Data de aprovação: 09/12/2020

A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS À LUZ DO ART. 5º, INCISO X, DA CONSTITUIÇÃO FEDERAL DE 1988.

Gabriel Franco Gomes Gonçalves[1]
Úrsula Bezerra e Silva Lira[2]

RESUMO

O presente artigo busca demonstrar a evolução tecnológica e o advento dos meios de comunicação, para ao que hoje pode chamar-se de Era Tecnológica, e como a utilização do banco de dados e o armazenamento de informações pessoais (*Big data*) tornaram-se mecanismos intrínsecos e inerentes a esse crescimento. Nesse sentido, imperioso se faz destacar a relação dessa evolução em detrimento dos direitos fundamentais, em especial à privacidade, uma vez que são partes que estão cada vez mais vulneráveis nessa questão, haja vista os constantes casos de escândalos nacionais e mundiais referentes aos controles dos dados e violações por parte de pessoas jurídicas, sejam elas de direito público ou privado, e independente de porte. Destarte, será imprescindível fazer uma análise da Lei Geral de Proteção de Dados Pessoais (LGPD), à luz do art. 5º, inciso X, da Constituição Federal de 1988. Dito isso, será preciso percorrer sobre a Era Tecnológica, a ascensão do meio digital, bem como fazer um estudo da LGPD, destacando as suas implicações, desafios e a reparação de danos causados em decorrência de seu descumprimento, a fim de resolver a problemática do impacto dessa lei não só para a população, mas também às pessoas jurídicas que manejam as supracitadas informações. Para tanto, o presente estudo será pautado a partir do método científico Hipotético-Dedutivo, buscando apresentar a eficácia da LGPD.

Palavras-chave: Era Tecnológica. Banco de dados. Direitos Fundamentais. LGPD. Implicações.

[1] Acadêmico do Curso de Direito do Centro Universitário do Rio Grande do Norte – UNI-RN. E-mail: gabrielgomes9612@gmail.com

[2] Professora Orientadora do Curso de Direito do Centro Universitário do Rio Grande do Norte – UNI-RN. E-mail: ursula@unirn.edu.br

THE GENERAL DATA PROTECTION LAW IN THE LIGHT OF ARTICLE 5, ITEM X, OF THE FEDERAL CONSTITUTION OF 1988.

ABSTRACT

This article intends to demonstrate the technological evolution and the advent of the means of communication, for what today can be called Technological Era, and how the use of the database and the storage of personal information (Big data) became mechanisms that are intrinsic and inherent to this growth. In this sense, it is imperative to highlight the relationship of this evolution to the detriment of fundamental rights, especially privacy, since they are parties that are increasingly vulnerable in this matter, given the constant cases of national and world scandals regarding data controls and violations by legal entities, whether under public or private law, and regardless of size. Therefore, it will be essential to carry out an analysis of the General Data Protection Law (LGPD), in the light of article 5, item X, of the Federal Constitution of 1988. That said, it will be necessary to go over the technological era, the rise of the digital medium, as well as conduct a study of the LGPD, highlighting its implications, challenges and the repair of damages caused as a result of its non-compliance, in order to solve the problem of the impact of this law not only for the population, but also for the legal entities that handle the aforementioned information. For this, the present study will be guided by the Hypothetical-Deductive scientific method. At the end, will seek for the effectiveness of the LGPD.

Keywords: Technological Era. Database. Fundamental Rights. LGPD. implications.

1 INTRODUÇÃO

Na medida em que há o avanço tecnológico, originário da revolução industrial, conjuntamente cresce a utilização e armazenamento de dados pessoais por parte de empresas, sejam elas de qualquer porte, ou de próprios órgãos públicos, que os fazem por questões de necessidades do trabalho, como uma loja de e-commerce, ou por ser essencial para subsistência da empresa, como as que trabalham diretamente com banco de dados.

Em contrapartida, ao se tratar de uma época em que o fornecimento de informações pessoais se tornou uma prática corriqueira para a sociedade, por ser necessária para o estrito cumprimento de várias atividades, as pessoas estão ficando cada vez mais vulneráveis, uma vez que acabam virando reféns do modo com que a empresa vai armazenar, tratar e proteger seus dados pessoais.

Aliado a esse ponto, está a forma como a ascensão digital impulsiona a coleta e utilização de banco de dados, uma vez que trata-se de um mundo cada vez mais conectado, em que há a migração de vários negócios para o meio digital, corroborando, assim, para um aumento da quantidade de conteúdos online e, consequentemente, informações pessoais cedidas.

Paralelamente, se há o anseio cada vez maior em se ter dados coletados, maiores e constantes serão os casos de violações destes, a exemplo do estudo feito pela IBM Security, que analisou as violações de dados sofridas por mais de 500 organizações pelo mundo, em que 80% dos incidentes estudados resultaram na exposição das informações de identificação pessoal de clientes (CAMBRIDGE, 2020).

À vista desse cenário, é de suma importância destacar até onde vai o respeito à privacidade de uma pessoa, já que se trata de um direito fundamental, e analisar quais os limites que a chegada da Lei Geral de Proteção de Dados Pessoais irá impor a essas pessoas jurídicas.

Dessa forma, a presente pesquisa pretende fazer uma análise da Lei Geral de Proteção de Dados pessoais à luz do art. 5º, inciso X, da Constituição Federal, porquanto, versando sobre a inviolabilidade do direito à intimidade, assegurando a privacidade e garantindo a sua plena eficácia.

Nessa direção, indaga-se sobre qual será o impacto da supracitada legislação, não somente para as empresas em geral, mas também, especialmente, para toda a população brasileira.

Com isso, tem-se como objetivo geral, para o presente estudo, analisar a relação da Lei Geral de Proteção de Dados Pessoas com o direito fundamental abarcado pela nossa Carta Magna Brasileira, que é o direito à intimidade, que engloba a privacidade das pessoas, consoante o art. 5º, inciso X, de seu escopo.

Para tanto, será preciso discorrer acerca da nova Era Tecnológica, atrelada a utilização dos dados pessoais; Observar a ascensão Digital e sua relação com a privacidade; Analisar a Lei Geral de Proteção dos Dados Pessoais, conforme os seus dispositivos e, por fim, verificar as implicações dela em casos de descumprimento do que ficou estabelecido, bem como de verificar os desafios de sua implementação.

Logo, partir-se-á do método científico Hipotético-Dedutivo, uma vez que vai partir de um problema, qual seja o uso indevido ou incorreto dos dados pessoais da sociedade, porquanto a falta de amparo legal, a fim de chegar-se a uma hipótese que são os aspectos positivos e benéficos que a referida lei traz consigo.

Nesse sentido, a presente pesquisa busca apresentar os pontos positivos da Lei Geral de Proteção de Dados com benefícios para empresa e sociedade.

