alcance da privacidade. E os específicos que são investigar o contexto histórico e constitucional da privacidade e sua proteção jurídica no Brasil; avaliar o nível de *enforcement* da LGPD para efetividade do controle sobre os dados sensíveis com vistas à proteção da privacidade; discutir os requisitos necessários para o processo de implementação de um programa de governança em privacidade.

No Brasil, a Lei Nº13.709/2018 (Lei Geral de Proteção de Dados Pessoais), mais conhecida como LGPD, ostentou inúmeras mudanças no ordenamento jurídico brasileiro, em harmonia com a mobilidade global de proteção de dados pessoais. Porém, há a necessidade de que seja discutido requisitos indispensáveis para que haja um processo de implementação de um programa de governança em privacidade.

A referida lei alterou, completamente, a maneira com as empresas que trabalhavam com dados de consumidores e como lidavam com essas informações. Deste modo, é importante que se tenha conhecimento sobre quais são os incentivos regulatórios, provenientes da LGPD, que sejam capazes de assegurar uma verdadeira proteção dos dados pessoais, visando uma maior segurança ao princípio da privacidade.

Isto posto, em conformidade com as informações relatadas neste primeiro tópico do

projeto, em relação aos procedimentos, a pesquisa em análise é bibliográfica-documental. “A pesquisa bibliográfica é feita a partir do levantamento de referências teóricas já analisadas, e publicadas por meios escritos e eletrônicos, como livros, artigos científicos, páginas de web sites.” (FONSECA, 2002, p. 32).

“A pesquisa documental recorre a fontes mais diversificadas e dispersas, sem tratamento analítico, ou de dados estatísticos tais como: tabelas estatísticas, jornais, revistas, relatórios, documentos oficiais, cartas, filmes, fotografias, pinturas, tapeçarias, relatórios de empresas, vídeos de programas de televisão, etc.” (FONSECA, 2002, p. 32). Nesta lógica, o procedimento técnico citado acima se adequa a pesquisa em tela, pois os dados a serem utilizados para elaboração da mesma serão secundários, ou seja, aqueles que já foram coletados e estão presentes em revistas, artigos científicos, jornais, internet, decisões judiciais, dentre outros.

## **2 CONTEXTO HISTÓRICO E CONSTITUCIONAL DA PRIVACIDADE E SUA PROTEÇÃO JURÍDICA NO BRASIL**

A percepção da privacidade, na sua essência, não é nova. Ela podia ser vista em várias sociedades e entendida de maneiras diferentes. Arendt (2005, p. 33) elucida que “na sociedade grega a diferenciação entre o âmbito público e privado referia-se à demarcação do âmbito familiar e político, sendo o modo de ordenamento de uma e outra diferentes”. Prosseguindo em caminho à Idade Média, apesar de não haver uma constatação da individualidade que de maneira universal se goza na atualidade, logo é possível reparar o desejo de isolamento. Deste modo, a chance de ter uma vida com privacidade começa a tornar-se um costume das pessoas com condições financeiras melhores, essa maneira de se comportar acabou sendo comum dentro das famílias nobres (DONEDA, 2006).

Para mais do âmbito político e econômico, é interna a modificação da compreensão de público e privado, e se apresenta como modo de exibição da personalidade. Por outra forma, apontando Cachapuz (2006, p. 66-68), a “[...] alteração fundamental tem origem numa conceituada emancipação psicológica [...]” do sujeito perante a sociedade e, com isso, “[...] aquilo que é privado em contraposição ao que é público deixa de ser identificado por um enfoque político para ganhar força na oposição entre o social e o íntimo”. Em outras palavras, a privacidade, na maneira como é entendida na atualidade, tem como alicerce a compreensão da relação do sujeito para com a sociedade (DONEDA, 2006).

A privacidade, consegue se consumir de maneira mais forte e efetiva devido as

mudanças socioeconômicas decorrentes da revolução industrial. Por motivo de existir uma preocupação com a vida íntima e privada, surge daí então a ânsia de que houvesse um amparo sobre essa inovação que estava se construindo, e então no século XIX introduziu-se a comunicação com as primeiras características de um direito à privacidade.

