UNIVERSIDADE FEDERAL DE SANTA CATARINA
CAMPUS ARARANGUÁ
CURSO DE TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO

MAYCON ANTÔNIO DANIEL

A EVOLUÇÃO E APLICAÇÃO DA SEGURANÇA DA INFORMAÇÃO POR MEIO DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD): UM ESTUDO DE CASO EM UMA INSTITUIÇÃO FINANCEIRA

ARARANGUÁ
2022

MAYCON ANTÔNIO DANIEL

A EVOLUÇÃO E APLICAÇÃO DA SEGURANÇA DA INFORMAÇÃO POR MEIO DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD): UM ESTUDO DE CASO EM UMA INSTITUIÇÃO FINANCEIRA

Trabalho Conclusão do Curso de Graduação em Tecnologias da Informação e Comunicação da Universidade Federal de Santa Catarina como requisito para a obtenção do título de Bacharel em Tecnologias da Informação e Comunicação.
Orientador: Prof. Dr. Giovani Mendonça Lunardi

ARARANGUÁ

2022

Ficha de identificação da obra elaborada pelo autor,
através do Programa de Geração Automática da Biblioteca Universitária da UFSC.

Daniel, Maycon Antônio
A EVOLUÇÃO E APLICAÇÃO DA SEGURANÇA DA INFORMAÇÃO POR MEIO DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD): UM ESTUDO DE CASO EM UMA INSTITUIÇÃO FINANCEIRA / Maycon Antônio Daniel ; orientador, Giovani Mendonça Lunardi, 2022.
64 p.

Trabalho de Conclusão de Curso (graduação) - Universidade Federal de Santa Catarina, Campus Araranguá, Graduação em Tecnologias da Informação e Comunicação, Araranguá, 2022.

Inclui referências.

1. Tecnologias da Informação e Comunicação. 2. Segurança da Informação. 3. Lei Geral de Proteção de Dados Pessoais. 4. Instituição Financeira. I. Mendonça Lunardi, Giovani. II. Universidade Federal de Santa Catarina. Graduação em Tecnologias da Informação e Comunicação. III. Título.

MAYCON ANTÔNIO DANIEL

A EVOLUÇÃO E APLICAÇÃO DA SEGURANÇA DA INFORMAÇÃO POR MEIO DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD): UM ESTUDO DE CASO EM UMA INSTITUIÇÃO FINANCEIRA

Este Trabalho Conclusão de Curso foi julgado adequado para obtenção do Título de "Bacharel em Tecnologias da Informação e Comunicação" e aprovado em sua forma final pelo Curso de Graduação em Tecnologias da Informação e Comunicação.

Araranguá/SC, 25 de março de 2022.

Documento assinado digitalmente
Vilson Gruber
Data: 30/03/2022 18:27:57-0300
CPF: 175.317.788-07
Verifique as assinaturas em https://v.ufsc.br

Prof. Vilson Gruber Dr.
Coordenador do Curso/Universidade Federal de Santa Catarina

Banca Examinadora:

Documento assinado digitalmente
Giovani Mendonca Lunardi
Data: 30/03/2022 14:48:01-0300
CPF: 520.394.559-49
Verifique as assinaturas em https://v.ufsc.br

Prof. Giovani Mendonça Lunardi, Dr.
Orientador/Universidade Federal de Santa Catarina

Documento assinado digitalmente
PAULO CESAR LEITE ESTEVES
Data: 30/03/2022 15:00:04-0300
CPF: 246.412.357-91
Verifique as assinaturas em https://v.ufsc.br

Prof. Paulo Cesar Leite Esteves, Dr.
Avaliador: Universidade Federal de Santa Catarina

Documento assinado digitalmente
Natana Lopes Pereira
Data: 30/03/2022 15:39:22-0300
CPF: 064.655.999-02
Verifique as assinaturas em https://v.ufsc.br

Prof.(a): Msc. Natana Lopes Pereira
Avaliador(a)/Universidade Federal de Santa Catarina (PPGEGC)

Dedico este trabalho a Amanda, que me dá incentivo e apoio em quaisquer decisões e momentos conturbados.

AGRADECIMENTOS

Agradeço primeiramente a Deus por me permitir construir esta jornada com dedicação empenho e sabedoria, principalmente forças para superar quaisquer obstáculos.

Aos meu país, Ana Lúcia e Rogério a qual que colocaram no mundo me proporcionam alegrias e nunca me deixaram faltar nada, também aos meu Avós em especial a minha vozinha que nos deixou este ano.

A instituição financeira, a mesma possibilitou a realização da pesquisa juntamente com chefe de setor de Tecnologia Michel.

A todos os profissionais que passaram pela minha formação acadêmica ao longo desse tempo.

E ao Professor Giovani Mendonça Lunardi pela sua dedicação e orientação durante o período de elaboração.

“O modo como você reúne, administra e usa a informação determina se vencerá ou perderá.”
Bill Gates

RESUMO

Este trabalho objetivou tratar sobre o impacto da Lei Geral de Proteção de Dados no meio bancário, no tocante a proteção de dados dos usuários de uma instituição financeira privada e como esta atua no quesito segurança da informação. O tema proteção de dados é importante por serem estas informações únicas de um sujeito, levando-o ao reconhecimento e/ou ao uso indevido por terceiros. Por conta disso o país promulgou a Marco Civil da Internet, mas se preocupou apenas com as informações dos sites, não tratando sobre as questões do acesso/cliente, vindo a tratar de forma muito superficial a questão da proteção de dados pessoais. E a LGPD trata as informações bancárias como dados sensíveis. Portanto, seja o ramo de negócio, ter-se-á que ditas informações apenas podem ser tratados pelas empresas se tiverem o consentimento do usuário. Frente ao exposto a questão problema a ser tratada nesta pesquisa é a seguinte: as Instituições Financeiras, por tratarem dos dados sensíveis de seus clientes, se encontram preparadas para cumprir as exigências da LGPD? A justificativa para esta pesquisa fundamenta-se no fato de que a adequação dos bancos a LGPD demanda esforço conjunto de diversas áreas que são produtoras e consumidoras de dados pessoais nas instituições. A metodologia adotada foi a estudo de caso, sendo estudada uma Instituição Financeira a fim de analisar quais meios adotados por no que se refere a segurança da informação de seus clientes, antes e depois da promulgação da LGPD, em particular no quesito proteção de dados dos mesmos.

Palavras-chave: LGPD. Segurança da Informação. Instituições Financeiras.

ABSTRACT

This work aimed to deal with the impact of the General Data Protection Law in the banking environment, regarding the protection of data of users of a private financial institution and how it acts in terms of information security. The issue of data protection is important because this information is unique to a subject, leading to recognition and/or misuse by third parties. As a result, the country enacted the Civil Rights Framework for the Internet, but was only concerned with information on the sites, not dealing with access/client issues, having treated the issue of personal data protection in a very superficial way. And the LGPD treats banking information as sensitive data. Therefore, whatever the line of business, it will be understood that such information can only be processed by companies if they have the user's consent. In view of the above, the problem question to be addressed in this research is the following: are Financial Institutions, by dealing with their customers' sensitive data, prepared to comply with the requirements of the LGPD? The justification for this research is based on the fact that the adequacy of banks to LGPD demands a joint effort from several areas that are producers and consumers of personal data in institutions. The methodology adopted was the case study, being studied a Financial Institution in order to analyze which means adopted by with regard to the security of the information of its customers, before and after the enactment of the LGPD, in particular in the question of data protection of the same.
.

Keywords: LGPD. Information security. Financial Institution.

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

LGPD Lei Geral de Proteção de Dados

GPO Política de Grupo

PSI Política de Segurança da Informação

ANPD Autoridade Nacional de Proteção de Dados

DLP Data Loss Preveniond

CPD Centro de Processamento de Dados

DPO Data Protection Officer

RGPD Regulamento Geral sobre a Proteção de Dados

SUMÁRIO

1 INTRODUÇÃO

O homem é um ser sociável por natureza e, por conta disso, criou os mais variados meios de comunicação, a fim de melhorar a vida em sociedade. A evolução tecnológica foi a responsável por auxiliar na passagem da era industrial para a da sociedade da informação, chegando-se à criação da internet que, dentre várias funções, também promove virtualização das relações pessoais.

Deste modo, pessoas são informadas e informam de maneira simples e dinâmica na rede, podendo vir a comprar via internet, assim como realizar operações financeiras através de aplicativos e sites bancários. Por conta disso a questão da proteção de dados passou a ser assunto sensível e constantemente debatido no meio jurídico.

O tema proteção de dados é importante por serem estas informações únicas de um sujeito, levando-o ao reconhecimento e/ou ao uso indevido por terceiros. Por conta disso o país promulgou o Marco Civil da Internet, mas se preocupou apenas com as informações dos sites, não tratando sobre as questões do acesso/cliente, vindo a tratar de forma muito superficial a questão da proteção de dados pessoais.

Eis então que o legislador viu a necessidade de criar a Lei Geral de Proteção de Dados (LGPD), por força da Lei de n. 13.709/2018, visando à proteção das informações privadas quando do tratamento, uso, manutenção, guarda e compartilhamento realizado buscando algum fim, seja econômico ou não.

É cediço que o setor financeiro brasileiro já se mostra robusto em relação ao seu ambiente protetivo de informações, sendo que a LGPD trouxe uma visão mais específico, quiçá, diferente para o cenário regulatório existente no setor. Isso porque a regra geral do sistema financeiro é pautada na conservação do sigilo dos dados pessoais e bancários do cliente, em particular aqueles que interferem diretamente na economia e na vida do cidadão, como por exemplo, seu perfil de crédito, ativos e dívidas.