2 A ERA TECNOLÓGICA E A UTILIZAÇÃO DOS DADOS PESSOAIS

Vivencia-se hoje um mundo em que as pessoas estão, mais do que nunca, interligadas entre si, sendo possibilitados meios de comunicação de onde quer que estejam, independentemente do continente que estiverem. Isso só é possível em decorrência das constantes transformações passadas pela sociedade mundial, para ao que hoje pode ser chamada de sociedade da informação, à ótica de uma era tecnológica. Nesse sentido expõe Takahashi (2000, p. 3):

> Assistir à televisão, falar ao telefone, movimentar a conta no terminal bancário e, pela Internet, verificar multas de trânsito, comprar discos, trocar mensagens com o outro lado do planeta, pesquisar e estudar são hoje atividades cotidianas, no mundo inteiro e no Brasil. Rapidamente nos adaptamos a essas novidades e passamos – em geral, sem uma percepção clara nem maiores questionamentos – a viver na Sociedade da Informação, uma nova era em que a informação flui a velocidades e em quantidades há

> apenas poucos anos inimagináveis, assumindo valores sociais e econômicos fundamentais.

No entanto, para que fosse possível chegar nessa posição, com tantos privilégios, não foi apenas de uma hora para outra. Na verdade, foi preciso séculos para se ter o que há atualmente, passando a população e o ambiente, ao qual estava inserida, por diversas mudanças.

Nesse sentido, um marco importante da história e um dos pilares para a Era Tecnológica foi a Revolução Industrial, originada na Inglaterra. Foi a partir dela que alterações e criações significativas aconteceram, bem como quando o desenvolvimento tecnológico começou a acontecer, fazendo com que surgissem diversas coisas capazes de influenciar e impactar o dia a dia de várias pessoas, não só àquela época, mas também até nos dias de hoje, especialmente pelo surgimento das máquinas.

Não obstante, foi a terceira revolução industrial, também chamada de revolução tecnocientífica, que impactou diretamente para a existência da supracitada sociedade da informação, tendo em vista que foi por causa dela que houve o advento não só da biotecnologia, da robótica, mas, principalmente, dos meios de telecomunicações, em especial do computador.

Esses meios de comunicação contribuíram tanto para conectar e interligar pessoas, como também para expandir relações e negócios anteriormente existentes. A partir desses canais, a utilização do chamado banco de dados evoluiu paralelamente ao crescimento da tecnologia, apresentando uma potencial capacidade de influenciar nos meios digitais.

Nesse sentido, para compreender o conceito de banco de dados, a Lei Geral de Proteção de Dados Pessoais em seu art. 5º, inciso IV, entende como banco de dados o “conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico” (BRASIL, 2018).

Vale salientar, para tanto, que a referida lei considera, em seu art. 5º, inciso I, como dados pessoais “informação relacionada a pessoa natural identificada ou identificável”, ou seja, todo aquele tipo de informação que seja capaz de identificar uma pessoa, seja nome, CPF e outros. Preceitua, ainda, em seu art. 5º, outros dois tipos de dados, a seguir descritos:

> 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;
> 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).

Não somente, Doneda (2011, p. 92) classifica que é “a ferramenta que possibilita a sistematização de volumes que podem chegar a ser gigantescos de informação e que teve seu potencial exponencialmente incrementado com o advento da informática”. Aponta, ainda, o seguinte:

> Bancos de dados são, em sua acepção fundamental, um conjunto de informações estruturado de acordo com uma determinada lógica – e esta lógica é sempre uma lógica utilitarista, uma lógica que procura proporcionar a extração do máximo de proveito possível a partir de um conjunto de informações. Sabe-se há um bom tempo que a informação pode gerar proveito, como resulta claro ao verificar que é milenar a prática de coleta sistematizada de informações por alguma modalidade de censo populacional, instrumento de imensa serventia para governantes de qualquer época – a ponto de os registros históricos a respeito não serem poucos. (DONEDA, 2011, p. 92)

Dessa forma, como se pode ver, não é de hoje que a utilização do banco de dados e a coleta sistematizada de informações existem. Na verdade, há anos essa prática ocorre, como o surgimento da primeira máquina de processamento de dados, em 1943, com o intuito de decifrar os códigos nazistas durante a segunda guerra mundial e, consequentemente, reduzindo um trabalho de semanas em horas, conforme expõe Silva (2019).

Nota-se, portanto, a importância não só para o contexto histórico, como também para a atualidade desse banco de dados e do grande conjunto de dados que hoje os dispositivos eletrônicos são capazes de suportar e armazenar, podendo ser chamado esse fenômeno de *Big Data*.

Imperioso se faz, então, destacar o motivo dos dados e seu posterior armazenamento serem tão importantes para o mundo na realidade atual, seja por parte de empresas, em que o porte delas é requisito indiferente, ou até mesmo por parte de órgãos e instituições públicas, sob um olhar do Estado.

A priori, a Era tecnológica traz consigo suas vantagens e desvantagens. Nessa direção, um dos pontos bastante controversos, que engloba tanto vantagens à ótica dos empreendedores, quanto desvantagens à luz dos titulares dos dados,

qual seja, qualquer pessoa física, é que, na atualidade, um dos motivos fundamentais acerca da importância dos dados pessoais se dá pela maneira econômica e de como eles agregam para fins comerciais.

Seguindo essa linha de raciocínio, através de dados coletados, há a possibilidade de uma empresa conseguir expandir e potencializar determinados tipos de ofertas para um nicho específico de consumidores, fazendo com que os conversores de vendas aumentem significativamente. Isso é possível porque, a partir dos dados pessoais e de seu tratamento, é possível que se entenda os perfis das pessoas e entenderem o potencial de se tornarem clientes, de acordo com os anseios e necessidades da pessoa. Com isso, meios de comunicação personalizados serão encaminhados para essa pessoa, com fins de persuasão. Não à toa, muita gente estranha o recebimento de ofertas por uma empresa diversa, se tratando de um produto ou serviço em que ela estava procurando.

Corroborando com esse viés, André Fatala, CTO da Luiza Labs, braço direito de tecnologia do Magazine Luiza, afirma que é preciso armazenar o maior número possível de dados sobre o consumidor, a fim de identificar o comportamento da pessoa, para, posteriormente, enviar conteúdos exclusivos, de acordo com o seu perfil (BRUM, 2017).

Alinhado a essa questão comercial dos dados pessoais, que é de grande relevância para os negócios, encontram-se também os fatores políticos, tendo em vista que, como já retratado, é possível – através dos dados pessoais – entender o comportamento de uma pessoa e sua personalidade. Por isso, é a partir desta possibilidade que os dados pessoais vão ter grandes interesses políticos também, já que, por meio dos tratamentos das informações, é possível ditar tendências e mecanismos de persuasão para tentar ganhar votos, em um eventual processo eleitoral. Foi nesse sentido que houve o grande escândalo nas eleições Norte-Americanas, no ano de 2016, ao qual houve a quebra da Cambridge Analytica, acusada de violar informações de 87 milhões de usuários do Facebook. Não obstante, a rede social ainda assim foi acusada, por entender ser cúmplice e facilitadora no esquema. De todo modo, a intenção era de colher os dados pessoais de usuários, a fim de entender as personalidades destes e traçar planos de persuadir e influenciar os votos deles (SUMARES; CARVALHO, 2018).