Como pontapé inicial da pesquisa realizada por Warren e Brandeis (1890), o direito à privacidade como personalidade jurídica independente é mecanismo moderno. Contudo, apesar de que a percepção de privacidade não venha a ser recente, é importante frisar que Warren e Brandeis (1890), deram um incentivo para que houvesse uma valorização e foco para esse direito em formação, de maneira independente e principal.

No artigo, os escritores, mostram as funções, os limites e outros traços desse direito novo, ocasionando uma aproximação desse direito com a proteção da personalidade humana.

Com o passar do século XX, o relacionamento da sociedade e do indivíduo com os ambientes público e privado sofreram modificações consideráveis, propiciando a popularização em prol da proteção da privacidade, bem como de sua prática.

A produção massiva de dados na sociedade digital, fenômeno denominado Big Data levou a outro fenômeno chamado de *datafication*. Enquanto o *Big Data* consiste na possibilidade de obtenção de novas informações desde a manipulação de uma grande quantidade de dados, gerando ideias possuidoras de utilidade, além de agregar valor significativo a bens e serviços, a *datafication* expressa a ideia de “[...] coleta de informações de tudo o que existe” (MAYER-SCHÖNBERGER; CUKIER, 2013, p. 10) ou “[...] o registro eletrônico de um fenômeno qualquer” (AMARAL, 2016, p. 10).

Com os dados e informações sendo alçados a condição de importante ativo para as organizações modernas, “Dataficação um fenômeno é colocá-lo num formato quantificado de modo que possa ser tabulado e analisado” (MAYER-SCHÖNBERGER; CUKIER, 2013, p. 54).

Desse modo, o direito à privacidade acaba amplificando seus limites, abrangendo novas pessoas, tendo sua presença em ambientes que anteriormente não eram compatíveis. Segundo Maria Celina B. de Moraes (1998, p. 68):

No final do século XIX se percebeu a necessidade concreta de garantir proteção a uma esfera de privacidade das pessoas, e a partir daí seguiram-lhe, ao longo do século XX, os demais direitos da personalidade. Variadas são as razões apontadas para essa circunstância histórica, mas a primeira, embora controversa, é a mais interessante: teria sido a completa ausência, nas sociedades ocidentais pelo menos até fins do século XVIII, da noção de vida privada, a qual somente veio a ter origem a partir de determinada concepção de civilização.

Em 1980, foi publicado o artigo “*The Right to Privacy*”, de Samuel Warren e Lois D. Brandeis (1980), texto que inaugura a reflexão sobre a necessidade de criar instrumentos

jurídicos capazes de garantir a privacidade nesta nova era digital. No mesmo ano da publicação do referido artigo, a OCDE publicou o “*Privacy Guidelines*”, e alguns anos depois a “*Declaration on Transborder Data Flows*”, estipulando novas metas e diretrizes para a proteção global de dados pessoais.

No Brasil, ao formularem a Constituição 1988 e o Código Civil de 2002 (Lei n. 10.406/2002) não usaram a palavra privacidade, mas sim os termos “vida privada” e “intimidade”, e não apresentaram conceituação para nenhum deles. A privacidade, precisa ser percebida como algo necessário para as pessoas, como uma prática para a liberdade humana. Ter privacidade é essencial ao sujeito.

Tanto na Constituição brasileira quanto na norma infraconstitucional, o direito à privacidade é tido como um direito fundamental e direito da personalidade. Logo, conforme o artigo 5º, inciso X, da Constituição Federal de 1988: “a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação” (BRASIL, 1988).

Seguindo a corrente exposta pelos autores já citados é possível compreender que o ordenamento jurídico brasileiro necessitou progredir para que pudesse seguir o progresso das ciências tecnológicas de comunicação e informação na sociedade contemporânea, com o propósito de garantir a tutela da privacidade, a não violação da intimidade, e também a práticas de tais direitos no âmbito virtual.

