UNIVERSIDADE FEDERAL DA PARAÍBA

CENTRO DE CIÊNCIAS JURÍDICAS

DEPARTAMENTO DE CIÊNCIAS JURÍDICAS

CURSO DE DIREITO

DANIEL AYRES DE MELO

PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS EM UMA OPERADORA DE PLANO DE SAÚDE E SUAS UNIDADES HOSPITALARES

SANTA RITA/PB
2020

DANIEL AYRES DE MELO

PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS EM UMA OPERADORA DE PLANO DE SAÚDE E SUAS UNIDADES HOSPITALARES

Trabalho de Conclusão do Curso de Direito, apresentado ao Centro de Ciências Jurídicas - Departamento de Ciências Jurídicas, da Universidade Federal da Paraíba (UFPB), como requisito parcial para obtenção do título de Bacharel em Direito.

Orientador: Prof. Dr. Adriano Marteleto Godinho.

SANTA RITA/PB
2020

FOLHA DE APROVAÇÃO

PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS EM UMA OPERADORA DE PLANO DE SAÚDE E SUAS UNIDADES HOSPITALARES

DANIEL AYRES DE MELO

Trabalho de Conclusão do Curso de Direito, apresentado ao Centro de Ciências Jurídicas - Departamento de Ciências Jurídicas, da Universidade Federal da Paraíba (UFPB), como requisito parcial para obtenção do título de Bacharel em Direito.

Aprovado em:____/____/____.

BANCA EXAMINADORA

_____
Professor Adriano Marteleto Godinho
Orientador

_____
Professora Adriana Ormond
Membro

_____
Professora Ana Paula Correia de Albuquerque Costa
Membro

Dedico este trabalho a minha esposa, Mônica Maria Carvalho e aos meus filhos, Matheus e Maria Luiza, que me incentivaram e suportaram minha ausência nas aulas e nos estudos por cinco anos.

AGRADECIMENTOS

Agradeço à Ciência jurídica, pela sua inspiração e desafios.

Aos familiares: minha mãe, Sônia Maria Ayres de Melo, minha esposa, Mônica Maria Carvalho e aos meus filhos, Matheus e Maria Luiza de Abrantes C. Ayres, pelo incentivo de buscar novos horizontes.

Ao Professor Dr. Adriano Marteleto Godinho, as incríveis aulas ministradas ao longo do curso que muito me inspiraram e pela dedicação e orientação prestada na elaboração deste Trabalho.

E a meus amigos Matheus Regis e Lucas Brenner que foram parceiros ao longo de todo o curso.

“Viver é automático, porém, bem viver, selecionando as questões que promovem os sentimentos e a inteligência a níveis mais elevados, para a conquista da sabedoria, deve ser o objetivo de máxima importância para todo viajante na indumentária carnal.”

(Joanna de Ângelis)

RESUMO

O presente trabalho tem a finalidade de mostrar a adequação de uma empresa de médio porte na área de saúde, com aproximadamente cento e cinquenta mil clientes e faturamento anual próximo de oitocentos milhões, à Lei Geral de Proteção de Dados (LGPD). Faz-se inicialmente uma análise dos impactos do uso indiscriminado dos dados pessoais dos cidadãos, por conseguinte a necessidade de um direito tutelador do bem jurídico dos dados pessoais, mostrando como a proteção a essas informações é um direito fundamental ao desenvolvimento da pessoa humana. Em seguida, é apresentada a evolução das normas jurídicas no Brasil relacionadas ao tema da proteção aos dados pessoais, bem como uma investigação dos temas relacionados à estrutura principiológica da LGPD, as bases legais que permitem o tratamento de dados pessoais pelas empresas e pelo governo, os principais atores envolvidos e as sanções e multas previstas. Por fim, levantam-se as atividades e ações necessárias a uma operadora de plano de saúde e suas unidades hospitalares de modo a se adequarem à legislação, garantindo a autodeterminação informativa de seus clientes e evitando as multas previstas pela não adequação a lei ou vazamento de dados pessoais.

Palavras-chave: dados pessoais, dados sensíveis, privacidade e proteção de dados pessoais. Lei Geral de Proteção de Dados. LGPD

ABSTRACT

The present work has the purpose of showing the adequacy of a medium-sized company in the health area, with approximately one hundred and fifty thousand customers and annual turnover close to eight hundred million, to the General Data Protection Law (LGPD). Initially, an analysis is made of the impacts of the indiscriminate use of citizens' personal data, therefore the need for a right to protect the legal good of personal data, showing how the protection of this information is a fundamental right for the development of the human person. Then, the evolution of the legal norms in Brazil related to the subject of protection of personal data is presented, as well as an investigation of the issues related to the LGPD's principle structure, the legal bases that allow the processing of personal data by companies and the government, the main actors involved and the penalties and fines provided for. Finally, the activities and actions necessary for a health plan operator and its hospital units are raised in order to comply with the legislation, guaranteeing the informative self-determination of its customers and avoiding the fines provided for non-compliance with the law or leakage of personal data.

Keywords: personal data, sensitive data, privacy and personal data protection. General Data Protection Act. LGPD

LISTA DE ABREVIATURAS E SIGLAS

LGPD	Lei Geral de Proteção de Dados
ANS	Agência Nacional de Saúde
GDPR	Regulamento Geral de Proteção de Dados Europeu
DPO	Encarregado de Dados ou *Data Protection Officer*
PbD	Privacy by Design

LISTA DE FIGURAS

SUMÁRIO

1. INTRODUÇÃO

Atualmente, fornecemos uma grande quantidade de dados pessoais para empresas com quem mantemos relações comerciais e para muitos serviços disponíveis na rede mundial de computadores sem que façamos nenhuma crítica sobre o destino e utilização dessas informações. As redes sociais buscam a todo momento saber quem estudou com você, a sua localização e os assuntos de seu interesse. Aparentemente recebemos vários serviços gratuitos na internet, sem saber que o pagamento é exatamente o fornecimento de nossas informações.

Passamos atualmente boa parte da nossa vida social conectados a uma vida eletrônica, através de nossos computadores, tablets e smartphones. A cada iteração os sistemas vão nos solicitando mais informações pessoais. Os serviços da Google, por exemplo, como tradutor, serviços de geolocalização, e-mail, armazenamento de dados, pesquisa, entretenimento e navegadores de internet são disponibilizados muitas vezes sem nenhum custo para o cliente. Como essas empresas são remuneradas?

Grandes empresas como Yahoo, Amazon, Netflix, Google e Facebook passaram a monitorar os dados pessoais e rastros digitais dos usuários de seus serviços para comercializar essas informações e gerar um grande volume de anúncios personalizados.

> Um paradoxo é que enquanto o consumo exige a sedução prazerosa dos consumidores, essa sedução também é resultado da vigilância sistemática numa escala de massa. Se isso não era óbvio em função de formas anteriores de marketing de base de dados, o advento da Amazon, do Facebook e do Google indica o atual estado da arte (LYON, 2013, p. 23).

Empresas que fornecem seguros de vida e de saúde podem utilizar os dados pessoais e médicos para decidirem se fornecem ou não serviços a seus clientes, inclusive com a utilização de programas de computadores capazes de emitirem decisões automatizadas.

A sociedade atual está organizada em torno da informação que passou a ser o elemento mais importante para o desenvolvimento econômico. A capacidade tecnológica de processamento de informação criou um novo poder. A sociedade que um dia já se organizou em torno da produção agrícola ou industrial, nos dias atuais, organiza-se em torno do poder tecnológico. Vivemos a era da sociedade da informação. Os dados e principalmente o conhecimento gerado passou a ser a mola

propulsora para geração de riqueza.

Dentro desse cenário, as informações pessoais de cada cidadão são o fator central para a engrenagem que faz girar a economia nos dias atuais. Há um crescimento exponencial no tratamento e compartilhamento dos dados, sendo esse intercâmbio utilizado para os mais variados fins. As pessoas passaram a ter uma atitude passiva dentro dessa dinâmica, enquanto seus dados de localização, preferências, compras, opiniões e pesquisas são armazenados e processados, gerando conhecimento e traçando os rumos da geração de necessidade do consumo. Cada clique nas redes sociais, sites, ferramentas e aplicativos armazenam um grande volume de dados.

Os softwares atuais conseguem monitorar até mesmo o estado emocional das pessoas que estão sendo monitoradas de forma impositiva sem qualquer autorização, consentimento ou até mesmo conhecimento que seus dados estão sendo armazenados, compartilhados e comercializados. Passamos a nesse momento ter uma violação das relações de consumo e da boa-fé.

Dentro desse cenário surge a LGPD, Lei Geral de Proteção de Dados Brasileira que foi sancionada no dia 14 de agosto de 2018 e entrará em vigor no dia 16 de agosto de 2020. A nova lei inaugura um novo cenário regulatório no país e foi inspirada pelo Regulamento Geral de Proteção de Dados Europeu (GDPR). Passa a tratar os assuntos relacionados à coleta, uso, portabilidade, armazenamento, processamento, compartilhamento e exclusão dos dados pessoais.

Dentre os princípios trazidos pela Lei podemos destacar que os dados pessoais só podem ser solicitados e armazenados se estiverem dentro do contexto necessário para a operação e para o fim específico que tenham sido informados ao titular de dados. O cidadão passa a ter uma melhor percepção sobre quem, como e para que seus dados serão utilizados e tratados.

Esse lapso temporal entre a sanção e a entrada em vigor se dá exatamente pela dificuldade e investimento necessário para que as empresas possam se adequar.

A metodologia utilizada no trabalho foi realizar uma grande revisão bibliográfica para entendimento da LGPD uma vez que essa lei é nova e a sua interpretação precisará passar por um processo de amadurecimento dos cidadãos, das empresas e do governo e também trazer a experiência prática do projeto que uma operadora de plano de saúde e suas unidades hospitalares seguiram para se adequar à lei.

Em síntese, o primeiro capítulo do estudo procurará relatar os impactos que o

uso indiscriminado de dados pessoais pode trazer ao desenvolvimento da pessoa humana e a importância de se estruturar um regulamento que proteja o direito fundamental à privacidade desse tipo de informação.

O segundo capítulo fará um apanhado da evolução histórica do desenvolvimento do tema no Brasil até a sanção da Lei Federal nº 13.709/2018 (“LGPD”) e também fará uma análise da nova Lei, avaliando a sua estrutura principiológica, suas bases legais, os principais atores envolvidos e as sanções e multas previstas.

Por fim, o terceiro capítulo fará um estudo de como foi o processo de adequação da Unimed João Pessoa e suas unidades hospitalares à Lei Geral de Proteção de Dados. Serão relatadas as principais etapas e atividades que as empresas do grupo trilharam para garantir maior proteção aos dados de seus clientes e evitar as multas previstas pelo vazamento de dados pessoais. Importante destacar que todas as informações trazidas no trabalho da empresa são públicas e podem ser facilmente acessadas no sítio eletrônico da Agência Nacional de Saúde(ANS).

O ambiente da área de saúde se torna ainda mais desafiador por causa do caráter extremamente sigiloso e do grande volume de dados sensíveis espalhados nos bancos de dados desse tipo de instituição. Com a nova lei, essas pessoas jurídicas de direito privado serão ainda mais responsabilizadas pela guarda, segurança e confidencialidade dos dados dos pacientes.

2. POR QUE UMA LEI DE PROTEÇÃO DE DADOS?

2.1. ECONOMIA DA INFORMAÇÃO

Todo o mercado coorporativo vem passando por mudanças profundas ocasionadas pela disrupção que a evolução tecnológica trouxe no sentido de romper com os padrões normais de movimento da sociedade. Está existindo uma verdadeira descontinuação em muito pouco tempo de padrões, modelos e tecnologias já consolidados por décadas. Empresas com a AirBnb, Ubber e Netflix redefiniram a forma convencional de pensar do mercado. Não é mais necessário ter carros para ser a maior empresa de transporte de passageiros do mundo, mas sim, ter uma grande capacidade de agregar aspectos tecnológicos e informacionais que permitem que fornecedores de serviços e consumidores se conectem em qualquer local de forma *on line*.

