UNIVERSIDADE FEDERAL DO ESTADO DO RIO DE JANEIRO
CENTRO DE CIÊNCIAS JURÍDICAS E POLÍTICAS
ESCOLA DE DIREITO

JOÃO PEDRO SOARES DA SILVEIRA

MÁRIO MADEIRA CARVALHO FERNANDES

LGPD: REALIDADE BRASILEIRA E COMPARATIVO INTERNACIONAL

RIO DE JANEIRO
2021

JOÃO PEDRO SOARES DA SILVEIRA
MÁRIO MADEIRA CARVALHO FERNANDES

LGPD: REALIDADE BRASILEIRA E COMPARATIVO INTERNACIONAL

Trabalho de Conclusão de Curso de graduação, apresentado à Universidade Federal do Estado do Rio de Janeiro, como requisito parcial para obtenção do grau de Bacharel em Direito.

Orientador: Ricardo Sichel

RIO DE JANEIRO
2021

Catalogação informatizada pelo(a) autor(a)

M363 Madeira Carvalho Fernandes, Mário
Soares da Silveira, João Pedro
LGPD: REALIDADE BRASILEIRA E COMPARATIVO INTERNACIONAL / Mário Madeira Carvalho Fernandes. -- Soares da Silveira, João Pedro. --
Rio de Janeiro, 2021.
80

Orientador: Ricardo Sichel.
Trabalho de Conclusão de Curso (Graduação) - Universidade Federal do Estado do Rio de Janeiro, Graduação em Direito, 2021.

1. Lei Geral de Proteção de Dados Pessoais. 2. Direitos da Personalidade. 3. Regulamento Geral sobre a Proteção de Dados. I. Sichel, Ricardo, orient. II. Título.

JOÃO PEDRO SOARES DA SILVEIRA

MÁRIO MADEIRA CARVALHO FERNANDES

LGPD: REALIDADE BRASILEIRA E COMPARATIVO INTERNACIONAL

Trabalho de Conclusão de Curso de graduação, apresentado à Universidade Federal do Estado do Rio de Janeiro, como requisito parcial para obtenção do grau de Bacharel em Direito.

Orientador: Ricardo Sichel

Aprovado em:

Banca examinadora:

_____

Prof. Dr. Ricardo Sichel (Orientador)
Universidade Federal do Estado do Rio de Janeiro - UNIRIO

_____

Prof. Dr. Celso de Albuquerque
Universidade Federal do Estado do Rio de Janeiro - UNIRIO

_____

Prof. Dr. André Ricardo Cruz Fontes
Universidade Federal do Estado do Rio de Janeiro - UNIRIO

AGRADECIMENTOS

Inicialmente agradecemos imensamente aos nossos queridos pais, cujo apoio incondicional incentivou-nos ao longo de toda essa jornada. Com certeza, qualquer agradecimento será insuficiente para representar toda a importância deles. Agradecemos o companheirismo dos nossos amigos da UNIRIO, onde tivemos o prazer de nos conhecermos e estudarmos juntos diariamente, cuja intensidade durou o tempo necessário para torná-lo inesquecível. Levamos conosco, sem sombra de dúvidas, lembranças de amizades raras, que durarão para o resto da vida. Finalmente, porém não menos importante, agradeço pelos sábios conselhos do professor e orientador Ricardo Luiz Sichel. Com toda a admiração e respeito, agradecemos a confiança, aprendizado e fundamentais orientações para a conclusão deste trabalho. Dessa forma, ainda que neste diminuto espaço, deixamos o nosso agradecimento a todos pelo apoio nos bons e maus momentos dessa jornada acadêmica. Hoje, somos o resultado da confiança e força de cada um de vocês. Obrigado!

RESUMO

O presente trabalho acadêmico tem como escopo promover uma breve análise da nova sistemática de proteção de dados no Brasil. Este trabalho de conclusão de curso estudará a evolução legislativa do tema no Brasil e sua problemática, sob a ótica dos novos desafios a serem enfrentados para a efetivação do direito fundamental da privacidade, a fim de proporcionar instrumentos mais claros e eficazes para os indivíduos zelarem pelas informações que lhe dizem respeito. Foi realizada uma pesquisa quantitativa para aferir o entendimento da população a respeito da privacidade dos dados e a promulgação da LGPD. Por fim, foi feito um breve resumo das principais legislações internacionais de proteção de dados e uma comparação entre a GDPR e a LGPD.

Palavras Chave: Direito Constitucional e Civil – Proteção de Dados Pessoais – LGPD – GDPR – Privacidade

ABSTRACT

The present academic work aims to promote a brief analysis of the new data protection system in Brazil. This course conclusion paper will study the legislative evolution of the theme in Brazil and its problematic, from the perspective of the new challenges to be faced for the realization of the fundamental right of privacy, in order to provide clearer and more effective instruments for individuals to watch over their information. A quantitative survey was carried out to assess the population's understanding of data privacy and the enactment of the LGPD. Finally, a brief summary of the main international data protection laws and a comparison between GDPR and LGPD was made.

Key Words – Constitutional and Civil Rights – Personal Data Protection – LGPD – GPDR – Privacy

SUMÁRIO

1. INTRODUÇÃO

O presente trabalho abordará um tema caro à sociedade moderna, a proteção de dados pessoais. Em um contexto de crescente utilização de recursos tecnológicos como internet, aplicativos, computadores, celulares, tablets, entre outros, que acompanham de forma praticamente constante o cotidiano de cada indivíduo, as coletas e trocas de informações, muitas vezes envolvendo dados pessoais, são ininterruptas ao longo do dia.

Essa interação íntima entre ser humano e tecnologia é reflexo das mudanças gritantes dos hábitos, das percepções de tempo e no modo como as atividades e tarefas são desempenhadas, das mais básicas e rotineiras possíveis às mais complexas. A relação de dependência do ser humano com a máquina se estende à execução de funções que outrora não necessitavam tal empenho e, além disso, estão, na maioria dos casos, atreladas à cessão dos dados pessoais de quem as utiliza.

Alguns dos inúmeros exemplos que podem ser citados é a maneira como o deslocamento ocorre em uma cidade. Antes das facilidades implementadas pela tecnologia da informação, quando se queria chegar a um local específico, o qual não se tinha conhecimento, alguns passos deveriam ser seguidos: utilizava-se uma lista de endereços, para descobrir o nome da rua e o número do local; o mapa da região era consultado, para se determinar qual a melhor caminho a ser seguido; perguntava-se a alguém as direções e pontos de referência para descobrir se a localidade alcançada era a correta. Neste cenário, nenhuma troca de informações pessoais estaria ocorrendo mandatoriamente entre os envolvidos nas ações praticadas.

Por outro lado, na atualidade, para a solução do mesmo problema, uma cadeia diferente de ações entra em curso. A pessoa interessada em descobrir como chegar a um local pode simplesmente buscar em seu celular, ligado ao internet, pelo nome do local que pretende visitar e todas as informações necessárias estarão em suas mãos, incluindo: endereço; pontos de referências; horário de funcionamento; qual o tempo estimado de percurso; qual o melhor caminho; quais serviços de transportes estão disponíveis, bem como seus valores; as avaliações de

frequentadores sobre a localidade; entre diversas outras informações, que podem ou não ser de interesse do usuário.

Pela análise dos casos apresentados, nota-se como a modernidade foi capaz de reduzir as etapas necessárias para se obter as respostas almejadas, agilizando e facilitando todo o processo. Porém, no curto período de tempo investido, várias informações pessoais foram trocadas: como a localização da pessoa que realizou a pesquisa; seu interesse do usuário pelo local pesquisado; as opiniões pessoais de diferentes pessoas por meio das avaliações consultadas; as informações sobre motoristas de aplicativos da região; fotos do local, que podem incluir imagens de outros frequentadores, entre outras que podem ser obtidas facilmente com apenas alguns passos.

Visto isso, a celeridade demandada e permitida pela vida moderna e seus desenvolvimentos tecnológicos, traz com ela também um novo custo para permitir seu pleno funcionamento, a coleta de informações pessoais dos que a utilizam.

As influências, desdobramentos e consequências, sociais e jurídicas, das mudanças na realidade, como está ora apresentada, serão detalhadas e analisadas no decorrer do trabalho.

O desenvolvimento das tecnologias da informação colocou os dados pessoais dos indivíduos em um patamar de compartilhamento, troca e valor nunca antes vislumbrado pelas sociedades que o precederam. A alcunha de “sociedade da informação” não é à toa, a informação e, por consequência, os dados, de onde ela é extraída, adquiriram um valores inéditos, passando a serem tratadas como produto e movimentando diferentes áreas econômicas, principalmente a publicidade.

O advento da exploração de dados pessoais, espécie dos direitos da personalidade, de maneira desenfreada, colocou os seus titulares em uma posição de submissão em relação às organizações que deles fazem uso, abrindo margem para possíveis abusos e danos. Com o intuito de conceder isonomia aos novos tipos de relações que surgiram, a legislação evoluiu no sentido de atribuir ao titular maior controle sobre seus dados, respeitando os princípios e direitos fundamentais da pessoa humana, consagrando o direito da autodeterminação informativa. Tal direito diz respeito à capacidade de uma pessoa poder determinar o tratamento a ser

empregado sobre seus dados pessoais, incluindo quais os dados que serão trabalhados, quem o realiza, como, por qual motivo, por quanto tempo e outras autonomias.

No caso brasileiro, em acordo com a evolução cenário mundial, o ordenamento jurídico prosperou para garantir os direitos e deveres referentes ao tratamento de dados pessoais, atingindo maior maturidade com a vigência da Lei Geral de Proteção de Dados Pessoais (LGPD).

Porém, apenas a criação de uma lei delimitando os limites para a utilização dos dados pessoais no brasil não é suficiente para que a uma proteção efetiva desse bem da personalidade realmente ocorra. Para tanto, é necessária a criação e implementação de uma cultura de proteção de dados, por parte da população e também das organizações que realizam tratamento.

Conforme será demonstrado no decorrer dos próximos capítulos, ainda falta à população em geral o conhecimento sobre as garantias legais que lhes são conferidas, dificultando, assim, que os direitos atribuídos sejam efetivamente exercidos. Assim, os danos e abusos se tornam banalizados e passam despercebidos, não havendo uma verdadeira mudança no tratamento de dados como pretendida pela legislação.

Na mesma direção, as organizações não se sentem obrigadas a cumprirem os requisitos da lei pela falta de pressão dos usuários e das agências de fiscalização. O que além de um dano para os cidadãos afeta a competitividade das empresas nacionais no mercado internacional, por não estarem adaptadas ao novo modelo de proteção de dados pessoais.

Logo, percebe-se que um investimento na divulgação das informações é necessário, bem como a aplicação efetiva de fiscalizações e sanções, caso contrário, a lei se tornará letra morta. Neste cenário, cidadãos e organizações se prejudicam, os primeiros por terem seus direitos ceifados, e os segundos por não estarem em compatibilidade com os paradigmas internacionais, prejudicando o comércio, negócios e relações com outros países.

Tendo em vista que a LGPD foi criada, com base na legislação europeia, uma das pioneiras no tema, como forma de se adaptar às mudanças no

entendimento a nível internacional, entender e comparar as similaridades e diferenças entre as normas nacionais e internacionais é de suma importância para se entender como se dará a implementação em território nacional e que aspectos precisam ser mais bem trabalhados.

1. HISTÓRICO SOBRE A PROTEÇÃO DE DADOS

2.1. Evolução da sociedade e os dados

A coleta e troca de informações sempre fez parte do desenvolvimento da sociedade. A capacidade de gerar, trocar e armazenar conhecimento permitiu que os seres humanos pudessem desenvolver técnicas, tecnologias, construções, mecanismos que não seriam possíveis com o trabalho de apenas um indivíduo isolado durante seu curto período de vida. Uma comunicação bem desenvolvida, ordenada e direcionada a geração e propagação de conhecimento sempre foi o grande trunfo dos humanos sobre o resto da natureza, indo desde o desenvolvimento da agricultura e criação de ferramentas básicas, até a construção de estações espaciais e conexão entre pessoas do mundo inteiro em menos de um segundo.

As informações, inicialmente transmitidas pela fala, dentro de uma comunidade específica e de difícil preservação, depois evoluindo para a forma escrita, melhor preservável e melhor transmissível, estavam atreladas a uma posição de poder. O Estado, a Igreja ou qualquer outra figura que assumisse a posição de autoridade em uma sociedade mantinham controle sobre a informação, como ela seria transmitida, armazenada, para quem e para qual finalidade.

A informação como uma ferramenta de controle é empregada pelos Estados há séculos, acumulando e organizando as informações sobre a sociedade de forma que os interesses do Estado fossem desenvolvidos. No que diz respeito a posição dos Estado absolutistas, Burke (2003, p. 112) afirma:

> O principal aqui diz respeito à acumulação de informações como formas tanto de reação como de auto-estímulo ao desejo crescente dos governantes de controlar as vidas do povo em geral, fosse para aumentar os impostos, alistá-lo no exército ou alimentá-lo em tempos de fome.

Na Idade Média, as informações passam a se submeter ao crivo da Igreja

Católica, exercendo um controle sobre a informação, bem como a interpretação que poderia ser a ela atribuída, além de delimitar a distribuição. Com ela surgem as primeiras burocracias (BURKE, P., 2003).

Com a chegada da era mercantilista, os Estados passaram a usar a burocracia para o recolhimento e tratamento das informações que lhes eram úteis. Porém, com a invenção da imprensa por Gutenberg, aumentando a capacidade humana de multiplicar, produzir e divulgar informações, elas ganham um aspecto público, em consequência ao seu barateamento e circulação facilitada. É iniciada a produção de periódicos e livros que alimentam um crescente mercado consumidor (BERNARDI, A. J., 2007).

A partir do surgimento do capitalismo, no período entre os séculos XVII e XVIII, a sociedade passa a entender a informação de uma forma diferente, seguindo a linha de pensamento da época, a organizando de maneira lógica e sistemática para a formação do conhecimento. A nova estrutura social forneceu ao conhecimento um caráter científico utilitário, saindo de uma visão estritamente de crescimento intelectual e pessoal humano para uma aplicação prática, tendo como foco o estudo e desenvolvimento tecnológico (BERNARDI, A. J., 2007).

Com a evolução da sociedade capitalista, os meios de proteção social foram mitigados, restando o indivíduo submetido à lógica do mercado e à padronização oriunda do fordismo/taylorismo, na chamada sociedade de massa. A comunicação de massa é implantada, advinda das tecnologias desenvolvidas, como rádio e televisão, tornando-se acessível e entendível pela maior parte da população.