Diante disso, acaba por se tornar uma causa também social, uma vez que o intuito principal era o de influenciar as questões políticas, mas acaba,

intrinsecamente, de forma coadjuvante, inferindo em questões sociais, haja vista que foi necessário adentrar na esfera particular das pessoas para alcançar o objetivo planejado.

Portanto, esses são uns dos motivos de os dados pessoais serem, na atualidade, um dos principais, senão o maior ativo do mundo, chegando até a substituir a posição que antigamente era destinada ao petróleo, este que já foi capaz de gerar inúmeros conflitos a quem estivesse disposto pelo seu domínio. No entanto, apesar de já ter ocupado o posto de fonte natural e bem mais valioso do planeta, impulsionando o crescimento e riquezas a várias nações, hoje os olhos estão muito mais voltados aos dados pessoais como sendo um mecanismo fundamental e gerador de riquezas para várias empresas e instituições, muito em razão da Era Tecnológica que se vive e pela ascensão, cada vez maior, dos meios digitais.

3 A ASCENSÃO DIGITAL E A PRIVACIDADE

Depois do advento dos aparelhos eletrônicos, fundamentalmente os computadores, os meios digitais têm crescido de forma exponencial, causando a migração não só das pessoas físicas, mas também das pessoas jurídicas, sejam elas públicas ou privadas, para o ambiente virtual.

Aliado a isso, outro fator muito importante e que potencializa esse acesso é que nos dias atuais, tudo é muito mais acessível como antigamente. Logo, se antes não havia possibilidade, tampouco condições de ter acesso a um computador para se conectar com o mundo digital, hoje há diversos tipos de eletrônicos, de variados preços, possibilitando que as pessoas, de uma forma ou de outra, tenham chances e proveito desses novos meios, contribuindo para uma maior conectividade e acesso ao meio digital, independente de classe e condições financeiras.

À vista dessa questão, Brookshear (2013, p. 125) aponta que “na última década, a tecnologia de telefones móveis avançou de dispositivos portáteis simples e de propósito singular para computadores de mão complexos e de múltiplas funções”. Aduz, ainda, que:

> Esses “telefones’’ são equipados com um amplo conjunto de sensores e interfaces, incluindo câmeras, microfones, bússolas, telas sensíveis ao toque, acelerômetros (para detectar a orientação do telefone e seu movimento) e diversas tecnologias sem fio para se comunicarem com outros

> smartphones e computadores. O potencial é enorme. (BROOKSHEAR, 2013, p. 10)

Assim, nota-se que através da aquisição de qualquer equipamento eletrônico desses, qual seja o celular, as pessoas terão tamanhas variedades em um só aparelho, possibilitando as mesmas funções que um computador traria, de uma forma muito mais econômica e, ainda, tendo acesso a todo tipo de informação.

Em contrapartida, apesar dessa maior acessibilidade à população aos meios de comunicação, paralelamente as empresas e órgãos privados também vão disputando espaço no mundo digital, o que abarca os prós e contras dessa chegada. As vantagens é que a sociedade pode ter muita coisa, precisando de pouco, ou seja, pode acessar produtos, conteúdos, bem como comprá-los sem sair do conforto de sua casa. Os contras é que, com o aumento do e-commerce no Brasil (comércio online), ao qual mais que dobrou no mês de junho, segundo Maciel (2020) – em decorrência, infelizmente, do COVID-19 e o impacto da pandemia – maiores também serão as quantidades de dados cedidos pelos titulares, de maneira constante.

Isso se dá em virtude da necessidade cada vez mais latente pela utilização dos bancos de dados, em que o anseio por armazenar informações pessoais cresce exponencialmente, sob um viés coletivo, em razão da importância em sua exploração econômica, de controle social e de poder, como já citado. Aliado ao fato da quantidade de volumes aos quais aparelhos eletrônicos são capazes de processar e armazenar as informações, sendo fácil o acesso a estas. Por isso a preciosidade dos dados pessoais, compactuando com termo denominado sociedade da informação. Nesse sentido, preceitua Reinaldo Filho (2006, p. 8-9):

> A disseminação do uso de computadores fez com que, nos dias atuais, não somente as agências governamentais que tradicionalmente coletavam dados pessoais, a exemplo dos Correios, os Departamentos de Trânsito e as repartições do Fisco, funcionassem como poderosos centros de processamento de informações pessoais, mas também todas as empresas privadas hoje adquiriram os meios para coletar, manipular, armazenar e transmitir dados de uma forma simples e a um custo relativamente baixo.

Dessa maneira, constantemente os consumidores estão sendo induzidos para que forneçam seus dados pessoais, ainda que não seja necessário ou que sejam informações em excesso do que realmente se precisa. Na prática, é comum muitas pessoas fornecerem suas informações e logo em seguida passarem a

receber e-mails, em alguns casos até de forma desagradável, sendo esse um reflexo das finalidades para utilização dos dados pessoais.

Por esse motivo, uma pesquisa realizada pelo Reclame AQUI constatou que 88,6% de 9.627 pessoas mostraram-se preocupadas pela forma com que as empresas armazenam, tratam e utilizam os seus dados, e com razão, visto que muitas vezes acabam tendo sua seara privada invadida de alguma forma indesejada (CARDOSO, 2019).

Sob essa ótica, fundamental se faz enfatizar que essa preocupação decorre tanto porque as pessoas não têm a cultura nem o senso de proteção de seus dados, disponibilizando-os de maneira fácil, quanto pelo fato delas não saberem quais estão sendo as finalidades para as quais estão sendo usados, por falta de transparência nas políticas de privacidades e nos termos de uso implementados pela pessoa jurídica. Logo, uma vez fornecidas as informações, a empresa estará sob o domínio dos determinados dados, em que poderá utilizar-se para os fins que achar pertinente, sejam eles lícitos ou ilícitos.

De toda sorte, é a partir daí que encontra-se o cerne da questão, já que – mesmo os titulares dos dados agirem com uma parcela de culpa, deixando de ler as referidas políticas disponibilizadas – na maioria das vezes quem age com a culpa é mesmo a empresa ou órgão público, por ultrapassar as fronteiras da vida privada, da intimidade e da privacidade da pessoa, seja por utilizar dos dados recebidos para fins diversos que não aquele especificado e exposto ao titular, por falta de transparência, não demonstrando as reais necessidades da coleta ou por tornarem em excesso as atividades fins utilizadas.