Estamos diante de uma nova era em que o volume de informação e a velocidade das trocas de dados eram impensáveis há poucos anos atrás. Há um crescimento exponencial dos dados com o uso massivo das novas tecnologias. Estima-se que o volume de informação dobre a cada dois anos. A consultoria EMC em seu estudo “A Universe of Opportunities and Challenges”, estima que o volume de dados passou de 166 Exabytes[1] para 988 Exabytes entre os anos de 2006 a 2010. A expectativa é que em 2020 atinja-se os 40 trilhões de Gigabytes.

Essa explosão tecnológica e informacional está reinventando o contexto social e econômico, quebrando antigos conceitos e paradigmas da sociedade contemporânea. A nova economia se fundamenta na informação. A liderança tecnológica define a condição de hegemonia dos Estados e dos Capitais, já que através dela são impostos os padrões gerais de reprodução e multiplicação dos ganhos tecnológicos (DUPAS, 2005).

[1] Exabyte – É uma unidade baseada em código binário (0 e/ou 1) para o armazenamento de informações computacionais. 1 exabyte possui 1024 petabytes, enquanto 1 petabyte possui 1024 terabytes. Uma foto digital possui alguns megabytes de tamanho, enquanto um computador pessoal possui uma média de 500 gigabaytes a 1 terabyte de espaço em disco.

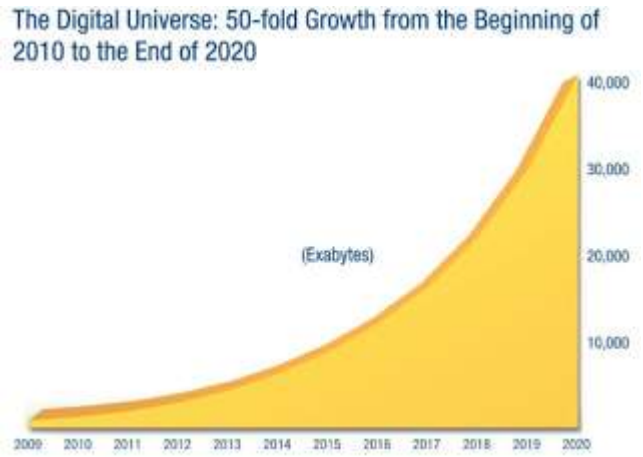

Figura 1 Estimativa de crescimento do volume de dados digitais de 2010 a 2020.

Fonte: https://www.emc.com/

Essa explosão tecnológica e informacional está reinventando o contexto social e econômico, quebrando antigos conceitos e paradigmas da sociedade contemporânea. A nova economia se fundamenta na informação. A liderança tecnológica define a condição de hegemonia dos Estados e dos Capitais, já que através dela são impostos os padrões gerais de reprodução e multiplicação dos ganhos tecnológicos (DUPAS, 2005).

A economia da informação e do conhecimento mostra-se como uma época em que a ruptura dos padrões acontece de forma muito rápida em comparação com eras anteriores. Toffler (1998) traz a ideia que a sociedade vem evoluindo em ondas, passando pela agricultura, indústria e serviços. Cada uma delas promovendo uma revolução na forma de produzir riquezas e nas relações sociais. A Revolução Agrícola trouxe mudanças significativas na produção de alimentos através de avanços na agricultura, novas tecnologias e técnicas capazes de aumentar a produtividade. A Revolução Industrial permitiu o surgimento das indústrias com o emprego de maquinário que acelerou a produção de mercadorias, a exploração dos recursos da natureza e provocou mudanças profundas nas relações de trabalho. A Revolução da Informação é fundamentada no conhecimento, nos dados e na comunicação como fonte de riqueza.

Passamos por duas revoluções em que se tinha a tangibilidade das fontes de riqueza, ou seja, a terra e a indústria, e que o progresso foi percebido ao longo de séculos. Estamos vivendo nesse momento uma revolução em que a informação,

elemento intangível, passa a ser o novo centro do capital e as mudanças são medidas em meses.

Segundo Castells (1999, p.50):

> Diferentemente de qualquer outra revolução, o cerne da transformação que estamos vivendo na revolução atual refere-se às tecnologias da informação, processamento e comunicação. A tecnologia da informação é para esta revolução o que as novas fontes de energia foram para as revoluções industriais sucessivas [...].

Dentro desse ambiente inovador e globalizado, saem na frente os Estados e empresas que estão no domínio das tecnologias e consequentemente na capacidade de gerar conhecimento dentro do enorme volume de dados disponíveis. Surge uma competição globalizada em que a capacidade de gerar inovações e organizar a informação disponível é essencial para a corrida concorrencial. As dinâmicas dessas novas atividades são obrigatoriamente afetadas pela infraestrutura de informações disponíveis.

A matéria-prima desse novo paradigma é a informação. A agregação de valor a produtos e serviços passa pela maior capacidade de gerar conhecimento a partir do dado disponível. O maior desafio é adquirir as habilidades necessárias para transformar os dados em um recurso econômico estratégico. Para isso, é necessário implementar novas tecnologias, programar grandes investimentos em pesquisa, ter mão de obra altamente qualificada, ou seja, apenas as economias avançadas detêm esse controle. Isso provoca um agravamento das desigualdades sociais, pois, enquanto os países desenvolvidos definem os produtos e padrões de consumo, os países menos desenvolvidos apenas seguem a definição. Isso muda de forma global a organização da distribuição das oportunidades de trabalho, o padrão de consumo e a distribuição de renda.

O crescimento de informação está diretamente ligado à super-rodovia que permite a sua circulação, a internet. Foi esse ambiente global de intercomunicação moldado pelos interesses econômicos que vem definindo os caminhos dessa nova era tecnológica. Dentro desse ambiente temos o comércio eletrônico que mudou rapidamente a lógica de funcionamento dos mercados tradicionais. Agora é possível atingir de forma personalizada o consumidor em qualquer ponto do planeta independentemente da localização da empresa. Para o funcionamento desse novo modelo a informação tornou-se insumo essencial para conexões mais assertivas com

o público alvo. O uso da informação e do conhecimento proporciona novas opções de produtos e serviços.

Para Castells (A galáxia... cit, p.57), “O que está surgindo não é uma economia ponto.com, mas uma economia interconectada com um sistema nervoso eletrônico”. Portanto, esse fluxo informacional é o centro para a geração de riquezas e o acúmulo de capitais. Um dos principais mecanismos para consolidar a economia da informação é a geração de conhecimento a partir dos dados pessoais dos cidadãos.

2.2. A IMPORTÂNCIA DE UMA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Na sociedade da informação, os dados dos consumidores passaram a ser base para a geração de riquezas. A capacidade de tornar essas informações em conhecimento produtivo está direcionando os negócios no mundo empresarial. O proprietário dos dados passa a ser um mero expectador do compartilhamento de suas informações. Daí, inclusive, surge a expressão consumidor de vidro, exatamente para cunhar a ideia de fragilidade das pessoas frente a coleta frenética de seus dados e armazenamento nos bancos de dados espelhados na nuvem[2].

Através da popularização da internet e dos smartphones, os consumidores passaram a compartilhar uma série de informações em tempo real. Enquanto navegam, por exemplo, nas redes sociais, os inúmeros cliques vão armazenando suas preferências, opiniões e necessidades. A vida parece não ter mais nenhum sentido se cada situação da vida não for exposta na rede. As pessoas expõem completamente sua privacidade na tentativa de buscar uma satisfação pessoal. Informações pessoais como idade, sexo, status civil, redes de relacionamento e preferências permitem que atualmente seja feito um mapeamento do perfil dos consumidores e dessa forma se consegue uma exploração de marketing muito mais específica e direcionada. Cerca de 92% dos sites americanos armazenam dados pessoais de seus usuários e realizam

---

[2] A definição de nuvem pode parecer obscura, mas, basicamente, é um termo utilizado para descrever uma rede global de servidores, cada um com uma função única. A nuvem não é uma entidade física, mas uma vasta rede de servidores remotos ao redor do globo que são conectados e operam como um único ecossistema. Estes servidores são responsáveis por armazenar e gerenciar dados, executar aplicativos ou fornecer conteúdos ou serviços, como transmissão de vídeos, webmail, software de produtividade ou mídias dispositivo com acesso à Internet. As informações estarão disponíveis em qualquer lugar, a qualquer hora. https://azure.microsoft.com/pt-br/overview/what-is-the-cloud/

processamentos para atingir seus interesses comerciais (Lessig, 1999, p.153 apud Castells, 2003, p.143).

O professor e sociólogo, David Lyon, em sua mais recente obra, Vigilância Líquida (2014), relata uma entrevista com o também sociólogo Zygmunt Bauman e nela traz a ideia que existe uma permanente vigilância que vem se transformando ao longo das décadas e que está sempre em mutação. Traz a ideia de uma vigilância em estado líquido que está em constante fluidez e movimento. Todos os cidadãos estariam sendo monitorados, observados, checados e acompanhados pelas empresas e pelos governos.

As organizações de vigilâncias modernas se fortalecem no momento em que o cotidiano das pessoas são expostas cada vez de forma mais nítida. Atualmente a sensação de vigilância é cada vez mais perceptível uma vez que sites, aplicativos, câmera e GPS nos smartphones servem para capturar cada passo que damos. “Submetemos à matança nossos direitos de privacidade por vontade própria. Ou talvez apenas consintamos em perder a privacidade como preço razoável pelas maravilhas oferecidas em troca” (BAUMAN, 2013, p. 28).

Com o uso da Inteligência Artificial são produzidos novos algoritmos capazes de analisar qualquer informação ou rastro produzidos nas redes sociais e aplicativos. Quanto mais pessoas e quanto mais tempo se passam utilizando esses serviços digitais, mais dados são produzidos e consequentemente mais aprendizado e conhecimento são gerados. Esses softwares já conseguem monitorar o estado emocional de seus usuários. O uso aparentemente inocente dos *emoji´s e emoticons* são usados se captar as emoções. Já existe tecnologia em desenvolvimento para que o celular através do reconhecimento facial identifique as emoções de seus proprietários apenas pelo fato de olhar para ele.

Cada vez mais é possível o uso de grandes bancos de dados e algoritmos que utilizam machine learning[3] para a realização de análises preditivas. Já é possível prever o futuro, sabendo quando acontecerá uma crise financeira, um suicídio ou um rompimento de uma relação amorosa. Temos, portanto, um consumidor

[3] Machine Learning é um conjunto de regras e procedimentos, que permite que os computadores possam agir e tomar decisões baseados em dados ao invés de ser explicitamente programados para realizar uma determinada tarefa. Programas de Machine Learning também são projetados para aprender e melhorar ao longo do tempo quando expostos a novos dados. Machine Learning tem estado no centro de muitos avanços tecnológicos nos últimos anos, como carros que dirigem, visão computacional e sistemas de reconhecimento de voz. http://www.cienciaedados.com/conceitos-fundamentais-de-machine-learning/

completamente transparente e uma capacidade de exploração publicitária sem precedentes na história. Os dados pessoais passam a ser um ativo financeiro e a matéria-prima para a geração de riqueza nas empresas.

Se pensarmos no modelo de negócio do Facebook ou Instagram, nada é cobrado para que os usuários criem suas contas e utilizem os serviços para se comunicarem, trocarem experiências, buscar informações ou compartilhar seus dados. Entretanto, em contrapartida, os consumidores fornecem seus dados pessoais para receberem publicidade digital que é o que monetiza essas empresas. Recentemente o Facebook comprou a empresa WhatsApp por US$ 22 bilhões[4]. A empresa de mensagens aparentemente não tem nenhuma fonte de receita. O principal interesse da aquisição será o compartilhamento de informações que permite que a rede social seja mais eficiente no envio de mensagens publicitárias. Houve uma atualização de termos de privacidade do aplicativo de mensagens para permitir esse compartilhamento de informações. Sempre que a empresa coleta dados pessoas, o consumidor é o produto.