Já no final do século XX, com a contínua evolução das tecnologias da informação, a internet e o computador pessoal são desenvolvidos, o que modifica a maneira como a informação interage com a sociedade. A forma como ela é produzida e circula se modifica, a partir da abertura da comunicação entre diferentes pontos e de forma bidirecional, interrompendo a padronização de conteúdo que se estabelecera.

Com as mudanças na sociedade de viés tecnológico e social a informação passou a assumir um caráter central, deixando de ser algo apenas restrito a um grupo seleto e passou a estar inserida no meio social de maneira

essencial para o seu funcionamento. O cenário descrito se inicia após a Segunda Guerra Mundial, atrelado não só à revolução tecnológica que deu origem à internet e aos computadores, como à exigência de uma mão-de-obra mais especializada. Tal conjuntura é conhecida por autores como a Terceira Revolução Industrial.

Segundo Klaus Schwab (2018, p. 28):

> Por volta de 1950, as principais tecnologias da Terceira Revolução Industrial – a teoria da informação e a computação digital – passaram por avanços revolucionários. Assim como ocorreu nos períodos anteriores, a Terceira Revolução Industrial não ocorreu por causa da existência das tecnologias digitais, mas pelas mudanças que essas tecnologias promoveram no nosso sistema econômico e social. A capacidade de armazenar, processar e transmitir informações em formato digital deu nova forma a quase todas as indústrias e mudou drasticamente a vida profissional e social de bilhões de pessoas.

A evolução tecnológica criou mecanismos capazes de processar e transmitir as informações em quantidade e velocidade nunca antes vislumbradas. As relações sociais, por sua vez, foram amplificadas para um estado em que as barreiras físicas já não significam obstáculos. Uma nova compreensão da relação entre tempo e espaço é estabelecida.

Um novo paradigma técnico-econômico passa a se estabelecer, denominado “sociedade da informação”, que se refere às mudanças de cunho técnico, organizacional e administrativo, que têm como base insumos de informação. A busca de energia mais barata, produção de mercadoria de forma mais eficiente e com mão-de-obra mais barata ficam mais distantes, uma ruptura do modelo de contrato social entre capital e trabalho, característico do capitalismo industrial (WERTHEIN, J., 2000).

Nesse sentido, Kumar (2006, p. 24) afirma:

> A sociedade da informação, segundo seus teóricos, gera mudanças no nível mais fundamental da sociedade. Inicia um novo modo de produção. Muda a própria fonte da criação de riqueza e os fatores determinantes da produção. O trabalho e o capital, as variáveis básicas da sociedade industrial, são substituídos pela informação e

> pelo conhecimento. A teoria do valor do trabalho, da maneira formulada por uma sucessão de pensadores clássicos, de Locke e Smith a Ricardo e Marx, é obrigada a ceder lugar a uma “teoria do valor do conhecimento”. Agora, “o conhecimento, e não o trabalho, é a origem do valor”.

Algumas características podem ser atribuídas a esse modelo, entre elas: a informação como matéria-prima, o ser humano opera a informação propriamente dita, diferente de usá-la como instrumento para a geração ou modificação de tecnologia; os efeitos das novas tecnologias têm impacto direto em toda atividade humana, devido a integração tão enraizada delas e das tarefas do cotidiano; todas as relações e atividades se comunicam e trabalham em rede; flexibilidade dos processos, com alta capacidade de reorganização e reconfiguração; crescente convergência de tecnologias, vários campos diferentes do saber se associam e crescem de maneira integrada (WERTHEIN, J., 2000).

As mudanças trazidas para a sociedade afetam, também, a maneira como o mercado se comporta. As indústrias, que antes ditavam os bens e serviços que seriam consumidos pela sociedade, agora estão submetidas às necessidades do público que pretende atender. As empresas se dedicam cada vez mais a ouvir e entender as demandas das pessoas para criar o produto que atenda a essas expectativas e corresponder à demanda existente. Caso contrário, acabará rendendo-se à concorrência.

Sobre o tema, de Masi (2014, p. 167) coloca:

> Durante toda a fase industrial, o modelo de organização que liga produto, produtor e mercado é o seguinte: a indústria produz bens, serviços e valores para depois impô-los à sociedade que, exatamente por isso, se chama “industrial”. Com a passagem da sociedade industrial à pós-industrial, as relações de força entre empresa e sociedade são invertidas: se o negócio constituía antes o sistema mais dinâmico, mais moderno, cientificamente antes sofisticado, hoje constitui um dos muitos sistemas que operam na sociedade e nem sempre o mais moderno e dinâmico (...). O esquema representativo das relações entre empresa e sociedade, entre empresa e mercado, está invertido em comparação ao anterior: agora é a sociedade que

> elabora as novas necessidades, os valores emergentes, a demanda latente. (...) Se a empresa não for capaz de elaborar essa decodificação, os seus bens e serviços serão recusados pelo mercado.

Com a internet e as várias possibilidades de interação e expressão de opinião (negativas e positivas) em tempo real, que atingem inúmeras pessoas, como por blogs, websites, redes sociais e etc., os consumidores passaram a influenciar uns aos outros com suas impressões sobre determinados produtos. As pessoas se tornam, praticamente, assistentes de vendas gratuitas, mesmo que não intencionalmente, determinando a aceitação da coletividade sobre um produto ou serviço (BIONI, B., 2021).

A partir desse fenômeno, como já mencionado, o mercado, e seus produtos e serviços, passam a se adaptar às opiniões produzidas, se modelando em vista dos pontos negativos e positivos assinalados pelos próprios consumidores, ora detentores de voz ativa com a amplificação das formas de se expressar (MATTOS, K., 2012). O consumidor deixa de ter uma posição apenas passiva e passa a ter uma participação ativa no ciclo de consumo, viabilizando os sistemas flexíveis de produção, no qual as tendências do mercado consumidor orientam a concepção, confecção e distribuição do bem de consumo (BIONI, B., 2021).

Nesse contexto de produção por demanda, os dados pessoais apresentam um papel basilar no funcionamento do novo mercado. Com o desenvolvimento da ciência mercadológica, principalmente relacionada aos bens e consumo e a sua divulgação, bem como a possibilidade técnica de organização de dados em grandes proporções, de forma inteligente e com possibilidade de realização de projeções (chegando ao patamar de Big Data), desenvolve-se esse mercado no qual as informações dos pessoais são o ativo (BIONI, B., 2021).

Nesta linha, a publicidade sofreu modificações. Ela deixou de ser algo padronizado e unificado, e passou a ser direcionada especificamente para cada usuário, que irá receber o material publicitário determinado. Com base nas preferências individuais dele é escolhido o produto que melhor se encaixa, sendo, portanto, mais efetiva no que se propõe, o consumo. As informações coletadas por

meio de histórico de navegação online, cadastros pessoais em sites ou lojas, cookies de navegação, publicações em redes sociais, localização de GPS, histórico de consumo, utilização de aplicativos e coletam dados em troca de serviços gratuitos, entre outros meios, serão utilizadas como combustível para essa modalidade de publicidade.

A partir da utilização dos dados pessoais coletados e com o avanço das tecnologias da informação, perfis cada vez mais detalhados e certeiros de potenciais consumidores são traçados. Monitorando-se o comportamento quase constantemente é possível inferir o estado emocional, financeiro, de saúde e outros aspectos para se correlacionar à mensagem publicitária ideal.

A utilização, troca, venda, fornecimento, distribuição, autorização de uso, armazenamento em banco de dados, realização de projeções, inferências, análises entre outras práticas relacionadas aos dados pessoais constituem o novo mercado da sociedade da informação. Ele tem como ponto principal a vigilância constante, observando o comportamento das pessoas que o movimentam.

De acordo com Bruno Bioni (2021, p. 42-43):

> (...) Mais do que isso, há um “varejo dos dados pessoais”. Para a operacionalização desse modelo de negócio, há uma complexa rede de atores que transaciona as informações pessoais dos consumidores, agindo cooperativamente para agregar mais e mais dados e, em última análise, tornar a mensagem publicitária ainda mais eficiente.

Essa hipervigilância e a criação de perfil virtual onisciente pelas empresas acaba por gerar uma despersonalização do indivíduo e afeta diretamente suas possibilidades de escolha, que perde o controle sobre a expressão de sua personalidade.

Dessa forma, a ciência jurídica necessitou se adequar à nova realidade, com o intuito de regular as novas relações sociais e se preparar para lidar com as problemáticas que dela surgem e proteger os dados pessoais utilizados como mercadoria. O indivíduo deve ser empoderado para exercer um controle sobre esse seus dados utilizados e não devendo o fluxo informacional ser submetido ao mercado e aos interesses econômicos existentes (BIONI, B., 2021).

Em decorrência da evolução do entendimento e necessidade de, ao longo dos anos, regular e proteger a utilização dos dados pessoais e proteção deste e outros direitos da personalidade, as sociedades adotaram diferentes modos de interpretação e aplicação dessas garantias.

2.2 Direitos da personalidade e proteção de dados

A construção do entendimento sobre os Direitos Fundamentais, entre eles os Direitos da Personalidade, está associada diretamente com o desenvolvimento da sociedade, da tecnologia e do período histórico vigente.

Norberto Bobbio (2004, p. 25) afirma nessa linha:

> (…) os direitos do homem, por mais fundamentais que sejam, são direitos históricos, ou seja, nascidos em certas circunstâncias, caracterizadas por lutas em defesa de novas liberdades contra velhos poderes, e nascidos de modo gradual, não todos de uma vez e nem de uma vez por todas. (...) os direitos não nascem todos de uma vez. Nascem quando devem ou podem nascer. Nascem quando o aumento do poder do homem sobre o homem — que acompanha inevitavelmente o progresso técnico, isto é, o progresso da capacidade do homem de dominar a natureza e os outros homens — ou cria novas ameaças à liberdade do indivíduo ou permite novos remédios para as suas indigências: ameaças que são enfrentadas através de demandas de limitações do poder; remédios que são providenciados através da exigência de que o mesmo poder intervenha de modo protetor.

Inicialmente, os direitos fundamentais pretendiam apenas garantir a separação entre o indivíduo e o Estado, atribuindo a aquele liberdade. Porém, com a evolução da sociedade, as necessidades e os desejos almejados foram aumentando e se modificando. Pode-se dividir as diferentes eras e os diferentes direitos almejados em gerações já amplamente definidas pela doutrina.

Os chamados direitos fundamentais de primeira geração estão inseridos

no contexto da Revolução Francesa, período de insurgência da população ao Estado absolutista. Eles estão atrelados a ideia de liberdade negativa, pretendendo a ruptura entre a sociedade e o Estado, tendo como exemplos o direito à vida, à propriedade, à inviolabilidade de domicílio, à liberdade de expressão, à liberdade política e religiosa, entre outros (DRESCH, R., 2021).

Nessa época, com o crescimento da visão jusracionalista, contendo traços metodológicos-sistemáticos rígidos e bem definidos, formando um sistema lógico-fechado, surgem as noções de negócio jurídico, relação jurídica e declaração da vontade. A ciência jurídica firma uma posição extremamente patrimonialista, a exemplo do Código Civil Napoleônico. Os direitos da personalidade, inerentes à condição de ser-humano, não ganham espaço no direito privado, por falta de meios para positivá-lo nesse contexto materialista e positivista (BIONI, B., 2021).

Durante os séculos XIX e XX, na segunda geração, os direitos políticos foram introduzidos aos como direitos fundamentais, fortalecendo o indivíduo como um tomador de decisões. Isso abriu espaço para a exigência de que o Estado trabalhasse para possibilitar o exercício das garantias individuais, indo além da isenção negativa do Estado, como relacionadas à educação, saúde, trabalho, moradia, alimentação, segurança, lazer e outros.

Já na terceira geração, que ganhou forças após a Segunda Guerra Mundial, cujas experiências terríveis abriram portas para uma mudança de pensamento, proliferou o ideal de princípio da dignidade humana em diferentes constituições pelo mundo, direitos transindividuais e aplicados à globalização, fraternidade e solidariedade. Objetivam o desenvolvimento, a paz, o meio ambiente, a comunicação, entre outros que são adicionados com o passar dos anos e o surgimento de novas necessidades sociais (DRESCH, R., 2021).

Ademais, no campo no direito privado, se observa o fenômeno da despatrimonialização do direito civil, representado por uma alteração do foco da tutela jurídica, distanciando-se do patrimônio e se voltando ao ser humano.

A Constituição Federal Alemã, por exemplo, começou a considerar a existência do direito ao livre desenvolvimento da personalidade, ao lado do princípio da dignidade da pessoa humana. A tutela dos direitos da personalidade pode ser

replicada às normas infraconstitucionais daquele país, possibilitando sua aplicação das relações privadas e a definição de quais seriam esses direitos (BIONI, B., 2021).

No Brasil, os direitos da personalidade foram contemplados de forma expressa pelo ordenamento no Código Civil de 2002, mesmo já sendo reconhecido por interpretação doutrinária. O novo Código Civil simbolizou o processo de despatrimonialização do direito civil, buscando uma humanização do direito privado, foco na proteção da tutela e promoção da pessoa humana. Nele foram enumerados alguns dos direitos da personalidade, como direito ao nome, à vida, à privacidade, à intimidade, à imagem, entre outros, por não se tratar de um rol taxativo. Se iniciou um novo tripé para a teoria geral do direito brasileiro: personalidade, negócio jurídico e patrimônio (AMARAL, F., 1999)

Os direitos da personalidade são aqueles necessários ao livre desenvolvimento e expressão da personalidade humana, características incorpóreas e corpóreas que compõem a projeção da pessoa humana, possuindo uma conotação extrapatrimonial. Frente à grande produção de dados pelas pessoas no universo da sociedade da informação, é possível enquadrar a proteção de dados pessoais como uma das espécies de direitos necessários ao fim de plena promoção da personalidade. Os dados pessoais adquirem a atribuição de um novo tipo de identidade, devendo, por conseguinte, revelar informações corretas, em fidelidade ao seu titular.

A proteção de dados é um direito da personalidade autônomo, não estando atrelado apenas ao direito à privacidade, pois ele está atrelado a outras questões próprias que vão além da privacidade. Ela está relacionada a autodeterminação, não discriminação, livre iniciativa, livre concorrência, e proteção ao consumidor, liberdade de expressão, de informação, de comunicação e de opinião, a inviolabilidade da honra e da imagem, da intimidade, desenvolvimento econômico e tecnológico, entre outras (DRESCH, R., 2021).

Além disso, o Brasil é signatário da Declaração de Santa Cruz de La Sierra (2003), que dispõe que a proteção de dados pessoais é um direito fundamental das pessoas.

Na atualidade a proteção de dados passou até uma importância crescente

e se tornando uma disciplina autônoma, buscando estabelecer um equilíbrio razoável entre a proteção dos dados pessoais e a circulação dos dados. Tem fundamentação no Direito Civil, por tratar de um direito da personalidade, e também gera repercussão no Direito do Consumidor, do Trabalho, Administrativo e Penal.