E a LGPD trata as informações bancárias como dados sensíveis. Portanto, seja o ramo de negócio, ter-se-á que ditas informações apenas podem ser tratados pelas empresas se tiverem o consentimento do usuário.

Frente ao exposto a questão problema a ser tratada nesta pesquisa é a seguinte: Qual o impacto da Lei Geral de Proteção de Dados em uma instituição financeira privada no quesito Segurança da Informação.

A justificativa para esta pesquisa fundamenta-se no fato de que a adequação dos bancos a LGPD demanda esforço conjunto de diversas áreas que são produtoras e consumidoras de dados pessoais nas instituições.

1.1 Objetivos

Nas seções abaixo estão descritos o objetivo geral e os objetivos específicos deste TCC.

1.1.1 Objetivo Geral

Este trabalho objetiva investigar sobre o impacto da Lei Geral de Proteção de Dados em uma instituição financeira privada, no tocante a proteção de dados dos usuários e como esta atua no quesito segurança da informação.

1.1.2 Objetivos Específicos

* Realizar uma breve análise histórica sobre a questão da proteção de dados no Brasil;

* Analisar a LGPD, em especial sobre sua definição, fundamentos e direito do titular de dados;

* Compreender a evolução e aplicação da segurança da informação dentro das instituições financeiras por conta da Lei de Proteção de Dados Pessoais (LGPD), com o intuito de auferir como elas vão lidar com a regulamentação e a proteção dos dados de seus clientes.

* Efetivar um estudo de caso em uma instituição financeira a fim de analisar quais meios adotados por ela, no que se refere a segurança da informação de seus clientes, antes e depois da promulgação da LGPD, em particular no quesito proteção de dados dos mesmos.

1.2 Estrutura do TCC

Após passarmos pela seção introdutória, o estudo neste trabalho está organizado das seguintes maneiras fundamentação teórica; procedimentos metodológicos; apresentação e análise dos resultados; e conclusão. A fundamentação teórica identifica revisões literárias com estudos teóricos e empíricos dentro do tema (LGPD), passando por demais assuntos desde a chegada das tecnologias até as suas leis e aplicações dentro de uma instituição financeira. O propósito é analisar como estas tecnologias e leis estão vigorando em uma Cooperativa de crédito. Em seguida, apresenta-se os procedimentos metodológicos realizando uma coleta de informações e pesquisa. Logo após são discutidos os resultados, apresentados as conclusões e sugestões para pesquisas futuras.

2 SOBRE A PROTEÇÃO DE DADOS NO BRASIL E A LGPD

Não há como tratar sobre a evolução da proteção de dados sem antes apresentar um esboço histórico e conceitual da internet.

2.1 A origem da rede mundial de computadores – internet

A internet ou rede mundial, como também é conhecida, surgiu na década de 60, por meio das forças militares norte-americanas, e tinha como objetivo criar um meio para transmissão de dados entre um computador e outro. Em 1969, a Agência de Projetos Avançados (ARPA), do Departamento de Defesa dos EUA, deixou a cargo da *Rand Corporation* a missão de desenvolver um sistema de telecomunicações que garantisse a não interrupção da comunicação com o comando daquele país, para o caso de um possível ataque nuclear russo. Esta missão foi batizada com o nome de Projeto *Arpanet* (PAESANI, 2014). Considere-se aqui que, à época, a chamada "Guerra Fria" (EUA x URSS) estava em pleno andamento, daí a preocupação, com fundamento, do governo dos EUA.

Retornando a análise sobre o Projeto Arpanet, é interessante expor que pequenas redes locais (LAN) foram criadas e posicionadas em lugares estratégicos do país, e coligadas por meio de redes de telecomunicação geográfica (WAN). Logo, se alguma cidade ou ponto estratégico fosse destruído por um ataque nuclear, este "conjunto de redes conexas", formada por redes locais distantes uma das outras, mas interligadas entre si, garantiriam a comunicação entre as redes que estavam nas cidades coligadas, este sistema de interligação de redes foi denominado de Internet, isto é, *Inter Networkimg* (PAESANI, 2014)

É inegável que a internet é uma realidade para boa parte dos seres humanos no planeta e seus efeitos podem ser observados na alteração do cotidiano de um grande número de pessoas, principalmente nos países mais desenvolvidos. Além disso, é indiscutível o conforto e as facilidades que esta rede propicia, tais como diversão, possibilidades de pesquisa, informação, produtos e serviços, entre outros; no entanto, esta mesma rede pode também incidir em insegurança e instabilidade social.

Atualmente, o cidadão comum pode ter fácil acesso à Internet, mas durante muitos anos tal possibilidade ficou restrita às instituições de ensino e pesquisa. A utilização da Internet teve um crescimento maior em 1973, quando o Departamento de Pesquisa Avançada da universidade da Califórnia e responsável pelo Projeto Arpanet, registrou o Protocolo de

Controle da Transmissão (protocolo TCP/IP – *Internet Protocol* ou Protocolo Internet) (PAESANI, 2014)

É de domínio público que os microcomputadores são um fenômeno recente na vida da grande maioria dos indivíduos, motivo pelo qual insta aqui explicar que foi a partir da década de 80 que tais aparelhos tiveram um custo relativamente reduzido, mas sendo acessível apenas a uma pequena parte da população, pelo menos no caso brasileiro e, na relação computador versus Internet, foi no início dos anos 90 que ela passou a ultrapassar a marca de um milhão de usuários sendo a partir dessa década que sua utilização foi também redirecionada a fins comerciais.

Sobre a evolução dessa nova forma de acesso à informação, existe um relatório do governo norte-americano intitulado "A Economia Digital Emergente", o que revelou que a internet está crescendo de forma imensurável. Segundo tal documento o número de pessoas que utilizam a internet tem dobrado a aproximadamente cada cem dias. Em 1994, por exemplo, cerca de três milhões de pessoas já possuíam acesso à Internet e, no final de 1998, este montante já superava os cem milhões de pessoas conectadas à rede (BERTIGES, 2007). Todavia, dados da União Internacional de Telecomunicações, uma agência da ONU divulgou um relatório que demonstra que, pela primeira vez, o número de usuários de internet vai ultrapassar a marca de três bilhões de usuários até o final de 2015.

O mais impressionante é que o avanço da rede superou todas as tecnologias anteriores a ela; para que o rádio atingisse mais de cinquenta milhões de ouvintes foram necessários cerca de trinta e oito anos de existência; a televisão levou treze anos para chegar a este mesmo número; já a Internet percorreu este mesmo caminho em apenas quatro anos.

No Brasil a internet somente foi liberada para uso comercial em 1995. A Portaria 148 do Ministério das Comunicações de 31 de maio de 1995, responsável pela aprovação do uso dos meios de rede pública de telecomunicações para acesso à internet no Brasil conceituou a internet como: "nome genérico que designa o conjunto de redes, ou meio de transmissão e comutação, roteadores, equipamentos e protocolos necessários à comunicação entre computadores, bem como o '*software*' e os dados contidos nestes computadores" (VENTURA, 2010).

Lago Júnior (2001, p. 19), mostrando-se mais preocupado com o enfoque técnico, apresentou o conceito de internet como "conjunto de redes, ou meios de transmissão e comutação, roteadores, equipamentos e protocolos necessários à comunicação entre computadores".

Já Leal (2007, p. 14) apresentou a seguinte definição:

> A internet é um sistema transnacional de comunicação, operacionalizado por um conjunto de computadores interligados, permitindo a consulta, recepção e transmissão de dados (textos, sons, imagens), entre pessoas físicas e jurídicas e entre máquinas (sistemas auto-aplicativos), de um ponto a outro do planeta.

Corrêa (2000, p. 08) apresentou conceituação que se tornou clássica, ao defender que a Internet é:

> [...] um sistema global de rede de computadores que possibilita a comunicação e a transferência de arquivos de uma máquina a qualquer outra máquina conectada na rede, possibilitando, assim, um intercambio de informações sem precedentes na história, de maneira rápida, eficiente e sem a limitação de fronteiras, culminando na criação de novos mecanismos de relacionamento (2000, p.08).

Finkelstein (2011, p. 35) também enriquece esta pesquisa ao explicar que a Internet trata-se de:

> [...] um conjunto de incontáveis redes de computadores que servem a milhões de pessoas em todo o mundo. A Internet, cuja origem acredita-se seja militar, acabou superando, e muito, seus objetivos iniciais. Ela parece ter se consolidado como uma estrutura básica mundial, que assegura a veiculação permanente da comunicação. A Internet é a maior rede de sistemas computadorizados do planeta. Tecnicamente nada mais é do que um sistema de vários computadores conectados entre si que compartilham informações e disponibilizam serviços ao redor do mundo

Não é incomum o questionanto em relação a como se faz possível a pesquisa via *World Wide Web* (WWW). Antes disso cabe apresentar neste momento, o conceito de *World Wide Web* (WWW), que muitas vezes é confundido com a própria Internet. A www é parte da Internet e permite a conexão entre diversos documentos espalhados pela Internet, e a sua criação em 1992 impulsionou a utilização da Internet. A www, portanto, é uma rede de alcance mundial, na qual as diferentes mídias integram-se e efetivam-se em conjunto

A considerar que na atualidade se trabalha, estuda, interage, compra e se realiza operações financeiras por meio da internet é que o Brasil, seguindo a GDPR (General Data Protection Regulation ou Regulamentação Geral de Proteção de Dados), criada pela União Europeia (UE), criou a Lei Geral de Proteção de Dados.