O consumidor precisa ceder para ter acesso aos serviços. Baumam e Lyon trazem também a ideia de uma vigilância pós-pan-óptica em que o próprio consumidor fornece suas informações saindo da situação em que “poucos vigiam muitos” para uma que “todos vigiam a todos”. As corporações que fazem a captação dos dados pessoais recebem a maior parte delas quando seus usuários fazem checkin nos aeroportos, fazem compras online, assistem vídeos e curtem suas preferências nas redes sociais. Toda essa coleta de dados acontece de forma automática e rotineira, não é mais possível sobreviver sem compartilhar dados. “A maioria das pessoas abre mão de seus direitos à privacidade para ter condições de usar a internet. Uma vez que se renunciou a esse direito à proteção da privacidade, os dados pessoais tornam-se propriedade legítima das firmas de internet e de seus clientes” (CASTELLS, 2003, 144).

As grandes empresas de tecnologia analisam os dados pessoais e as preferências de seus usuários e oferecem produtos de forma customizada. A Netflix prevê já com grande assertividade a preferência de seus clientes e sugere os filmes

[4]http://g1.globo.com/economia/negocios/noticia/2014/10/preco-de-compra-do-whatsapp-pelo-facebook-sobe-us-22-bilhoes.html

baseado nesse conhecimento. A personalização é uma estratégia essencial para grandes empresas como: Yahoo, Google, Facebook, YouTube e Microsoft Live (PARISER, 2012, p.13).

Eli Pariser em seu livro, *O filtro invisível* (2012), desfaz a ideia que a internet é um local livre e sem amarras em que as pessoas conseguem acessar todo tipo de informação e passa a expor uma realidade em que os usuários estão vivendo em uma bolha, recebendo apenas as informações que as grandes organizações acham que são interessantes para eles. Para o autor, os filtros a que os internautas são submetidos gera uma espécie de determinismo informativo, o histórico passado define o que será visto no futuro.

Os consumidores são inseridos em um círculo fechado de conteúdo pois existe um determinismo do que será lhe apresentado baseado no seu perfil e no histórico de acessos que realizamos. Para Pariser (2012, p 103), “os sistemas de filtragem do Google, por exemplo, dependem amplamente do nosso histórico na rede e daquilo em que clicamos (indicadores de clique) para inferir as coisas das quais gostamos ou não”. Para o autor, os grandes sites, antes de estabelecer os filtros e a personalização que limitam a liberdade dos navegadores, tentam entender as pessoas e suas preferências e depois vão fazendo ajustes a partir das interações com as ferramentas.

A causa primária para a criação dessa bolha, segundo Parisier, está na geração de publicidade que a verdadeira fonte de renda dessas estruturas que controlam a internet.

> As massas de dados acumulados pelo Facebook e pelo Google têm dois propósitos: para os usuários, são a chave para a oferta de notícias e resultados pessoalmente relevantes; para os anunciantes, os dados são a chave para encontrar possíveis compradores. A empresa que tiver a maior quantidade de informações e souber usá-las melhor ganhará os dólares da publicidade. (Parisier, p. 41)

A captação de informações pessoais é na maioria das vezes feita sem o conhecimento e consentimento do proprietário dos dados o que viola alguns princípios com o da boa-fé e como se estabelece as relações de consumo.

Temos as palavras de Laura Schertel Mendes: “É preciso criar novas soluções para enfrentar os desafios crescentes da sociedade da informação, preservando as conquistas já obtidas referentes à proteção da personalidade e da dignidade do indivíduo”.

Nesse momento não estamos mais falando apenas na invasão de privacidade,

mas também em ultrapassar um universo ainda mais restrito que é o direito à intimidade, ambas garantias constitucionais. Foi estabelecido um monitoramento imperativo das pessoas.

A necessidade de uma lei para proteção dos dados pessoais surge exatamente para regular essa relação, para permitir o livre desenvolvimento do ser humano. Também para estabelecer a melhor forma de relacionamento entre os consumidores e as empresas, definindo se será baseada em confiança, na proteção da privacidade ou no consenso, evitando uma relação prejudicial em especial para o lado mais fraco da relação.

2.3. DIREITOS DA PERSONALIDADE E DADOS SENSÍVEIS

Da década de 1990 em que o acesso à internet era bem limitado para os dias atuais, estamos passando por um verdadeiro processo de disrupção tecnológica. Ao lado das inúmeras vantagens dessa era digital, estamos vinculadas as suas desvantagens e uma delas é não cometer deslizes. Somos continuamente vigiados. Praticamente se perdeu o direito de ser esquecido. Uma simples discussão com um familiar fica registrado indefinidamente nos aplicativos de mensagens, um relacionamento amoroso que passou pelas redes sociais e foi rompido, dificilmente pode ser esquecido. Tudo aquilo que for registrado e for incômodo pode um dia ser recuperado em uma simples busca no Google. Perdemos a capacidade de gerenciar nossas informações e registros.

A facilidade que temos de receber cada vez mais um marketing personalizado, sugestões de filmes e reportagens de nosso interesse é conseguida graças à evolução dos algoritmos, da inteligência artificial e de uma massa impensável de dados pessoais que estão espalhados na rede mundial de computadores. É possível traçar um perfil exato das pessoas que facilmente pode ser usado para discriminá-las e atingir suas garantias constitucionais como o direito da personalidade. Dados são comercializados com empresas de seguros de carros que podem utilizar as informações para cobrar mais caro pelos seguros ou mesmo com seguradoras de saúde que impeçam a aceitação do cliente. Empresas de aprovação de crédito podem dispor de programas de computadores discriminatórios que impeçam a concessão do crédito após a análise das informações como o local da moradia ou origem racial. Portanto, uma série de abusos, violações e prejuízos materiais e emocionais podem

ser cometidos pelo compartilhamento indiscriminado e sem regulamentação dos dados pessoais.

As empresas atuam como verdadeiras acumuladoras de dados pessoais de seus clientes. Qual o sentido de fornecer o nome dos seus genitores ao comprar um livro? Ou mesmo, informar a sua religião para a compra de um carro. O direito a ter o controle de seus dados pessoais precisa voltar a ser do cidadão, podendo ele livremente conceder ou retirar o acesso a seus dados pessoais.

Todo esse processo de revolução tecnológica que vivemos tem movimentado o mundo jurídico no sentido de garantir a tutela dos bens jurídicos envolvendo a personalidade e a dignidade da pessoa humana.

Para Sérgio Souza a personalidade é o primeiro dos bens jurídicos e assim o autor define: “a personalidade é um complexo de características interiores com o qual o indivíduo pode manifestar-se perante a coletividade e o meio que o cerca, revelando seus atributos materiais e morais. Com efeito, no sentido jurídico, a personalidade é um bem, aliás, o primeiro pertencente à pessoa”(SOUZA, 2002, p. 01)

Os direitos da personalidade foram exatamente positivados no ordenamento jurídico para garantir aos cidadãos uma proteção contra lesões em seus bens mais íntimos, ou seja, protegendo a integridade física, moral e intelectual dos titulares do direito. Nossa Constituição de 1998, em seu art. 1º, III, traz o princípio da dignidade da pessoa humana como um dos fundamentos basilares de República Federativa do Brasil. Além disso, o nosso Direito Civil vem passando por um processo de maior humanização nos últimos tempos, ou seja, colocando o ser humano em destaque, diminuindo a influência do patrimônio, afinal a *ultima ratio* do Direito é o homem. Nosso Código Civil de 2002 traz em sua essência a proteção do homem com uma atenção especial aos direitos da personalidade na tentativa de consolidar o alcance da dignidade do ser humano.

A personalidade de uma pessoa pode ser entendida como um conjunto de características que tornam o ser humano único e nesse contexto a proteção dos dados pessoais representa uma extensão desse sentido. É necessário que o Direito passe a tutelar qualquer forma de desrespeito ou hostilidade que tentem atingir a individualidade. Dados pessoais podem ser definidos como uma informação relacionada a uma pessoa que possa identificá-la, como um cpf, um nome ou dados de localização. Ainda mais restrito, temos a definição de um dado pessoal sensível que seriam uma categoria de informações relacionadas a origem racial, dados

biométricos ou ainda sua orientação sexual e política. Portanto, os dados pessoais podem ser considerados como um prolongamento de seus titulares.

A Lei Geral de Proteção da Dados vem exatamente trazer um conjunto de normas que promovam um processo de governança capaz de tutelar os interesses dos cidadãos, impedindo qualquer manipulação ou uso de dados que impactem no desenvolvimento da personalidade de um indivíduo sem uma base legal ou consentimento de seus proprietários. A proteção de dados pessoais vem atuar para evitar manipulações dessas informações sem autorização que permitam a criação de perfis e modelos de comportamento que possam influenciar negativamente na vida das pessoas, principalmente de forma a afrontar os direitos da personalidade ou direitos fundamentais do ser humano.

Diante da atual imersão que se vive no mundo digital, surge a necessidade de uma tutela jurídica que garanta a possibilidade do indivíduo se relacionar livremente sem a possibilidade de decisões automatizadas que promovam práticas discriminatórias e estigmatizações.

3. PROTEÇÃO DE DADOS NO BRASIL

A temática da proteção de dados no Brasil ganhou força recentemente com a publicação da Lei 13.709 em agosto de 2018 com entrada em vigência para agosto de 2020. Nossa Lei Geral de Proteção de Dados surge em parte pela pressão internacional pois, ao ter uma Lei o Brasil entra para um elenco de mais de 100 países[5] que estão coerentes com a necessidade de proteção de dados pessoais. Além disso, a Lei Europeia de Proteção de Dados, GDPR, tem eficácia extraterritorial e diversas empresas brasileiras que possuem filiais e contratos com a Europa corriam o risco de sofrerem multas altíssimas ou mesmo terem seus negócios suspensos. Ainda contribuindo para a implantação de uma norma no Brasil que resguarde os dados pessoais, temos a questão do Brasil estar há algum tempo tentando ingressar na Organização para a Cooperação e Desenvolvimento Econômico (OCDE) e um dos requisitos também é a adequação aos requisitos de privacidade de dados pessoais, especificados em um documento(OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data) publicado pela própria instituição já na década de 1980 e revisado em 2013. As regras contidas nesse documento influenciaram as Leis de diversos países

Outro fator, é a necessidade do momento atual de imersão tecnológica que o mundo vive, em que já não é mais possível viver desconectado do mundo cibernético. Há, portanto, uma necessidade urgente de se criar um instrumento normativo capaz de tutelar os direitos dos cidadãos no sentido que eles possam interagir livremente nessa nova realidade virtual sem restrições a sua privacidade, além também de impedir que algoritmos e decisões automatizadas possam promover práticas discriminatórias.

O Brasil seguiu uma trilha até ter a sua Lei de proteção de dados publicada. Pode-se extrair da nossa Constituição Federal de 1988 em uma intepretação conjunta dos artigos 1º, III; 3º, I e IV, 5º, X, XII e LXXII[6] que já se existe uma previsão

[5] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1951416

[6] Art. 1º, III - a dignidade da pessoa humana;
Art. 3º, I - construir uma sociedade livre, justa e solidária;
Art. 3º, IV - promover o bem de todos, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação.
Art. 5º, 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;

e um direito fundamental no sentido de garantir uma proteção aos dados pessoais. O Superior Tribunal de Justiça através da Ministra relatora Nancy Andrighi no julgamento da EDcl no REsp 1630889/DF no dia 27/11/2018 afirma que:

> **“**os direitos à intimidade e à proteção da vida privada, diretamente relacionados à utilização de dados pessoais por bancos de dados de proteção ao crédito, consagram o direito à autodeterminação informativa e encontram guarida constitucional no art. 5º, X, da Carta Magna, que deve ser aplicado nas relações entre particulares por força de sua eficácia horizontal e privilegiado por imposição do princípio da máxima efetividade dos direitos fundamentais**.”**

No âmbito das leis infraconstitucionais existe uma série de dispositivos que sinalizam a preocupação dos legisladores em iniciar uma garantia jurídica ao direito de ter os dados pessoais devidamente protegidos. No Código de Defesa do Consumidor(Lei 8.078/90) temos nos artigos 43, 72 e 73 já existe uma previsão expressa do direito do consumidor em ter uma proteção e transparência nas informações armazenados nos bancos de dados.