Em razão disso, estariam essas pessoas jurídicas infringindo direitos da personalidade e garantias constitucionais, haja vista que são resguardados aos titulares no art. 5º, inciso X, da Constituição Federal, que vai dizer que “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação” (BRASIL, 1988).

Com efeito, mesmo tendo sido fortificado pela Constituição Federal, o direito à privacidade já era estabelecido dentro dos direitos fundamentais de 1ª dimensão, em que a proteção à vida privada e à intimidade já vinha sendo aplicada na sociedade e nas legislações que a acompanhavam. Então, as pessoas já vinham ganhando liberdade em relação às interferências, ainda que estatal, mas

fomentando a questão da privacidade para nos dias atuais ter sua devida importância. Nessa direção, aduz Fernandes (2017, p. 325):

> Por isso mesmo, os direitos de primeira geração (ou dimensão para alguns) seriam chamados também de direitos de liberdade: direitos civis e políticos, que inaugurariam o constitucionalismo do Ocidente, no final do século XVIII e início do século XIX. Seu titular é, então, o indivíduo, ao passo que encontra no Estado o dever de abstenção.

Evidencia-se, além do mais, que o direito à privacidade encontra respaldo não só na Carta Magna do Brasil, mas também na Lei Geral de Proteção de Dados Pessoais (LGPD), que surge justamente com o objetivo tutelar os direitos fundamentais de liberdade e privacidade de todo titular de dados que esteja em território brasileiro. Para tanto, aduz a referida lei que sua disciplina tem como fundamento o respeito à privacidade (BRASIL, 2018).

Outrossim, para respaldar de vez o que está sendo tratado, o Código Civil, sem seu artigo 21, tratou de tutelar o âmbito privado de um indivíduo, no que tange a privacidade, ao estabelecer que “a vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma” (BRASIL, 2002).

Isto posto, quando se fala no princípio da máxima eficácia dos direitos fundamentais, quer dizer que estes são dotados de aplicabilidade imediata (FERNANDES, 2017, p. 369).

Dessa forma, além dos direitos já assegurados pelo artigo 5º, inciso X, da Constituição Federal, tramita hoje na Câmara dos Deputados a PEC nº 17/2019, que busca alterar “a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais” (BRASIL, 2019). Dessa forma, os dados pessoais da população poderão ganhar o aparato necessário para sua segurança, bem como poderão ser incorporados como um direito de personalidade.

Nesse seguimento, faz-se imprescindível trazer à baila o que o Departamento de Saúde e Serviços Humanos dos EUA abordou ao relacionar a privacidade com sua utilização no mundo digital, ao qual vivencia a sociedade atual:

> A privacidade pessoal de um indivíduo é diretamente afetada pelo tipo de divulgação e uso feito de informações identificáveis sobre ele em um

> registro. Um registro contendo informações sobre um indivíduo em forma identificável deve, portanto, ser regido por procedimentos que concedem ao indivíduo o direito de participar na decisão de qual será o conteúdo do registro e qual divulgação e uso serão feitos das informações identificáveis em isto. Qualquer registro, divulgação e uso de informações pessoais identificáveis não regidas por tais procedimentos devem ser proibidos como prática de informação injusta, a menos que tal registro, divulgação ou uso seja especificamente autorizado por lei. (U.S., 1973)

Significa dizer, portanto, que em uma sociedade movida a dados pessoais, que permite identificar gostos e personalidades, cada vez mais aumenta a vigilância sobre as pessoas e estas sequer sabem que estão sendo vigiadas, muito menos para quais atividades suas informações estão sendo utilizadas, não sabendo distinguir se para fins lícitos ou ilícitos. Nessa direção, aduzem Costa e Oliveira (2019, p. 26):

> Essa vigilância social centra-se em um “olhar que vê sem ser visto”, algo que nos é perceptível nas novas tecnologias de comunicação e suas redes sociais, nas quais os controladores de dados nos observam, recolhem e utilizam nossos dados pessoais, sem que tenhamos quaisquer tipos de ingerência nesse processo.

Dessa maneira, mesmo havendo todo o respaldo jurídico quando se trata dos direitos da personalidade, em especial da vida privada, ainda assim as pessoas estão sujeitas às violações, visto que, a partir do momento em que são fornecidas informações pessoais, o domínio e controle dos dados ficarão, agora, sob quem os recebeu. Então, as pessoas com todas as garantias constitucionais, continuam à mercê de empresas e órgãos que coletam seus dados.

Diante disso, em uma tentativa de diminuir os riscos e de dar maior autonomia ao titulares desses dados, bem como de efetivar, justamente, uma gerência desses dados, que estava faltando, a LGPD trouxe em seu escopo a questão do consentimento, que é uma das bases legais, em que os controladores (para fins da Lei, poder ser uma pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais) dos dados deverão respeitar e implementar em seu negócio. Para tanto, a referida Lei conceitua o consentimento como uma “manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada” (BRASIL, 2018).

Nesse contexto, a LGPD estabelece, ainda, em seu art. 7º, o rol de bases legais, este sendo requisito para que possa haver, de fato, o tratamento de dados

por parte dos controladores, ou seja, “para que o tratamento seja lícito, deverá estar presente, em concreto, ao menos uma das bases legais” (LIMA, *et al*., 2019, p. 20). O consentimento, portanto, é uma das hipóteses do supracitado rol, sendo ele o mais utilizado entre os agentes de tratamento.

Não obstante ser uma das bases legais e as pessoas demonstrarem preocupação ao fornecerem seus dados pessoais, o consentimento pelo tratamento acaba se tornando prejudicado, justamente por ele ser dado majoritariamente de maneira superficial. A explicação disso é que, embora os titulares tenham ganhado maior autonomia e uma maior gerência de sua vida privada com a LGPD, as pessoas ainda não têm conhecimento ou não pararam para estudar ainda sobre essa legislação que as protege, ratificando a ideia da falta de cultura de proteção dos dados por parte dos próprios titulares, que não são instruídos e que não buscam fundamentos para fiscalizar e garantir os seus direitos.

Ainda, a população, muitas vezes, é persuadida a dar o seu precioso consentimento para que, enfim, possa consumir determinado tipo de conteúdo ou conseguir efetuar alguma atividade que lhe seja necessária. Para tanto, os destinatários dos dados fornecidos acabam oferecendo mecanismos rápidos para conseguir o consentimento, que é o seu único objetivo para alcançar os tão esperados dados. Então, por vezes são colocadas políticas vagas, sem transparência com o titular, mas com facilidade de consentir, como os conhecidos “li e aceito” ou “concordo”, impostos em políticas de privacidade e termos de uso, que muitas vezes não são lidos em razão, exatamente, da falta de cultura, bem como da urgência na consumação do conteúdo ou da atividade. Nesse sentido, compactuando com esse entendimento, Costa e Oliveira (2019, p. 35) apontam, acertadamente, o que vem a seguir:

> Desse modo, em um contexto no qual a aceitação dos termos de uso em redes sociais é a condição primordial para sua utilização, as pessoas tendem a acatarem as chamadas cláusulas take it or leave it (em tradução livre, “pegar ou largar), que designam essa condição enrijecida, à qual os usuários são submetidos ao acessarem as redes. Assim, ou aceitam todas as disposições contratuais de uso, criadas unilateralmente pelas empresas e apresentadas em uma estrutura de consentimento não dialogal, ou então não podem ser um membro daquele espaço de sociabilidade digital.