Destarte, ainda que a revolução tecnológica tenha trazido tanto progresso social e econômico, a internet também causa problemas como, por exemplo, o acesso quase ilimitado a dados que, muitas vezes, dizem respeito à privacidade e até mesmo à intimidade dos indivíduos (CARVLHO NETO, 2013).

2.2 Breve análise histórica sobre a proteção de dados

É importante compreender como a privacidade tornou-se um direito fundamental, sujeito à proteção pelo estado jurisdicional, tornando-se ainda mais avultoso com o avanço da tecnologia. Para tanto mister considerar que a Constituição do Império (1824) já reconhecia o o direito à privacidade ao proteger o "segredo da carta" e a "inviolabilidade da casa", mas não fazia menção ao sigilo em si, estando mais pautada ao direito de propriedade, uma vez que não protegia o conteúdo, mas sim a invasão/obstrução.

O direito à privacidade se encontra previsto no art. 12 da Declaração Universal dos Direitos Humanos (1948), o qual dispõem: "ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito à proteção da lei".

Mas foi a Constituição Federal de 1988, ora ainda vigente que trouxe mais garantias sobre o tema, ao prever em seu artigo 5º, X, que "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação".

No início da década de 90 a Lei nº 8.078/90, conhecida como Código de Defesa do Consumidor previu o direito de o consumidor ter acesso a "informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele". Em seguida foi a vez da Lei de Interceptação Telefônica e Telemática (Lei nº 9.296/96) que passou a reconhecer o direito à privacidade restringindo o uso desse método investigativo sempre sob o amparo de uma ordem judicial.

Eis que em 2002 o Código Civil apresentou capítulo defendendo os Direitos da Personalidade e instrumentos a fim de coibir a violação do mesmo. Mas foi a Lei Carolina Dieckman (12.737/12) que acrescentou dispositivos ao Código Penal, tipificando como crime sujeito à prisão e multa a invasão de computadores, tablets e demais dispositivos eletrônicos. A questão é que as penas são pouco inibidoras, sendo muitas situações enquadráveis nos

procedimentos dos Juizados Especiais, o que poderia contribuir para a não eficiência no combate ao crime cibernético no Brasil.

Porém, foi somente a partir do Marco Civil da Internet a palavra "privacidade" passou a constar no sistema jurídico brasileiro, estabelecendo princípios, garantias, diretos e deveres a serem observados no ambiente digital. A Lei n. 12.965 foi inspirada mediante os seguintes princípios para a Internet no Brasil:

> (...) liberdade, privacidade e direitos humanos; governança democrática e colaborativa; universalidade; diversidade; inovação; neutralidade da rede; inimputabilidade da rede; funcionalidade, segurança e estabilidade; padronização e interoperabilidade e ambiente legal e regulatório.

O Marco Civil é considerado um tipo de "Constituição da Internet" na atual conjuntura do país, tendo os seguintes fundamentos de acordo com Jesus e Milagre:

> (a) o reconhecimento da escala mundial da rede de computadores: a Internet não deve ser uma rede pertencente a um ou outro país, mas um instrumento mundial;
> (b) os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais: os direitos humanos devem ser respeitados na Internet e este ambiente deve disponibilizar meios para o exercício da cidadania;
> (c) a pluralidade e a diversidade: não deve haver discriminação no ambiente cibernético, no qual deve ser respeitada toda e qualquer diversidade;
> (d) a abertura e a colaboração: a Internet deve ser livre, aberta e colaborativa;
> (e) a livre iniciativa, a livre concorrência e a defesa do consumidor: na Internet, todos devem ter liberdade de inovar, criar e desenvolver negócios, sempre respeitando as regras de defesa do consumidor também no ambiente digital e;
> (f) a finalidade social da rede: a Internet, além de um ambiente de comércio, também é um elemento para transformação social. (JESUS; MILAGRE, 2014, p20).

O Marco Civil da Internet é Lei de grande proeminência para a sociedade brasileira, uma vez que teve o objetivo de garantir a segurança jurídica de suas normas e reforçar os direitos e garantias nele assegurados.

Mesmo assim ainda se verificava um esforço por parte do judiciário em manter a preservação dos dados e de sua circulação. Prova disso é o fato de o Superior Tribunal de Justiça, em julgamento sobre a possibilidade de compartilhamento de dados de seus clientes usuários de cartões de crédito, ter vetado tal conduta (BULLA, 2017).

Destarte, foi com a Lei Geral de Proteção de Dados, Lei 13.709/18, que o país começou a ter uma discussão madura em relação à proteção de dados, ou seja, que levasse em conta o atual paradigma da privacidade na era digital. Isso porque não se pode pensar em uma proteção apenas no mundo real, deixando de lado o foro digital, pois o paradigma da

privacidade remete a conservação de sua inviolabilidade, ato consagrado pela nossa Carga Magna desde 1988, devendo ser preocupação, destarte, das leis que dela precisam derivar.

2.3 Lei geral de proteção de dados

De antemão, cabe aqui um adendo, fazendo-se necessário auferir, como Bioni o fez (2018) no que se refere a relação entre os dados dos usuários captados pelos provedores de aplicação de internet e a ascensão de verdadeiros impérios. Isso porque, através da inteligência gerada pela ciência mercadológica, especialmente quanto a segmentação dos bens de consumo (marketing) e a sua promoção (publicidade), os dados pessoais dos cidadãos converteram-se em um fator vital para a engrenagem da economia da informação. Além disso, "com a possibilidade de organizar tais dados de maneira mais escalável (e.g., Big Data), criou-se um (novo) mercado cuja base de sustentação é a sua extração e comodificação" (BIONI, 2018, p. 530).

Visando combater tais práticas, a Lei 13.709/18 possui diversos artifícios jurídicos que buscam regular a questão dos dados pessoas e sua administração, em respeito master aos direitos do indivíduo, tratando seus dados com transparência e responsabilidade. Assim é de Cots e Oliveira (2018) prelecionam em relação ao objetivo da LGPD, que é o de:

> (...) proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade natural. O verbo "proteger" diz muito sobre a forma como o legislador enxergou o titular dos dados, ou seja, em posição desigual em relação aos responsáveis pelo tratamento de dados, ficando patente sua vulnerabilidade. (COTS; OLIVEIRA, 2018, p31)

A hipossuficiência do usuário tratada aqui é muito semelhante a atribuída pelo comprador/consumidor via Código de Defesa do Consumidor, por reconhecer as limitações técnicas tão complexo quanto à captação e processamento de dados, muitas vezes representando um obstáculo quase instransponível entre o indivíduo e seus dados.

Ter-se-á enfim uma Lei que venha a ter a capacidade de venerar conquanto a privacidades dos dados por meio de mecanismos de defesa, pois o art. 1º da Lei 13.709/2018 delimita seu intuito e sua finalidade, abarcando os dados de pessoas naturais e jurídicas independente de sua natureza:

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

O art. 2º da LGPD trata da proteção dos direitos fundamentais, os quais referida Lei dá amparo, sendo o da liberdade de expressão, inviolabilidade da intimidade, direitos humanos e iniciativa, ou seja, que o tratamento na rede seja realizado em respeito aos direitos individuais:

> Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
>
> I - o respeito à privacidade;
> II - a autodeterminação informativa;
> III - a liberdade de expressão, de informação, de comunicação e de opinião;
> IV - a inviolabilidade da intimidade, da honra e da imagem;
> V - o desenvolvimento econômico e tecnológico e a inovação;
> VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
> VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais. (BRASIL, 2018, Art. 2)

Já o artigo subsequente trata sobre a abrangência e limitação da aplicabilidade em relação à proteção de dados, determinando que dita lei estenda sua jurisdição a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados.

Ao artigo 4º coube à tarefa de limitar a aplicação da lei para aplicações pessoais, questões jornalísticas e artísticas, bem como fins de segurança.

O artigo 5º da LGPD traz conceitos importantes acerca do tema, como segue:

> I - Dado pessoal: informação relacionada à pessoa natural identificada ou identificável;
> II - Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
> III - Dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

> IV - Banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico; (BRASIL, 2018, Art. 5).

Fica claro que o intuito da proteção dada mediante a LGPD é o resguardo dos direitos fundamentais e privacidade para o "livre desenvolvimento da personalidade da pessoa natural" (art.1).

Em respeito à exclusividade de propriedade dos dados por parte do titular a LGPD reconhece em seu artigo 17 a 22 os direitos que o titular possui sobre as suas informações, solidificando a noção de que o tratamento sobre dados só ocorre de forma correta quando esta acontece com o total consentimento daquele a quem as informações pertencem.

É também mister analisar que a partir do capítulo VI ao VIII, que contempla os artigos 37 a 54, disciplina-se os comportamentos permitidos pelos agentes que irão utilizar os dados tal como se definem boas práticas em relação ao tratamento de dados, a responsabilização legal e como ocorre a fiscalização.

Como crítica ter-se-á o fato de a LGPD ter sofrido diversos vetos presidenciais, sendo o mais grave o art. 55 que antevia a criação da Autoridade Nacional de Proteção de Dados (ANPD), corroborando assim para uma ausência de fiscalização comprometendo a aplicação técnica da lei, não colocando o país no mesmo patamar do Regulamento Geral sobre a Proteção de Dados (RGPD) da União Europeia, continuando a impedir o ingresso do mesmo na OCDE. Mas, felizmente a Lei 13.853/2019 alterou a Lei 13.709/2018, sendo uma das mudanças, a redação do art. 55, que efetivamente cria a Autoridade Nacional de Proteção de Dados, restringindo, contudo, o aumento de qualquer despesa para seu surgimento e funcionamento (COST; OLIVEIRA, 2018).