> 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.
> Art. 72. Impedir ou dificultar o acesso do consumidor às informações que sobre ele constem em cadastros, banco de dados, fichas e registros: Pena Detenção de seis meses a um ano ou multa.
> Art. 73. Deixar de corrigir imediatamente informação sobre consumidor constante de cadastro, banco de dados, fichas ou registros que sabe ou deveria saber ser inexata: Pena Detenção de um a seis meses ou multa.

A Lei de Acesso às Informações (lei 12.527/11) em sua seção V traz os procedimentos para a classificação do sigilo de informações no âmbito da administração pública federal. A Lei do Cadastro Positivo (lei 12.414/11) prevê a formação e consulta a banco de dados com informações de adimplemento das pessoas físicas e jurídicas. Traz também alguns princípios como transparência e finalidade que serão posteriormente utilizados pela LGPD.

Art. 5º, 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;

Art. 5º, LXXII - conceder-se-á *habeas data:* a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público; b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo;

O Decreto do Comércio Eletrônico (decreto 7.962/13) em seu artigo 4º, inciso VII traz que os fornecedores devem utilizar mecanismos de segurança eficazes para pagamento e para tratamento de dados do consumidor.

O Marco Civil da Internet (Lei 12.965/14) estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Em seu artigo 3º, inciso II traz a proteção à privacidade como um dos princípios que disciplinam o uso da internet. O Decreto 8.771/16 regulamenta a lei anterior e estabelece mecanismos de armazenamento e fornecimento ao setor público de dados cadastrais.

A Lei Geral de Proteção de Dados Pessoais do Brasil(LGPD) veio para centralizar a legislação sobre dados pessoais e substituir ou aperfeiçoar mais de 40 normas que disciplinavam de alguma forma o armazenamento e manipulação desses tipos de informações. A LGPD atua nos setores públicos e privados e tem gerência sobre dados online e off-line armazenados em bancos de dados.

O Brasil precisava avançar em relação as suas normas sobre a garantia da privacidade dos dados pessoais de seus cidadãos. A LGPD veio, portanto, diminuir a insegurança jurídica que se tinha em torno desse tema e que deixava o país em desvantagem competitiva em relação ao mundo.

Foi trilhado um longo caminho até que a Lei n. 13.709/18 fosse aprovada pelo plenário do Senado Federal em 10 de julho de 2016 e promulgada pelo então presidente Michel Temer em 14 de agosto de 2018. O processo legislativo teve início em 2010 com uma consulta pública promovida pelo Ministério da Justiça. Em 13 de junho de 2012 o deputado Milton Monti do PR/SP apresentou o projeto de lei PL 4060/2012 cuja ementa atual dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014. Em 13 de maio de 2016 surge a proposta de lei PL 5276/2016 de autoria do poder executivo que dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural.

Inicialmente a Lei passaria por um processo de dezoito meses para entrar em vigência, entretanto, a redação consolidada da LGPD sancionada pelo presidente Jair Bolsonaro concedeu uma extensão de seis meses fixando a entra em vigor para o dia 16 de agosto de 2020. Ainda existe uma indecisão sobre esse tema pois no dia 30 de outubro de 2019, o deputado Carlos Bezerra do MDB/MT apresentou o Projeto de Lei nº 5.762/2019 propondo a prorrogação em dois anos de entrada em vigor, o que alteraria a data para 15 de agosto de 2022.

Esse foi o caminho percorrido em nosso país para que pudesse ser formado um regulamento contendo princípios, direitos, obrigações e sanções capaz de proteger os direitos a liberdade, privacidade e a livre desenvolvimento da personalidade humana, garantindo um ambiente de confiança no mundo digital.

3.1. ESTRUTURA DA LEI BRASILEIRA

No geral, a versão da lei brasileira tem por base a lei Europeia(GDPR) que possui 11 capítulos e 99 artigos. Nossa norma ficou mais compacta e em alguns casos dá margem a interpretações subjetivas aumentando a insegurança jurídica. Ao todo, a lei é composta por 10 capítulos, organizados em 65 capítulos.

CAPÍTULO I - DISPOSIÇÕES PRELIMINARES(arts 1º ao 6º)

CAPÍTULO II - DO TRATAMENTO DE DADOS PESSOAIS(arts 7º ao 16), Seção I - Dos Requisitos para o Tratamento de Dados Pessoais; Seção II - Do Tratamento de Dados Pessoais Sensíveis; Seção III - Do Tratamento de Dados Pessoais de Crianças e de Adolescentes; Seção IV - Do Término do Tratamento de Dados

CAPÍTULO III - DOS DIREITOS DO TITULAR(arts 17 ao 22);

CAPÍTULO IV - DO TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO; Seção I - Das Regras; Seção II - Da Responsabilidade;

CAPÍTULO V - DA TRANSFERÊNCIA INTERNACIONAL DE DADOS;

CAPÍTULO VI - DOS AGENTES DE TRATAMENTO DE DADOS PESSOAIS; Seção I - Do Controlador e do Operador; Seção II - Do Encarregado pelo Tratamento de Dados Pessoais; Seção III - Da Responsabilidade e do Ressarcimento de Danos;

CAPÍTULO VII - DA SEGURANÇA E DAS BOAS PRÁTICAS; Seção I - Da Segurança e do Sigilo de Dados; Seção II - Das Boas Práticas e da Governança;

CAPÍTULO VIII - DA FISCALIZAÇÃO; Seção I - Das Sanções Administrativas;

CAPÍTULO IX - DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD) E DO CONSELHO NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS E

DA PRIVACIDADE; Seção I - Da Autoridade Nacional de Proteção de Dados (ANPD); Seção II - Do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade;

CAPÍTULO X - DISPOSIÇÕES FINAIS E TRANSITÓRIAS

3.2. PRINCÍPIOS DA LGPD

A LGPD é uma normativa que traz um rol de princípios em seu artigo 6º que tem a função de nortear o tratamento de dados pessoais. Tanto a Lei europeia como a brasileira possuem uma base principiológica forte para permitir uma proteção mais efetiva aos dados pessoais garantindo privacidade, inviolabilidade da intimidade, da honra e da imagem além de evitar ações que impactem o livre desenvolvimento da personalidade do ser humano, ao mesmo tempo em que tenta garantir que não haja descontinuidade do desenvolvimento econômico e dos avanços tecnológicos.

Os princípios definidos na LGPD facilitam a interpretação da norma, contribuem para garantir a sua eficácia e servem também para facilitar o entendimento dos titulares dos dados.

A nova lei possui uma lista 10 princípios que devem ser levados em consideração no tratamento de dados pessoais:

I. **Finalidade:** As empresas se tornaram verdadeiras acumuladoras de informações de seus clientes. Com a LGPD não será mais possível tratar dados pessoais sem que se tenha um fim específico, legítimo, explícito e informado. Para cada informação que for armazenada ou tratada é necessário que a organização possua uma justificativa lógica para a utilização desses dados. Um bom exemplo para ilustrar esse princípio seria as empresas que solicitam o e-mail de seus clientes para ser utilizado como login de algum aplicativo e passar a utilizá-lo para outro fim como o envio de informações com ofertas de produtos. Portanto, qualquer informação pessoal deve estar dentro dos limites da lei e não pode ter sua finalidade desviada do seu propósito originário sem ser devidamente comunicado ao titular dos dados.

II. **Adequação:** É necessário que exista uma harmonia entre a finalidade da atividade da empresa e o contexto da informação tratada. Por exemplo, poderíamos pensar em uma farmácia que comercializa medicamentos e solicitasse o nome e cpf da mãe do titular ou solicitasse informações como

orientação sexual. Ora, fica claro que as informações solicitadas não estão adequadas a situação exposta. Portanto, o tratamento de dados pessoais precisa estar dentro de um contexto adequado ao fim estabelecido.

III. **Necessidade:** As organizações devem se concentrar nas informações realmente essenciais aos seus negócios, ou seja, deve ser solicitado o mínimo de informações necessárias para atingir as finalidades definidas. Quanto mais informações forem solicitadas, maior se torna a responsabilidade da empresa e maiores as chances de penalidades.

IV. **Livre acesso:** O cidadão, titular dos dados, precisa de forma simples e gratuita ter acesso a todas as suas informações que estejam na posse da pessoa jurídica. Além disso, precisa também ser informado da duração e a quais tratamentos as suas informações serão submetidas.

V. **Qualidade dos dados:** Os titulares devem ter a garantia que seus dados são verdadeiros, íntegros e atualizados. Esse princípio precisa estar alinhado com a finalidade e necessidade definida para o tratamento dos dados.

VI. **Transparência:** Esse princípio é um dos mais importantes, inclusive servindo para calibrar as multas previstas na lei. A empresas precisam demonstrar transparência em todos os seus atos, repassando informações claras e precisas. Também dentro da lógica desse princípio, nenhuma ação de forma oculta pode ser realizada sem o consentimento dos titulares dos dados.

VII. **Segurança:** As empresas precisam se utilizar de meios jurídicos, administrativos e tecnológicos para evitar que de forma acidental ou ilícita haja a destruição, perda, alteração ou difusão dos dados pessoais de seus clientes. A lei exige que as melhores técnicas de segurança sejam adotadas em relação aos dados. Por considerar um princípio importante, a lei detalhou melhor nos artigos 46, 47, 48 e 49 o entendimento do que são as boas práticas para a segurança dos dados.

VIII. **Prevenção:** Um princípio que obriga as empresas a buscarem medidas de proteção aos dados antes que os danos ocorram.

IX. **Não Discriminação:** Dentre os dados pessoais existe um grupo ainda mais delicado que são os dados pessoais sensíveis que dizem respeito a orientação sexual e religiosa, origem racial, opiniões políticas, dentre outras. Em nenhuma hipótese esses dados podem promover algum tipo de discriminação ou abusos. Inclusive, esse tema vem sendo muito discutido por causa da utilização da inteligência artificial para decisões automatizadas.

X. **Responsabilização e Prestação de Contas:** As empresas precisarão demonstrar que estão seguindo as boas práticas de mercado para estarem aderentes a lei. Um bom exemplo disso é que as pessoas jurídicas possuam seus relatórios de Impacto à Proteção de Dados Pessoais que é uma ferramenta capaz de evidenciar a aderência à lei. Podemos destacar ainda que as empresas precisam elaborar uma Política de Segurança de Informação e terem um plano de respostas a incidentes.

3.3. BASES LEGAIS PARA TRATAMENTO DE DADOS PESSOAIS

A LGPD permite que o cidadão tenha um maior controle sobre suas informações pessoais, permitindo que ele seja o protagonista sobre o destino de suas informações. Uma norma de proteção de dados pessoais permite que sejam definidos padrões mínimos para o armazenamento e tratamento de um dado pessoal, passando a trazer um equilíbrio maior entre as empresas que utilizam os dados para viabilizar seus negócios e os verdadeiros proprietários das informações.