Por estar ligada a assuntos complexos e que dizem respeito a diferentes áreas do Direito, o ordenamento jurídico deve estar apto a receber esse direito e a ele ser compatível. Além disso, uma normatização específica para garantir a proteção de dados pessoais é necessária.

2.3 Legislação de proteção de dados e Criação da LGPD

Um caso emblemático que trouxe luz para a premência e importância da tutela quanto à proteção de dados pessoais foi o caso da decisão da Corte Constitucional alemã a respeito da Lei do Censo de 1983 do país.

A Lei ora em tela determinava que os cidadãos fornecessem um rol de dados pessoais com o intuito de verificar a distribuição geográfica da população pelo território alemão. Porém, além disso, a ela previa que tais informações fornecidas pudessem ser cruzadas com outros registros existentes para atender uma finalidade genérica de permitir a execução de atividades administrativas de diferentes escopos e não específicas (MARTINS, L., 2005).

Diante de tal arbitrariedade e da falta de clareza dos fins almejados, bem como as incertezas quanto às futuras coletas de dados, sua aplicabilidade e privacidade, uma miríade de ações foram ajuizadas perante o Tribunal Constitucional alemão. A Corte findou por declarar a inconstitucionalidade parcial da lei, entendendo que a finalidade dos dados compartilhados deveria ser clara, se dedicando unicamente às atividades de recenseamento (MARTINS, L., 2005).

A decisão referida gerou alta repercussão pelas conclusões e entendimentos firmados, que acabaram refletindo no restante da Europa. O raciocínio empregado foi no sentido de entender a proteção de dados pessoais como uma espécie dos direitos da personalidade, autônoma, e que o consentimento

do titular apresenta limites e funções específicas, estando a autodeterminação informacional além do mero consentimento do titular, ou seja, desatrelada a ele.

De acordo com o Tribunal, a atividade de processamento de dados pessoais necessita de limites, devendo ser aplicadas medidas de precaução organizacionais e processuais para prevenir a violação do direito da personalidade, mesmo que o consentimento do titular esteja presente. Tais práticas tem como intuito permitir que a utilização das informações pessoais não interfiram no desenvolvimento da personalidade dos cidadãos.

Entendeu-se que qualquer dado pessoal, sendo ele sensível (que diz respeito a algo íntimo ou possa ser objeto de discriminação) ou não, pode, em associação a outras informações, trazer um efeito prejudicial ao titular, revelando revelar informações que tragam estigmas e possibilitar práticas de discriminação social. Compreende-se disso, a exigência colocada pelo Tribunal de que os dados pessoais fossem anonimizados e de emprego restrito a finalidade particular predeterminada.

Ainda na década de 1980, a Organização para o Desenvolvimento e Cooperação Econômica (OCDE) estipulou diretrizes sobre o tema da proteção de dados pessoais. As diretrizes emitidas tinham o intuito de conferir segurança jurídica ao cidadão, ao Estado e ao setor privado sobre como deve ocorrer o fluxo de dados desse tipo, trazendo confiança a todas as partes envolvidas nessas relações e permitindo o seu prosseguimento.

As primeiras leis gerais de proteção de dados começam a surgir em alguns países europeus, entre eles Áustria, França, República Federal da Alemanha e Noruega.

Em 1981, se estabelece a Convenção 108 do Conselho da Europa para a Proteção das Pessoas Singulares no que tange o Tratamento Automatizado de Dados Pessoais. Ela foi o primeiro instrumento juridicamente vinculativo de abrangência internacional para a proteção de dados pessoais, com o intuito de garantir a todas as pessoas o respeito pelos seus direitos e liberdade fundamentais, principalmente à privacidade, face ao tratamento automatizado dos seus dados.

A União Europeia passa a adotar as normativas de proteção de dados da

Diretiva 95/46/CE de 1995, estipulada pelo parlamento europeu e conselho da União Europeia, que versa sobre a proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação deles. Essa diretiva teve o papel de estabelecer definições básicas sobre dados pessoais entre outros aspectos correlatos, além de impor um sistema abrangente que acabou afetando também as nações fora da Europa.

Em abril de 2016, o Parlamento Europeu e o Conselho Europeu, adotam o Regulamento nº 2016/679, a “General Data Protection Regulation” (GDPR), revogando a diretiva de 1995. A norma, que entrou em vigor em 2018, estabelece as regras para proteção de todos os cidadãos da UE contra violações da privacidade e dos dados pessoais, estabelecendo um quadro claro e coerente para as empresas. Entre os direitos concedidos aos cidadãos estão: o consentimento claro e positivo do tratamento dos seus dados; o direito de receber informações compreensíveis sobre os mesmos; o direito ao esquecimento, possibilidade de solicitar a supressão dos seus dados; o direito a transferência dos seus dados para outra operadora de serviços; o direito ao conhecimento do estado de segurança de seus dados. As regras se aplicam às empresas que operam na UE, mesmo que tenham sede fora dela. Além disso, é permitida a imposição de medidas corretivas às empresas que violem as regras, advertências e multas.

A GDPR estabelece, ainda, que os Estados Membros da UE somente poderão realizar comércio e serviços, no que se refere a utilização de dados pessoais, com outras nações somente quando elas adotarem legislações minimamente semelhantes às dela, com o intuito de garantir a proteção dos dados de cidadãos europeus mesmo quando o tratamento de dados ocorra fora do território da União Europeia.

Tal restrição impulsionou que diversos países, incluindo o Brasil, se mobilizassem para agilizar a tramitação e promulgação de suas respectivas legislações de proteção de dados, para não haver uma perda de competitividade nas relações com o bloco europeu.

No ordenamento brasileiro, podem ser ressaltados alguns marcos normativos que adentram a seara da proteção de dados.

O direito à privacidade das informações pessoais é assegurado pela Constituição da República Federativa do Brasil (CRFB), como versa o artigo 5º, inciso XII:

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

Da mesma forma, o direito à privacidade também é contemplado na CRFB, no artigo 5º, inciso X: “X - 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”.

O Código de Defesa do Consumidor (CDC) também já iniciou um esboço da proteção de dados pessoais no Brasil, no que se refere ao direito de acesso aos seus dados pessoais, bem como o direito a veracidade dados, a exclusão, a prazo de validade de utilização e a correção, quando forem objeto de tratamento pelas empresas:

> Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.
>
> § 1° Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos.
>
> § 2° A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele.
>
> § 3° O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas.

> § 4° Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público.
>
> § 5° Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores

A Lei de Acesso à Informação (12.527/2011) também adentrava o tema no que se refere ao tratamento de dados pessoais realizado pelo poder público. Ela apresenta a definição de dados pessoais: “Art. 4º Para os efeitos desta Lei, considera-se: IV - informação pessoal: aquela relacionada à pessoa natural identificada ou identificável;”.

Além disso, dita lei estabelece, em seu artigo 31, as diretrizes para o tratamento das informações pessoais, respeitando os direitos fundamentais da pessoa humana, garantindo o direito ao acesso pelo titular, o direito à privacidade e o controle sobre o acesso dos dados por terceiros e a sua divulgação, bem como as hipóteses que permitem o compartilhamento dos dados sem o consentimento expresso. Dentre esses casos é possível destacar: prevenção e diagnóstico médico; realização de estatísticas, de forma anonimizada; cumprimento de ordem judicial; defesa dos direitos humanos; proteção do interesse público.

Destaque também ao Marco Civil da Internet (Lei nº 12.965/2014), primeiro a estabelecer os princípios, direitos e garantias do uso da internet no Brasil. Traz algumas diretrizes gerais para o uso dos dados na internet, mas não garante a proteção de dados de maneira estruturada, abrangente e completa.

Entre os direitos que podem ser destacados estão: inviolabilidade da intimidade e da vida privada; inviolabilidade e sigilo do fluxo de comunicações pela internet; não fornecimento a terceiros de dados pessoais, salvo quando há consentimento expresso ou nas hipóteses da lei; consentimento expresso para a coleta, uso , armazenamento e tratamento de dados pessoais; fornecimento de informações claras e completas sobre a coleta, uso, armazenamento, tratamento e proteção de dados pessoais, podendo ser usado apenas para finalidades

justificadas, específicas e legais; exclusão dos dados pessoais ao término da relação entre as partes.

Motivado pelos movimentos internacionais já citados, principalmente pelas restrições europeias quanto às relações comerciais com países que não adotassem leis de proteção de dados compatíveis, os legisladores reuniram e desenvolveram as normas referentes ao assunto em um código único. Surgem daí os movimentos para a criação da Lei Geral de Proteção de Dados (LGPD), seguindo os moldes da GDPR.

Sancionada em 14 de agosto de 2018, a LGPD teve como objetivo elevar a privacidade e proteção de dados pessoais iniciada nos dispositivos anteriores, além de fornecer o poder às entidades reguladoras para fiscalização das organizações que lidam com o tema, em especial a Autoridade Nacional de Proteção de Dados (ANPD). A lei reforça também os direitos do consumidor no contexto da sociedade da informação, em que os dados são tratados como mercadoria.

A nova normativa garantiu aos cidadãos brasileiros um maior controle e direitos sobre a utilização de seus dados pessoais, independente da onde ocorra esse tratamento, se é realizado por instituições privadas ou públicas, independente do meio empregado ou se realizado por pessoa física ou jurídica. Esses direitos saem do plano da relação de consumo e passam a ser direitos fundamentais da pessoa humana.

Nas palavras de Pinheiro (2020, p. 16):

> O espírito da lei foi proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, trazendo a premissa da boa-fé para todo o tipo de tratamento de dados pessoais, que passa a ter que cumprir uma série de princípios, de um lado, e de itens de controle técnicos para governança da segurança das informações, de outro lado, dentro do ciclo de vida do uso da informação que identifique ou possa identificar uma pessoa e esteja relacionada a ela, incluindo a categoria de dados sensíveis.

A Lei entrou em vigor em 18 de setembro de 2020 em relação à maioria

de seus artigos, mas as sanções presentes só estarão válidas a partir de 1º de agosto de 2021. Tendo vista a realidade da sociedade atual e a implementação da nova normativa, este trabalho é de grande importância para entender como as partes ligadas ao tratamento de dados pessoais se encontram no que se refere a adaptação à normativa, bem como o comparativo com a legislação europeia para se perceber as diferenças e adaptações que deverão ser realizadas no caso brasileiro.

2. OBJETIVOS DA LGPD E ENTENDIMENTO POPULAR

A sanção e vigor da Lei Geral de Proteção de Dados Pessoais representa um considerável avanço para a proteção de dados no Brasil, trazendo exigências para as empresas e organizações e tutela os cidadão em diferentes aspectos.

Direitos e garantias foram previstos em diferentes pontos da Lei, com o intuito de garantir um maior controle de cada indivíduo sobre os seus dados pessoais, que ele cede no contexto social que ora opera. Além disso, são estabelecidas restrições sobre as condições em que tais dados serão recolhidos e para quais finalidades, bem como estabelece sanções no caso do não cumprimento das exigências e cria uma autoridade nacional para fiscalizar todo o andamento.

A esse respeito, Mendes e Doneda (2018, p. 566) relatam:

> A lei aprovada proporciona ao cidadão garantias em relação ao uso de seus dados, a partir de princípios, de direitos do titular de dados e de mecanismos de tutela idealizados tanto para a proteção do cidadão quanto para que o mercado e setor público possam utilizar esses dados pessoais, dentro dos parâmetros e limites de sua utilização.

Juntamente com a Lei de Acesso à Informação, o Marco Civil da Internet e o Código de Defesa do Consumidor, a LGPD completa o marco regulatório brasileiro que representa a Sociedade da Informação. Ela, sob a interpretação dos princípios constitucionais (dignidade da pessoa humana, sigilo de dados, privacidade, proteção do consumidor e outros), representa uma evolução das garantias e direitos fundamentais dos cidadãos. Porém, sem prejudicar o uso econômico dos dados, apenas o regulando baseado nos mesmos princípios.

A lei deixa expresso, em seu artigo 6º, alguns princípios que devem nortear o tratamento de dados pessoais, além da boa-fé. Dentre eles, cabe o destaque ao seguintes: o princípio da finalidade, que se trata da vinculação entre o tratamento de dados específicos a uma finalidade determinada, legítima, explícita e comunicada ao titular; o princípio da adequação e da necessidade, levantando que o

tratamento empregado deve ser compatível a finalidade desejada e informada ao titular, devendo ser o mínimo necessário, restringido aos dados pertinentes e de maneira proporcional; o princípio do livre acesso, que permite aos titulares a consulta facilitada e gratuita a respeito da forma e duração do tratamento e a integralidade dos dados pessoais; o princípio da qualidade dos dados, que se refere a exatidão das informações, se mantendo claras, exatas, relevantes e atualizadas, para permanecerem de acordo com as necessidades e finalidades previstas.

Além dos já citados, têm-se ainda: o princípio da transparência, preconizando informações claras, precisas e de fácil acesso sobre os trâmites de tratamento e seus agentes; o princípio da segurança, associado a utilização de medidas técnicas e administrativas propícias a defender os dados pessoais de acesso não autorizado, bem como situações acidentais ou ilícitas que resultem em perda, destruição, modificação, comunicação ou compartilhamento; o princípio da prevenção, que compreende a incorporação de medidas para prevenir danos decorrentes do tratamento de dados pessoais; o princípio da não discriminação, que impede a realização de tratamento de dados de forma discriminatória ou abusiva, ou que tenha está finalidade; o princípio da responsabilização e prestação de contas, delimitando que o agente deve demonstrar a adoção de medidas eficazes e capazes par ao cumprimento das normas de proteção de dados pessoais.

Seguindo os princípios apresentados, a LGPD versa sobre o tratamento de dados pessoais, por pessoas naturais ou jurídicas, realizado por qualquer meio, procurando garantir a proteção dos direitos fundamentais, da privacidade e permitir o desenvolvimento da personalidade da pessoa natural titular dos dados. As normas gerais precisam ser observadas a nível nacional, compreendendo a União, os Estados, o Distrito Federal e os Municípios.

Para o tratamento dos dados pessoais seguir os princípios apresentados e estar em harmonia com o restante do ordenamento, alguns requisitos são impostos pela lei. Modalidades diferentes de bases normativas foram criadas para recepcionar os casos possíveis de tratamento. São eles: quando o consentimento do titular é fornecido; para o cumprimento de obrigação legal ou regulatório pelo controlador; quando recolhido pela administração pública para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas, com previsão

legal, em regulamentos ou respaldada em contratos, convênios ou instrumentos congêneres; quando realizado por órgãos de pesquisa para a realização de estudos, havendo, quando possível, a anonimização dos dados; quando necessário a execução de contrato ou procedimento preliminar do qual o titular seja parte e a pedido deste.