2.3.1 Proteção de Dados Pessoais

A Lei 13.709/2018 busca, através de uma série de artifícios jurídicos, regular a questão dos dados pessoais, assim como a maneira com que são administrados, de forma que o seu intuito seja sempre o respeito aos direitos dos indivíduos, tratando os dados com transparência e responsabilidade. "O objetivo da LGPD é o de "proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade natural". O verbo "proteger" diz muito sobre a forma como o legislador enxergou o titular dos

dados, ou seja, em posição desigual em relação aos responsáveis pelo tratamento de dados, ficando patente sua vulnerabilidade.” (COTS; OLIVEIRA, 2018).

Foi o art. 7ª. da Lei 13.709/2018 que trouxe a previsão em relação aos requisitos para que se realize o tratamento dos dados pessoais. Merece destaque o fato de o principal elemento a ser observado é o consentimento do titular, sendo que a coleta de dados para fins particulares e, portanto, não econômicos são apreciados pela Lei aqui em estudo.

Todavia, em análise ao referido artigo, o consentimento não é sinônimo de tratamento dos dados por tempo indeterminado, sendo que em relação aos dados pessoais sensíveis, a LGPD determina cautela ainda maior, justamente por serem dados que são ainda mais íntimos e privados do titular. Por isso os tratados dados sensíveis corresponde a uma atenuação ao princípio da privacidade.

Tendo isso em vista, o legislador foi acautelado ao separar as hipóteses de tratamento dos dados sensíveis dos demais, no art. 11º, como segue *in verbis:*

> Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
> I - Quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;
> II - Sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
> a) cumprimento de obrigação legal ou regulatória pelo controlador;
> b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
> c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
> d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
> e) proteção da vida ou da incolumidade física do titular ou de terceiros;
> f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou (Redação dada pela Lei nº 13.853, de 2019) Vigência.
> g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais. (BRASIL, 2018, Art.11)

Em relação ao prazo de término do tratamento de dados, o artigo 15 da LGPD elenca seis hipóteses que, se não cumpridas, se fará ter uma violação dos direitos fundamentais à privacidade do titular:

> I - Verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;
> II - Fim do período de tratamento;
> III - Comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º desta Lei, resguardado o interesse público; ou
> IV - Determinação da autoridade nacional, quando houver violação ao disposto nesta Lei. (BRASIL, 2018, Art. 15).

Tais normas foram necessárias, como já previamente analisado, tão somente porque para a prática mercadológica, os dados pessoais sensíveis são apenas efetivos para auferir lucro, direcionar a publicidade e realizar práticas abusivas (PINHEIRO, 2020).

Destarte a legislação aqui em comento, enfim, chegou para atribuir valor especial aos dados, atribuindo-lhes fator integral na formação da personalidade humana e, expropria-lo de tais dados é um atentado a sua personalidade e a seus direitos fundamentais.

Sobre isso Borges, realizando uma crítica comparativa entre a legislação brasileira e a europeia, assim comente: “Por análise comparativa das diretivas europeias, verifica-se que o rol de definições do anteprojeto de lei dos dados pessoais é significativo e consistente para abranger diversas hipóteses fáticas, relacionadas ao que o anteprojeto define como tratamento de dados. Observa-se também que o anteprojeto brasileiro recepciona o conceito do consentimento como um dos elementos titulados dados pessoais.” (BORGES, 2018, p. 530).

2.3.2 Tipos de Dados

Desde dos primórdios a identificação é essencial na vida do cidadão, como possuir sua documentação afim de poder adquirir algo ou ter direito perante as leis, visto isso os dados pessoais, consoante preleciona de Pinheiro (2020) deve ser considerado aquela informação que pode vir a distinguir o indivíduo de um grupo, tornando essa pessoa identificável. Já os dados do tipo “sensíveis” e que a LGPD trata de maneira ainda mais preocupada.

No primeiro quesito, ou seja, informação identificável é aquela que deriva do seu nome completo, número de CPF, quanto informações a ela relacionadas, de diversas naturezas ou, ainda, de um padrão de compra/intenção por parte de um indivíduo. Por sua vez, o do tipo sensível é aquele que remete a personalidade da pessoa, tais como: origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso,

filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural (física).

Por sua vez, o dado tipo anonimizado é permitido a critério da autorização do seu titular, sendo este o que mantem seu titular anônimo, seja este do tipo pessoal ou sensível. Para tanto, ele precisou ser tratado para que as informações do titular não possam ser vinculadas ao seu titular original, perdendo a possibilidade de associação, direta ou indireta, a um indivíduo.

2.3.3 Princípios

É o artigo 6º da Lei Geral de Proteção de Dados que elenca os princípios a serem observados no tratamento de dados, prevendo em seu caput que o princípio da boa-fé deverá ser considerado concomitantemente. Os princípios para os fins da LGPD são:

> I - Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
> II - Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
> III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
> IV - Livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
> V - Qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
> VI - Transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
> VII - Segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
> VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
> IX - Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
> X - Responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

A consiederar que a LGPD rege tanto o setor privado como o público pode-se verificar

uma colisão de dois princípios, quais sejam: a necessidade de consentimento do titular quanto ao tratamento e coleta de seus dados pessoais (privacidade) e a transparência do poder público, que deve garantir a divulgação das informações relevantes aos cidadãos (publicidade). Isso porque o Estado, que precisa prezar pela transparência e democracia das informações, precisará também respeitar a privacidade dos indivíduos, mas ambos os princípios precisarão coexistir, a fim de afastar qualquer totalitarismo estatal (PACETE, 2018).

Vale destacar o fato de o art. 4º. da LGPD excluir a aplicação da lei em questões exclusivas no que se refere a segurança pública, defesa nacional, segurança do Estado ou em casos de investigação e infração nacional. Mas, como o mesmo autor supracitado defende dita exceção pode poderá servir de justificativa para a criação de um Estado de constante vigilância, sendo necessária uma ponderação entre ditos princípios, garantindo assim a proporcionalidade.

2.3.4 Prazos e Sanções da LGPD

Apesar de sancionada em 14 de agosto de 2018, com previsão de entrar em vigor a partir do dia 28 de dezembro de 2018, uma MP de número 869/2018 deu nova redação ao art. 65 da LGPD, passando a Lei 13.709/18 a vigorar a partir o dia 16 de agosto de 2020. No entanto, é prerrogativa que as punições começassem a ser aplicadas em agosto de 2021.

Tal medida foi necessária por ter a LGPD causado uma inópia no que se refere a readequação dos sites e prestadores de serviço, pois a nova lei tratou de auferir maior proteção dos dados pessoais do que aquela apresentada pelo Marco Civil da Internet. Isso tudo impulsionada pelos padrões internacionais que veta que empresas europeias façam negócio com aquelas domiciliadas em países que não contam com uma legislação específica de tratamento/proteção de dados.

Foi o artigo 52 da LGPD o responsável por impor sanções administrativas aos infratores da Lei 13.709/18, definindo o seguinte:

> I – Advertência, com indicação de prazo para adoção de medidas corretivas;
> II – Multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
> III – multa diária, observado o limite total a que se refere o inciso II;
> IV – Publicização da infração após devidamente apurada e confirmada a sua ocorrência;
> V – Bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
> VI – Eliminação dos dados pessoais a que se refere a infração;
> X – 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;
> XI – 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;
> XII – Proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

Cots e Oliveira (2019, p. 202) analisando o artigo em comento, esclarecem que qualquer violação à LGPD, mesmo que sob matéria menos objetiva "como, por exemplo, a inobservância dos princípios" enseja possíveis sanções previstas.

Outrossim, os mesmos autores esclarecem que os puníveis pelas sanções administrativas são os agentes de tratamento de dados pessoais, ou seja, o controlador e operador. Destarte, o encarregado não se enquadra como agente de tratamento, não sendo responsável pela sanção.

No tocante as sanções administrativas, ficou sob incumbência do parágrafo 1º, do artigo supracitado, o seu estabelecimento:

> [...] § 1º As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios:
> I - a gravidade e a natureza das infrações e dos direitos pessoais afetados;
> II - a boa-fé do infrator;
> III - a vantagem auferida ou pretendida pelo infrator;
> IV - a condição econômica do infrator;
> V - a reincidência;
> VI - o grau do dano; VII - a cooperação do infrator.
> VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei;

> IX - a adoção de política de boas práticas e governança;
> X - a pronta adoção de medidas corretivas; e
> XI - a proporcionalidade entre a gravidade da falta e a intensidade da sanção.
> [...].

Portanto, fica nítida a importância de se observar todos os aspectos para fixação da sanção, pois "não faria qualquer sentido, por exemplo, penalizar uma empresa de forma mais gravosa do que a necessária para regularizar o tratamento de dados pessoais que ela realiza" (FRAZÃO, *et al*., 2019, p. 692).

2.3.5 Agentes

O local de armazenamento dos dados é intitulado pela Lei tão somente como banco de dados, implicando que há um ou mais agentes que o controle, estes que terão responsabilidade sobre a estrutura. Assim, coube aos incisos V a IX enumerarem os agentes, passivos e ativos, dando total importância a figura do titular.