Após uma lei de proteção de dados, os controladores precisam de uma finalidade que justifique cada ação de tratamento das informações, assim como encontrar uma base legal que justifique os atos. Essa é uma das ações mais relevantes para dar segurança e respaldo jurídico as empresas quanto a possibilidade de processar informações pessoais. A lei brasileira trouxe um arcabouço ampliado que possui dez bases legais para fundamentar o tratamento dos dados. A princípio, não há hierarquia definida entre as hipóteses legais previstas na lei. Cada empresa precisa avaliar qual é a base legal mais interessante para cada situação específica, pois cada opção trará consigo um conjunto de direitos e obrigações. Apesar das empresas poderem escolher de uma forma estratégica qual base legal mais se adequa ao caso concreto, essa escolha precisa estar alinhada com os princípios

definidos na lei.

A LGPD em seu artigo 7º elenca o rol de dez hipóteses em que pode haver legalmente o tratamento de dados pessoais. A primeira base legal é também a mais conhecida busca pela obtenção do consentimento do titular, conforme o inciso I prevê, essa hipótese para ser válida, precisa ser acompanhada de algumas características como a manifestação livre, informada e inequívoca de forma a deixar clara a manifestação de vontade do titular que precisa ter ciência das finalidades específicas para as quais está fornecendo seus dados. Essa é a alternativa que possibilita uma maior autodeterminação informacional do indivíduo, pois permite que ele tenha mais autonomia e controle sobre o destino de suas informações. O § 4º do art. 8º da LGPD reforça a observância ao princípio da finalidade, pois aduz que “O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas. ”.

O consentimento fica vinculado ao controlador que solicitou e qualquer operação que implique no tratamento por outro controlador precisa passar por uma novo processo de consentimento, nos termos do § 5º do art. 7º da LGPD, segundo o qual “O controlador que obteve o consentimento referido no inciso I do caput deste artigo que necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei.”

Outro ponto de destaque em relação ao consentimento é o seu caráter temporário, ficando para o cidadão o direito de revogá-lo a qualquer tempo de forma simplificada. Por fim, podemos ressaltar que o consentimento precisará passar por um novo processo de autorização sempre que aspectos relacionados a finalidade, a forma e a duração do tratamento forem modificados, e ainda, quando for alterada a identificação do controlador.

A segunda hipótese prevista é a obrigação legal ou regulatória pois determinados dados pessoais são armazenados por força de lei ou de algum regulamento estabelecido pelas agências reguladoras e o governo. Um exemplo claro disso é que periodicamente as operadoras de planos de saúde ficam obrigadas a enviar dados de seus clientes para a Agência Nacional de Saúde(ANS), dentre essas informações estão o nome, cpf, data de nascimento, sexo e nome da mãe.

A próxima base legal foi criada para atender a necessidade da administração pública quanto a execução de Políticas Públicas. Ficaria inviável a ideia de

consentimento por toda a população para que o governo pudesse ter acesso a esse tipo de informação. Portanto, o tratamento de dados pessoais pelo Poder Público deve se orientar por meio dos princípios que direcionam a administração pública, acrescidos dos princípios incorporados na própria LGPD.

A quarta hipótese é para atender os estudos por órgãos de pesquisa, nesse caso específico, a Lei Geral de Proteção de Dados em seu artigo 5, XVIII traz a definição desse tipo de empresa[7]. Importante destacar que o tratamento de dados pessoais por essas instituições, sempre que possível, deverá trabalhar com a anonimização ou a pseudonimização das informações, de forma que não se possa mais relacionar as informações com o indivíduo proprietário dos dados.

A próxima possibilidade como base legal é a execução de um contrato ou procedimentos preliminares, nessa situação, o titular dos dados está relacionado a execução de um contrato e o acesso a algumas informações pessoais são necessárias. Poderíamos pensar em um aluguel de um carro em que os dados da habilitação do condutor são essenciais para que se possa satisfazer a obrigação contratual.

Uma outra hipótese é para possibilitar o exercício regular de direitos em processo judicial, administrativo ou arbitral, portanto, para o fim específico a que esses processos se propõe os dados pessoais podem ser utilizados. Em seguida temos a possibilidade de tratarmos dados pessoais para a proteção da vida ou da incolumidade física e para tutela da saúde, quando não for possível conseguir o consentimento dos titulares para esses casos previstos é possível tratar dados pessoais observando os princípios gerais da lei.

A nona hipótese prevista é o legítimo interesse e dentre as possibilidades é a mais polêmica e a que se deve tomar mais cuidado exatamente por causa da sua flexibilidade. Pode ser utilizada como uma alternativa quando não for encontrada uma outra base legal, entretanto, existem alguns limitadores para que essa opção possa ser empregada. Há necessidade de ser realizar um teste de proporcionalidade, avaliando se existe concretamente um interesse legítimo pelo controlador, se o tratamento dos dados está sendo realizado baseado no princípio da minimização dos

[7] Art. 5º, XVIII - órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico;

dados e também é importante garantir que não há violação de direitos e liberdades fundamentais do titular dos dados. Importante destacar, por fim, que essa base legal não poder ser fomentada para o tratamento de dados pessoais sensíveis.

A última base legal permite a proteção do crédito, ou seja, existe a possibilidade de se tratar dado pessoal em situações que busquem a prevenção à fraude e a proteção do crédito. Não seria possível excluir o cadastro de devedores de bases de dados como o Serasa e SPC, simplesmente porque não houve o consentimento dos titulares dos dados.

3.4. PRINCIPAIS ATORES DA PROTEÇÃO DE DADOS PESSOAIS: CONTROLADOR E OPERADOR

Dentre os atores especificados na Lei, temos dois que merecem destaques, o Controlador e o Operador. A Lei define o Controlador em seu artigo 5º, inciso VI, como: “pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;” No mesmo artigo e inciso, VII, define o Operador como: “pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;”. Portanto, conforme o artigo 39, o Operador fica limitado a realizar o tratamento dos dados de acordo com o que for solicitado pelo Controlador, pois é desse a responsabilidade pelo cumprimento da Lei Geral de Proteção de Dados.

Ambos devem manter, de acordo com o artigo 37, os registros das operações de tratamento que realizaram, especialmente nas situações em que o processamento se der pelo legítimo interesse do Controlador. O artigo 40 prevê que o Controlador é obrigado a fornecer o relatório de impacto[8] a Autoridade Nacional de Dados[9] sempre que for solicitado, além disso, tem o ônus da prova em demonstrar que o consentimento do titular foi obtido nos termos da lei.

3.5. RESPONSABILIDADES, RESSARCIMENTOS E SANÇÕES ADMINISTRATIVAS

[8] Artigo 5º, XVII, LGPD - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

[9] Artigo 5º, XIX, LGPD - autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

A LGPD dedicou dentro do capítulo “Dos Agentes de Tratamento de Dados Pessoais” uma seção específica para tratar da responsabilidade civil e do ressarcimento de danos. Mesmo o Código Civil regulando a Responsabilidade Civil em seus artigos 186 e 927, a norma de proteção de dados pessoais brasileira apresentou artigos específicos para tratar do tema. De acordo com o artigo 43, a categoria escolhida foi a Responsabilidade Civil Subjetiva.

A responsabilidade civil extracontratual subjetiva é composta por três características fundamentais: culpa, dano e nexo causal. A subjetividade se apoia na ideia de culpa, ou seja, é necessário a presença de um agente que tenha dado causa ao dano de forma dolosa ou culposa. Essa responsabilidade inicia com uma atividade danosa, prevista em lei, praticada por um autor que assume a obrigação de reparar seus atos ilegais. Quem causou o dano assume a responsabilidade de indenizar, entretanto, é possível atribuir responsabilidade civil há alguém por um dano que não foi causado diretamente por ele, mas que foi causado por um terceiro com quem mantinha relação, seria uma responsabilidade civil indireta.

O escritor DINIZ (2015, p.35) aduz que:

> “(...) a responsabilidade civil é a aplicação de medidas que obriguem uma pessoa a reparar o dano moral ou patrimonial causado a terceiros, em razão de ato por ela mesma praticado, por pessoa por quem ela responde, por alguma coisa a ela pertencente ou de simples imposição legal.”

Para CAVALIEIRI FILHO (2005, p.95), o dano pode ser definido como:

> (...) o grande vilão da responsabilidade civil. Não haveria que se falar em indenização, nem em ressarcimento, se não houvesse dano. Pode haver responsabilidade sem culpa, mas não pode haver responsabilidade sem dano. (...), o dano constitui o seu elemento preponderante. Tanto é assim que, sem dano, não haverá o que reparar, ainda que a conduta tenha sido culposa ou até dolosa.

Em seu artigo 42, a LGPD traz as características que definem a Responsabilidade Civil, não restando dúvida quanto a obrigação de reparar o dano que pode ser individual ou coletivo e deve ser em função da violação da norma de tratamento de dados pessoais. O inciso I classifica como sendo solidária a responsabilidade da relação entre Controlador e Operador, desde que esse

descumpra as obrigações da lei ou não cumpra com as instruções definidas pelo Controlador. O § 2º possibilita a inversão do ônus da prova em favor do titular dos dados. Sendo para o autor impossível ou muito difícil produzir a prova, é possível que o Juiz inverta o ônus da prova para que o réu a produza, desde que possa ser feito sem grandes dificuldades. Na nova Lei essa inversão pode acontecer quando a alegação for verossímil, quando houver hipossuficiência para fins de produção de prova ou ainda quando a produção da prova pelo titular for excessivamente onerosa.

O Artigo 43 prevê três hipóteses de excludente de ilicitude, ou seja, situações em que não existirá responsabilidade dos agentes de tratamento de dados. Sempre que não for realizado o tratamento de dados pessoais que lhes é atribuído, quando não houver violação à legislação de proteção de dados ou se o dano for decorrente de culpa exclusiva do titular dos dados ou de terceiros.

O art. 44 enumera as situações em que existirá a ilegalidade no tratamento de dados. Será passível de responsabilidade um agente que deixar de observar a legislação de proteção de dados ou quando não fornecer a segurança que o titular poderia dele esperar, levando em consideração o modo como o tratamento é realizado, o resultado e os riscos que razoavelmente dele se esperam e as técnicas de tratamento disponíveis à época.

Após definir os aspectos da responsabilidade civil a que os agentes de tratamento de dados estão sujeitos, a Lei enumera as sanções administrativas em caso de descumprimento da norma, são elas:

- advertência, com indicação de prazo para adoção de medidas corretivas;
- multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
- multa diária, observado o limite total anterior;
- publicização da infração;
- bloqueio dos dados pessoais a que se refere a infração até a sua regularização; e
- eliminação dos dados pessoais a que se refere a infração;
- Suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;

- suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;
- proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

A aplicação das sanções conforme o artigo 52, prevê que precisará existir um procedimento administrativo que possibilite a oportunidade da ampla defesa e avalie os critérios abaixo para calibração das penalidades:

- A gravidade e a natureza das infrações e dos direitos pessoais afetados;
- A boa-fé do infrator;
- A vantagem auferida ou pretendida pelo infrator;
- A condição econômica do infrator;
- A reincidência;
- O grau do dano;
- A cooperação do infrator;
- A adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados;
- A adoção de política de boas práticas e governança;
- A pronta adoção de medidas corretivas;
- A proporcionalidade entre a gravidade da falta e a intensidade da sanção

Percebe-se que as sanções são bem rigorosas, vão desde multas pecuniárias que podem chegar a 50 milhões de reais, a penalidades que podem impactar na imagem das empresas e suspender suas atividades.

4. O QUE FAZER PARA ADEQUAR UMA OPERADORA DE PLANO DE SAÚDE E SUAS UNIDADES HOSPITALARES A LGPD?

4.1. DESAFIOS DA ÁREA DA SAÚDE SUPLEMENTAR NA ADEQUAÇÃO A LGPD

Em setembro de 2019, as operadoras de saúde que formam o subsistema de saúde suplementar possuíam 47.095.095 de clientes[10], ou seja, atendem mais de 22% da população brasileira. Essa atividade econômica é controlada pelo setor privado e é extremamente regulada pela Agência Nacional de Saúde Suplementar (ANS). Esse sistema recebe o nome de suplementar porque além da obrigação da contribuição compulsória da seguridade social para ter acesso ao Sistema Única de Saúde (SUS), o contribuinte pode fazer o pagamento de um seguro privado.