Legislação para proteção de dados pessoais não é algo novo no ordenamento jurídico do Brasil e do mundo. O primeiro registro legal de proteção de dados aconteceu em 1824, na Constituição do Império, na qual se mencionava a proteção do “segredo da carta” e da “inviolabilidade da casa”. Um conceito mais voltado para a propriedade, protegendo claramente o meio físico e não seu conteúdo, mas indiretamente sendo protegido. (MACIEL, 2019).

Com o intuito de regularizar as garantias, os princípios, os direitos e deveres para o manuseio da internet no Brasil, foi criado o Marco Civil da Internet (Lei nº 12.965/14). A referida Lei nº 12.965/14, determina que a proteção dos dados pessoais, registros de conexão e matéria das vias privadas precisam se atentar a conservação da vida privada, da honra, da intimidade e da imagem das pessoas envolvidas de maneira direta e indireta (art. 10). A lei estabelece o preceito a proteção da privacidade, contudo a novidade no agrupamento de Leis brasileiras ocorreu devido a elaboração do preceito a proteção dos dados pessoais (art. 3º, inciso II e III). (BRASIL, 2014)

Mesmo que o Marco Civil da Internet tenha se tornado peça fundamental para a proteção dos dados pessoais e da comunicabilidade por meio da internet, muitos pontos ainda ficavam



irresolutos, então com a finalidade de preencher tais brechas foi legitimada a Lei no 13.709/18, nomeada “Lei Geral da Proteção de Dados Pessoais” (LGPD). A referida Lei modifica o Marco Civil da Internet e possui como princípios: O respeito à privacidade (inciso I do art. 2º), dignidade da pessoa humana (inciso VII do art. 2º), bem como a inviolabilidade da intimidade, honra e imagem (inciso IV do art. 2º). (BRASIL, 2014)

Além do mais, o art. 1º do dispositivo citado, diz: “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.”

### 3 A LEI GERAL DE PROTEÇÃO DE DADOS

Em um primeiro momento é importante frisar que a Lei Geral de Proteção de Dados surge como o principal marco regulatório de proteção de dados pessoais independentemente do meio no Brasil.

Essa lei brasileira adveio como reflexo da lei europeia *General Data Protection Regulation* da UE 2016/679 que trata da proteção de dados pessoais considera que ter direito sobre os próprios dados é a garantia para que haja a sua proteção e a efetivação de um princípio fundamental na atual economia digital, pois “todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito” (UNIÃO EUROPEIA, 2016, p. 3).

Um dos casos que gerou polêmica foi o vazamento de dados pelo Facebook em 2018, que gerou uma grande polêmica no tocante ao uso de dados pelas empresas de redes sociais, influenciando diversos países em seus ordenamentos jurídicos a criarem leis que favorecessem a proteção de dados.

O Brasil, dentre as nações integrantes do G20, foi o último país a promulgar uma Legislação específica versando sobre a proteção dos dados pessoais, com base no RGPD da União Europeia, editou no dia 14 de agosto de 2018 a Lei nº 13.709/2018, que 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. (Medida Provisória nº 869, p.1)

Os bancos de dados se tornaram uma constante, crescente e valiosa, passando os indivíduos a serem identificados pelas informações coletadas, sejam por agentes públicos ou privados. Com o aprimoramento da técnica, fez-se destas informações um ativo econômico, social e político, capaz de aumentar lucros de grandes corporações, de influenciar eleições, e

de diagnosticar problemas e soluções sociais.

Após o acontecimento as redes sociais passaram a ter todos os passos dos usuários monitorados com a finalidade de transformar em informações estratégicas no *Google Analytics* e outros mecanismos. Com a inclusão dessas informações pessoais no sistema é possível que robôs e algoritmos criem estratégias mais eficientes e personalíssimas para o perfil. Ademais o seu uso em plataformas de publicidade, os dados são relevantes para apresentar aos consumidores anúncios com mais precisão.