De acordo com Agostinelli (2018) o tratamento de dados envolve, de maneira geral, diversos sujeitos, tais como: editores, empresas de publicidade e seus provedores. Por conta disso, defende ser de extrema necessidade estabelecer quais os papéis e responsabilidades de cada um, de uma forma adequada à legislação a que se submetem, facilitando, assim, a própria execução dessas normas.

Destarte, coube a LGPD, apresentar os conceitos dos agentes de tratamento de dados em seu art. 5º, assim de acordo com os incisos IV e V, controlador é a "pessoa natural ou jurídica, de direito público ou privado, a quem competem às decisões referentes ao tratamento de dados pessoais"; e operador a "pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador" (BRASIL, 2018).

Esses agentes possuem como função informar violações de dados a agência nacional de proteção de dados, criar mecanismos para sua proteção, entre outras. O controlador e o operador possuem responsabilidade solidária quanto a incidentes de segurança de informação, uso indevido ou não autorizado dos dados, ou se agirem em desconformidade com a LGPD. No entanto a responsabilidade do operador será limitada as suas obrigações contratuais (MONTEIRO, 2018).

Consoante LGPD, mais específicamente por conta do art. 18, é o titular dos dados que detem o poder sobre eles, tendo assim o direito de, a qualquer momento, exigir do controlador uma “prestação de contas” sobre o que está sendo feito com seus dados, ter acesso imediato e poder realizar correções a estes, bem como pedir a eliminação dos seus dados tratados, salvo se em hipóteses do art. 16:

> Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades: I - cumprimento de obrigação legal ou regulatória pelo controlador; II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados (BRASIL, 2018).

Nas situações em que o consumidor opor-se ao tratamento dos dados, caberá à empresa elimina-los imediatamente, ou explicar com fundamento legal ao titular o porquê de não o fazê-lo.

No que se refere aos dados de clientes bancários, ter-se-á que as principais alterações que a aplicação da LGPD trazem para o setor financeiro são:

> Consentimento do cliente: a empresa deverá solicitar autorização explicitamente, sem opção de adesão automática, e expressar claramente como serão tratados os dados do cliente;
> Direito à eliminação das informações: as instituições financeiras devem eliminar seus dados se você quiser, a não ser que haja alguma outra lei restringindo essa ação que sirva como justificativa válida;
> Efeitos de uma violação de dados: as instituições financeiras devem notificar a autoridade supervisora responsável, caso tenha havido qualquer violação de dados em seus arquivos;
> Gestão do fluxo de dados.
> Por conta do exposto as instituições financeiras precisarão adotar diferentes processos de gestão, controle e operação de dados para assegurar a rastreabilidade da informação e a segurança de dados, principalmente aqueles considerados sensíveis. A instituição que ficará responsável pela fiscalização da aplicação da LGPD é a ANPD, Agência Nacional de Proteção de Dados (NOVAES, 2021).

2.4 As instituições financeiras e a LGPD

A LGPD está bem alinhada ao Regulamento Geral de Proteção de Dados na União Europeia e, tratando-se de instituições financeiras ela é bem detalhada posto serem considerados dados pessoais sensíveis.

As empresas de serviços financeiros trabalham com informações altamente confidenciais que incluem dados pessoais e registros financeiros, de grande interesse para um invasor cibernético**.** Para garantir que esses dados confidenciais sejam protegidos adequadamente, instituições locais e internacionais estabeleceram regulamentos de conformidade em nível de segurança cibernética para empresas e organizações do setor**.**

A Lei em comento exige que as empresas avaliem e tratem os riscos às informações dos clientes em todas as áreas de sua operação, incluindo três áreas que são particularmente importantes para a segurança da informação: Gestão e Treinamento de Funcionários; Sistemas de informação; e Detectando e Gerenciando Falhas do Sistema. Um dos primeiros passos que as empresas devem tomar é determinar quais informações estão coletando e armazenando e se elas têm uma necessidade comercial de fazê-lo. Pode-se reduzir os riscos às informações do cliente se souber o que tem e manter apenas o que precisa.

Dependendo da natureza de suas operações comerciais, Rubens (2019) preleciona que as empresas devem considerar a implementação das seguintes práticas:

Gerenciamento e treinamento de funcionários. O sucesso do seu plano de segurança da informação depende muito dos funcionários que o implementam. Considerar:

- Verificar referências ou fazer verificações de antecedentes antes de contratar funcionários que terão acesso às informações do cliente.
- Pedir a cada novo funcionário que assine um acordo para seguir os padrões de confidencialidade e segurança de sua empresa para lidar com as informações do cliente.
- Limitar o acesso às informações do cliente a funcionários que tenham um motivo comercial para vê-las. Por exemplo, dê aos funcionários que respondem às consultas dos clientes acesso aos arquivos dos clientes, mas apenas na medida em que eles precisarem para realizar seus trabalhos.
- Controlar o acesso a informações confidenciais exigindo que os funcionários usem senhas “fortes” que devem ser alteradas regularmente. (Senhas difíceis de decifrar exigem o uso de

pelo menos seis caracteres, letras maiúsculas e minúsculas e uma combinação de letras, números e símbolos.)

- Usando protetores de tela ativados por senha para bloquear os computadores dos funcionários após um período de inatividade.
- Desenvolvimento de políticas para uso adequado e proteção de laptops, PDAs, telefones celulares ou outros dispositivos móveis. Por exemplo, certifique-se de que os funcionários armazenem esses dispositivos em um local seguro quando não estiverem em uso. Além disso, considere que as informações do cliente em arquivos criptografados estarão melhor protegidas em caso de roubo de tal dispositivo.
- Treinar os funcionários para que tomem medidas básicas para manter a segurança, confidencialidade e integridade das informações do cliente, incluindo:
    - Armários e armários de arquivo onde são guardados os registos;
    - Não compartilhar ou postar abertamente senhas de funcionários em áreas de trabalho;
    - Criptografar informações confidenciais do cliente quando transmitidas eletronicamente por meio de redes públicas;
    - Encaminhar chamadas ou outras solicitações de informações de clientes para indivíduos designados que foram treinados sobre como sua empresa protege os dados pessoais;
    - Relatar tentativas suspeitas de obter informações do cliente para o pessoal designado.
- Lembrar regularmente a todos os funcionários a política de sua empresa — e a exigência legal — de manter as informações do cliente seguras e confidenciais. Por exemplo, considere postar lembretes sobre sua responsabilidade pela segurança em áreas onde as informações do cliente são armazenadas, como salas de arquivos.
- Desenvolvimento de políticas para funcionários que trabalham à distância. Por exemplo, considere as ou como os funcionários devem ter permissão para manter ou acessar os dados dos clientes em casa. Além disso, exija que os funcionários que usam computadores pessoais para armazenar ou acessar dados de clientes usem proteções contra vírus, spyware e outras intrusões não autorizadas.
- Imposição de medidas disciplinares para violações da política de segurança.
- Impedir que funcionários demitidos acessem informações de clientes desativando imediatamente suas senhas e nomes de usuário e tomando outras medidas apropriadas. Sistemas de informação. Os sistemas de informação incluem design de rede e software e processamento, armazenamento, transmissão, recuperação e descarte de informações. Aqui

estão algumas sugestões sobre como manter a segurança ao longo do ciclo de vida das informações do cliente, desde a entrada de dados até o descarte de dados.

- Saiba onde as informações confidenciais do cliente estão armazenadas e armazene-as com segurança. Certifique-se de que apenas funcionários autorizados tenham acesso. Por exemplo:
    - Certifique-se de que as áreas de armazenamento estejam protegidas contra destruição ou danos causados por riscos físicos, como incêndio ou inundações.
    - Armazene os registros em uma sala ou armário que esteja trancado quando não for vigiado.
    - Quando as informações do cliente são armazenadas em um servidor ou outro computador, certifique-se de que o computador seja acessível apenas com uma senha "forte" e seja mantido em uma área fisicamente segura.
    - Sempre que possível, evite armazenar dados confidenciais de clientes em um computador com conexão à Internet.
    - Mantenha registros de backup seguros e mantenha os dados arquivados seguros armazenando-os off-line e em uma área fisicamente segura.
    - Mantenha um inventário cuidadoso dos computadores de sua empresa e de qualquer outro equipamento no qual as informações do cliente possam ser armazenadas.
- Tome medidas para garantir a transmissão segura das informações do cliente. Por exemplo:
    - Ao transmitir informações de cartão de crédito ou outros dados financeiros confidenciais, use um Secure Sockets Layer (SSL) ou outra conexão segura, para que as informações sejam protegidas em trânsito.
    - Se você coletar informações on-line diretamente dos clientes, torne a transmissão segura automática. Alerte os clientes contra a transmissão de dados confidenciais, como números de conta, por e-mail ou em resposta a um e-mail não solicitado ou mensagem pop-up.
    - Se você precisar transmitir dados confidenciais por e-mail pela Internet, certifique-se de criptografar os dados.
- Descarte as informações do cliente de forma segura e, quando aplicável, de acordo com a norma. Por exemplo:
    - Considere designar ou contratar um gerente de retenção de registros para supervisionar o descarte de registros contendo informações de clientes. Se você contratar uma empresa de descarte externa, faça a devida diligência com antecedência, verificando as

referências ou exigindo que a empresa seja certificada por um grupo industrial reconhecido.