Resta claro, dessa forma, a importância da ferramenta que é o consentimento, como uma tentativa de dar poderes às pessoas para que fiscalizem

qual o destino e qual a finalidade que seus dados estão sendo submetidos, a fim de manter sua privacidade e intimidade preservadas, já que qualquer função a mais, fora daquelas que forem permitidas, será considerado um desvio e, consequentemente, uma violação de seus direitos de personalidade. É o que sustenta Carvalho e Pedrini (2019, p. 371):

> Outrossim, considera-se comportamento agravante na segurança da informação a utilização de dados de outrem com a pretensão de divulgá-los na internet, sem a prévia anuência, isso porque, ao concretizar essa conduta, torna-se pública a intimidade e a privacidade, garantidos como direitos fundamentais individuais na CRFB/88.

Desse modo, para além das legislações como mecanismos de fomento de proteção dos dados pessoais e dos direitos fundamentais em questão, fundamentalmente a privacidade e intimidade, faz-se imprescindível que as pessoas alimentem a cultura de proteção e comprem a ideia de fiscalizadores de suas informações, assim como que as empresas se mostrem acessíveis e transparentes ao requisitar e tratar dados pessoais da população, como também demonstrem sua devida responsabilidade e respeito à LGPD, pois uma coisa não tem como negar: a ascensão digital não vai parar, restando ao direito, ao respaldo jurídico e à população acompanhar, pois só assim para garantir a segurança dos dados, juntamente da vida privada das pessoas.

Para reforçar tal pensamento, Costa e Oliveira (2019, p. 38) aduzem o que segue:

> Portanto, o desafio para a adequação do consentimento apresentado nas redes sociais com a LGP está na eficiência dos termos de uso dessas redes para contemplarem um recolhimento do consentimento que capacite os usuários a exercerem a autodeterminação informativa. Desse modo, é preciso que os indivíduos compreendam quais dados estão sendo utilizados pelas redes das quais são usuários, como estão sendo utilizados, por quanto tempo e de quais formas as empresas estão se responsabilizando para garantirem uma esfera digital segura para o livre exercício da personalidade das pessoas, visto que nos encontramos em uma sociedade altamente moldada a partir da vigilância sobre nossos dados pessoais.

4 A LGPD, SUAS IMPLICAÇÕES E DESAFIOS

A constante evolução da tecnologia e dos meios de comunicação, bem como da migração de relacionamentos pessoais e profissionais para o ambiente digital,

fizeram não só com que a população se tornasse parte hipossuficiente na relação, dada a vulnerabilidade gerada acerca de pessoas que agem de má fé nesse ambiente e que são praticantes de crimes cibernéticos, como também para corroborar com a ideia criada de que a internet é “terra sem lei”, justamente pela dificuldade de controle estatal e de amparo jurídico dentro dessa esfera.

Diante disso, intrínseca a essa evolução está a quantidade de violações aos direitos fundamentais e de personalidade, principalmente no tocante à privacidade, intimidade e à imagem, haja vista que são questões recorrentes e que trazem bastante controvérsias e litígios quando se trata de ambiente virtual. Isso ocorre em razão, repita-se, da evolução tecnológica, em que a capacidade de gerar, transmitir e tratar informações está cada vez mais fácil, como a questão da utilização dos dados pessoais e da importância que é o banco de dados para as relações humanas atuais, sendo possível interferir em esferas sociais, política e econômicas. À exemplo disso e que foi um alerta para as autoridades nacionais e internacionais perceberem que a segurança no mundo virtual, dos direitos fundamentais e dos dados pessoais é uma questão imprescindível, é o caso emblemático da Cambridge Analytica, ao qual foi possível coletar e armazenar dados pessoais com o intuito de manipular as pessoas por meio de conteúdos totalmente personalizados às suas personalidades.

Ato contrário ao exposto, o Ministro Relator Herman Benjamim, ao julgar Recurso Especial interposto pelo Google – sendo este acusado, por meio de Ação Civil Pública, de veicular comunidades ofensivas aos internautas, especialmente à criança e adolescente, em rede social – pontuou o seguinte:

> A internet é o espaço por excelência da liberdade, o que não significa dizer que seja um universo sem lei e sem responsabilidade pelos abusos que lá venham a ocorrer. No mundo real, como no virtual, o valor da dignidade da pessoa humana é um só, pois nem o meio em que os agressores transitam nem as ferramentas tecnológicas que utilizam conseguem transmudar ou enfraquecer a natureza de sobreprincípio irrenunciável, intransferível e imprescritível que lhe confere o Direito brasileiro. Quem viabiliza tecnicamente, quem se beneficia economicamente e, ativamente, estimula a criação de comunidades e páginas de relacionamento na internet é tão responsável pelo controle de eventuais abusos e pela garantia dos direitos da personalidade de internautas e terceiros como os próprios internautas que geram e disseminam informações ofensivas aos valores mais comezinhos da vida em comunidade, seja ela real ou virtual. (BRASIL, 2010, p. 7-8)

Com isso, constata-se que, por mais que seja difícil de obter controle, a internet é sim terra com leis, com fiscalizadores que têm a função de resguardar direitos e garantias da população, quando estiverem ameaçados, e de responsabilizar terceiros, quando estes concretizarem a violação aos direitos.

Nesse sentido, surge um importante e pioneiro instrumento regulatório do ambiente virtual: O Marco Civil da Internet, sob a égide da Lei 12.965/2014, que tem o intuito, justamente, de proteger os dados pessoais da população, ainda que não de forma específica e detalhada, mas garantindo a preservação da privacidade e intimidade, com fulcro nos princípios estabelecidos em seu art. 3º, que seguem com fins de proteger a privacidade e os dados pessoais, na forma da lei. Ainda, é garantido o direito de inviolabilidade da intimidade e da vida privada e do sigilo de suas comunicações no mundo digital, estando, ainda, resguardado o direito à indenização em caso de ocorrência de violações (BRASIL, 2014).

Não à toa, diversos são os casos que já foram julgados com base no Marco Civil da Internet, sendo necessário trazer à tona uma decisão em sede de Ação Civil Pública, em que, fundamentada consoante o art. 7º, inciso VI, VII, VIII e IX, determinou que a Microsoft Informática LTDA oferecesse ferramentas operacionais simples, claras e diretas, corroborando com a máxima da transparência perante a sociedade (SÃO PAULO, 2018).