Sua entrada em vigor no Brasil ocorreu em 2020, embora tenha sido aprovada em 2018, na Lei 13.853/18, a MP 869 de 2018, convertida na Lei 13.853/2019, criando ANPD, mas agora como órgão da administração pública direta, assegurada autonomia técnica e decisória, mas não financeira (art.55-A e 55-B). Tendo como principal função garantir a aplicação da lei, elaborando suas diretrizes e sanções administrativas.

Danilo Doneda (2011, p. 8), expoente literato no estudo da proteção de dados no país, discorre sobre a importância e necessidade do organismo:

Outra característica é a disseminação do modelo das autoridades independentes para a atuação da lei – tanto mais necessária com a diminuição do poder de “barganha” com o indivíduo para a autorização ao processamento de seus dados, e também o surgimento de normativas conexas na forma, por exemplo, de normas específicas para alguns setores de processamento de dados (para o setor de saúde ou de crédito ao consumo). Hoje, pode-se afirmar que um tal modelo de proteção de dados pessoais é representado pelos países europeus que transcreveram para seus ordenamentos as Diretivas europeias em matéria de proteção de dados, em especial a já mencionada Diretiva 95/46/CE e a Diretiva 2000/58/CE (conhecida como Diretiva sobre privacidade e as comunicações eletrônicas.).

Passam assim as Autoridades Nacionais de Proteção de Dados, diante desta reorganização social, pautada nas interações virtuais, a tutelarem direitos e a interferirem na vida privada dos usuários, de modo que uma vez consubstanciada sua independência técnica, cria-se o desejo de refletir sobre sua legitimidade de atuação.

A legislação dispõe sobre as normas de tratamento de dados pessoais por empresas privadas, poder público ou por outras pessoas e por qualquer meio, com a finalidade clara de proteção as garantias fundamentais constitucionais de liberdade e privacidade.

Ademais, é imprescindível apresentar três definições importantes trazidas por esse dispositivo:

- 1) “Dado pessoal, como toda informação relacionada à pessoa natural identificada ou identificável.” (Art. 5º, inciso I, Lei nº 13.709/2018);
- 2) “Dado pessoal sensível, é aquele dado que advém da origem racial, 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” (Art. 5º, inciso II, Lei nº 13.709/2018);

- 3) “Tratamento, 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” (Art. 5º, inciso X, Lei nº 13.709/2018);

A Lei nº 13.709/2018 aborda em seu texto, art. 2º, os dez princípios que fundamentam a sua criação e legislação, sendo essencial para essa pesquisa o seu conhecimento. Os três primeiros princípios versam sobre a finalidade, necessidade e adequação onde os dados não podem mais atuar de forma genérica ou indeterminada as empresas devem explicitar em seu contrato para que usarão cada um dos dados pessoais e essa finalidade não poderá ser alterada no decorrer do contrato e utilizar os dados essenciais para o seu negócio e têm que ser compatíveis com a finalidade informada.

Já os princípios do livre acesso, qualidade de dados e transparência garantem ao titular o direito a consulta simples e gratuita das informações que a empresa possui a seu respeito, que estas sejam verdadeiras e exatas, não podendo de forma alguma compartilhar de forma oculta para outras empresas, mesmo que estas sejam essenciais, qualquer compartilhamento de dados deve ter a anuência do titular.

No Artigo 6º da LGPD, vêm elencados 10 princípios norteadores para aplicação da Lei em nosso ordenamento jurídico. Ao analisar os avanços legislativos referentes a proteção de dados no mundo, podemos observar que inúmeras normas procedimentais presentes no *Report of the Secretary Advisory Committee on Automated Personal Data Systems*, de 1973, foram utilizadas de forma contínua em várias legislações internacionais de proteção de dados, gerando, assim, a base do sistema europeu. Diante do exposto foi consolidado os princípios das normas de proteção de dados:

Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento; III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados; IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais; V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento; VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do

tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial; VII - segurança: utilização de medidas 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 difusão; VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas. (BRASIL, 2018)

Neste sentido, o artigo 6º, inciso VI da LGPD traz a transparência como um dos princípios que norteiam esta legislação. A transparência expressa a garantia aos titulares de informações que sejam claras, precisas e facilmente acessíveis acerca da realização do tratamento e os respectivos agentes de tratamento. Isso implica na obrigação de serem disponibilizados aos titulares, a qualquer momento, acesso livre e irrestrito aos seus dados pessoais que estão sendo objeto de tratamento pelo controlador” (FEIGELSON; SIQUEIRA: 2019, p. 37).

Neste cenário: “Na perspectiva do princípio da transparência, o art. 9º, § 1º, da LGPD estabelece que o consentimento 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.” (FEIGELSON; SIQUEIRA, 2019, p. 38).

Os princípios da segurança e prevenção garantem a responsabilidade das empresas para gerar a proteção dos dados que esta possui tomando medidas profiláticas para proteger de ataque de hackers, por exemplo. Arelado a esses dois fundamentos é importante aliar ao Princípio da não discriminação, onde o uso de dados jamais poderá ser utilizado com fins de discriminar ou promover abusos.

Por fim, apresenta o Princípio da Responsabilização e Prestação de contas como obrigação principal para as empresas apresentarem provas e evidências de todas as medidas adotadas para demonstrarem a sua boa-fé.

Toda a sua estrutura é voltada principalmente a esses princípios norteadores, bem como os conceitos apresentados, para fins de melhor entendimento do leitor, será feito no próximo tópico a explicitação dos pontos que a lei trouxe na relação empresa e titular dos dados.

#### **4 A INFLUÊNCIA DA LGPD NAS EMPRESAS E O ACESSO AOS DADOS DOS USUÁRIOS**

A Lei de Geral de Proteção de Dados (Lei nº 13.709/2018) trouxe inúmeras inovações quando se trata da proteção dos usuários diante do fornecimento dos seus dados a empresas,

principalmente as redes sociais e firmar que trabalham em meio eletrônico.

Primeiramente, é imprescindível frisar o conceito de finalidade: “realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades” (art. 6º, inciso I, Lei nº 13.709/2018).

Sendo assim, fica claro que as empresas necessitam do consentimento para determinada finalidade que têm de ser especificada para o tratamento de dados, isto é, a finalidade deverá ser demonstrada de forma clara e transparente na hora da informação passada da empresa para o cliente.

Um dos princípios da LGPD é o consentimento do titular, como vemos no artigo 5º:

Art. 5º Para os fins desta Lei, considera-se: 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)

O consentimento consiste na livre manifestação, informada e inequívoca, pela qual o titular dos dados dá seu aval para que seus dados pessoais sejam coletados para aquela finalidade específica, devendo estes serem bem claros e destacados.

Gradativamente mais comum, logo depois da entrada em vigor da lei, são os avisos em sites ou aplicativos, informando e pedindo a permissão do usuário para coletar seus dados. O consentimento é uma das partes centrais da LGPD, e é com ele que se inicia a aplicação da lei através dos atores envolvidos. Nesse sentido, Tepedino (2020, p. 292) apresenta o entendimento que:

A base legal do consentimento para o tratamento de dados do titular representa instrumento de autodeterminação e livre construção da esfera privada. Permite diferentes escolhas e configurações em ferramentas tecnológicas, o que pode ter reflexos diretos na personalidade do indivíduo. Ainda que represente figura de grande relevância nas leis de dados, o consentimento não é a única hipótese para o tratamento de dados pessoais nem é hierarquicamente superior às demais bases legais dispostas na Lei 13.709/18.