Outras bases legais adotadas são: quando se almeja o exercício regular do direito em processo judicial, administrativo ou arbitral; com o intuito de proteger a vida ou a integridade física do titular ou terceiro; para a tutela da saúde; quando necessário para atender aos interesse legítimos do controlador ou de terceiros, exceto nos casos em que os direitos e liberdades fundamentais do titular prevaleçam, no que se refere a proteção de dados pessoais; para a proteção do crédito.

O consentimento merece um destaque maior, por se tratar do principal requisito de validade. Isso se deve a sua maior utilização em comparação às outras modalidades de base de adequação, sendo aplicado, inclusive, nos casos de dados pessoais considerados sensíveis, assim classificados por terem como teor atributos capazes de gerar preconceitos ou discriminações frente a sociedade que se inserem. Para tanto, a lei estabelece que o consentimento deve ser expresso, livre e informado por manifestação própria, fornecido por meio escrito ou outro que demonstre a manifestação da vontade do titular, além de estar atrelado a finalidade pré-determinada. O ônus probatório recai sobre o controlador no que tange a obtenção do consentimento nos moldes legais.

Outro destaque com relação ao consentimento, nas relações de consumo, é que a noção de consentimento “livre” implica que o não fornecimento do consentimento, aceitação das condições impostas, não pode ser um impeditivo para a utilização do serviço ou o acesso ao produto (BLUM, R., et al., 2019).

A proteção desses dados implica na manutenção do direito à intimidade, colaborando na autodeterminação informativa, e do direito à identidade pessoal, impedindo sua alteração por informações inexatas ou incompletas. Para tanto, é necessário que as pessoas tenham conhecimento e controle sobre a coleta e o processamento dos dados oferecidos, principalmente dos dados pessoais, que são o que identificam, possibilitando a limitação no seu uso e a diminuição de eventuais

falhas, ilegalidades e danos.

Os direitos atribuídos aos titulares de dados, especificamente dispostos na lei, em sintonia com os princípios e objetivos da normativa, são em sua maioria instrumentos para permitir a preservação da personalidade e evitar que danos a ela ocorram. É assegurado à pessoa natural a titularidade de seus dados pessoais e garantidos os direitos fundamentais. Face ao controlador, o titular é possuidor de alguns direitos específicos, em relação aos dados por ele tratados, mediante requisição, entre eles: a confirmação da existência de tratamento; acesso aos dados; correção de dados; anonimização, bloqueio ou eliminação de dados; portabilidade dos dados a outro fornecedor de serviço ou produto; eliminação dos dados pessoais tratados; obter informação quanto quais entidades públicas e privadas o controlador realizou uso compartilhado de dados; obter informação quanto a possibilidade de não fornecer consentimento e suas consequências; e requerer a revogação do consentimento.

Para avaliar o conhecimento da população quanto a utilização de seus dados e seus direitos, bem como a divulgação de tais garantias para empresas e pessoas, um questionário foi desenvolvido com algumas perguntas que endereçam o tema proposto.

A pesquisa foi criada e respondida por meio da plataforma Google Forms e foi respondida por cerca de 100 pessoas durante o período que esteve disponibilizada. Os participantes que aceitaram participar do projeto apresentam faixa etária diversa, indo de 17 a 70 anos, bem como áreas de atuação profissional distintas, incluindo profissionais do direito e da área da saúde (maioria), além de outros ramos.

Inicialmente, foi perguntado se os participantes já haviam questionado o motivo da coleta de determinado que fora requerido ao realizar compra, contratar serviço ou preencher um cadastro.

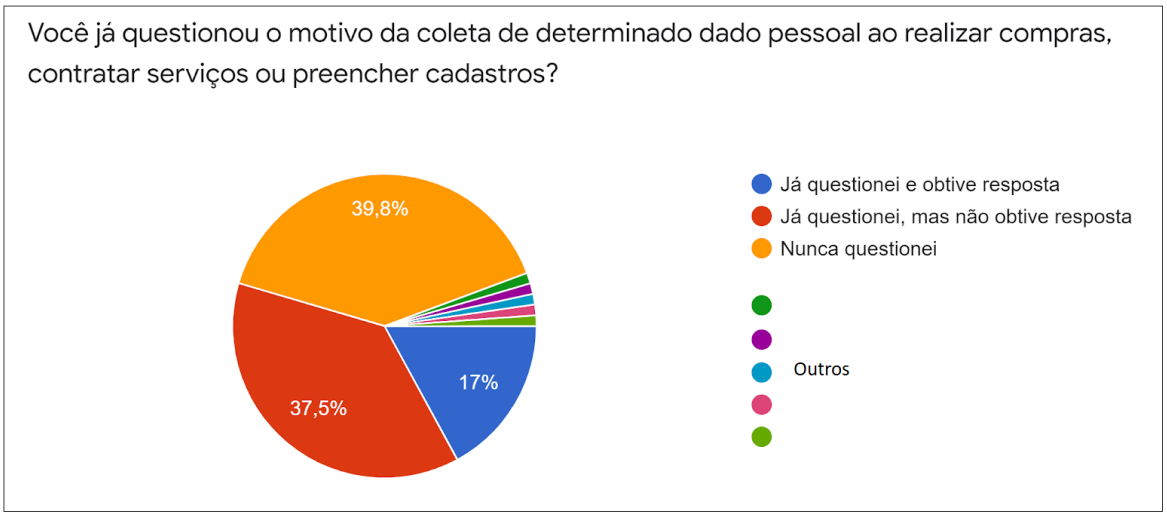

fig. 1

Como possível observar no gráfico com o resultado, um pouco mais da metade dos participantes (57,48%, incluindo as respostas por extenso que não aparecem na legenda do gráfico e estão representadas pelas outras cores) já questionou o motivo do recolhimento de dados, em consonância com o direito do titular de obter informações sobre o recolhimento dos seus dados e as consequências caso este não seja efetuado, bem como os princípios da transparência e livre acesso. Embora represente uma porcentagem considerável, ainda é um número baixo, levando em consideração a importância que os dados adquiriram na sociedade e os prejuízos que o uso equivocado ou desnecessário dessas informações pode causar a autodeterminação do titular, incluindo o vazamento de informações, o compartilhamento com terceiros não divulgado e ou fraudes e ocorrências.

É possível notar que 39,8% não têm conhecimento a respeito das garantias que lhe são atribuídas pela lei ou simplesmente não se importam com o que acontecem com suas informações pessoais, possivelmente por desconhecer os riscos e o valor que elas representam. Isso mostra que o esclarecimento a respeito do tema ainda é bastante escasso para esta parcela da população, o que prejudica o cidadão por deixá-lo exposto na nova realidade que vigora.

Ademais, 37,5% dos pesquisados afirmou que mesmo após a realização da indagação, a empresa permaneceu sem um posicionamento quanto ao motivo do

recolhimento dos dados. Entende-se que uma considerável parcela das empresas ainda não está adaptada aos novos paradigmas da LGPD, ferindo o princípio da finalidade, transparência, necessidade, livre acesso e prevenção, bem como o artigo 9º, inciso I, que determina que o titular tem direito ao acesso facilitado, de forma clara, adequada e ostensiva, às informações acerca da finalidade específica do tratamento de seus dados pessoais cedidos. Tal prática, além de prejudicar o titular, pelos motivos anteriormente apresentados, prejudica a imagem da empresa aos clientes e prejudica a concorrência nacional e internacional, ela estará atuando de forma desigual e incompatível com o mercado nacional e internacional. Fica claro que as empresas ainda precisam passar por um processo de adaptação mais frutífero e que a fiscalização de ocorrências nesse sentido é mais do que necessária.

Os dois próximos gráficos são representações dos resultados de duas perguntas diferentes, mas que servem ao mesmo propósito: entender a adequação dos termos de uso e políticas de privacidade das organizações à legislação, bem como a atenção que o público a eles dedica.

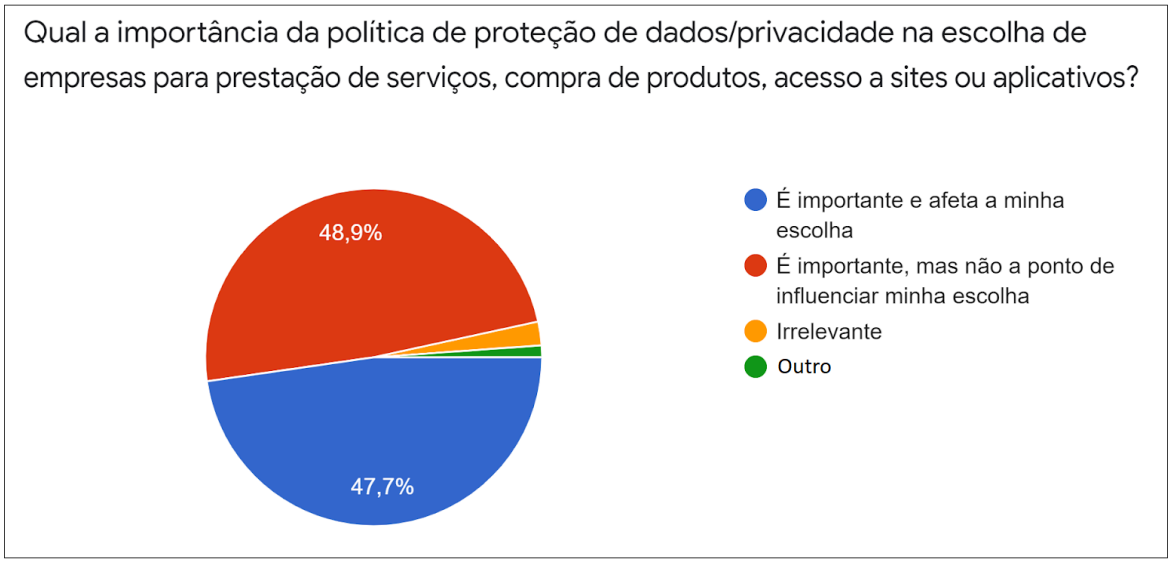

Fig. 2

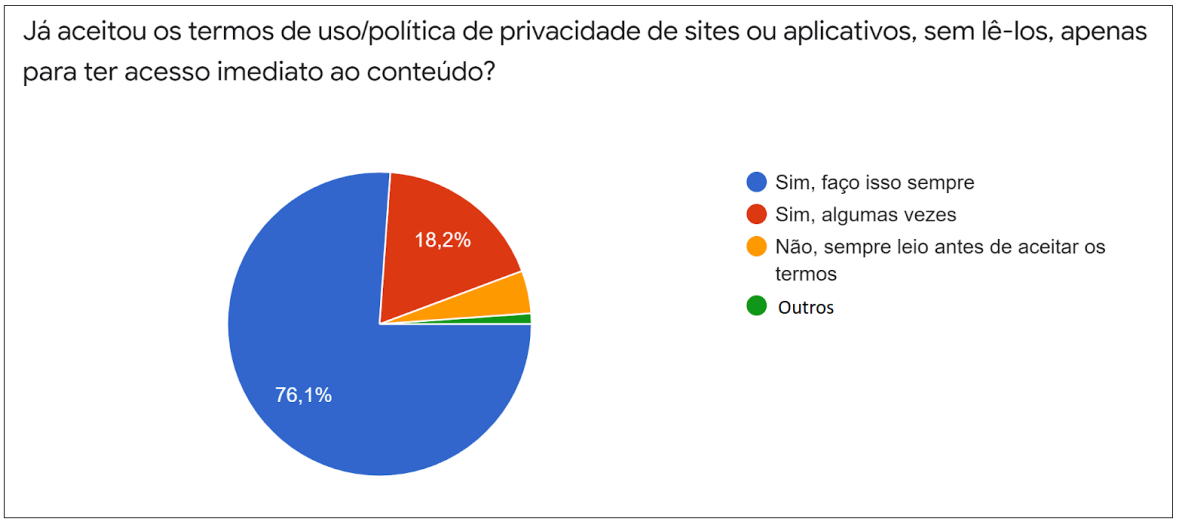

Fig. 3

A primeira pergunta diz respeito à importância dada aos termos de uso ou políticas de privacidade, utilizados frequentemente para obter o consentimento do titular para o fornecimento de seus dados para permitir a utilização do serviço ou produto ofertado. Embora a grande maioria dos entrevistados afirme que eles são importantes, apenas cerca da metade os deixa influenciar na escolha de consumo de serviço, produto, site ou aplicativo. Isso revela que, mesmo dando uma certa importância às medidas de proteção de dados empregadas pela empresa, elas não teriam uma relevância tão grande a ponto de afetar a escolha. Opinião considerada problemática, devido ao alto potencial danoso da utilização indevida de dados pessoais, evidenciando, novamente, uma deficiência da divulgação do tema para a população.

Em relação à segunda pergunta, a mesma conclusão pode ser obtida, ao notar que a maioria dos pesquisados apenas aceita os termos sem ao menos ler-los. Porém, o que se pode aferir é, além do ponto acima posto, que as organizações falham em construir políticas e termos atrativos e de fácil assimilação para o cidadão médio. Frequentemente se nota que tais documentos são apenas longos textos, bastante técnicos e monótonos, que falham em passar efetivamente as informações necessárias ao titular de dados, ferindo os princípios da transparência, finalidade e o artigo 9º da lei.

Além disso, por sua vez, quando aceitos os termos, estes não são a

expressão do verdadeiro consentimento, pois a própria lei o define como uma manifestação livre, informada e inequívoca do titular aceitando o tratamento de seus dados. Logo, não é o caso quando apenas se aceita os termos para ter o acesso desejado, sem a realização de uma ponderação sobre o seu conteúdo, invalidando o principal requisito para se permitir o tratamento de dados.

Far-se-ia necessário a adaptação desses textos para que cumpram a função que lhes é cabida, tendo em consideração a velocidade da vida moderna, cada vez mais exigindo respostas rápidas e eficientes a todos os eventos que cercam o dia-a-dia, bem como a dependência cada vez maior de produtos, serviços e informações que estão atreladas ao tratamento de dados no contexto da sociedade da informação.

Outra questão apurada na pesquisa foi o recebimento de propagandas ou outros meios de contato de organizações com as quais nunca se tenha estabelecido contato direto. A grande maioria dos participantes afirmou que já recebeu esse tipo de contato, de maneira constante (55,7%) ou ocasionalmente (40,9%). Cabe ressaltar que o consentimento para o compartilhamento de dados com terceiros deve ser destacado e específico (art. 7º, § 5º), além de vedado no caso de dados sensíveis para se obter vantagem econômica (art. 11, § 4º). No contexto de uma política de privacidade e termos de uso ineficientes para o recolhimento do consentimento, demonstrado pela análise das questões anteriores, mostra-se preocupante os resultados ora obtidos.