A Agência Nacional de Saúde Suplementar é uma autarquia sob regime especial vinculada ao Ministério da Saúde, sendo responsável pela regulação, normatização e fiscalização das atividades das empresas que atuam na assistência suplementar à saúde. Tem a função de garantir a defesa do interesse público, regulando a relação entre as operadoras de planos de saúde e consumidores.

A regulamentação no setor foi iniciada com a Lei nº 9.656/98 e depois foi aprofundada com a Lei nº 9.961/00, responsável por criar a Agência Nacional de Saúde Suplementar. Esse segmento econômico é fortemente controlado através de um extenso regramento jurídico e normativo. O governo controla praticamente tudo, ou seja, desde a cobertura assistencial com a definição de um rol de procedimentos que precisam ser autorizados pelas empresas, até os reajustes anuais de preços que limita a possibilidade de repasse de custos para os consumidores. A intenção primária do governo no exercício desse controle é garantir que as operadoras e seguradoras do sistema de saúde suplementar atendam a população de forma eficiente e célere, evitando distorções no setor em relação a competitividade. Os dados da ANS mostram redução significativa do número de operadoras de planos de saúde em atividade no

[10]http://www.ans.gov.br/perfil-do-setor/dados-gerais

país, no ano 2000 eram 1456, atualmente são apenas 727[11], o que representa uma redução de cerca de 50%.

As Operadoras também sofrem ação regulatória da ANVISA, CADE e dos conselhos e associações como a AMB (Associação Médica Brasileira), a Abramge (Associação Brasileira de Medicina em Grupo), a Anahp (Associação Nacional de Hospitais Privados), a Abraidi (Associação Brasileira de Importadores e Distribuidores de Implantes), Abimed (Associação Brasileira da Indústria de Alta Tecnologia de Produtos de Saúde) e a Abradilan (Associação Brasileira de Distribuição e Logística de Produtos Farmacêuticos). Além disso, o Poder Judiciário vem impactando o setor profundamente com decisões que passam a definir novas regras.

A LGPD aumentará ainda mais o poder regulatório do Estado na área da saúde suplementar, na medida em que os dados de saúde são as informações mais sensíveis dos cidadãos. Além de dados pessoais como nome, CPF, nome da mãe, data de nascimento, endereço, as operadoras de planos de saúde possuem muitas informações sensíveis como prontuários eletrônicos, declarações de saúde, resultados de exames, patologias psicológicas, dados biométricos e genéticos. Facilmente identifica-se que esse tipo de dado tem a capacidade de manipular determinadas circunstâncias da vida de seus proprietários.

A atividade das operadoras de saúde e suas unidades de atendimento, pela natureza da prestação do serviço, exige que ocorra o tratamento de dados pessoais e ainda mais, que exista a troca dessas informações para outras operadoras, corretoras, administradoras de benefício, prestadores de serviços médicos e para o próprio órgão regulador. A troca de informações entre os diversos atores envolvidos na contraprestação dos serviços médicos é essencial para que se preste um atendimento com qualidade e eficiência. Será necessário, portanto, que seja realizado o trabalho cuidadoso de se encontrar o devido fundamento legal dentro da LGPD que autorize a manipulação, guarda e tratamento desses dados pessoais de milhões de brasileiros.

A ANS já vem atuando nesse tema e atualmente já existem mais de vinte resoluções normativas que disciplinam o trânsito de dados entre as operadoras e a agência reguladora. Além disso, os conselhos também emitem regulamentos sobre o tema, a exemplo do Conselho Federal de Medicina que publicou a Resolução n. 1.605,

[11] http://www.ans.gov.br/perfil-do-setor/dados-gerais

de 31/12/2009 que trata das regras sobre revelação de ficha ou prontuário médico e a Resolução n. 1.821, de 23/11/2007 que dispõe sobre o prontuário médico eletrônico. Mais recentemente tivemos a publicação da Lei nº 13.787 de 27/12/2018 que dispõe sobre a digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente.

Uma das funções da LGPD é centralizar o arcabouço jurídico quanto à proteção de dados pessoais e será necessário um processo de adequação das legislações esparsas que de alguma forma já regulam sobre o tema. Uma peça importante nesse cenário será a Autoridade Nacional de Dados (ANPD), criada pela Medida Provisória 869/2018 e instituída como órgão da Administração Pública Direta, integrante da Presidência da República, que deverá dar um direcionamento sobre as omissões e interpretações da LGPD, além de estabelecer normas e diretrizes que permitam mais facilmente a sua implementação, garantindo a efetividade da aplicação da lei. Provavelmente, esse órgão, em um futuro próximo, deverá junto com a ANS passar por um processo de integração e harmonização das normas vigentes garantindo que as operadoras de serviços médicos possam se adequar, em especial, nos pontos controversos da lei.

A entrada em vigor da LGPD trará impactos para a ANS e para todo o setor que precisará repensar a forma de transacionar dados pessoais para se adequar as exigências e princípios da lei.

4.2. SENSIBILIZAÇÃO, FORMAÇÃO DO COMITÊ DA LGPD E AVALIAÇÃO E DIAGNÓSTICO DE MATURIDADE

O início da jornada em busca da adequação à LGPD foi a sensibilização da alta administração e das principais lideranças da empresa. O processo foi realizado pela área de Tecnologia da Informação e pelo setor Jurídico. A ideia foi mostrar os principais conceitos da lei, os prazos e os riscos em relações as sanções. Em seguida foi montado o comitê da LGPD composto por representantes das principais áreas da organização. Foram selecionadas para participar as áreas de Gestão de Pessoas, Tecnologia da Informação, Financeiro, Marketing, Comercial, Jurídico, Relacionamento com o cliente, Compliance e Controles internos, Planejamento Estratégico, Ouvidoria, Enfermagem e Contabilidade. Foi elaborado um documento formal que foi assinado pelos representantes.

As principais atividades desse comitê são:

- Realizar a manutenção do engajamento e conscientização das partes interessadas;
- Manter todas as áreas cientes das principais ações na proteção de dados pessoais;
- Avaliar e opinar em novos projetos que envolvam tratamento de dados pessoais;
- Acompanhar o projeto de adequação a Lei Geral de Proteção de Dados Pessoais;
- Realizar ações contínuas de conscientização para colaboradores e médicos cooperados sobre a importância do tema.

Em seguida foi feito um levantamento minucioso em cada uma dessas áreas em relação à Lei Geral de Proteção de Dados e a maturidade em relação à Segurança da Informação.

As principais atividades dessa etapa foram:

- Reunião prévia para apresentação e definição de critérios;
- Aplicação do questionário de avaliação do nível de conformidade;
- Compilação dos resultados;
- Elaboração dos relatórios.

Foi aplicado um questionário com mais de cem perguntas para cerca de cinco funcionários em cada setor participante do comitê de LGPD. Foram abordados temas em relação ao envolvimento da alta gestão no cumprimento da lei, a existência de normas internas e regulamento sobre o tema de proteção de dados pessoas, o nível de maturidade em segurança da informação, aspectos relacionados a capacitação dos colaboradores no tema, o envolvimento da empresa nos últimos cinco anos em incidentes, vazamentos, fraudes, furtos e ações judiciais relacionados a proteção de dados pessoais, o uso de tecnologias que evitem o vazamento de informações, a existência de mapeamento de dados pessoas, dentro outras questionamentos que possibilitam a extração da maturidade da empresa e de seus colaborados sobre a proteção de dados pessoais. Esse questionário gerou um relatório com uma pontuação sobre cada uma das áreas abordadas

4.3. MAPEAMENTO DE DADOS

O processo de mapeamento de dados é uma das etapas mais importantes para ficar em *compliance* com a LGPD, também é uma das atividades mais trabalhosas do processo de adequação a lei. Não é possível proteger adequadamente os dados quando não se conhece quais informações pessoais estão sendo coletadas, quais processos realizam o tratamento desses dados e com quem são compartilhados.

Com o mapeamento, toda a empresa passa a ter uma visão mais objetiva e clara sobre todos os processos que realizam tratamento de dados pessoais. No inventário dos dados é necessário que aconteça uma categorização, informando se são sensíveis, se estão anonimizados ou se são informações de menores de idade. Além disso, é necessário identificar quais sistemas e ferramentas de informação tratam os dados, qual a finalidade, se existe previsão de transferência internacional e onde e por quanto tempo serão mantidos. Também é importante mapear os atores do tratamento de dados, levantando quem é o titular do dado e quem são os controladores e operadores.

O Mapeamento de dados, portanto, tem a função de auxiliar a empresa a entender se as informações coletadas são realmente importantes para atingir os objetivos da organização e se esse tratamento está coerente com os princípios da LGPD, como por exemplo, finalidade, adequação e necessidade.

Esse processo foi delegado para todas as equipes e setores da empresa. Para que o trabalho acontecesse de forma mais efetiva, foi realizado um treinamento com os responsáveis pela atividade. A ferramenta utilizada foi uma planilha excel pré-formatada com todas as colunas que deveriam ser preenchidas.

As informações solicitadas foram: o nome do processo, o nome do sistema que gerencia as informações, quais dados pessoais e sensíveis são tratados, a forma de coleta, a finalidade, a base legal que justifica o tratamento, quem é o titular dos dados e os agentes de tratamento, quem são os responsáveis pelo processo, o local de armazenamento dos dados, o volume de dados, a forma de proteção, a periodicidade e o local de *backup*, o tempo de armazenagem dos dados, se existe log das transações, as permissões acesso, o período de retenção das informações, a forma de exclusão dos dados, se existe transferência ou compartilhamento dos dados e o método de transferência.

As principais vantagens desse trabalho foram:

- Avaliar a importância dos processos de tratamento de dados pessoais para a empresa;

- Verificar se essas informações estão sendo tratadas dentro dos princípios da LGPD;
- Mapear o ciclo de vida das informações;
- Identificar os dados mais sensíveis;
- Fornecer o subsídio necessário para a etapa de mapeamento de riscos;
- Avaliação das bases legais que justificam o tratamento dos dados.

Por fim, o mapeamento de dados além de servir de base para o levantamento das ações necessárias a adequação da nova Lei, servirá também de guia para que o Encarregado de Dados faça uso durante ações reclamatórias, auditorias e fiscalizações.

4.4. AVALIAÇÃO DE SEGURANÇA DA INFORMAÇÃO (SECURITY ASSESSMENT)

Cerca de US$ 8 trilhões são gastos devidos a crimes cibernéticos em todo o mundo, de acordo com informações trazias pelo Global Risk Report 2018[12] elaborado pelo Fórum Econômico Mundial. Os ataques cibernéticos, em especial, têm a função de violar o acesso às informações privadas para de alguma forma obter vantagens financeiras. Com o permanente aumento desses ataques, as empresas precisam continuamente investir em segurança digital, prevenindo os riscos de vazamento de informações.

A LGPD traz em seu artigo 46 e 47 que é necessário tomar medidas preventivas e efetivas que garantam a redução dos riscos de acesso indevido aos dados pessoais.

> Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.
> § 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.

[12] http://www3.weforum.org/docs/WEF_GRR18_Report.pdf

> § 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.
> Art. 47. Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término.

Nenhum ambiente tecnológico está completamente livre de ameaças. O processo de *Security Assesment* propõe uma auditoria de segurança da informação em sistemas, aplicações, banco de dados e redes de computadores, buscando descobrir vulnerabilidades, explorar fraquezas e mensurar os riscos no ambiente tecnológico. A importância desse processo é exatamente realizar um mapeamento de todas as ameaças e montar um plano de ação para minimizá-las.

Como nem sempre é possível se livrar de todas as fragilidades mapeadas seja por limitações técnicas ou orçamentárias, é importante que essas ameaças sejam classificadas de acordo com a probabilidade de ocorrer e impacto ao negócio da empresa para que se possa priorizar as ações.