- Queime, pulverize ou triture papéis contendo informações do cliente para que as informações não possam ser lidas ou reconstruídas.
- Destrua ou apague dados ao descartar computadores, discos, CDs, fitas magnéticas, discos rígidos, laptops, PDAs, telefones celulares ou qualquer outra mídia eletrônica ou hardware que contenha informações do cliente. Detectando e Gerenciando Falhas do Sistema. O gerenciamento de segurança eficaz exige que sua empresa detenha, detecte e se defenda contra violações de segurança. Isso significa tomar medidas razoáveis para evitar ataques, diagnosticar rapidamente um incidente de segurança e ter um plano para responder de forma eficaz. Considere implementar os seguintes procedimentos:

- Monitorando os sites de seus fornecedores de software e lendo publicações relevantes do setor para obter notícias sobre ameaças emergentes e defesas disponíveis.
- Manter programas e controles atualizados e apropriados para impedir o acesso não autorizado às informações do cliente. Tenha certeza de:
  - verifique com os fornecedores de software regularmente para obter e instalar patches que resolvam vulnerabilidades de softwares;
  - usar software antivírus e anti-spyware que seja atualizado automaticamente;
  - manter firewalls atualizados, principalmente se você usar uma conexão de Internet de banda larga ou permitir que os funcionários se conectem à sua rede de casa ou de outros locais externos;
  - assegure-se regularmente de que as portas não utilizadas para o seu negócio sejam fechadas;
  - transmitir prontamente informações e instruções aos funcionários sobre quaisquer novos riscos de segurança ou possíveis violações.
- Usar procedimentos apropriados de supervisão ou auditoria para detectar a divulgação imprópria ou roubo de informações do cliente. É sábio:
  - manter registros de atividade em sua rede e monitorá-los em busca de sinais de acesso não autorizado às informações do cliente;
  - usar um sistema de detecção de intrusão atualizado para alertá-lo sobre ataques;

- monitorar as transferências de informações de entrada e saída para indicações de comprometimento, como grandes quantidades inesperadas de dados sendo transmitidos de seu sistema para um usuário desconhecido;
- insira uma conta fictícia em cada uma de suas listas de clientes e monitore a conta para detectar quaisquer contatos ou cobranças não autorizadas.

- Tomar medidas para preservar a segurança, confidencialidade e integridade das informações do cliente em caso de violação. Se ocorrer uma violação:

  - tomar medidas imediatas para proteger qualquer informação que tenha sido ou possa ter sido comprometida. Por exemplo, se um computador conectado à Internet estiver comprometido, desconecte o computador da Internet;
  - preservar e revisar arquivos ou programas que possam revelar como a violação ocorreu;
  - se possível e apropriado, traga profissionais de segurança para ajudar a avaliar a violação o mais rápido possível.
- Considerar notificar consumidores, autoridades policiais e/ou empresas no caso de uma violação de segurança. Por exemplo:
  - notificar os consumidores se suas informações pessoais estiverem sujeitas a uma violação que represente um risco significativo de roubo de identidade ou dano relacionado;
  - notificar a aplicação da lei se a violação puder envolver atividade criminosa ou houver evidências de que a violação resultou em roubo de identidade ou dano relacionado;
  - notificar as agências de crédito e outras empresas que podem ser afetadas pela violação. Consulte Comprometimento de Informações e Risco de Roubo de Identidade: Orientação para o Seu Negócio.

Faz-se mister enfatizar que os dados bancários são um ativo valioso no mercado e, com isso, surge uma discussão entre privacidade e segurança, conceitos que não podem ser confundidos. Isso porque, o direito à privacidade é muito mais amplo e dentro dele há o aspecto de segurança da informação, devendo as companhias adotarem as medidas de defesa necessárias, salvaguardas e mecanismos de mitigação, incluindo os casos de violação de dados, que rompe com o famigerado princípio da finalidade, elementar no

ordenamento jurídico no tocante à proteção e privacidade dos dados pessoais (CASTRO; MANO; BARONOVSKY, 2021).

À medida que as empresas de serviços financeiros precisam evoluir para garantir a prestação de serviços de qualidade ao cliente, também precisam assegurar que suas soluções de segurança da informação sejam realmente capazes de proteger os dados confidenciais que capturam e transmitem. Por meio do uso de tecnologias de segurança, as instituições asseguram que os dados trafegados nas transações não corram riscos durante as operações.

2.4.1 Gestão de Dados

Gestão de Dados pode ser compreendida como um conjunto de processos e políticas - geralmente auxiliares por software especializado - que permite que uma organização consolide suas informações financeiras mantenha uma conformidade com as regras e leis contábeis e produz os relatórios detalhados. O gerenciamento de dados financeiros mantém uma estrutura de dados projetados por lógica (como diferentes planos de contas de dados) para fornecer diferentes planos de dados financeiros.

As ameaças à segurança de dados de instituições financeiras são elevadíssimas e, assim sendo Silva (2019) preleciona que o primeiro passo para a segurança da informação neste segmento é estar ciente das maiores ameaças de segurança de dados descobertas e ativas atualmente. Os ataques cibernéticos contra serviços financeiros e outros setores cresceram em número, tamanho e sofisticação, segundo informações da PWC (2018).

A adesão de novos serviços e tecnologias também coloca a segurança de dados em risco. O número e a variedade de vulnerabilidades estão crescendo à medida que as empresas terceirizam processos internos, transferem dados para a computação em nuvem e se conectam aos clientes por meio de mais canais (ALLEASY, 2019).

Essas falhas na segurança cibernética levaram mais de 40 estados nos EUA criarem uma legislação específica de privacidade. Em 2018, foi a vez da Europa seguir o modelo e aprovar a GDPR, *General Data Protection Regulation*, válida para toda empresa que coletar, processar ou tratar dados da União Europeia (ALLEASY, 2019).

Eis que o Brasil criou a LGPD exigindo a regulamentação para o uso, proteção e transferência de dados pessoais no país e estabelece de modo claro quem são as figuras envolvidas e quais são suas atribuições, responsabilidades e penalidades que deverão ser

aplicadas no caso de incidentes. Segundo a nova lei, as organizações financeiras devem criar suas Políticas de Segurança Cibernética de acordo com o porte da empresa, a natureza e a complexidade das operações. Também deve ser considerada a sensibilidade dos dados com os quais a instituição lida.

Uma maneira de aprimorar a proteção de dados no setor bancário é garantir a conformidade adequada de segurança de dados financeiros com os padrões do setor, leis internacionais e regulamentações locais. Neste trabalho, analisa os principais requisitos aos quais deve-se prestar atenção e descreve as sete recomendações mais eficazes a serem seguidas ao criar uma estratégia de segurança cibernética para uma organização financeira.

As instituições financeiras trabalham em estreita colaboração com dados altamente confidenciais, como informações de identificação pessoal e registros financeiros. E como esses dados podem ser facilmente monetizados ou usados para fraudes financeiras, geralmente são alvos de ciber criminosos.

Para garantir operações seguras e a proteção adequada de dados confidenciais, órgãos reguladores locais e internacionais estabelecem requisitos de conformidade de segurança para instituições financeiras. Em particular, esses requisitos podem ajudá-lo a delinear:

1. quais pontos problemáticos prestar atenção ao criar uma estratégia de segurança cibernética;
2. quais práticas e tecnologias implementar para uma melhor proteção de dados.

Atender aos requisitos de conformidade de segurança financeira fornece a uma organização vários benefícios essenciais, incluindo:

- visão clara dos dados e sistemas mais críticos
- melhor compreensão de quais ferramentas e práticas de segurança cibernética usar;
- maior segurança para informações valiosas;
- tempo reduzido para resposta a incidentes de segurança cibernética.

O não cumprimento das regulamentações obrigatórias, por sua vez, não apenas priva as instituições financeiras desses benefícios, mas também leva a:

- multas extensas por não conformidade;
- perdas financeiras decorrentes de vazamentos de dados, interrupções operacionais e ações judiciais;
- danos graves à reputação
- perda de confiança do cliente.

As organizações normalmente precisam cumprir mais de um conjunto de requisitos. Existem regulamentos obrigatórios e consultivos, bem como leis internacionais, federais e regionais. Ao combinar os requisitos de várias leis e normas, as instituições financeiras podem criar estratégias de segurança cibernética mais eficazes do que quando seguem apenas um único conjunto de requisitos. Então, em quais padrões de TI, regulamentações internacionais e leis locais os players do setor financeiro devem se concentrar.

2.4.2 Tecnologias para proteção dos dados em instituições financeiras

Tendo em vista novas informações e praticas de utilização dessas, precisou-se se proteger ainda mais de ataques cibernéticos devido as brechas que passam a integrar com aumento de tecnologia, com isto novas medidas foram tomadas:

> Recentemente, a Accenture trabalhou em conjunto com a Oracle criando um roteiro para fortalecer a resiliência dos negócios e garantir sua continuidade diante das crescentes ameaças.
>
> Um ponto importante é que você pode reduzir melhor o risco de segurança de dados criando uma infraestrutura que evite violações, em vez de somente reagir a um evento. Mesmo que você consiga repelir um ataque, o desempenho do sistema será degradado durante o incidente — diminuindo as operações e reduzindo a produtividade da equipe.
>
> A segurança de rede e o uso de um antivírus, por si só, simplesmente não fará o trabalho. Você precisa criar segurança em toda a sua infraestrutura, diretamente no núcleo. Aqui estão algumas perguntas que você precisa fazer:
>
> - As políticas de TI aderem aos padrões do setor com relação à segurança de dados?
> - Quais medidas estão em vigor para proteger contra acesso não autorizado ou uso indevido por usuários privilegiados?
> - Quais medidas existem para proteger contra corrupção de dados e danos irrecuperáveis e intencionais aos dados?
>
> Para garantir a segurança de dados o roteiro criado pela Oracle junto com a Accenture adota uma abordagem de ciclo de vida completo com base em quatro pilares. Vamos ver cada um brevemente agora (ALLEASY, 2019).