Foi perguntado também quais das operações de direito do titular, que podem ser requeridas ao controlador, já foram requeridas. De todas elas, a que foi praticada pela maioria foi o cancelamento de cadastro, colocando fim ao tratamento dos dados do titular (77,3% dos participantes). Logo em seguida, a exclusão de algum dado específico (38,6%) e a correção de dados (30,7%). Esses resultados provam um certo nível de preocupação das pessoas com a qualidade das informações que são fornecidas e com o término da utilização de seus dados quando não é mais necessário.

Em contrapartida, operações que demandam um conhecimento maior da lei e das garantias atribuídas, como portabilidade de dados ou acesso a informações sobre compartilhamento de dados com terceiros, apareceram em menos respostas

(18,2% e 20,5% respectivamente). Essas informações, revelam novamente, uma pouca divulgação, pelos poder público, empresas e meios de comunicação, sobre as garantias do cidadão qual a proteção de dados.

As informações sobre possíveis danos relacionados ao tratamento de dados pessoais foram também averiguadas, no caso, sobre a violação ou vazamento desses dados.

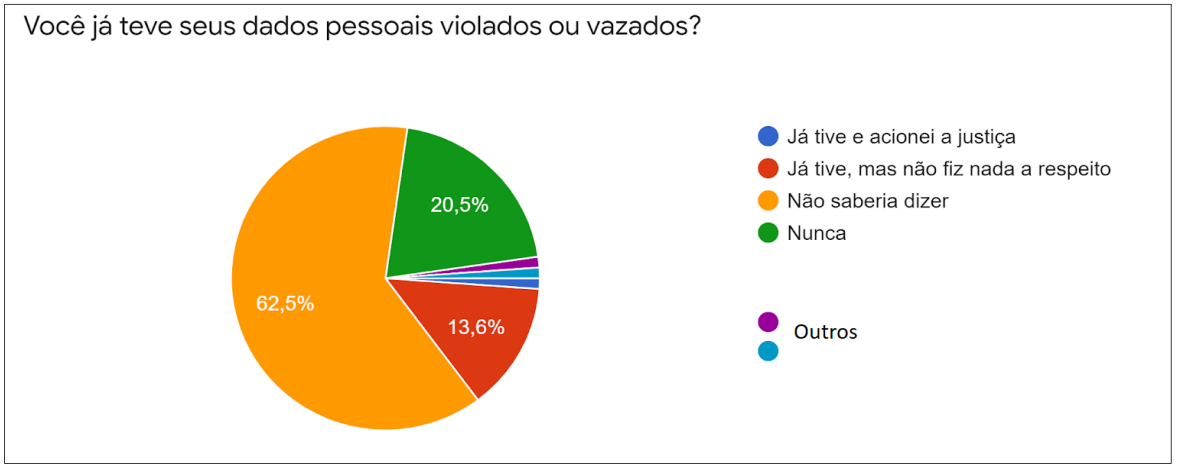

Fig. 4

Os resultados obtidos revelam que a maioria das pessoas não consegue dizer se já teve alguma vezes seus dados vazados ou violados, revelando a falta de acesso a mecanismos de busca sobre a situação e integridade dos dados tratados, em oposição ao princípio da qualidade dos dados, e a falta de comunicação das organizações quando tais eventos ocorrem, indo contra o princípio da transparência e se isentando da responsabilidade sobre o tratamento dos dados atribuída pela lei.

Outra informação importante que se extrai é a ausência de realização de demandas na justiça buscando a resolução dos problemas e responsabilização dos culpados. Mais uma evidência da falta de informação e acesso da população aos mecanismos necessários para garantir a integridade de seus direitos fundamentais.

Um último tópico foi abordado de forma mais específica, o conhecimento da Lei Geral de Proteção de Dados Pessoais.

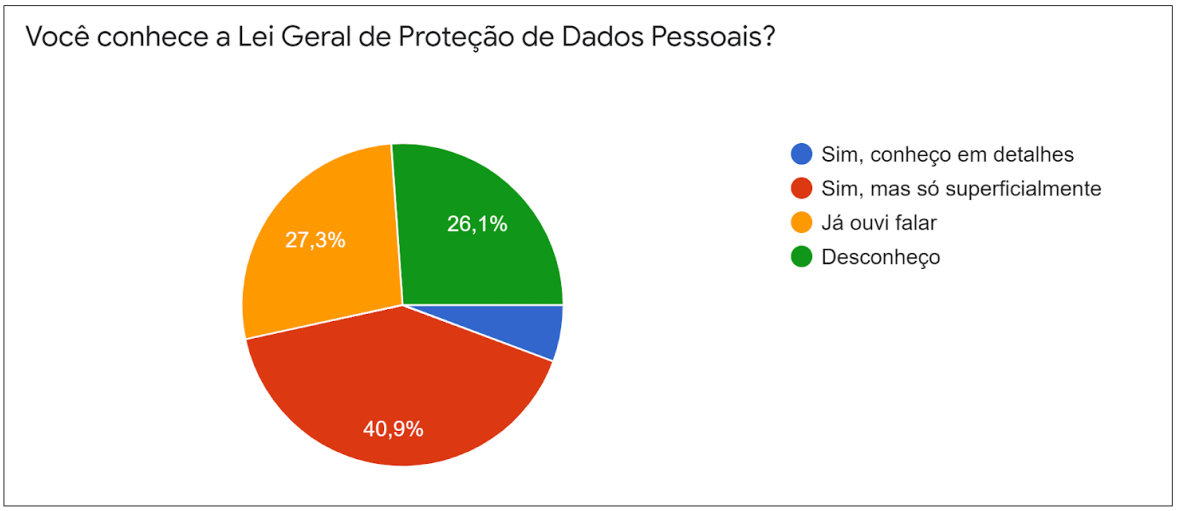

Fig. 5

Novamente, se conclui que a falta de acesso às informações a respeito da proteção de dados pessoais é uma forte característica, dessa vez corroborada pelo desconhecimento da maioria do grupo de amostra sobre a LGPD.

Por fim, a partir de todas as análises feitas, destaca-se que a criação de uma verdadeira cultura de proteção de dados no Brasil ainda está em processo de formação. Para que tal processo possa atingir a maturidade desejada, as empresas, por público e meios de comunicação precisam difundir mais as obrigações e garantias presentes na LGPD para a população, para que ela exerça plenamente seus direitos e para que exija das organizações um comportamento compatível.

A seguir, será tratada um pouco mais sobre a situação das organizações e as melhorias que ainda devem ser feitas nesse sentido.

3. APLICAÇÃO DA LGPD NO BRASIL: ADEQUAÇÃO DAS ORGANIZAÇÕES À NORMATIVA

4.1. Cenário pré-LGPD

A LGPD, seguindo os moldes da GDPR, fornece, aos titulares dos dados pessoais, direitos sobre as suas informações pessoais, permitindo que eles exerçam, sobre elas, maior controle, além de atribuir maiores responsabilidades às organizações que realizam o tratamento desses dados, permitindo que todos os envolvidos atuem com considerável segurança jurídica. Porém, entre a letra da lei e a realidade, muito ainda tem que se avançar no cenário brasileiro.

Nesse contexto, o desenvolvimento de tecnologias e aplicação prática dos princípios de Segurança da Informação são primordiais para que as organizações possam se adequar aos novos paradigmas de proteção e manuseio das informações pessoais de clientes e funcionários. Políticas internas e externas são necessárias, bem como aplicação de softwares e hardwares e o treinamento das pessoas que exercerão tais funções, visto que o fator humano é também um dos vários que precisam se adaptar à conjuntura atual. Entre as normas técnicas pode se destacar a NBR ISO/IEC 27002, 2013.

Políticas e normas de segurança da informação são de suma importância para garantir a proteção dos dados pessoais que se tenham armazenado e permitir a sua utilização, respeitando os princípios da confidencialidade, integridade e disponibilidade, entre outros presentes da legislação. Os usuários dos dados e os responsáveis pela manutenção da segurança da informação devem estar em sintonia, treinados e capacitados para exercer as funções de acordo com as diretrizes estabelecidas, devendo ser este ambiente garantido pela organização que detém os dados (NBR ISO/IEC 27002 - 2013).

No que tange a proteção de dados pessoais, o consentimento é considerado um fator relevante e que apresenta destaque no texto da GDPR, que ressalta que a empresa deve assegurar que este consentimento deve ser realizado de forma clara e expressa, bem como deve responder por eventuais falhas e

ocorrências que recaiam sobre os dados que, sob sua responsabilidade, estiverem. Os dados devem ser tratados respeitando a lei vigente, de forma equitativa e transparente, estando atento à finalidade para as quais estes foram fornecidos (LOVELL, M. et al., 2018).

A questão da segurança pode ser dividida ainda em aspectos físicos e lógicos (FERREIRA, F. et al., 2008), os primeiros compreendem as restrições de acesso a localidade consideradas de importância, e os segundos têm relação com o modo de utilização dos softwares, bem o seu desenvolvimento e a rede que são empregados para o tratamento dos dados mantidos pela organização.

A LGPD segue orientações semelhantes nesse sentido. Porém, na prática das empresas, poder público e organizações presentes ou atuantes no território nacional, alguns pontos relevantes ainda precisam ser trazidos à realidade.

Para avaliar a mencionada situação, realizou-se, em 2018, uma análise na qual restou demonstrado que as empresas brasileiras, em grande parte, não estão preparadas para atender as demandas previstas na LGPD, sancionada naquele mesmo ano pela Presidência da República do Brasil (PIURCOSKY F. et al., 2019).

Foram ouvidas sete empresas, de pequeno, médio e grande porte, pertencentes aos setores de Indústria, Comércio e Serviços, e que mantêm atuação local e com o resto do país. Os entrevistados faziam parte do setor de tecnologia da informação, com cargo de decisão e controle direto sobre os dados organizacionais ou tratamento dos dados.

A maioria das empresas entrevistadas não possuíam uma política de segurança da informação definida. Muitas também não estavam familiarizadas com a nova legislação, desconhecendo seus princípios e diretrizes, incluindo a exigência do consentimento do titular para a manipulação de determinados dados coletados e o controle sobre o método utilizado para o recolhimento desses dados (PIURCOSKY F. et al., 2019).

Identificou-se também a necessidade de se remodelar e atualizar os bancos de dados, para que possam estar compatíveis com as exigências trazidas pela LGPD, entre elas a possibilidade da realização da portabilidade dos dados

cadastrados de um fornecedor de serviços ou produtos para outro e o direito a exclusão dos dados cadastrados de clientes, tomadores de serviços ou ex-funcionários (PIURCOSKY F. et al., 2019).

Outro fator de risco para a segurança dos dados e que é objeto de regulação pela legislação brasileira é a questão do acesso por terceiros dos dados tratados pelas empresas. Todas as organizações questionadas não tinham uma regularização específica nesse sentido, não garantindo ao usuário que seus dados estariam ou não sendo fornecidos ou manipulados por terceiros (PIURCOSKY F. et al., 2019).

Para sanar essas deficiências e se alcançar um estado de adequação à legislação ora vigente, o desenvolvimento de uma nova cultura de proteção de dados pessoais e a implantação de compliance à nova normativa, envolvendo diversos setores de uma organização e atuação multidisciplinar, incluindo as áreas de segurança da informação, gestão, tecnologia da informação e também a jurídica.

4.2. Melhorias a serem implementadas e adequação à lei

Com o objetivo de orientar a aplicação prática das normativas criadas, a lei define quatro figuras, elencadas no artigo 5º, inciso IX, com atribuições e responsabilidades distintas, que, atuando em conjunto, operam as garantias previstas no texto legal. São elas o controlador e o operador (agentes de tratamento), e o encarregado, as quais serão mais bem detalhadas a seguir.

O Controlador é a pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais; o Operador é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador; o Encarregado é a pessoa indicada pelo controlador e pelo operador que atua realizando a comunicação entre o controlador, os titulares dos dados pessoais e a Autoridade Nacional de Proteção de Dados.

Esses atores, inseridos nos quadros das empresas que necessitam dos

dados pessoais para exercer suas atividades, devem estar em sintonia com a legislação, exigindo treinamento e adequação, para que suas tarefas específicas sejam desempenhadas de forma a garantir a proteção dos dados objeto de tratamento. Especificamente, o Encarregado é o responsável por coordenar a utilização das informações e a adequação à lei, bem como responder aos titulares dos dados pessoais, restando responsável pela criação de uma política de segurança em alinhamento com a lei. (PESSOA, C.R. et al., 2020)

Para que essa coordenação se implemente, é necessária uma mudança dos objetivos e entendimentos da gestão das organizações que realizaram esse trabalho, desenvolvendo uma nova cultura de uso de dados. Uma equipe multidisciplinar deve atuar para primeiramente conhecer das mudanças que precisam ocorrer, as informações e parâmetros a serem cumpridos, e as pessoas envolvidas, para que a seguir se realizem os investimentos em tecnologia necessários e adquirir as ferramentas próprias para mover o maquinário idealizado. Tendo em vista que o titular, por exemplo, poderá, a qualquer tempo, conhecer dos dados tratados, modificá-los, transportá-los ou retirá-los, um sistema mais maleável e inteligente é indispensável. Uma visão completa do cenário deve ser empregada para que todas as áreas (técnicas, administrativas, jurídicas, etc.) envolvidas tenham sincronia com a lei (Pessoa, C.R., 2016).

Nesse sentido, a LGPD prevê, em seu artigo 46, que os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas com o intuito de proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou outra forma de tratamento inadequado ou ilícito. Para que as medidas de segurança da informação tenham verdadeira efetividade, um esforço em conjunto dos agentes de tratamento é essencial.

No que tange às medidas técnicas, referidas na lei, são aquelas adotadas no escopo da Tecnologia da Informação, com o emprego de funcionalidades com intuito de garantir a segurança das informações. Entre eles são destacados, ferramentas de autenticação de acesso ao sistema, mecanismos de segurança em hardware e software, controle do tráfego de dados em rede, instrumentos para detectar invasão ao sistema, criptografia, entre outros. (Jimene,

C., 2019).

O encarregado, como previamente exposto, deve estar associado a uma equipe multidisciplinar, envolvendo gestão, segurança da informação, tecnologia da informação e comunicação e jurídica. Esse grupo deve estar incumbido de conhecer os processos relacionados ao tratamento das informações; conhecer as normas e implementar as práticas de segurança da informação; entender o ciclo da informação dentro da organização que integra; realizar análises de riscos; conhecer as ferramentas tecnológicas que possibilitaram o tratamento devido aos dados; estar a par da legislação vigente para se adequar a ela (PESSOA, C.R. et al., 2020).