A principal atividade dessa fase é o teste de penetração (*Penetration testing, Pentest*) que consiste em simular tentativas de invasão e ataques cibernéticos de forma controlada para avaliar a segurança dos sistemas de computadores. O *Pentest* vai avaliar o grau de facilidade ou dificuldade de se invadir um sistema e conseguir acesso indevido as informações.

Para o trabalho em questão foi contratada uma empresa especializada que avaliou vários ativos de tecnologia da informação por cerca de 30 dias. Foi feito um mapeamento dos riscos atuais dos data centers[13], servidores, computadores, sistemas e equipamentos da rede de computadores.

Foram analisados os ativos abaixo:

- Acesso físico e segurança dos data centers;
- Conectividade (Redes de Acesso e Wifi);
- Firewall;
- Antivírus;
- AntiSpam;

[13] Data Center é um ambiente projetado para abrigar servidores, sistemas de armazenamento de dados e ativos de rede(*switches*, roteadores). É o local onde ficam armazenados todos os sistemas e dados de uma empresa. O objetivo principal de um Data Center é garantir a disponibilidade de equipamentos que rodam sistemas cruciais para o negócio de uma organização.

- Servidores de arquivos;
- Servidor de email;
- Servidores de aplicação;
- Banco de Dados;
- Backups;
- Site institucional
- Aplicações disponíveis na internet.

O produto final dessa auditoria foi um relatório contendo a metodologia, as atividades utilizadas com toda a coleta de evidências, o mapeamento da análise de vulnerabilidades devidamente categorizadas pelo grau de criticidade e a identificação das ações para mitigação das falhas. Além disso, foi simulado um Phishing Scan[14] para identificar a maturidade dos colaboradores em relação a esse tipo de ataque.

4.5. DEFINIÇÃO DO ENCARREGADO DEPROTEÇÃO DE DADOS (DPO)

A Lei Geral de Privacidade de Dados permitiu o surgimento de um novo profissional, o Encarregado de Dados ou *Data Protection Officer* (DPO). O artigo 5º, inciso VIII traz o conceito do cargo: “encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)”. O Encarregado de dados poderá ser uma pessoa física ou jurídica.

O texto da LGPD traz que o DPO deverá:

- Adotar providências e prestar esclarecimentos sobre o tratamento dos dados, tanto para a ANPD quanto para os titulares dos dados, servindo de um canal de comunicação entre os atores envolvidos no processo. Os dados de contato do Encarregado deverão ser divulgados publicamente, preferencialmente no website da empresa;
- Capacitação e orientação sobre privacidade e proteção de dados para todos os funcionários da empresa;

[14] Phising scam é uma técnica utilizada para tentar obter informações pessoais como logins, senhas, informações bancárias, número de cartão de crédito. Os fraudadores enviam milhares de e-mails e tentam levar os usuários a sites que aparentemente parecem ser oficiais mas na verdde apenas tem a função de coletar essas informações.

- Monitorar a conformidade da lei, avaliando processos e documentações;

De acordo com o § 3º do artigo 41, a autoridade nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, definido também sobre em quais hipóteses não será necessário à sua presença levando em consideração as características da organização, como o porte e volume de tratamento de dados.

Para exercer suas funções, esse profissional deverá antes de tudo ser encaixado no organograma da empresa de forma que ele possa ter autonomia e independência para acompanhar e auditar todo o fluxo de informações pessoais, ou seja, do momento em que surge a necessidade de coleta de um dado pessoal até o seu processo de descarte. Deve se reportar ao mais alto nível da empresa não podendo ser punido no exercício de sua função, além de não executar outras responsabilidades que possam causar conflito de interesses com o seu papel.

É recomendável que esse especialista tenha uma formação interdisciplinar, com conhecimentos em segurança da informação, governança, compliance e leis. Precisa conhecer os processos de negócio, sistemas de informação e ter habilidades em comunicação, pois além de se relacionar internamente com toda a companhia precisará ser o interlocutor entre titulares de dados e a ANPD.

Uma pesquisa realizada pela IAPP(*International Association of Privacy Professionals*) nos EUA, Canada e Europa demonstra que o maior percentual de DPO's está alocado no setor jurídico das organizações.

Figura 2 – Formação dos profissionais que estão assumindo o cargo de DPO.
Fonte: www.opiceblum.com.br

Um ponto importante de destaque é que a LGPD não especifica as

responsabilidades jurídicas do Encarregado de Dados, talvez por ele ter um papel principalmente consultivo e preventivo, pois, em geral, não é dele a decisão sobre o tratamento dos dados. A princípio, as obrigações recaem sobre controladores e operadores que, de fato, são quem realizam os tratamentos das informações pessoais. Entretanto, é possível imaginar uma possível responsabilidade subjetiva do DPO por dano ocasionado à organização ou ao titular se comprovado o dolo ou culpa e o nexo causal.

O processo de seleção do DPO na empresa seguirá a ideia acima, ou seja, será selecionado um profissional que reúna boa parte das características que um DPO precisa como conhecimentos jurídicos e em segurança da informação, além de conhecimento nos negócios da empresa.

4.6. AVALIAÇÃO DE RISCOS (RISK ASSESSMENT)

O processo de avaliação de riscos é essencial pois ajudará no processo de assimilar os riscos regulatórios existentes no tratamento de dados pessoais. Com essa ferramenta é possível estabelecer prioridades e planejar as ações mais urgentes. Essa análise deve ser construída sobre o prisma do titular dos dados.

Superado o processo de conhecer melhor a empresa nas etapas anteriores de avaliação e diagnóstico de maturidade, avaliação dos riscos de segurança da informação e o mapeamento de dados é chegada a hora de realizar uma avaliação dos riscos em relação a LGPD.

Para Cicco e Fantazzini(2003), um risco se manifesta como uma incerteza quanto à ocorrência de um determinado evento indesejado e também a probabilidade de perda que uma empresa pode sofrer em consequência de um ou de vários eventos indesejados. Na área de tecnologia da informação, um risco é um impacto negativo, uma origem de possíveis perdas derivadas da exploração de uma vulnerabilidade. (STONEBURNER, GOGUEN, FERINGA, 2002).

De acordo com o PMBOK (2004), risco é um evento ou condição incerta que se ocorrer trará efeitos positivo ou negativo para um projeto. O gerenciamento desses riscos tem a função de aumentar a probabilidade e o impacto de eventos positivos e reduzir a probabilidade e o impacto de eventos negativos.

Uma ameaça é uma fonte que irá explorar as vulnerabilidades podendo causar danos. Vulnerabilidades são falhas nos processos de segurança, nos projetos ou nos

controles internos de um sistema, que, se explorados, podem ocasionar danos(STONEBURNER, GOGUEN e FERINGA, 2002). Para essas vulnerabilidades apresentarem riscos precisa existir a possibilidade de serem exploradas. Daí a importância no processo de mapeamento dos riscos.

Nessa atividade serão inicialmente identificados e documentados todos os eventos, as ameaças e as causas dos riscos. Identificado os riscos é necessária uma etapa de avaliação das probabilidades e impactos. Um dos objetivos também dessa fase é a elaboração do Relatório de Impacto que é a versão brasileira do *Data Protection Impact Assessment* – DPIA, previsto na Lei de Proteção de Dados Europeia(GPDR).

A LGPD em dois momentos faz referência a necessidade de empresas privadas gerarem os seus relatórios de impactos:

> Art 10, § 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.
> Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.

O Relatório de Impacto é um documento que deverá ser elaborado pelo controlador para identificar, analisar e mitigar os riscos de incidentes às liberdades civis e aos direitos fundamentais dos titulares**.** Esse relatório tem também a função de mostrar a viabilidade do tratamento dos dados pessoais. Sempre que houver um incidente com esse tipo de informação, a Agência Nacional de Dados poderá solicitar o relatório de impacto. Importante relembrar que as sanções passarão sempre por um processo para calibração das penalidades, portanto, ter esse documento estruturado e robusto demostra cuidado e boa-fé da empresa com os dados de seus clientes.

Na empresa que foi objeto de estudo, as seguintes atividades foram realizadas no processo de *Risk Assessment*:

• Definição dos riscos legais relacionados à proteção de dados;

• Definição dos critérios de classificação de riscos (fator, impacto, probabilidades, áreas);

• Identificação e classificação de riscos inerentes, avaliação de controles, definição de riscos residuais e mapa de calor, através da realização de entrevistas

com os responsáveis de cada setor;

• Definição das estratégias de mitigação de riscos;

• Elaboração do relatório de riscos.

4.7. POLÍTICA DE PROTEÇÃO DE DADOS E CONFORMIDADE DOCUMENTAL

A companhia atualmente já possui um grande volume de normas internas, entretanto, todas elas precisarão passar por um processo de revisão no sentido de se adequarem à Lei Geral de Proteção de Dados. Por se tratar de uma cooperativa médica, além dos dados de seus cooperados, são tratadas informações de colaboradores e clientes.

A base desse processo é a criação de uma política de privacidade e proteção de dados. Esse documento vai conter um programa global dentro da operadora de plano de saúde e suas unidades hospitalares para garantir que todo o tratamento de dados pessoais sigam rigorosos padrões de segurança. Essa política deverá ser cumprida por todos os colaboradores e prestadores de serviços.

Abaixo segue todos documentos que passarão pelo processo de revisão ou criação:

- Elaboração da política de privacidade e proteção de dados;
- Revisão da Política de Segurança da Informação;
- Criação das Minutas dos termos de Uso e da Política de Privacidade do Site;
- Redação de cláusulas contratuais relacionadas à privacidade e proteção de dados para clientes e fornecedores;
- Identificação dos processos para os quais é necessário o consentimento;
- Elaboração dos termos de consentimento;
- Revisão das políticas de backup de dados;
- Criação de um processo de resposta a incidentes.

4.8. CULTURA DE PROTEÇÃO DE DADOS E O MODELO "*PRIVACY BY DESIGN*"

Uma das etapas importantes do programa de adequação LGPD é a implantação de uma cultura de proteção de dados pessoais dentro da organização. A empresa possui cerca de dois mil colaboradores e mil e setecentos cooperados.

Capacitar e sensibilizar todo esse contingente humano para cuidar dos dados de terceiros é um dos grandes desafios do projeto. Foi montado uma grande estrutura de capacitação e divulgação do tema. Em cada setor foi eleito um embaixador de proteção de dados para atuar dentro de suas áreas orientando e vigiando o cumprimento da política de privacidade e proteção de dados.

Foi definido também um plano de comunicação para garantir que todos os atores fossem comunicados de forma clara e eficiente. Para se ter o resultado esperado, primeiro foi definido o objetivo do plano que era elevar o nível de maturidade da organização em privacidade e proteção de dados pessoais, em seguido o público alvo foi definido e segmentado. Além disso, foram definidos os canais de mídia adequado para obtenção dos melhores resultados, um cronograma para implementação de todas as ações, uma metodologia para monitoramento e avaliação dos resultados.

Dentro desse processo de mudança cultural, surge a metodologia *Privacy By Design* (PbD) que prevê a implantação da proteção de dados desde o início do desenho do novos produtos ou execução de novos projetos que envolvam tratamento de dados pessoais. No regulamento brasileiro os princípios da PbD podem ser observados no artigo 46:

> Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.
> §2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou serviço até a sua execução.

O cuidado com os dados pessoais deve percorrer todo o ciclo de vida dos novos produtos e processos, partindo da coleta, passando pelo tratamento e acabando com o descarte dos dados. Toda a solução será desenhada por padrão seguindo os princípios da proteção de dados pessoais. Esse método preza pelo respeito a privacidade do titular dos dados, ou seja, o objeto central sempre que envolver dado pessoal é o proprietário das informações e a privacidade deve guiar as ações do controlador dos dados.