Ademais, as próprias relações de consumo, regidas pelo Código de Defesa do Consumidor, em Lei 8.078/90, estão suscetíveis à proteção da camada mais hipossuficiente da relação, que é a população, ora consumidores, ao estabelecer, por exemplo, em seu art. 6º, que é direito das pessoas o acesso à informação de forma clara e adequada, sendo o referido artigo norteador de todo seu escopo (BRASIL, 90).

Ainda, em um panorama internacional, após 4 (quatro) anos deliberando, em abril de 2016 foi aprovado o Regulamento Geral de Proteção de dados (RGPD ou, do inglês, General Data Protection Regulation – GDPR), que abrange 31 nações da Europa, incluindo os 28 Estados-Membros que compõem a União Europeia. Surge, exatamente, em razão da grande quantidade de fluxo de dados que já vinha ocorrendo e potencializado em razão de violações que também aconteciam, sendo o caso da Cambridge Analytica o ápice para que houvesse sua aprovação e, posteriormente, a sua eficácia. Dessa forma, configura-se uma grande norma

mundial referente à proteção de dados pessoais e da vida privada da população. (LIMA, *et al.*, 2019).

Inspirada em todas as citadas legislações, especialmente no Regulamento Europeu, qual seja a RGPD, foi promulgada em 2018 a Lei 13.709, denominada como Lei Geral de Proteção de Dados Pessoais (LGPD) e entrou em vigor em 18 de setembro de 2020. Nesse contexto, muito parecida com a RGPD, a LGPD vem com o intuito, propriamente, de tutelar direitos e garantias abarcados pela Constituição Federal, ao sustentar em seu art. 17 que "Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade" (BRASIL, 2018), ou seja, direitos da personalidade, uma vez que, embora as legislações anteriores, o país era carente de uma legislação específica voltada à proteção de dados pessoais, que suprisse todas as lacunas que as outras normas deixavam.

Não somente, a LGPD além de ser uma garantidora dos direitos fundamentais, ela ainda tem o intuito de regulamentar e fiscalizar todas as formas de tratamentos dos dados pessoais, desde sua coleta até a sua destinação final, que é a atividade fim pela qual as empresas e instituições públicas deverão deixar clara em suas respectivas políticas.

É nesse viés que o art. 6º da LGPD vai dizer que as atividades de tratamento dos dados deverão observar a boa-fé e 10 (dez) princípios. Todos estes são imprescindíveis, mas ganha relevância o princípio da finalidade, que é a "realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades", bem como o da transparência, que é a "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" (BRASIL, 2018). Isso porque as empresas deverão adotá-los já em um primeiro contato com o titular dos dados, ao qual será feito por meio de suas políticas de privacidade e dos termos de uso, onde as finalidades deverão estar bem especificadas, como também de maneira clara. Dessa maneira, qualquer atividade exercida fora do que estava explícito nas finalidades, considera-se violação no tratamento. É o que preceitua Carvalho e Pedrini (2019, p. 371):

> Além do mais, o próprio ato de ter acesso a informações sigilosas e pessoais e usá-las para fins diversos, sem o prévio consentimento, já caracterizaria o risco à violabilidade da privacidade e a configuração de prática abusiva, pois, consoante a autodeterminação informativa, ao detentor da informação é dado o direito de ter a ciência de quais os locais, sejam estes físicos ou não, tramitam seus dados.

É evidente, em verdade, que a realidade tecnológica atrai as pessoas para uma interação maior com ela, seja para simplesmente consumir determinado tipo de conteúdo, seja para efetuar determinado tipo de transação financeira, ou melhor, para efetuar certo tipo de compra na internet. No entanto, são nessas pequenas relações que a infração à seara privada das pessoas acaba sendo realizada, podendo gerar desde pequenos a grandes danos no setor pessoal de alguém, em alguns casos até irreparáveis. Logo, corroborando com a ideia, apontam Carvalho e Pedrini (2019, p. 369):

> Infere-se do exposto que são diversos os modos de transgressão à privacidade de dados em plataformas de comunicação, como a internet ou semelhantes, principalmente, quando são capturadas e/ou vendidas por outrem, sem a comunicação e autorização prévia, ocasionando, com isso, a violação à liberdade de autodeterminação do indivíduo acerca de seus próprios dados.

No caso principal exposto pelos autores acima, em que para além da coleta, são vendidos para terceiros os dados pessoais recebidos, eles expressam o seguinte:

> Há de se observar que é comum o ato de um usuário disponibilizar suas informações, a saber, perante a contratação de determinados serviços. Todavia, não se deve confundir esse comportamento com o repasse clandestino, o que é defeso, pois, além de ferir disposições constitucionais, torna o usuário plenamente vulnerável a ações de pessoas físicas ou jurídicas más intencionadas a diversos propósitos.

E é, propriamente, nesse sentido que a primeira sentença com base na LGPD se deparou: Ao julgar ação de indenização por danos morais, a empresa Cyrela Brazil Realty S.A. empreendimentos e participações foi condenada a pagar R$ 10.000,00 (dez mil reais) a título de danos morais, por transmitir dados titularizados pelo autor a empresas estranhas do que restou demonstrado em sua finalidade (SÃO PAULO, 2020).

Imperioso faz-se salientar que esse é apenas um exemplo do tipo de punição que pode ocorrer aos infratores da LGPD, que no caso foi a sanção civil.

Entretanto, a Lei ainda prevê as hipóteses de sanções penais e administrativas. Todas definidas pelo Código de Defesa do Consumidor, que não substituem as sanções administrativas impostas pela própria Lei Geral de Proteção de Dados Pessoais, conforme dispõe o artigo 52, parágrafo segundo da referida lei (BRASIL, 2018). Salienta-se, ademais, que as sanções administrativas constantes na LGPD entram em vigor apenas no dia 1º de agosto, por força da Lei 14.010/20 (SERPRO, 2020).

Essas últimas citadas poderão ir desde multas pecuniárias até multas plenamente administrativas. Aquelas, poderão chegar até o limite de 50 milhões de reais. Estas, apesar da denominação administrativa, a depender do tamanho e da potencialidade da empresa, poderá ser infinitamente pior do que a pecuniária. À exemplo disso, a sanção constante no inciso VI do artigo 52, que vai falar da eliminação dos dados pessoais coletadas dos bancos de dados da empresa, poderá decretar o fim desta, uma vez que há empresas que vivem do tratamento de dados, ou seja, toda a sua receita econômica advém dos dados armazenados (BRASIL, 2018).

Por esse motivo, nota-se a importância das empresas e órgãos públicos adotarem políticas de boas práticas e de governança, conforme dispõe em seu art. 50, Caput (BRASIL, 2018):

> 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.

Uma vez implementadas, havendo algum tipo de violação ou vazamento dos dados armazenados, as políticas de boas práticas e de governança poderão ser levadas em conta, sendo uma provável causa de relaxamento da sanção. Esse é apenas um exemplo do rol de critérios estabelecidos pelo parágrafo 1º do art. 52 da LGPD, que poderão ser analisados no caso concreto para benefício ou malefício da pessoa infratora (BRASIL, 2018).