Uma política de governança de dados é um documento que descreve formalmente como os dados organizacionais serão gerenciados e controlados. Algumas áreas comuns cobertas pelas políticas de governança de dados são:

- **Qualidade dos dados** – garantir que os dados sejam corretos, consistentes e livres de "ruídos" que possam impedir o uso e a análise.
- **Disponibilidade de dados** – garantindo que os dados estejam disponíveis e sejam fáceis de consumir pelas funções de negócios que os exigem.
- **Usabilidade de dados** – garantir que os dados sejam claramente estruturados, documentados e rotulados, permite uma pesquisa e recuperação fáceis e são compatíveis com as ferramentas usadas pelos usuários de negócios.
- **Integridade dos dados** – garantindo que os dados mantenham suas qualidades essenciais mesmo quando são armazenados, convertidos, transferidos e visualizados em diferentes plataformas.

- **Segurança de dados** – garantir que os dados sejam classificados de acordo com sua sensibilidade e definir processos para proteger as informações e evitar perda e vazamento de dados (IMPERVA, 2021).

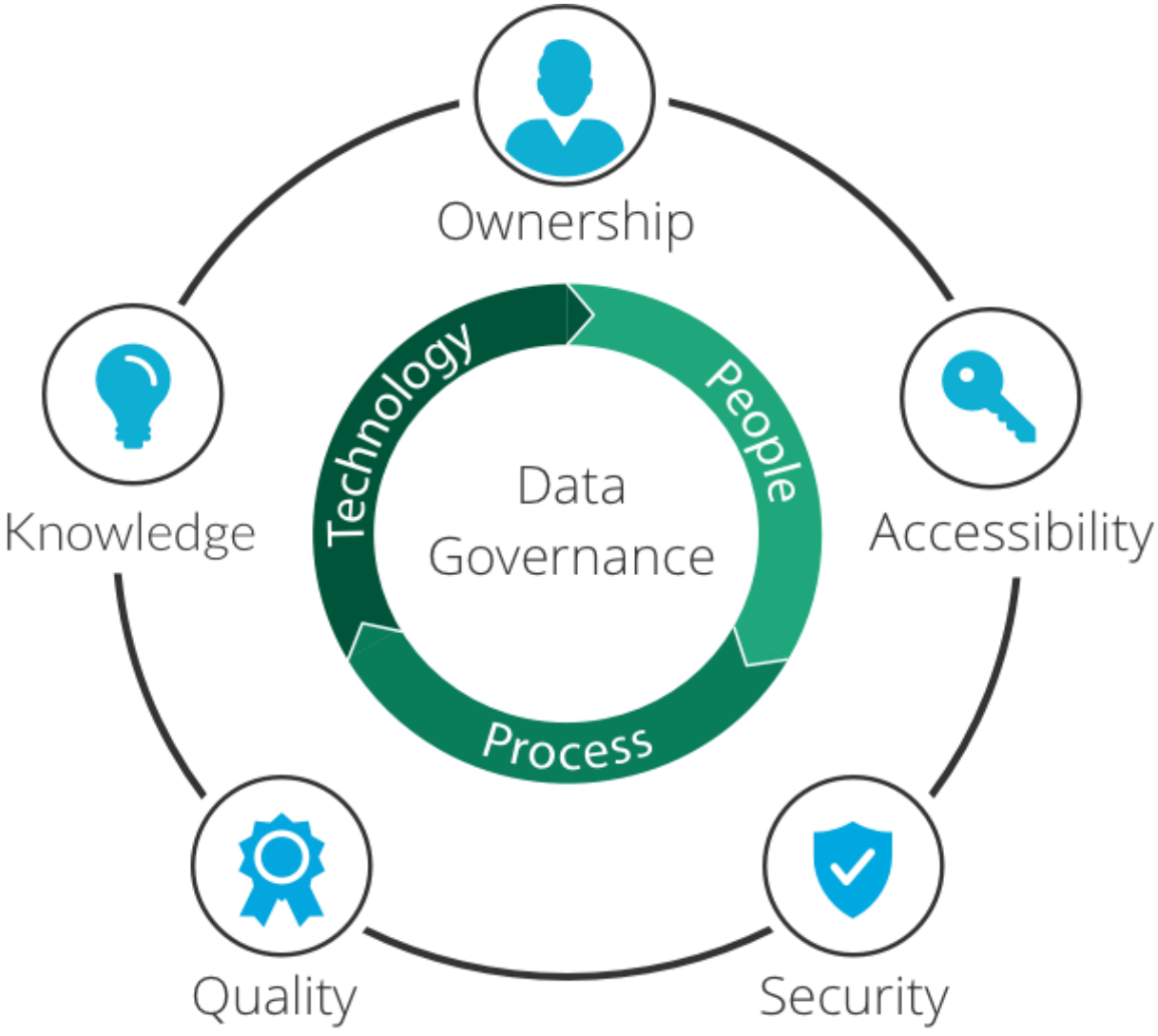

Figura 1 - Representação esquemática da política de governança de dados / FONTE: https://www.imperva.com/learn/wp-content/uploads/sites/13/2019/01/Data-Governance.png

Abordar todos esses pontos requer uma combinação certa de habilidades de pessoas, processos internos e a tecnologia apropriada.

- **Administradores de dados**

Um administrador de dados é uma função organizacional responsável por aprovar a política de governança de dados. Os administradores de dados geralmente são especialistas no assunto que estão familiarizados com os dados usados por uma função ou departamento de negócios específico. Eles garantem a adequação dos elementos de dados, tanto conteúdo quanto metadados, administram os dados e garantem a conformidade com os regulamentos.

- **Governança de dados versus gerenciamento de dados**

A governança de dados é uma estratégia usada, enquanto o gerenciamento de dados são as práticas usadas para proteger o valor dos dados. Ao criar uma estratégia de governança de dados, você incorpora e define práticas de gerenciamento de dados. Exemplos e políticas de governança de dados direcionam como as tecnologias e soluções são usadas, enquanto o gerenciamento aproveita essas soluções para realizar tarefas.

- **Estruturas de Governança de Dados**

Uma estrutura de governança de dados é uma estrutura que ajuda uma organização a atribuir responsabilidades, tomar decisões e agir sobre dados corporativos. As estruturas de governança de dados podem ser classificadas em três tipos:

•Comando e controle – a estrutura designa alguns funcionários como administradores de dados e exige que eles assumam responsabilidades de governança de dados.

•Tradicional – a estrutura designa um número maior de funcionários como administradores de dados, de forma voluntária, com alguns servindo como “administradores de dados críticos” com responsabilidades adicionais.

•Não invasivo – a estrutura reconhece as pessoas como administradores de dados com base em seu trabalho existente e na relação com os dados; todos que criam e modificam dados se tornam um administrador de dados para esses dados.

Os elementos essenciais de uma estrutura de governança de dados incluem:

•Financiamento e apoio à gestão – uma estrutura de governança de dados não é significativa, a menos que seja apoiada pela administração como uma política oficial da empresa.

- Engajamento do usuário – garantir que aqueles que consomem os dados entendam e cooperem com as regras de governança de dados.
- Conselho de governança de dados – um órgão formal responsável por definir a estrutura de governança de dados e ajudar a implementá-la na organização.

Embora muitas empresas criem estruturas de governança de dados de forma independente, existem vários padrões que podem ajudar a formular uma estrutura de governança de dados, incluindo COBIT, ISO/IEC 38500 e ISO/TC 215.

2.4.3 Estratégia de governança de dados

Uma estratégia de governança de dados informa o conteúdo da estrutura de governança de dados de uma organização. Requer que você defina, para cada conjunto de dados organizacionais:

- Onde: Onde está fisicamente armazenado
- Quem: Quem tem ou deve ter acesso a ele
- O quê: Definição de entidades importantes como “cliente”, “fornecedor”, “transação”
- Como: Qual é a estrutura atual dos dados
- Qualidade: qualidade atual e desejada dos dados de origem e conjuntos de dados consumíveis
- Objetivos: O que queremos fazer com esses dados
- Requisitos: O que precisa acontecer para que os dados atinjam as metas

2.4.4 O que é uma Política de Governança de Dados e por que ela é importante?

As políticas de governança de dados são diretrizes que podem ser utilizadas para garantir que seus dados e ativos sejam usados adequadamente e gerenciados de forma consistente. Essas diretrizes geralmente incluem políticas relacionadas à privacidade, segurança, acesso e qualidade. As diretrizes também abrangem as funções e responsabilidades daqueles que implementam políticas e medidas de conformidade.

O objetivo dessas políticas é garantir que as organizações sejam capazes de manter e proteger dados de alta qualidade. As políticas de governança formam a base de sua estratégia de governança mais ampla e permitem que você defina claramente como a governança é realizada.

2.4.5 Funções de governança de dados

As operações de governança de dados são realizadas por vários membros da organização, incluindo equipe de TI, profissionais de gerenciamento de dados, executivos de negócios e usuários finais. Não há um padrão estrito para quem deve preencher as funções de governança de dados, mas existem funções padrão que as organizações implementam.

- 2.4.5.1 Diretor de Dados

Os diretores de dados geralmente são executivos seniores que supervisionam seu programa de governança. Essa função é responsável por atuar como um defensor do programa, trabalhando para garantir pessoal, financiamento e aprovação para o projeto e monitorar o progresso do programa.