Por padrão, deve ser incorporado o princípio da minimização de dados. A proteção aos dados deixa de ser um processo apenas do setor de *compliance* e passar a fazer parte do próprio negócio, a empresa passa a ter um comportamento preventivo e não mais reativo.

Portanto, implantar a metodologia de PbD na concepção de novos projetos é incorporar uma nova cultura na empresa que passa a repensar na forma de criar novos serviços e produtos de forma a privilegiar a proteção da privacidade sem atrapalhar o desenvolvimento econômico.

A seleção de um comitê de LGPD composto por gestores de várias áreas da empresa e de um DPO que conhece bem o negócio da empresa e os processos de negócio servirá para que mais facilmente a metodologia *privacy by design* seja incorporada em toda a organização.

5. CONCLUSÃO

O estudo realizado para a elaboração do presente trabalho, passou por uma extensa análise bibliográfica de livros, legislações, artigos, matérias jornalísticas, além da participação em palestras e cursos sobre o tema da privacidade e proteção de dados pessoais que passou a ter grande relevância no meio jurídico, em especial, após a publicação da Lei 13.709 em agosto de 2018 com entrada em vigência para agosto de 2020.

O trabalho abarcou no primeiro capítulo a problemática dos dados pessoais após a popularização da internet e a nova dinâmica das relações sociais e comerciais com o surgimento de tecnologias disruptivas que vem promovendo grandes mudanças dentro de uma sociedade da informação em que o elemento central para o desenvolvimento econômico é a capacidade de extrair conhecimento do grande volume de dados disponíveis. De um lado temos os consumidores que desconhecem os seus direitos e os riscos de fornecerem seus dados pessoais dentro desse ambiente digital, associado a uma exposição excessiva de suas vidas íntimas na rede. Do outro lado temos as empresas e governos que se tornaram verdadeiros acumuladores de dados pessoais e com o uso de algoritmos e da inteligência artificial passam a controlar as pessoas dentro de uma bolha de consumo, promovendo uma exploração publicitária sem limites na história e praticando uma série de abusos e violações que atacam a dignidade da pessoa humana e ferem os direitos da personalidade dos cidadãos.

Esse processo de revolução tecnológica gerou mudanças no mundo jurídico no sentido de procurar alternativas para garantir a tutela desses bens jurídicos tão caros a sociedade e de elevar a proteção de dados pessoais a categoria de um direito autônomo e fundamental. Diante disso, muitos países estão estabelecendo uma série de leis e regulamentos para dar maior garantia em relação a privacidade dos dados pessoais. O Brasil está implementando um novo marco regulatório com a sanção da Lei Geral de Proteção de Dados (LGPD) e vem exigindo uma grande adequação das empresas brasileiras quanto a cultura da proteção de dados pessoais. O segundo capítulo, fez uma análise histórica desse tipo de regulamento no país até o surgimento de uma lei específica que passou de forma mais clara a defender e tutelar os direitos dos titulares de dados pessoais. O trabalho procurou esmiuçar os principais aspectos da LGPD, avaliando, principalmente, a sua estrutura principiológica que veio nortear

a coleta, o uso e a guarda dos dados pessoais, as bases legais que permitem as empresas realizarem o tratamento de dados pessoais e as responsabilidades e sanções administrativas quando houver violação da lei.

A norma brasileira de proteção de dados buscou centralizar em seu código várias outras leis esparsas que existiam sobre o tema buscado garantir que as empresas respeitem as expectativas dos titulares dos dados quando ao fluxo informacional de seus dados pessoais. Entretanto, a aplicação da lei para garantir a autodeterminação informativa dos indivíduos, ou seja, para evitar que o interesse econômico afete o desenvolvimento da personalidade do ser humano pelo uso abusivo de dados pessoais em muito dependerá da atuação fiscalizatória e de novos regulamentos que surgirão através da Agência Nacional de Dados.

Para finalizar o trabalho, o terceiro capítulo explorou, de forma prática, o processo de adequação à Lei Geral de Proteção de Dados dentro de uma Operadora de Plano de Saúde e de suas unidades hospitalares. A implementação da lei dentro desse ambiente de prestação de serviços de saúde se torna ainda mais complexo e desafiador pelo grande volume de dados sensíveis que trafegam por inúmeros processos da organização.

A LGPD estabelece critérios ainda mais rígidos para dados sensíveis, exigindo que estejam rigorosamente alinhados aos princípios da lei e com os benefícios esperados aos titulares dos dados. O novo regulamento representa uma mudança cultural de responsabilidade em relação aos dados pessoais dos clientes.

A empresa estudada vem passando por um longo processo de implementação de uma cultura da integridade digital. Assim como em várias outras empresas, a LGPD passará por um período de amadurecimento e terá uma curva de aprendizagem para sua adequada interpretação.

Garantir a segurança dos dados de saúde de seus clientes, não é necessariamente algo novo e em um ambiente já extremamente regulado pela Agência Nacional de Saúde, entretanto, a Lei Geral de Proteção de Dados traz novos aspectos e torna o processo mais rígido, com previsões de multas milionárias e maiores impactos a marca em caso de vazamento de informações.

De forma geral, a atividade inicial para adequação da empresa foi sensibilizar a alta administração sobre a importância do tema, mostrando os principais aspectos da lei e os riscos de não estar de acordo com a LGPD. Em seguida foi realizado um inventário de todos os processos e fonte de dados que coletam, tratam e armazenam

dados pessoais. Esse mapeamento foi a base de todo o trabalho que se seguiu, pois a partir dele é possível verificar se cada um dos processos de tratamento de dados pessoais é realmente necessário para a empresa e se estão de acordo com os princípios e bases legais previstos pela lei.

Além da empresa investir na capacitação de vários colaboradores sobre o tema, será necessário a nomeação de um Encarregado de Dados(DPO), cargo que precisará de conhecimentos multidisciplinares e independência para atuar na proteção de dados pessoais e na interlocução com a Autoridade Nacional de Dados e titulares de dados.

A etapa seguinte foi avaliar toda a infraestrutura de tecnologia da informação e uma avaliação dos riscos para detectar as principais vulnerabilidades da empresa em relação a proteção da privacidade e dos dados pessoais dos clientes. Essas atividades se desdobraram em várias ações como a revisão das políticas de segurança da informação, backup de dados e controle de acesso. Além disso, foram necessários investimentos em infraestrutura tecnológica, segurança da informação e criptografia de dados.

Em seguida foi realizado a criação de uma política de privacidade e uma revisão documental para garantir que contratos e termos de consentimentos estejam de acordo com a LGPD.

Por fim, serão implementadas ações de longo prazo para criação de uma cultura de proteção de dados pessoais com ações capazes de sensibilizar e orientar todos os setores, colaboradores e cooperados. A organização seguirá com a implantação de uma modelo de governança de dados que se adeque a realidade operacional de suas atividades.

A experiência com a implantação do novo regulamento mostrou que as empresas brasileiras precisam iniciar o quanto antes seus processos de adequação a lei 13.709/2018, sendo necessários vários meses de trabalho e consideráveis investimentos em segurança da informação, capacitação de pessoas e consultoria jurídica.

REFERÊNCIAS

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: Linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

PINHEIRO, Patrícia Peck. **Proteção de Dados Pessoais:** Comentários à Lei N. 13.709/2018. São Paulo: Saraiva Jur, 2018. 118 p.

NAVARRO, Ana Maria Neves de Paiva. **O direito fundamental à autodeterminação informativa**. Departamento de Pós-Graduação UFRJ, LETACI. Rio de Janeiro, 2011.

MENDES, Laura Schertel. **Transparência e privacidade: violação e proteção da informação pessoal na sociedade de consumo**. Departamento de Pós-Graduação Unb. Brasília, 2008.

Guidelines on the Protection of Privacy and Transzborder Flows of Personal Data, disponível em: www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html

PARISER, Eli. **O filtro invisível:** o que a internet está escondendo de você. Rio de Janeiro: Zahar, 2012.

CASTELLS, Manuel. **A galáxia da internet.** Rio de Janeiro: Jorge Zahar Ed., 2003.

SOUZA, Sérgio Iglesias Nunes de. **Responsabilidade civil por danos à personalidade**. Barueri, SP: Manole, 2002. p. 01.

CASTELLS, M. A. **Sociedade em Rede – a era da informação: economia, sociedade e cultura**. Vol. 1. 5 ed. São Paulo: Paz e Terra, 1996.

CARVALHO, Luiz et al. Desafios de Transparência pela Lei Geral de Proteção de Dados Pessoais. In: **Anais do VII Workshop de Transparência em Sistemas**. SBC, 2019. p. 21-30.

BAUMAN, Zygmunt; LYON, David. **Vigilância Líquida.** Rio de Janeiro: Zahar, 2014

DINIZ, Maria Helena. **Curso de Direito Civil Brasileiro: Responsabilidade Civil**. Vol.7. 29ª. ed. São Paulo: Saraiva, 2015.

DE CICCO, F.; FANTAZZINI, M. L. **Tecnologias consagradas de gestão de riscos: riscos e probabilidades**. São Paulo: Séries Risk Management, 2003.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados(LGPD)**. Diário Oficial da União: seção 1, Brasília, DF, p. 59, 15 ago. 2018.

STONEBURNER, G.; GOGUEN, A.; FERINGA, A. **Risk Management Guide for Information Technology Systems**. Gaithersburg: NIST – National Institute of Standards and Technology, 2002. 54p. (Special Publication 800-30). Disponível em:

https://csrc.nist.gov/publications/detail/sp/800-30/archive/2002-07-01. Acesso em: 10 jan. 2020.

Manyika, James; Chui, Michael; Brown, Brad; Bughin, Jacques; Dobbs, Richard; Roxburgh, Charles & Byers, Angela Hung. (2011). **Big data: The Next Frontier For Innovation, Competition, And Productivity**. McKinsey Global Institute. Disponível em: http://www.mckinsey.com/insights/business_technology/big_data_the_next_frontier_for_innovation. Acesso em: 13 de dez. 2029

CAVALIERI FILHO, Sérgio. **Programa de responsabilidade civil**. 10ª. ed. São Paulo: Atlas, 2012.

PIETROBON, Louise; PRADO, Martha Lenise do; CAETANO, João Carlos. **Saúde suplementar no Brasil: o papel da Agência Nacional de Saúde Suplementar na regulação do setor**. 2008. Disponível em: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0103-73312008000400009 Acesso em: 01 fev. 2020.

DUARTE, M.C.R. **A assistência suplementar no Brasil: história e características da cooperativa de trabalho Unimed** In: NEGRI, B.; GIOVANNI, G. Brasil: radiografia da saúde. Campinas: Unicamp, 2001. p. 363–393.

BRASIL. Lei nº 9.656. Dispõe sobre os Planos de Assistência à Saúde. Brasília, 1998.

BRASIL. Lei n.º 9.961/2000. Dispõe sobre a criação da ANS. Brasília, 2000(a).

ABNT NBR ISO/IEC 27001:2006: Tecnologia da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos.

ABNT. NBR ISO/IEC 27002:2005: Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação.

DALLARI, Analluza Bolivar. **Impactos da LGPD na saúde suplementar e a aprovação de parecer sobre MP 869/2018.** 2019. Disponível em: <https://www.conjur.com.br/2019-mai-07/analluza-dallari-impactos-lgpd-saude-suplementar>. Acesso em: 20 dez. 2019.

Especialistas esclarecem impactos da LGPD na saúde. 2019. Disponível em: <https://portaltelemedicina.com.br/blog/especialistas-esclarecem-impactos-da-lgpd-na-saude>. Acesso em: 02 fev. 2020.

_____, José Carlos. **Governança eletrônica: para onde é possível caminhar?** Disponível em: <http://www.polis.org.br/uploads/745/745.pdf>. Acesso em: 16 dez. 2019.

PMI. **Um Guia do Conhecimento em Gerenciamento de Projetos**. Guia PMBOK®. Quarta Edição – EUA: Project Management Institute, 2008.