Dessa forma, evidencia-se a fundamental importância da LGPD como instrumento principal que regulamenta a proteção dos dados pessoais da população

e, consequentemente, dos seus direitos fundamentais e garantias constitucionais, estabelecendo os modos de tratamento, bem como punições para quem violar a privacidade, intimidade e liberdade das pessoas. Não somente, há ainda a possibilidade de diminuição da punição caso a pessoa jurídica em questão estabeleça mecanismos de compliance, a fim de mitigar os riscos de violações.

5 CONSIDERAÇÕES FINAIS

Infere-se, portanto, como um reflexo de um mundo cada vez mais conectado, onde há o avanço próspero e desenfreado do ambiente virtual, em que as pessoas estão cada vez mais suscetíveis a verem a sua vida, a sua privacidade, a sua intimidade, a sua liberdade, a sua imagem, enfim, seus direitos de personalidade violados, a Lei Geral de Proteção de Dados Pessoais (LGPD) surge como uma esperança a dar não só ao Brasil, mas ao mundo uma prudência maior, mantendo as relações consumeristas em pleno equilíbrio, além da máxima de garantidora dos direitos fundamentais.

Nesse sentido, constatou-se que a Cultura de Proteção aos Dados Pessoais precisa ser tanto alimentada, quanto disseminada, seja dentro das empresas ou instituições públicas, seja pela própria população. Isso porque muitas pessoas, atualmente, afirmam que se preocupam ao fornecer seus dados para quem está coletando, mas proporcionalmente são os casos de pessoas que pouco conhecem ou pararam para estudar a supracitada legislação que protege suas informações, ou até mesmo não tem conhecimento algum sobre ela.

Por isso, a LGPD vem oferecer diversas vantagens à população, que figura como titulares dos dados, ao dar autonomia no processo de tratamento, feito pelos agentes responsáveis, dos seus dados, como a tão importante questão do consentimento, que é base legal e requisito para que o tratamento possa, de fato, ocorrer. Ademais, terá não apenas os seus direitos fundamentais resguardados, com fulcro no art. 17, como também direitos dentro do próprio manejo dos dados, podendo, inclusive, revogar o seu consentimento, consoante o art. 18 da LGPD (BRASIL, 18).

Ato contínuo, como a Lei 13.709/18 já encontra-se em vigor, em que a necessidade de adequação das pessoas jurídicas, sejam elas de direito privado ou público, é premente e fundamental, por conseguinte torna-se o aumento na busca

mecanismos que garantam a inviolabilidade da privacidade e da adoção de práticas de boa governança e de tratamento de qualidade e de acordo com a LGPD. Com isso, estará efetivando não só os dispositivos da citada legislação, como também de direitos fundamentais abarcados na Constituição Federal de 1988, especialmente do artigo 5º, inciso X. Para tanto, estará trazendo não só benefícios à empresa, que implantou a cultura de proteção de dados em seu estabelecimento interno, como também à própria população, que poderá contar com mais segurança de seus dados a partir das medidas e de políticas adotadas por ela.

Dessa forma, ao garantir a adequação de sua empresa ou instituição pública, novamente estas têm a ganhar, ou seja, mais ainda serão os benefícios voltados a elas, pois restou claro que as pessoas irão preferir, ou melhor, já estão preferindo empresas que estão saindo na frente, se adequando à LGPD e tomando todas as medidas cabíveis para mitigar riscos de violações e fomentar a segurança das informações pessoais dos titulares. À vista disso, estará concretizada a credibilidade que a sociedade vai dar em troca da adequação à Lei e, posteriormente, ganhará destaque em relação à concorrência.

Conclui-se, assim, que a Lei Geral de Proteção de Dados Pessoais veio, de fato, para somar e trazer vantagens não só à população, visto que terá seus direitos fundamentais assegurados, mas também às empresas e instituições públicas, pelo patamar que o respeito e adequação a LGPD lhe impõe, já que estará, agora, coletando e tratando os dados pessoais da sociedade de forma responsável, corroborando para uma ambiente virtual cada vez mais seguro e livres de interferências na privacidade e intimidade das pessoas.

REFERÊNCIAS BIBLIOGRÁFICAS

AMORIM, L. **O impacto da LGPD na transformação digital acelerada pelo COVID-19**. Vtex. Disponível em: https://vtex.com/pt-br/blog/gestao/lgpd-transformacao-digital-covid/. Acesso em: 06 set. 2020.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil.** Brasília, DF: Presidência da República. [2020]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 14 nov. 2020.

BRASIL. Câmara dos Deputados. **Proposta de Emenda à Constituição nº 17/2019**. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os

direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2210757. Acesso em: 16 nov. 2020.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. **Diário Oficial da União**: Brasília, DF, 10 jan. 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/L10406compilada.htm. Acesso em: 14 nov. 2020.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Diário Oficial da União**: Brasília, DF, 23 abr. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 23 nov. 2020.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre o tratamento e proteção dos dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). **Diário Oficial da União**: Brasília, DF, 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 06 set. 2020.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. **Diário Oficial da União**: Brasília, DF, 11 set. 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 24 nov. 2020.

BRASIL. Superior Tribunal de Justiça (2. Turma). **Recurso Especial 1117633/RO**. Processual Civil. Orkut. Ação civil pública. Bloqueio de comunidades. Omissão. Não-ocorrência. Internet e dignidade da pessoa humana. Astreintes. Art. 461, §§ 1º e 6º, do CPC. Inexistência de ofensa. Recorrente: Google Brasil Internet LTDA. Recorrido: Ministério Público do Estado de Rondônia. Relator: Min. Herman Benjamin, 09 de março de 2010. Disponível em: https://scon.stj.jus.br/SCON/jurisprudencia/toc.jsp?livre=%28%28%22RESP%22.CLAS.+E+%40NUM%3D%221117633%22%29+OU+%28%22RESP%22+ADJ+%221117633%22.SUCE.%29%29&b=ACOR&thesaurus=JURIDICO. Acesso em: 23 nov. 2020.

BROOKSHEAR, J. G. **Ciência da Computação**: Uma visão abrangente. 11. ed. Porto Alegre: Bookman, 2013.

BRUM, R. **Dados como a alma do negócio**: como o Magazine Luiza usa IoT com propriedade. E-Commerce Brasil. 2017. Disponível em: https://www.ecommercebrasil.com.br/noticias/dados-como-alma-do-negocio-como-o-magazine-luiza-faz-uso-do-iot-com-propriedade/. Acesso em: 23 set. 2020.