A integração entre os diferentes setores da organização e profissionais é essencial para que se possa cumprir a lei, incluindo a implementação de medidas administrativas, como criação de políticas de proteção de dados, políticas de privacidade, código de ética e conduta, entre outras (PESSOA, C.R. et al., 2020).

Outra mudança, cuja aplicação é primordial para que as organizações se adaptem à nova realidade trazida pela LGPD, é a adaptação dos contratos de adesão para a utilização dos dados pessoais.

Anteriormente às determinações inseridas com a norma ora estudada, não havia uma previsão específica a respeito dos contratos de concessão de consentimento deveriam ser firmados, nem mesmo o conteúdo obrigatório a ser contemplado. Ademais, a privacidade e a proteção de dados eram tratadas de forma genérica, massante, ininteligível e sem possibilidade de acordo e discussão entre as partes, condicionando o consumidor à aceitação total dos termos para usufruir dos serviços e produtos. Nesse contexto, o consentimento é meramente algo automatizado e ausente de reflexão, ou seja, meramente formal e fictício.

Agora na vigência da lei, os princípios legais e constitucionais passam a ser aplicados na elaboração desses contratos de forma rígida, tornando-os mais transparentes e diretos. Isso permite que o consentimento e as outras possibilidades de legitimação do tratamento de dados pessoais, dispostas no artigo 7º da Lei, estejam claras para as partes envolvidas. A Lei, em seu artigo 8º, ainda atribui ao controlador o ônus de comprovar que o consentimento foi obtido dentro dos moldes legais, podendo levar à nulidade do contrato no caso de descumprimento.

As mudanças trazidas pela LGPD estão também acompanhadas de medidas coercitivas, como multas e outras sanções, em virtude de possíveis danos causados, bem como as de caráter administrativo impostas pela Autoridade Nacional de Proteção de Dados (ANPD), com o intuito de trazer real aplicabilidade e cumprimento às normas estabelecidas.

A responsabilidade estabelecida pelos artigos 42 a 46 da LGPD é referente a danos morais ou materiais, podendo ser individuais ou coletivos, que ocorram no tratamento de dados pessoais, considerados extensões da personalidade das pessoas físicas, se enquadrando em um direito da personalidade, objeto de proteção.

A Lei trata especificamente a respeito da responsabilização das figuras do controlador ou do operador, podendo ser atribuída a uma das figuras de forma individual, em decorrência da autoria do dano. Porém, existem algumas hipóteses de responsabilização solidária entre os dois, como nos casos de relação jurídica consumerista abrangendo titular dos dados, controlador e operador (conforme artigos 12 e 18 do CDC), e nos casos previstos no parágrafo 1º do artigo 42 da LGPD.

Distintamente, as hipóteses de responsabilização do encarregado não são expressas na LGPD, mas podem ocorrer em cenário de existência de uma relação consumerista com as outras partes envolvidas no tratamento dos dados, seguindo os ditames do CDC, expressamente aceito pela LGPD em seu artigo 45.

Há ainda a possibilidade de inversão do ônus probatório, inserida pelo parágrafo 2º do artigo 42, em prol do titular dos dados. A necessidade de aplicação deve ser aferida pelo magistrado quando há hipossuficiência para produção de provas ou ela for excessivamente onerosa, nos mesmo moldes do determinado no CDC a respeito das relações de consumo. Esse instrumento busca proteger os interesses dos titulares dos dados, que são, a princípio, a parte mais frágil da relação, pois não tem total conhecimento, nem os meio, para acesso às informações sobre tratamento em seus dados, atribuindo maior encargo sobre os agentes de tratamento, que devem fornecer prova por terem as melhores condições de fazê-lo.

Neste sentido, versa Rizzato Nunes (2012, p. 852):

> “(…) hipossuficiência, para fins da possibilidade de inversão do ônus da prova, tem sentido de desconhecimento técnico e informativo de produto ou do serviço, de suas propriedades, de seu funcionamento vital e/ou intrínseco, de sua distribuição, dos modos especiais e controle, dos aspectos que podem ter gerado o acidente de consumo e o dano, das características do vício, etc”

Em virtude do ora exposto, é mister que as organizações realizem um planejamento de implantação de políticas de proteção de dados pessoais e gestão das informações, pois laudos de auditoria que comprovem o manejo correto, transparente do tratamento de dados serão necessários em eventuais litígios que tenham como objeto danos a dados pessoais. Além disso, esse planejamento é primordial para se entender se houve envolvimento dos agentes de tratamento acusados, se eles atuaram em conformidade com a lei ou se o dano é decorrente de terceiros ou exclusiva do titular dos dados, o que poderia levar à exclusão da responsabilidade, como versa o artigo 43 da LGPD (CAPANEMA, W., 2020).

No que tange às sanções administrativas, elas são aplicadas pela ANPD nos casos que forem constatados descumprimento à legislação (artigo 55-J, inciso IV). Em seu artigo 52, a LGPD determina que as sanções administrativas que os agentes de tratamento estão sujeitos em razão das infrações cometidas às normas previstas na Lei.

Entre as sanções possíveis, merecem destaque a aplicação de multa, que pode ser aplicada em proporção ao faturamento do todo o grupo econômico (mesmo que apenas uma empresa tenha cometido a infração), podendo chegar ao valor de R$ 50.000.000,00 (cinquenta milhões de reais), a publicização da infração após devidamente apurada e confirmada a sua ocorrência, incorrendo em prejuízo para a imagem da organização e a perda da confiança de parceiros e clientes, e o bloqueio dos dados pessoais referentes a infração, até a regularização, ou mesmo a sua eliminação.

O último caso apresentado, pode representar uma perda significativa para a organização ou até mesmo impedir o seu funcionamento, pois os dados são ferramentas essenciais para o prosseguimento das atividades de empresas de

diferentes ramos de negócios.

Para a aplicação das sanções, de qualquer espécie, será realizada uma avaliação proporcional ao grau do dano causado, o tipo de infração cometida e quais foram os direitos violados. Considera-se também as vantagens que foram obtidas ou pretendidas com a ocorrência do fato, a econômica do autor, se houve boa-fé na ação, se é um caso de reincidência e se ocorreu cooperação com a investigação, bem como se os mecanismos internos aptos a impedir esse acontecimento ou mitigar seus danos foram implementados.

Outra inovação trazida pela Lei e que merece destaque são a considerável gama de direitos subjetivos atribuídos ao titular de dados pessoais, estes apresentados no Capítulo III. Eles devem ser observados pelos controladores, operadores e encarregados em qualquer hipótese de tratamento de dados pessoais, estando sujeitos a sanções na hipótese de descumprimento.

Um extenso rol de direitos é listado nos incisos do artigo 18, mas tal lista não é taxativa, podendo ser reconhecido o exercício do direito que for necessário à proteção dos direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade do titular, como entendimento do artigo 1º da Lei. Isso se deve a sua classificação como direito da personalidade, se tratando de uma nova modalidade de externalização da identidade da pessoa, devendo ser tutelada em compatibilidade com as novas tecnologias e a realidade em que está inserido. Dessa forma, pretende-se atribuir ao titular o domínio e o acesso aos dados pessoais, bem como a capacidade de monitorar esses dados fornecidos e o tratamento que sobre eles é realizado (WONTROBA, B. et al., 2020).

Para o exercício desses direitos, a lei estabelece, nos parágrafos do artigo 18, que o titular pode acionar os envolvidos no processo de tratamento, os órgãos de defesa do consumidor e a ANPD a qualquer momento e sem qualquer custo para tanto. Para tanto, esses entes precisam disponibilizar mecanismos e canais claros e eficientes para permitir a realização dos requerimentos e envio das respostas, sob risco de se configurar uma restrição ou impedimento aos direitos dos titulares.

Logo, as empresas e órgãos públicos envolvidos com o tratamento estão

obrigadas a desenvolver e implementar os recursos necessários visando atender às novas demandas trazidas. Entre eles é possível destacar: a permissão de acesso aos dados que estão sendo tratados; possibilidade de retificação dos dados coletados; a portabilidade dos dados para outras entidades; exclusão dos dados armazenados; confirmação do tratamento realizado; pedido de anonimização dos dados; entre outras medidas de caráter técnico e administrativo que possibilitem o exercício dos direitos do titular. Tais requerimentos devem gerar processos que, por sua vez, mesmo que internos, devem respeitar os princípios fundamentais do contraditório, ampla defesa e o devido processo legal (artigo 5º, inciso LIV, da CRFB), além de não descartarem o acionamento da via judicial para o cumprimento da demanda (artigo 5º, XXXV, da CRFB).

Novamente, a implementação dos princípios da LGPD no funcionamento da organização e a atenção das regras estabelecidas são essenciais para o prosseguimento das atividades normais das organizações.

4.3. Cenário pós-LGPD

Com a entrada em vigor da Lei Geral de Proteção de Dados, em 18 de setembro de 2020, as organizações passam a ser obrigadas a cumprir o que versa a nova normativa a respeito da proteção de dados pessoais. Porém, análises recentes mostram que muitas das medidas frisadas anteriormente ainda estão pendentes de materialização no cenário brasileiro.

Em pesquisa realizada em 2020, com 175 organizações de capital predominantemente brasileiro, apenas uma pequena parte delas estava em um nível médio (8% das participantes) ou alto (5% das participantes) de adequação aos parâmetros da lei. Dentre as organizações que apresentavam maior maturidade quanto ao atendimento dos requisitos, estão as de maior receita e com o maior investimento em proteção de dados, na faixa de mais de 15 milhões em investimento (GANUT, M., et al., 2020).

Entre as empresas com maior nível de adequação, se visualiza uma preponderância de dois grupos: o setor farmacêutico e hospitalar, e o de óleo/gás.

Isso pode estar relacionado à natureza dos dados tratados por essas empresas, no caso do primeiro grupo são dados sensíveis, por se referirem ao estado de saúde da pessoa, e no segundo grupo são dados referentes a transações financeiras de alto valor, necessitando de atenção especial.

A pesquisa também mostrou que as empresas que apresentam uma baixa maturidade em relação aos novos requisitos da LGPD (61% das entrevistadas) têm receita e áreas de atuação variadas. Pode-se perceber que a maioria das empresas em geral não está adaptada à normativa, mesmo estando sujeitas às obrigações previstas, já que não existe empresa que, pelo menos em nível básico, não realize tratamento de dados pessoais. Outro dado considerado preocupante é o fato de 25% das participantes com baixa adequação ainda cogitam se vão realizar ou não a adequação necessária (GANUT, M., et al., 2020).

Ao serem questionadas sobre as dificuldades que teriam que enfrentar para se adequar à LGPD, a maioria das empresas respondeu que a falta de definições claras da ANPD sobre a fiscalização, implementação da lei e aplicação das sanções.

A ANPD ainda está começando a desempenhar o seu papel de guardiã da proteção de dados no Brasil e da LGPD, para tanto, foi publicada a Portaria nº 11 de 27 de janeiro de 2021, da Presidência da República/Autoridade Nacional de Proteção de Dados, que estabelece a agenda regulatória da ANPD para a implementação os projetos de regulamentação iniciais do órgão. Seguindo esse planejamento, em 22 fevereiro de 2021 foi iniciada a tomada de subsídios com o intuito de auxiliar o desenvolvimento da regulamentação de recebimento de notificações de incidentes relacionados a dados pessoais, nos termos do artigo 48 da lei, bem como a divulgação das orientações a serem seguidas pelos agentes de tratamento em caso de incidentes de proteção de dados. Além disso, o Regimento Interno do órgão foi publicado apenas em 10 de março de 2021, demonstrando, novamente, que as atividades ainda estão em fase inicial.

Esse relativo início das atividades e desconhecimento de como serão realizadas as medidas de fiscalização, bem como a atual falta de orientações mais específicas de procedimentos por parte do órgão, pode atrapalhar o interesse das empresas em se adequar às normativas, receio do trabalho realizado tiver que ser

descartado ou revisado em momento futuro quando as práticas exigíveis estiverem mais bem descritas.

Outro ponto levantado pela pesquisa é a implementação de uma governança de privacidade, com uma política de privacidade bem estabelecida. Como já mencionado, uma mudança na política e na cultura das organizações é essencial para a proteção de dados, devido ao caráter multidisciplinar do processo e por estar atrelado a praticamente todos os setores da empresa. Foi verificado que 45% das empresas já possuem programa de privacidade e proteção de dados, mas apenas 12% delas apresentam alto grau de compatibilidade com a LGPD (GANUT, M., et al., 2020).

A implementação da figura do encarregado, importante para o desempenho de um tratamento correto dos dados pessoais, também foi questionada pela pesquisa. Verificou-se que 41% das organizações já nomearam um encarregado, principalmente aquelas que realizaram maiores investimentos no que tange a proteção de dados.

A pesquisa também revelou que a GDPR e a ISO 27701, norma da ABNT sobre técnicas de segurança e gestão da privacidade da informação, adaptada a LGPD, são mais utilizadas como base para a criação das políticas de proteção de dados, por existir maior material acadêmico e profissional como referência. Se criticou também o caráter aparentemente mais genérico da norma, pois um conteúdo mais específico para a área de atuação da empresa e técnico é preferível.

Mesmo sendo aplicável a diferentes setores de forma geral, a LGPD estabelece uma base para a proteção de dados no Brasil, estabelecendo princípios e diretrizes a serem seguidas, bem como os atores essenciais e mínimos para esse funcionamento, além de criar uma autoridade nacional para regular essa questão. Portanto, o seu estudo e implementação são importantes para as organizações, mesmo com a falta de estudos e práticas especificamente sobre ela, devido a sua recente criação.

O atendimento aos direitos dos titulares é outro ponto de destaque que foi avaliado. Entre as organizações que apresentavam um menor nível de adequação às regras de proteção de dados, ou seja, ainda estão no início do seu processo de

adaptação, preferiram focar nas atividades de mapeamento e categorização dos dados pessoais e na implementação de canais de atendimento e comunicação com o titular. Apenas 21% delas já estabeleceram os procedimentos necessários para o atendimento dos direitos dos titulares, estando este no estágio de planejamento para a maior parte delas. Observa-se que mesmo com a vigência da lei, que atribui essa gama de direito aos titulares e exige das empresas o seu cumprimento, a maioria ainda não é capaz de atender essa demanda caso seja acionada (GANUT, M., et al., 2020).

Outra adequação de relevância considerável para as organizações é a relação entre controlador e operador. Como já mencionado, restou estabelecida no artigo 42 da LGPD as hipóteses de responsabilidade solidária entre os agentes de tratamento, podendo o operador responder solidariamente com o controlador por danos causados, quando aquele descumprir as obrigações legais ou quando não seguir as instruções lícitas do controlador.