Caso ela precise ser modificada posteriormente, o usuário deverá ser informado e dar o seu consentimento novamente, como é comumente visto nos termos de política e privacidade das empresas de redes sociais, como Instagram, Facebook e Gmail. Conforme França (2014, p. 8):

Os dados das redes sociais online podem ser usados para extrair informações sobre padrões de interações interpessoais e opiniões. Esses dados podem auxiliar no entendimento de fenômenos, na previsão de um evento ou na tomada de decisões. Com a ampla adoção dessas redes, esses dados aumentaram em volume, variedade e precisam de processamento rápido, exigindo, por esse motivo, que novas abordagens no tratamento sejam empregadas. Aos dados que possuem tais características (volume, variedade e necessidade de velocidade em seu tratamento), chamamo-los de Big Data.

Frazão (2018), aborda a questão do consentimento quanto ao uso de dados dos usuários, ao afirmar que:

(...) a manifestação de vontade precisa ser (i) livre e inequívoca, (ii) formada mediante o conhecimento de todas as informações necessárias para tal, o que inclui a finalidade do tratamento de dados, e (iii) restrita às finalidades específicas e determinadas que foram informadas ao titular dos dados.

Ademais, a LGPD (Lei nº 13.709/2018) aborda em um capítulo específico os direitos voltados aos titulares dos dados, com diversas disposições que trazem algumas alterações para as empresas. Cabe atentar-se ao fato de que o consentimento se torna ainda mais qualificado, quando se pretende o tratamento de dados pessoais sensíveis (art. 11, I, Lei nº 13.709/2018) e de menores de idade, evento em que o consentimento deverá ser manifestado por um dos pais ou responsável legal pelo menor (art.14, § 1º, Lei nº 13.709/2018).

Vale frisar que, um dos principais cuidados que a empresa deverá ter é a disponibilização em um meio de acesso fácil e imediato das pessoas aos dados que o empreendedor está utilizando. MAGRANI (2014, p. 158) ao afirmar que, “malgrado tratar-se de espaços privados, os usuários não podem sujeitar-se a termos de uso abusivos que restrinjam de forma desproporcional seus direitos garantidos na Constituição Federal de 1988.”

Estas informações devem ser explícitas de forma eletrônica e até mesmo impressa, mas sempre de forma clara, numa linguagem acessível e simples, diante de recursos visuais, auditivos e qualquer outro que for considerado necessário levando em consideração as características personalíssimas de cada usuário, sejam estas motoras, sensoriais e mentais:

A LGPD reconhece que, para que o cidadão seja capaz de controlar o fluxo de seus dados pessoais, é necessário lhe atribuir certos direitos subjetivos em face daqueles responsáveis pelo controle de tais dados (FEIGELSON; SIQUEIRA, 2019, p. 120)

O titular dos dados pode editar, torna-los anônimos e até mesmo excluir quando quiser, saber se foram compartilhados, com quem e portar para outra firma responsável. Segundo Torres (2009, p. 24):

Novas tecnologias e aplicações, como os blogs, as ferramentas de busca, os fóruns, as redes sociais e tantas outras aplicações on-line foram utilizadas pelos internautas para, literalmente, assumir o controle, a produção e o consumo da informação, atividades antes restritas aos grandes portais.

A LGPD aborda outras definições de responsabilidade voltadas aos agentes de tratamentos de dados, que tem como finalidade garantir a aplicação da lei nas empresas e principalmente a proteção dos dados dos usuários.

Até chegar aos clientes existem três tipos de agentes de processamento de dados. O primeiro é conhecido como controlador, uma pessoa física ou jurídica que toma as providências sobre o procedimento dos dados pessoais. Existe também, o operador que é quem executa o

processamento dos dados perante as decisões e orientações do controlador. Em suma, as empresas devem nomear um encarregado que faz uma espécie de “ponte” entre o controlador e os titulares dos dados e a Autoridade Nacional de Proteção de Dados, ou seja, quem gerencia o tratamento dos dados na empresa.

Segundo a legislação em tela, as empresas deverão proporcionar medidas de segurança para proteção de dados pessoais diante de possíveis invasões no sistema, destruição, perda e alterações. Se por ventura vier a acontecer algum incidente o responsável a comunicação a autoridade nacional e aos usuários afetados será do controlador, este deverá informar os riscos que estão relacionados, quais seriam as medidas necessárias para reverter todo e qualquer prejuízo, podendo ser comunicado a mídia em casos de grande repercussão.