CAMBRIDGE, M. **Estudo da IBM mostra que contas comprometidas de funcionários levaram às violações de dados mais caras durante o ano passado**. IBM Security. 2020. Disponível em: https://www.ibm.com/blogs/ibm-comunica/estudo-da-ibm-mostra-que-contas-comprometidas-de-funcionarios-

levaram-as-violacoes-de-dados-mais-car+as-durante-o-ano-passado/. Acesso em: 23 set. 2020.

CARDOSO, A. P. **88,6% dos consumidores se preocupam com o uso de seus dados**. ReclameAQUI. 2019. Disponível em: https://noticias.reclameaqui.com.br/noticias/88-6-dos-consumidores-se-preocupam-com-o-uso-de-seus-dados_3779/. Acesso em: 23 set. 2020.

CARVALHO, G. P; PEDRINI, T. F. Direito à Privacidade na Lei Geral de Proteção de Dados Pessoais. **Revista da Esmesc**. Florianópolis. v. 26. n. 32. p. 363-382, 2019. DOI: http://dx.doi.org/10.14295/revistadaesmesc.v26i32.p363. Disponível em: https://revista.esmesc.org.br/re/article/view/217/186. Acesso em: 15 nov. 2020.

COSTA, R. S; OLIVEIRA, S. R. Os Direitos da Personalidade frente à Sociedade de Vigilância: privacidade, proteção de dados pessoais e consentimento nas redes sociais. **Revista Brasileira de Direito Civil em Perspectiva**. Belém. v. 5. n. 2. p. 22-41, 2019. Disponível em: https://www.indexlaw.org/index.php/direitocivil/article/view/5778/pdf. Acesso em: 15 nov. 2020.

DIGISYSTEM**. O impacto do COVID-19 e da LGPD na segurança dos dados e informações pessoais dentro dos hospitais**. 2020. Disponível em: <https://www.digisystem.com.br/o-impacto-do-covid-19-e-da-lgpd-na-seguranca-dos-dados-e-informacoes-pessoais-dentro-dos-hospitais/#:~:text=25%20ago,O%20impacto%20do%20COVID%2D19%20e%20da%20LGPD%20na%20seguran%C3%A7a,informa%C3%A7%C3%B5es%20pessoais%20dentro%20dos%20hospitais&text=Com%20a%20evolu%C3%A7%C3%A3o%20das%20solu%C3%A7%C3%B5es,dos%20dados%20de%20seus%20usu%C3%A1rios>. Acesso em: 06 set. 2020.

DONEDA, D. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico Journal of Law [EJJL]**, v. 12, n. 2, p. 91-108, 13 dez. 2011. Disponível em: https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315. Acesso em: 23 set. 2020.

DONEDA, D. **Da Privacidade à Proteção de Dados Pessoais**. Rio de Janeiro: Renovar, 2006.

FERNANDES, B. G. **Curso de Direito Constitucional**. 9. ed. Salvador: Juspodivm, 2017.

LIMA, A. C. *et al*. **LGPD Lei Geral de Proteção de Dados Pessoais**: Manual de Implementação. São Paulo: Revista dos Tribunais, 2019.

MACIEL, R**. Pandemia faz vendas online crescerem 100% no Brasil em junho**; entenda. Canaltech. 2020. Disponível em: https://canaltech.com.br/e-commerce/vendas-via-e-commerce-dobram-em-junho-no-brasil-169241/. Acesso em: 23 set. 2020.

NEVES, D.; SOUSA, R. **Revolução Industrial**. Brasil Escola. Disponível em: https://brasilescola.uol.com.br/historiag/revolucao-industrial.htm. Acesso em: 23 set. 2020.

REINALDO FILHO, D. R. **Privacidade na sociedade da informação**. Orientadora: Eneida Melo Correia de Araújo. 2006. 250 f. Dissertação (Mestrado em Direito Privado) – Centro de Ciências Jurídicas da Faculdade de Direito do Recife, Universidade Federal de Pernambuco – UFPE, Recife, 2006. Disponível em: https://repositorio.ufpe.br/handle/123456789/4642. Acesso em: 14 nov. 2020.

SÃO PAULO. Justiça Federal de 1º grau. 9ª vara cível. **Ação Civil Pública nº 5009507-78.2018.4.03.6100**. Autor: Ministério Público Federal – PR/SP. Réu: Microsoft Informática LTDA, União Federal. Juíza Federal Cristiane Farias Rodrigues dos Santos. São Paulo, SP, 27 de abril de 2018. Disponível em: http://www.omci.org.br/jurisprudencia/250/coleta-de-dados-pessoais-sem-autorizacao/. Acesso em 25 nov. 2020.

SÃO PAULO. Tribunal de Justiça. 13ª Vara. **Ação de Indenização por Dano Moral nº 1080233-94.2019.8.26.0100**. Requerente: Fabricio Vilela Coelho. Requerido: Cyrela Brazil Realty S/A Empreendimentos e Participações. Juíza: Tonia Yuka Koroku. São Paulo, SP, 29 de setembro de 2020. Disponível em: https://esaj.tjsp.jus.br/cpopg/show.do?processo.codigo=2S0013T8I0000&processo.foro=100&processo.numero=1080233-94.2019.8.26.0100&uuidCaptcha=sajcaptcha_3b57f71d08f44c228ef13c020f1843be. Acesso em: 15 nov. 2020.

SEMANA JURÍDICA UNI-RN: O direito e as novas tecnologias. 7. 2020. Natal. **A proteção de dados pessoais no Brasil: O que muda agora?**. Natal: Centro Universitário do Rio Grande do Norte – UNI-RN, 2020. Disponível em: https://www.youtube.com/watch?v=3Ot3GFqUpIs. Acesso em: 29 nov. 2020.

SERPRO. **LGPD entra em vigor**: Lei Geral de Proteção de Dados Pessoais começa a valer nesta sexta, dia 18. Governo Federal. 2020. Disponível em: https://www.serpro.gov.br/lgpd/noticias/2020/lgpd-entra-em-vigor. Acesso em: 24 nov. 2020.

SILVA, V. M. **Big Data**: Definição e Um Breve Histórico. StratioBD do Brasil. 2019. Disponível em: https://medium.com/@stratiobd/big-data-defini%C3%A7%C3%A3o-e-um-breve-hist%C3%B3rico-a389abcf6a3. Acesso em: 23 set. 2020.

SUMARES, G.; CARVALHO, L. **Cambridge Analytica**: tudo sobre o escândalo do Facebook que afetou 87 milhões. Olhar Digital. 2018. Disponível em: https://olhardigital.com.br/noticia/cambridge-analytica/74724. Acesso em: 14 nov. 2020.

TAKAHASHI, T. (Org.). **Sociedade da informação no Brasil**: livro verde. Brasília: Ministério da Ciência e Tecnologia, 2000.

U.S. Department of Health & Human Services. **Records, computers and the rights of citizens.** Office of the Assistant Secretary for Planning and Evaluation. 1973.

Disponível em: https://aspe.hhs.gov/report/records-computers-and-rights-citizens#8. Acesso em: 23 set. 2020.