A obrigação solidária está definida nos artigos 264 a 285 do Código Civil e é empregada nos casos definidos em Lei ou pela vontade das partes e se refere às obrigações que possuem mais de um devedor ou credor, cada um com direito ou obrigação à dívida por inteiro. No caso estabelecido pelo artigo 42 da LGPD, se trata de uma responsabilidade passiva, em que o controlador e o operador podem ser acionados, em conjunto ou individualmente, para responder pela totalidade do dano causado ao titular dos dados pessoais.

Nesse sentido, Fiuza (2009, p. 334) esclarece sobre a solidariedade passiva:

> "(...)Há vários credores, respondendo cada um deles individualmente por toda a dívida. O credor pode exigir de apenas um, de alguns ou de todos que paguem toda a dívida. Cada um responde pela dívida toda. Pagando um ou alguns dos devedores solidários, terão direito de regresso contra os demais, cobrando-lhes a parte que lhes cabia."

Portanto, um contrato bem estabelecido, isonômico e em conformidade com a legislação, entre essas partes, é essencial para evitar possíveis responsabilizações e perdas em casos de dano ao titular, já que o erro praticado por

uma das partes pode resultar em perdas para ambas.

Considerando esse cenário, a pesquisa avaliou que 85% das organizações consideram fundamental a avaliação dos operadores, com quem se pretende partilhar os dados pessoais dos seus clientes ou colaboradores, quanto à capacidade de atender os requisitos legais. Porém, apenas 27% implementaram ações para revisar os contratos firmados e 29% realizaram ações para avaliar a capacidade dos operadores de realizar o tratamento de dados de forma segura (GANUT, M., et al., 2020).

No que tange a proteção contra ameaças e segurança da informação, 61% das participantes já possuem um programa de segurança da informação e 56% já possuem um departamento de segurança da informação.

Como se pode analisar, em dois anos de diferença entre os estudos trazidos, o primeiro a época da publicação e o segundo quando da sanção, as mudanças no entendimento das organizações quanto ao atendimento dos requisitos legais e da importância de uma robusta política de proteção de dados, mesmo que apresentando certa evolução, ainda carecem excelência. Pode ser aferido quando se compara a criação de políticas de privacidade, que mesmo evoluindo ainda falta uma substância maior para atender as necessidades dos titulares.

A aplicação das medidas apresentadas anteriormente ainda se mostra necessária, principalmente para os setores que lidam com dados sensíveis e com grande número de pessoas e valores. Com o início da aplicação das sanções previstas na LGPD para agosto de 2021, as adequações precisam ser fortemente aceleradas para que a conformidade seja alcançada nesta data.

Mesmo sem a aplicabilidade das sanções trazidas pela LGPD, a lei já começou a ser aplicada, devendo a evolução do comportamento e o estabelecimento da cultura de proteção de dados nas organizações serem fomentados pelos seus dirigentes. Garantindo a segurança jurídica para as partes envolvidas, competitividade nacional e internacional e respeito aos direitos fundamentais.

4. LEGISLAÇÕES INTERNACIONAIS DE PRIVACIDADE DE DADOS E A LGPD

5.1. Principais legislações de Privacidade no Mundo

A preocupação com a proteção de dados pessoais na era digital não é uma exclusividade do Brasil, muitos países também externaram essa preocupação e criaram leis visando a regulamentação desses dados.

Com o aumento expressivo da coleta de dados pessoais na era informacional que vivemos, faz-se mister o aumento na preocupação do tratamento dado aos mesmos.

Vazamentos se tornaram constantes com dados pessoais sendo comercializados livremente na internet. Cada vez mais as pessoas têm interesse em saber o que acontece com os seus próprios dados.

Nesse contexto as principais legislações existentes são: o Regulamento Geral sobre a Proteção de Dados (GPDR), o California Consumer Privacy Act of 2018 (CCPA), Protection and Electronic Documents Act (PIPEDA), a Act on the Protection of Personal Information (APPI), a Lei de proteção de dados pessoais 25.326 (LDPA) e a Lei Geral de Proteção de Dados 13.709/2018 (LGPD).

5.2. Regulamento Geral sobre a Proteção de Dados (GDPR)

A GPDR é a legislação que versa sobre a proteção de dados em território europeu, é considerada por especialistas como o maior conjunto de normas de proteção à privacidade online já criado. Fruto de intenso debate legislativo a GPDR foi aprovada como Regulamento nº 679/2016. Por se tratar de um regulamento o mesmo não precisa ser ratificado por cada estado membro, se tornando uma legislação de interna de cada país.

A GPDR influenciou legislações em todo o mundo devido ao alto padrão no processamento de dados pessoais, inclusive o Brasil. Tendo introduzido conceitos como o controlador e o operador de dados. Trazendo novos parâmetros para o tratamento de dados.

Algumas das motivações para criação da GPDR foram o respeito a privacidade e a proteção de dados pessoais sobre um viés de respeito aos direitos e liberdades fundamentais. Sendo os avanços tecnológicos e as economias cada vez mais digitais grandes impulsionadores da legislação.

Trata-se de um projeto de regulação virtual que faz parte de uma série de iniciativas com foco na proteção do usuário, exercendo o cumprimento de direitos e deveres de pessoas físicas e jurídicas no meio digital.

Portanto, a principal proposta é que o usuário saiba quais informações está fornecendo aos serviços dos quais usufrui, bem como impor que as entidades justifiquem a finalidade do uso desses dados.

Vale dizer que os dados englobados pela lei GPDR podem ser os mais diversos. Isto é, sejam informações menores, como cookies do navegador, ou maiores, como nome ou endereço. Todos são pertinentes e cobertos pelas regras.

5.3. California Consumer Privacy Act of 2018 (CCPA)

A Lei de Privacidade do Consumidor da Califórnia é a primeira lei de proteção de dados a ser promulgada dentro dos Estados Unidos da América. A Lei entrou em vigor no dia 1 de janeiro de 2020. Já a regulação dessa Lei, ou seja, o órgão que o mantém funcionando e aplica penalidades em caso de descumprimento, é o Advogado Geral da Califórnia (AG), que começou a atuar no dia 1 de julho de 2020.

Tendo como inspiração a GDPR a novel legislação californiana versa sobre os direitos de privacidade dos consumidores da Califórnia e impõe diretrizes sobre o tratamento de dados pessoais realizado pelas empresas.

Algumas das obrigações das empresas inclui: gerar comunicados; respeitar pontos estipulados pela regulamentação geral de proteção de dados; garantir direitos aos titulares dos dados; requisitar o consentimento para captação e tratamento dos dados de menores de idade e recusar transferências de dados.

O objetivo primário da Lei CCPA é o de proteger e assegurar os direitos de privacidade de dados para os residentes da Califórnia. Para isso, a legislação prevê mais responsabilidade e transparência por parte das empresas.

A Lei de proteção de dados na Califórnia diz que todos os californianos têm o direito de saber: quais dados pessoais são coletados; se as informações são comercializadas ou divulgadas, e para quem isso é feito; negar as vendas de seus dados e requisitar uma exclusão dos dados pessoais.

5.4. Act on the Protection of Personal Information (APPI)

A lei de proteção de dados do Japão, o Act on the Protection of Personal Information (APPI), adotada em 2003 é uma das primeiras regulações de proteção de dados na Asia. A lei recebeu uma completa reformulação em setembro de 2015 depois de uma serie vazamentos de dados de alto nível chocar o país, deixando claro que o APPI estava defasado. A emenda entrou em efeito no dia 30 de maio de 2017, um ano antes da Regulação Geral de Proteção de Dados da União Europeia.

A atualização trouxe com ela o estabelecimento da Comissão de Proteção de dados pessoais (PPC), uma agência independente que, entre outros, protege os direitos e interesses dos indivíduos e promove a própria e efetiva utilização dos dados pessoais.

A APPI é aplicável a todos os negócios que lidam com dados individuais no Japão. Isto se refere tanto a companhias que oferecem bens e serviços no Japão com escritórios dentro do país ou àquelas com escritório fora do país. Assim sendo, similarmente a GDPR, a lei de privacidade japonesa tem um alcance extraterritorial.

Enquanto a versão anterior da lei de privacidade só era aplicável a negócios que contivessem em sua base de dados 5.000 indivíduos identificáveis em pelo menos um dia nos últimos 6 meses, a emenda APPI removeu essas restrições, expandindo o alcance da lei para incluir todos os operadores de negócios que processam informações pessoais para propósitos de negócios, mesmo aqueles como uma base de dados de alguns indivíduos.

Organizações do governo central, governos locais, agências administrativamente independentes, as quais são regidas por outros escopos de regulação, estão isentas de seguir a APPI.

A APPI distingue entre duas categorias de dados protegidos: informações pessoais e informações pessoais com cuidados especiais requeridos. O primeiro se refere informações pessoais identificáveis (PII) como nome, data de nascimento, endereço de e-mail ou dados biométricos. A recente atualização da APPI esclareceu que informações pessoais também incluem referências numéricas que possam ser utilizadas para identificar um indivíduo específico como o número da carteira de motorista ou número do passaporte.

Informação pessoal com cuidado especial requerido é uma nova categoria introduzida sob a emenda APPI que se refere a dados que posem ser base para discriminação ou preconceito. Histórico médico, estado civil, raça, crenças religiosas e históricos criminais, entre outros, estão dentro dessa categoria. Operadores de negócios tem restrições no processamento dessas informações e sempre precisam de consentimento do indivíduo referido.

A APPI também específica que dados anonimizados, porque foi retirado a informação que poderia ser usada para identificar indivíduos, não precisa seguir o mesmo rígido processo que os dados pessoais. Por exemplo, companhias não precisam perguntar ao usuário para transferir os dados, mas tem que anunciar publicamente e tem de garantir que o recebedor saiba que os dados estão anonimizados. A razão por trás dessas estipulações é o “Big Data”: desta forma, negócios podem continuar a usar informações para análises estatísticas.

Sob a APPI, as pessoas podem requerer que o operador do negócio diga o propósito do uso do dado pessoal, como eles podem acessar os dados, corrigir ou

suspender a sua utilização e onde reclamações podem ser feitas em relação ao manejo dos dados pessoais.

Eles também podem requerer que as empresas corrijam ou deletem informações pessoais incorretas; podem requerer a suspenção ou a eliminação das informações pessoais se elas forem usadas em excesso ao propósito declarado, se foram transferidas sem consentimento prévio ou foram adquiridas por fraude.

Diferente de outras regulações internacionais, a APPI não inclui notificação mandatória de vazamento de dados. O PPC vai contactar diretamente a empresa quando tiver conhecimento do vazamento de dados e vai formalmente requisitar que o problema seja resolvido. Se a empresa falhar em fazê-lo, então o PPC irá emitir uma ordem administrativa requerendo formalmente que a companhia adote medidas em relação ao vazamento de dados.

Se a ordem administrativa também for ignorada, o operador de dados poderá ser multado em até quatro mil e seiscentos dólares ou enfrentar um ano de prisão.

5.5. Lei de proteção de dados pessoais 25.326 (LDPA)

A Lei de Proteção de Dados Pessoais N.º 25.326, incluindo o Decreto Regulamentar N.º 1558/2001 e regulamentos suplementares (“PDPA”) da Argentina, é uma lei federal argentina que se aplica à proteção de dados pessoais na Argentina e à transferência internacional de dados pessoais para processamento.

Em julho de 2018, a autoridade em proteção de dados da Argentina (Agencia de Acceso a la Información Pública, “ADPA”) emitiu a Disposição 47/2018 (“Disposição 47”) sob os termos da PDPA, que revogou a Disposição N.º 11/2006 relacionada a medidas de segurança que os controladores de dados precisariam considerar ao processar dados pessoais.

A Disposição 47 descreve novas medidas de segurança recomendadas que estão alinhadas com as melhores práticas e padrões internacionais, além de

visarem proteger a confidencialidade e integridade dos dados pessoais durante seu processamento, da coleta de dados à exclusão. Em especial, essa nova resolução atualizou a lista de medidas e controles recomendados para a gestão, planejamento, controle e melhoria da segurança ao processar dados pessoais.

Tais medidas de segurança recomendadas estão divididas em atividades relacionadas por categorias de processamento, incluindo coleta de dados, controles de acesso, controles de alteração, backup e recuperação, gestão de vulnerabilidade, remoção e exclusão de dados, incidentes de segurança e ambientes de desenvolvimento. Além disso, a Disposição 47 inclui uma lista de medidas de segurança aplicáveis a “dados confidenciais” (conforme definição contida no PDPL).

5.6. Comparativo entre a Lei Geral de Proteção de Dados 13.709/2018 (LGPD) e o Regulamento Geral de Proteção de Dados

Conforme já mencionado anteriormente, a Lei Geral de Proteção de Dados aprovada em 2018 depois de uma batalha de anos, coloca o Brasil ao lado de mais de 100 países onde há normas específicas para definir limites e condições para coleta, guarda e tratamento de informações pessoais.

A lei se baseia na GDPR que vem a ser a lei europeia de proteção de dados. As grandes diferenças e similaridades são:

Escopo Territorial

Tanto a LGPD quanto o GDPR se aplicam a qualquer indivíduo ou empresa que trate dados pessoais dentro de suas respectivas jurisdições, independentemente de onde esse tratamento é realizado.

Dados Pessoais

Tanto o GDPR quanto a LGPD definem dados pessoais de forma semelhante – ou seja, informações relacionadas ou referentes a uma pessoa física identificada ou identificável. Ambos também estabelecem proteções aprimoradas

para dados pessoais sensíveis, definidos de forma semelhante. Nenhuma das leis se aplica a dados anônimos.

Princípios de Tratamento e Privacidade

As organizações sujeitas ao GDPR também perceberão as semelhanças com os princípios de tratamento da LGPD. O GDPR estabelece seis princípios de tratamento: Licitude, lealdade e transparência; limitação das finalidades; minimização dos dados; exatidão; limitação da conservação; integridade e confidencialidade; e responsabilidade. No entanto, a LGPD especifica dez princípios: Finalidade; adequação; necessidade; livre acesso; qualidade dos dados; transparência; segurança; prevenção; não discriminação; e responsabilização. Dessa forma, as organizações sujeitas à LGPD deverão garantir seu tratamento de acordo com os princípios recentemente estabelecidos, caso não sejam abrangidos pelos princípios do GDPR.

Bases legais para o tratamento

Tanto o GDPR quanto a LGPD exigem que os controladores estabeleçam uma base legal para tratar dados pessoais. Ambas as leis fornecem bases semelhantes, mas cada uma contém algumas variações. De fato, o GDPR estabelece seis bases legais, enquanto a LGPD permite dez bases legais.

Relações entre controlador e operador

O GDPR estabelece requisitos mais rigorosos para a relação controlador-operador. Ele exige que um contrato com condições específicas ou outras condições legais oriente a relação entre o controlador (também conhecido como responsável pelo tratamento) e o operador (também conhecido como subcontratante ou processador). A LGPD, por sua vez, requer apenas que o operador execute o tratamento de acordo com as instruções do controlador, e que o controlador verifique a conformidade do operador.