A obrigatoriedade de prestação de contas sobre as medidas de segurança de dados é uma das mudanças obrigatórias da LGPD. Onde a Autoridade Nacional de Proteção de Dados pessoais vem a solicitar aos controladores da empresa um relatório de impacto a proteção de dados pessoais. Esse documento deve listar a descrição dos processos de tratamento de dados pessoais. A essa prestação de conta nomeamos de *Accountability*.

#### **4 CONSIDERAÇÕES FINAIS**

Conforme exposto durante o trabalho ficou evidente que as situações que envolvem questões relacionadas as empresas, segurança, créditos, redes sociais, informações e até mesmo os rumos de um Estado Democrático de Direito dependem, paulatinamente mais, do uso contínuo de dados pessoais e de processos totalmente automatizados de tomar decisões que podem ter impactos diretos nas nossas vidas, inclusive podendo nos sujeitar a práticas abusivas com o mal-uso dos dados.

Para que se possa evitar e coibir que ocorra violações de tais liberdades e direitos fundamentais, é preciso compreender como funcionam os processos de colheita de dados, que vai da anuência do usuário até o uso desses dados pelas empresas.

Logo, diante dessas inovações e acesso de dados pessoais no espaço virtual e suas consequências, considerou-se necessária a elaboração de legislações específicas sobre o tema. Legislação essa conhecida como Lei Geral de Proteção de Dados, Lei nº 13.709/201.

Para as empresas privadas, transformou-se em um novo desafio o manuseio dos dados dos titulares. Para solucionar tal problemática, as empresas levaram mais a sério as funções dos Termos de Uso e Políticas de Privacidade, que informam sobre a utilização dos dados pessoais

de forma clara, servindo também para demonstrar os objetivos da empresa na manipulação dos dados pessoais dos usuários, sendo crucial a importância do consentimento do titular dos dados.

Para os titulares dos dados a lei contribui para garantir que não haja espalhamento de dados, ou que sejam utilizados de forma indevida garantindo neste mundo progressivamente mais digital a segurança devida aos documentos, nomes, números de conta fornecidos pelos clientes.

Por fim, diante das alterações da LGPD, é evidente que houve uma revolução no que diz respeito a distribuição de dados pessoais no universo virtual, com o novo modo de ver das empresas e dos usuários garantindo proteção para estes e simultaneamente apresentando algumas dificuldades de acesso. O uso de termos de aceite, identificação em dois fatores de contas em redes sociais, contratos para regulamentando o uso de dados, aliado a esses fatores uma atualmente no Brasil, gozamos de uma legislação mais rígida diante dos crimes que punem o vazamento de dados ou fotos íntimas.

As empresas que devem se adequar a este novo cenário e consequências desta nova legislação, que como função do direito veio para acompanhar a evolução social diante das informações pessoais dispostas na internet.

## REFERÊNCIAS

ARENDDT, Hannah. **A condição humana**. Tradução de Roberto Raposo. 10. ed. Rio de Janeiro:Forense Universitária, 2005.

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. Forense, 2019, p.118.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/constituicao/constituicaocompilado.htm](http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm)>. Acesso em: 22 out. 2019.

BRASIL. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/113709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm)>. Acesso em: 22 out. 2019.

CACHAPUZ, Maria Cláudia. **Intimidade e vida privada no novo código civil brasileiro: uma leitura orientada no discurso jurídico**. Porto Alegre: Sergio Antonio Fabris Ed., 2006.