Direito do Titular dos Dados

As organizações familiarizadas com o GDPR reconhecerão os direitos dos titulares de dados sob a LGPD. Ambas as leis concedem direitos similares aos indivíduos no que diz respeito aos seus dados pessoais. De acordo com cada lei,

por exemplo, o titular dos dados tem o direito de apagar/eliminar, ser informado, acessar, revogar o consentimento, corrigir dados inexatos ou desatualizados, não discriminação e portabilidade de dados, entre outros. Contudo, as leis apresentam diferenças. Por exemplo, o GDPR é mais normativo, a LGPD dá aos indivíduos o direito de anonimizar dados em determinadas circunstâncias e, embora a LGPD dê aos titulares dos dados o direito de revisar decisões automatizadas, ela não concede o direito de revisão humana de tais decisões.

Transferências internacionais de dados pessoais

Tanto o GDPR quanto a LGPD impõem restrições à transferência de dados pessoais para países terceiros ou organizações internacionais, permitindo tais transferências somente de acordo com fundamentos específicos. Por exemplo, cada lei reconhece o conceito de adequação da proteção de dados de países terceiros, assim como regras corporativas globais/regras corporativas vinculadas às empresas, cláusulas contratuais padrão e certificados/códigos de conduta. No entanto, a Autoridade Nacional de Proteção de Dados do Brasil (ANPD) ainda deve tomar as decisões de adequação e estabelecer regras para os demais mecanismos legais de transferência.

Registro de Tratamento de dados

Tanto o GDPR quanto a LGPD exigem que as organizações mantenham registros de suas atividades de tratamento. Entretanto, o GDPR especifica de forma mais detalhada as informações sujeitas à manutenção de registros.

Avaliação de impacto sobre a proteção de dados

Tanto o GDPR quanto a LGPD exigem que os controladores realizem avaliações de impacto sobre a proteção de dados para avaliar o risco de certas atividades de tratamento. Entretanto, o GDPR detalha quando requer tais avaliações, assim como os aspectos que as avaliações devem cobrir. A LGPD, por outro lado, simplesmente declara que a ANPD pode decidir quando um controlador deve conduzir tal avaliação e não dispõe de detalhes sobre os critérios para essa avaliação.

Nomeação do responsável pela proteção de dados

Tanto o GDPR quanto a LGPD exigem a nomeação de responsáveis pela proteção de dados (DPOs). Enquanto o GDPR exige que tanto os controladores quanto os operadores nomeiem os DPOs, a LGPD exige apenas que os controladores o façam. No entanto, o GDPR contém exceções sobre quando não são necessários DPOs.

Segurança de dados e violações de dados

Tanto o GDPR quanto a LGPD exigem que os controladores e operadores implementem medidas de segurança apropriadas para proteger os dados pessoais. O GDPR é mais normativo a este respeito, enquanto a ANPD possui autoridade para emitir orientações sobre medidas de segurança específicas a serem adotadas. Em caso de violação de dados, tanto o GDPR quanto a LGPD exigem que os controladores notifiquem a autoridade de supervisão, assim como os titulares dos dados afetados, em determinadas circunstâncias. Entretanto, o GDPR exige que um controlador informe uma violação de dados dentro de 72 horas após sua descoberta, e dispensa a notificação se a violação não atingir um certo limite de severidade. A LGPD apenas exige a comunicação dentro de um prazo razoável, cabendo à ANPD estabelecer diretrizes ou regras sobre este período.

Execução – Penalidades monetárias, sanções etc.

O não cumprimento ou a violação do GDPR ou da LGPD sujeitará os controladores e operadores a potenciais multas, sanções ou processos civis. As penalidades ou sanções específicas de cada lei são diferentes. Sob o GDPR, por exemplo, dependendo do tipo de violação, a penalidade pode ser de: 2% do faturamento anual global da organização ou 10 milhões de euros, o que for maior; ou 4% do faturamento anual global ou 20 milhões de euros, o que for maior. Em relação à LGPD, dependendo do tipo de violação, a ANPD pode emitir uma multa de até 2% do faturamento de uma organização no Brasil (de acordo com o seu último exercício, excluindo impostos), até um total máximo de 50 milhões de reais por infração.

Conclusão da comparação

Apesar das semelhanças entre as leis, a conformidade com o GDPR não garante a conformidade com a LGPD. Considerando que a implementação da conformidade com a LGPD está bem próxima, as organizações que tratam os dados

pessoais de indivíduos do Brasil ou que tratam dados pessoais no Brasil devem considerar imediatamente a revisão de seus processos e da estrutura de dados atuais de modo a identificar e resolver quaisquer falhas de conformidade com a LGPD.

5. CONCLUSÃO

O presente trabalho trouxe como tema a evolução legislativa da proteção da privacidade dos dados pessoais no Brasil, a qual culminou com a promulgação da Lei Geral de Proteção de Dados (LGPD) 13.709/2018. A LGPD constitui um marco para as instituições privadas e públicas, por tratar da proteção dos dados pessoais.

Ao mesmo tempo em que ocorre a celeridade demandada e permitida pela vida moderna dos desenvolvimentos tecnológicos ocorre também o compartilhamento da coleta de informações pessoais dos que a operacionalizam, nesse sentido a legislação evoluiu atribuindo ao titular um maior controle sobre os seus dados, uma vez que é a parte mais vulnerável, respeitando os princípios e os direitos fundamentais da pessoa humana, consagrando o direito a capacidade de ter sua privacidade preservada.

Para que os cidadãos não tenham os seus direitos ceifados não basta somente existir a criação da LGPD, devem ocorrer divulgação das informações bem como aplicação efetiva de fiscalizações e sanções, caso contrário a lei se tornará letra morta.

A LGPD está intimamente relacionada a GDPR que vem a ser a regulamentação da proteção dos dados na Europa, Regulamento 2016/279, uma vez que uma das exigências dos membros da UE seria a comercialização como países que adotassem legislações minimamente semelhante as dela, com o intuito de garantir a proteção de dados dos europeus fora da área da UE.

Comparando a LGPD com as demais normas existentes de privacidade no mundo, tais como: o Regulamento Geral sobre a Proteção de Dados (GDPR), o California Consumer Privacy Act of 2018 (CCPA), Protection and Electronic Documents Act (PIPEDA), a Act on the Protection of Personal Information (APPI), a Lei de proteção de dados pessoais 25.326 (LDPA) e a Lei Geral de Proteção de Dados 13.709/2018 (LGPD), apresentadas nesse trabalho fica o entendimento que a LGPD se assemelha a GDPR, pois as duas definem dados pessoais de forma semelhante, ambas também estabelecem proteções aprimoradas para dados

pessoais sensíveis, definidos de forma semelhante. Nenhuma das leis se aplica a dados anônimos.

Apesar da semelhança das leis, a conformidade com a GDPR não garante a conformidade com a LGPD. Considerando que a implementação da conformidade com a LGPD está bem próxima, as organizações que tratam os pessoais de indivíduos no Brasil ou que tratam pessoais no Brasil devem considerar imediatamente a revisão de seus processos e a revisão da estrutura de dados atuais de modo a identificar e resolver qualquer falhas de conformidade com a LGPD.

A LGPD completa o marco regulatório brasileiro que representa a sociedade da informação, sobre a interpretação dos princípios constitucionais, representando uma evolução das garantias e direitos fundamentais dos cidadãos. Porém, sem prejudicar o uso econômico dos dados apenas o regulando baseado nos mesmos princípios.

Para avaliar o conhecimento da população quanto a utilização de seus dados e seus direitos, este trabalho desenvolveu um questionário com algumas perguntas que endereçam o tema proposto. Após a análise da pesquisa aplicada foi notório o alto percentual de desconhecimento, por parte do grupo pesquisado, acerca dos questionamentos feitos. Concluindo-se que a falta de informação a respeito da proteção de dados pessoais é uma forte característica, corroborando para o desconhecimento da maioria dos pesquisados sobre a LGPD.

Destaca-se que a criação de uma verdadeira cultura de proteção de dados no Brasil ainda está em processo de formação. Para que tal processo possa atingir a maturidade desejada, as empresas, por públicos e meios de comunicação precisam difundir mais as obrigações e garantias presentes na LGPD para a população, para que ela plenamente saiba de seus direitos e para que exija das organizações um comportamento compatível. Sendo que a implementação dos princípios da LGPD no funcionamento da organização e a atenção das regras estabelecidas são essenciais para o prosseguimento das atividades normais das organizações.

Mesmo ainda sem as aplicabilidades das sanções trazidas pela LGPD, a lei já começou a ser aplicada, devendo a evolução do comportamento e o

estabelecimento da cultura de proteção de dados nas organizações serem fomentados pelos seus dirigentes. Garantindo a segurança jurídica para as partes envolvidas, competitividade nacional e internacional e respeito aos direitos fundamentais.

6. REFERÊNCIAS

AMARAL, Francisco. Evolução a Orlando Gomes. Revista de direito comparado, n. 17, 2º sem. 1999.

ANPD inicia processo de regulamentação sobre incidentes de segurança com tomada de subsídios. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-inicia-processo-de-regulamentacao-sobre-incidentes-de-seguranca-com-tomada-de-subsidios. Acesso em 29/03/2021.

BERNARDI, A. J. Informação, Comunicação, Conhecimento: Evolução e Perspectivas. TransInformação, Campinas, 19(1): p. 39-44, jan./abr., 2007.

BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento / Bruno Ricardo Bioni. - 2. ed. - [3. Reimpr.] - Rio de Janeiro: Forense, 2021.

BLUM, Renato Opice; SCHUCH, Samara. Compartilhamento e comercialização de dados pessoais em ambiente on-line. Contraponto jurídico. Ed. 2019

BOBBIO, Norberto, 1909 - A era dos direitos / Norberto Bobbio; tradução Carlos Nelson Coutinho; apresentação de Celso Lafer. — Nova ed. — Rio de Janeiro: Elsevier, 2004.— 7ª reimpressão.

BURKE, P. Uma história social do conhecimento de Gutenberg a Diderot. Rio de Janeiro: Jorge Zahar Editor, 2003.

CAPANEMA, Walter Aranha. A responsabilidade civil na Lei Geral de Proteção de Dados. Cadernos Jurídicos, São Paulo, ano 21, nº 53, p. 163-170, Janeiro-Março/2020.

DE MASI, Domenico. O Futuro do Trabalho: fadiga e ócio na sociedade pósindustrial. Tradução: Yadyr A. Fugueiredo. 11 ed. Rio de Janeiro: José Olympio, 2014.

DRESCH, Rafael, STEIN, Lílian. Direito Fundamental à Proteção de Dados como Garantia de Capacidade Humana Básica. Indaiatuba, São Paulo: Editora Foco, 2021.

FERREIRA, F. N. F., & Araújo, M. T. de. Política de segurança da informação guia prático para elaboração e implementação. (1st ed.). Rio de Janeiro, RJ: Ciência Moderna, 2008

FIUZA, César. Direito civil: curso completo. 13. ed. rev. e atual. Belo Horizonte: Editora Del Rey, 2009.

GANUT, Marcos, MAGALHÃES, Eduardo. Nível de Maturidade do Mercado Brasileiro para a Lei Geral de Proteção de dados – LGPD. DISPUTES AND INVESTIGATIONS CYBER RISK SERVICES, Alvarez e Marsal, outubro de 2020.

GHAFIR, I., Saleem, J., Hammoudeh, M., Faour, H., Prenosil, V., Jaf, S., … Baker, T. Security threats to critical infrastructure: the human factor. Journal of Supercomputing, 74(10), 2018.

JIMENE, Camilla do Vale. In: LGPD: Lei Geral de Proteção de Dados Comentada / Viviane Nóbrega Maldonado, Renato Opici Blum, coordenadores. São Paulo: Thomson Reuters Brasil, 2019.

KLEE, Antonia e PEREIRA, Alexandre. Cadernos Adenauer xx (2019), nº3 Proteção de dados pessoais: privacidade versus avanço tecnológico - A Lei Geral de Proteção de Dados (LGPD): uma visão panorâmica. Rio de Janeiro: Fundação Konrad Adenauer, outubro 2019

KUMAR, K. Da sociedade pós-industrial à pós-moderna: novas teorias sobre o mundo contemporâneo. Rio de Janeiro: Zahar Editor, 2006.

LIMA, Renata e BRITO, Anya. SOCIEDADE DA INFORMAÇÃO NA AMBIÊNCIA DA NOVA EMPRESARIALIDADE. Revista Jurídica (FURB) v. 24, nº. 54, mai./ago. 2020.

LOVELL, M., & Foy, M. A. General Data Protection Regulation (GDPR). Bone & Joint 360, 7(4), 41–42, 2018

MARTINS, Leonardo. Introdução à jurisprudência do Tribunal Constitucional Federal Alemão. Cinquenta anos de jurisprudência do Tribunal Constitucional Alemão: Fundação Konrad Adenauer, 2005.

MATTOS, Karla Cristina da Costa e Silva. O valor econômico da informação nas relações de consumo. São Paulo: Almedina, 2012.

MENDES, Laura Schertel; DONEDA, Danilo. Comentário à nova Lei de Proteção de Dados (Lei 13.709/2018): o novo paradigma da proteção de dados no Brasil. Revista de Direito do Consumidor, São Paulo, v. 120, p. 566, 2018

NUNES, Luiz Antonio Rizzato. Curso de direito do consumidor. 7. ed. São Paulo: Editora Saraiva, 2012.

PESSOA, C.R., Oliveira, C., Nunes, B. EFEITOS E PROJEÇÕES SOBRE A VIGÊNCIA DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) E O PAPEL DO ENCARREGADO DOS DADOS PESSOAIS. CONTECSI USP - International Conference on Information Systems and Technology Management, 2020

PESSOA, Cláudio Roberto Magalhães. Gestão da informação e do conhecimento no alinhamento estratégico em empresas de engenharia. Tese de doutorado defendida na Universidade Federal de Minas Gerais, 2016.

PINHEIRO, Patrícia Peck. Proteção de dados pessoais: comentários à Lei n. 13.709/2018 (LGPD) / Patrícia Peck Pinheiro - 2. ed. - São Paulo: Saraiva Educação, 2020.

SCHWAB, Klaus. Aplicando a Quarta Revolução Industrial. Tradução: Daniel Moreira Miranda. São Paulo: EDIPRO, 2018.

WONTROBA, Bruno Gressler. ÁBILA, Paola Gabriel. Lei Geral de Proteção de Dados: os direitos do titular dos dados pessoais. Informativo Justen, Pereira, Oliveira e Talamini, Curitiba, nº 163, setembro de 2020.