CANCELIER, Mikhail Vieira de Lorenzi. **O Direito à Privacidade hoje: perspectiva histórica e o cenário brasileiro**. Sequência (Florianópolis), Florianópolis, n. 76, p. 213-239, May 2017. Disponível em: <[http://www.scielo.br/scielo.php?script=sci\\_arttext&pid=S2177-70552017000200213&lng=en&nrm=iso](http://www.scielo.br/scielo.php?script=sci_arttext&pid=S2177-70552017000200213&lng=en&nrm=iso)>. Acesso em 21 de maio de 2021



COLOMBO, Cristiano; FACCHINI NETO, Eugênio. **Violação dos direitos de personalidade no meio ambiente digital: a influência da jurisprudência europeia na fixação da jurisdição/competência dos tribunais brasileiros.** *Civilistica.com*. Rio de Janeiro, a. 8, n. 1, 2019. Disponível em: <<http://civilistica.com/violacao-dos-direitos-de-personalidade/>>. Data de acesso 16 de out de 2021

DA SILVA, Lucas Gonçalves; CURY, Jacqueline Taís Menezes Paez. **Proteção jurídica dos direitos à privacidade e à intimidade diante das novas tecnologias informáticas.** *Relações Internacionais no Mundo Atual*, v. 3, n. 24, p. 111-132, 2019.

DONEDA, Danilo. **Da privacidade à proteção dos dados pessoais.** Rio de Janeiro: Renovar, 2006.

DONEDA, Danilo. **A proteção dos dados pessoais como um direito fundamental.** *Espaço Jurídico Journal of Law [EJL]*, v. 12, n. 2, 2011, p.101-102.

FEIGELSON, Bruno; SIQUEIRA, Antonio Henrique Albani (coords.). **Comentários à lei geral de proteção de dados: Lei 13.709/2018.** São Paulo: Revista dos Tribunais, 2019.

FERNANDES MACIEL, Rafael. **Manual Prático sobre a Lei Geral de Proteção de Dados Pessoais.** 1ª ed. Goiânia-GO, 2019.

FRANÇA, T. C.; FARIA, F. F.; RANGEL, F. M.; FARIAS, C. M.; OLIVEIRA, J. **Big Social Data: Princípios sobre coleta, tratamento e análise de dados sociais.** Artigo publicado nos anais do XXIX Simpósio Brasileiro de Banco de Dados (SBBD) 2014. Curitiba. 2014, p. 8. Disponível em:<<http://www.inf.ufpr.br/sbbdsbsc2014/sbbd/proceedings/artigos/pdfs/127.pdf>>. Acesso em 10 de out de 2021.

FRAZÃO, Ana. **Nova LGPD: a importância do consentimento para o tratamento dos dados pessoais.** Disponível em: <<https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-a-importancia-do-consentimento-para-o-tratamento-dos-dados-pessoais-12092018>>. Acesso em 13 de out de 2021.

MAGRANI, Eduardo. **Democracia conectada: a internet como ferramenta de engajamento político-democrático.** Curitiba: Juruá. 2014, p. 158.

MEDIDA PROVISÓRIA nº 869, de 2018. (2019). **Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados, e dá outras providências.** (2019). Brasília, DF. Disponível em: <<https://www.congressonacional.leg.br/materias/medidas-provisorias/-/mpv/135062>>. Acesso em 13 de out de 2021.

MORAES, Maria Celina Bodin de. **Na medida da pessoa humana: estudos de direito civil constitucional.** Rio de Janeiro: Renovar, 2010, p. 121-122.

RODOTÀ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje.** Rio de Janeiro: Renovar, 2008, p.28-32.

TEPEDINO, Gustavo. FRAZÃO, ANA. OLIVA, Milena Donato. **Lei Geral de Proteção de**

**Dados e suas repercussões no Direito Brasileiro.** Revista dos Tribunais, 2ªed. São Paulo – SP, 2020.

TORRES, Claudio, **A bíblia do marketing digital.**, São Paulo: Novatec, 2009.Pg. 24

WARREN, Samuel D.; BRANDEIS, Louis D. **The right to privacy.** **Harvard law review**, v. 4, n. 5, p. 193-220, 1890. Disponível em: <<https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf>>. Acesso em 10 de ago de 2021.