- 2.4.5.2 Gerente e Equipe de Governança de Dados

Os gerentes de governança de dados podem ser cobertos pela função de diretor de dados ou podem ser funcionários separados. Essa função é responsável por gerenciar sua equipe de governança de dados e ter uma função mais direta na distribuição e gerenciamento de tarefas. Essa pessoa ajuda a coordenar os processos de governança, lidera sessões de treinamento e reuniões, avalia as métricas de desempenho e gerencia as comunicações internas.

- 2.4.5.3 Comitê de Governança de Dados

O comitê de governança de dados é um comitê de fiscalização que aprova e direciona as ações da equipe de governança e do gestor. Esse comitê é normalmente composto por proprietários de dados e executivos de negócios.

Eles seguem as recomendações dos profissionais de governança de dados e garantem que os processos e as estratégias estejam alinhados com os objetivos de negócios. Esse comitê

também é responsável por resolver disputas entre unidades de negócios relacionadas a dados ou governança.

- 2.4.5.4 Administradores de dados

Os administradores de dados são os membros individuais da equipe responsáveis por supervisionar os dados e implementar políticas e processos. Essas funções geralmente são preenchidas por profissionais de TI ou de dados com experiência em domínios e ativos de dados. Os administradores de dados também podem desempenhar um papel como engenheiros, analistas de qualidade, modeladores de dados e arquitetos de dados.

2.4.6 Um modelo de governança de dados em 4 etapas

Gerenciar princípios de governança de dados de forma eficaz requer a criação de uma função de negócios, semelhante a recursos humanos ou pesquisa e desenvolvimento. Essa função precisa ser bem definida e deve incluir as seguintes etapas do processo:

1.**Descoberta** — processos dedicados a determinar o estado atual dos dados, quais processos dependem dos dados, quais recursos técnicos e organizacionais suportam os dados e o fluxo do ciclo de vida dos dados. Esses processos derivam insights sobre dados e uso de dados para uso em processos de definição. Os processos de descoberta são executados simultaneamente e são usados iterativamente com os processos de definição.

2.**Definição** — processos dedicados à documentação de definições de dados, relacionamentos e taxonomias. Nesses processos, os insights dos processos de descoberta são usados para definir padrões, medidas, políticas, regras e estratégias para operacionalizar a governança.

3.**Aplicação** — processos dedicados a operacionalizar e garantir o cumprimento das estratégias e políticas de governança. Esses processos incluem a implementação de papéis e responsabilidades de governança.

4.**Medição** — processos dedicados a monitorar e medir o valor e a eficácia dos fluxos de trabalho de governança. Esses processos fornecem visibilidade das práticas de governança e garantem a capacidade de auditoria.

2.4.7 Modelo de maturidade de governança de dados

Avaliar a maturidade de suas estratégias de governança pode ajudá-lo a identificar áreas de melhoria. Ao avaliar suas práticas, considere os seguintes níveis.

- Nível 0: Desconhecido

As organizações de nível 0 não têm consciência do significado da governança de dados e nenhum sistema ou conjunto de políticas definido para dados. Isso inclui a falta de políticas para criar, coletar ou compartilhar informações. Nenhum modelo de dados é descrito e nenhum padrão é estabelecido para armazenamento ou transferência de dados.

Itens de ação:

Os planejadores de estratégia e arquitetos de sistemas precisam informar os líderes de TI e de negócios sobre a importância e os benefícios da governança de dados e do gerenciamento de informações corporativas (EIM).

- Nível 1: Consciente

As organizações de nível 1 entendem que carecem de soluções e processos de governança de dados, mas têm poucas ou nenhuma estratégia em vigor. Normalmente, os líderes de TI e de negócios entendem que o EIM é importante, mas não tomaram medidas para impor a criação de políticas de governança.

Itens de ação:

Planejadores e arquitetos precisam começar a determinar as necessidades da organização e desenvolver uma estratégia para atender a essas necessidades.

- Nível 2: Reativo

As organizações de nível 2 entendem a importância e o valor dos dados e têm algumas políticas em vigor para proteger os dados. Normalmente, as práticas usadas para proteger os dados por essas organizações são ineficazes, incompletas ou aplicadas de forma inconsistente.

Itens de ação:

As equipes de gerenciamento precisam pressionar por consistência e padronização para a implementação de políticas.

- Nível 3: Proativo

As organizações de nível 3 estão trabalhando ativamente para aplicar a governança, incluindo a implementação de medidas proativas. A governança de dados faz parte de todos os processos organizacionais. No entanto, normalmente não existe um sistema universal de governança. Em vez disso, os proprietários das informações são responsáveis pelo gerenciamento.

Itens de ação:

As organizações precisam avaliar a governança no nível departamental e centralizar as responsabilidades.

- Nível 4: Gerenciado

As organizações de nível 4 desenvolveram e implementaram consistentemente políticas e padrões de governança. Essas organizações categorizaram seus ativos de dados e podem monitorar o uso e o armazenamento de dados. Além disso, a supervisão da governança é realizada por uma equipe estabelecida com funções e responsabilidades.

Itens de ação:

As equipes devem rastrear ativamente as tarefas de gerenciamento de dados e realizar auditorias para garantir que as políticas sejam aplicadas de forma consistente.

- Nível 5: Eficaz

As organizações de nível 5 alcançaram estruturas confiáveis de governança de dados. Eles podem ter indivíduos em suas equipes com certificações de governança de dados e especialistas estabelecidos. Essas organizações podem alavancar efetivamente seus dados para obter vantagem competitiva e melhorias na produtividade.

Itens de ação:

As equipes devem trabalhar para manter a governança e verificar a conformidade. As equipes também podem investigar ativamente métodos para melhorar a governança proativa. Por exemplo, pesquisando as melhores práticas para casos de governança específicos, como governança de big data.

2.4.8 Práticas recomendadas de governança de dados

Uma iniciativa de governança de dados deve começar com amplo suporte de gerenciamento e aceitação das partes interessadas que possuem e gerenciam os dados (chamados custodiantes de dados).

É aconselhável começar com um pequeno projeto piloto, sobre um conjunto de dados que é especialmente problemático e que precisa de governança, para mostrar às partes interessadas e à gestão o que está envolvido e demonstrar o retorno do investimento da atividade de governança de dados.

Ao implantar a governança de dados em toda a organização, use modelos, modelos e ferramentas existentes quando possível para economizar tempo e capacitar as funções organizacionais para melhorar a qualidade, acessibilidade e integridade de seus próprios dados. Avalie e considere o uso de ferramentas de governança de dados que podem ajudar a padronizar processos e automatizar atividades manuais.

Mais importante ainda, construa uma comunidade de administradores de dados dispostos a assumir a responsabilidade pela qualidade dos dados. De preferência, esses devem ser os indivíduos que já criam e gerenciam conjuntos de dados e entendem o valor de tornar os dados utilizáveis para toda a organização.

3 PROCEDIMENTOS METODOLÓGICOS: ESTUDO DE CASO

Além da pesquisa bibliográfica, foi realizada uma pesquisa de campo em janeiro de 2022, com estudo de caso em uma Instituição financeira que, por não ter dado a autorização de divulgação de seu nome, será aqui chamada de Banco Alpha. A ideia foi a de analisar quais meios adotados por ela, no que se refere à segurança da informação de seus clientes, foi adotado depois da promulgação da LGPD, em particular no quesito proteção de dados dos mesmos.

O Banco Alpha iniciou suas atividades em setembro de 1989, tendo como missão contribuir para o desenvolvimento econômico e social dos associados, por meio da cooperação financeira e de serviços, promovendo a melhoria de vida da comunidade; como visão a de ser reconhecido pela sociedade como a melhor opção financeira e de serviços na região, possuindo autonomia financeira para o atendimento das necessidades dos associados.

A instituição em estudo sempre se preocupou com a segurança das informações de seus clientes. Isso é corroborado no momento em que se verificam políticas do mesmo antes da LGPD, as quais incluíam investimento constante na Segurança da Informação, que compreende um conjunto de medidas que visam proteger e preservar as informações utilizadas nas atividades diárias da Instituição, atribuindo-lhes confiabilidade. Assim, os seguintes elementos constituem os pilares da Segurança da Informação dessa Cooperativa:

Confidencialidade: A informação somente pode ser acessada por pessoas explicitamente autorizadas. É a proteção de sistemas de informação para impedir que pessoas não autorizadas tenham acesso.

Disponibilidade: A informação deve estar disponível no momento em que a mesma for necessária.

Integridade: A informação deve ser recuperada em sua forma original (no momento em que foi armazenada). É a proteção dos dados ou informações contra modificações intencionais ou acidentais não autorizadas.

Legalidade: Garante a legalidade da informação; a aderência de um sistema à legislação e as características das informações que possuem valor legal dentro de um processo de comunicação, em que todos os elementos estão de acordo com as cláusulas contratuais pactuadas ou a legislação vigente.

Rastreabilidade: Trata-se da identificação dos diversos passos de uma transmissão de informação, identificando os participantes, os locais e horários de cada etapa da transmissão.

Veracidade: Corresponde à informação calcada em acontecimentos verídicos ou argumentos lógicos, compatíveis com a necessidade da organização.

Neste contexto, o investimento em Segurança da Informação já visava aumentar a produtividade da Instituição, através de um ambiente mais organizado e confiável, proporcionando maior controle dos riscos.

No tocante as informações de como os Dados eram coletados: Os Dados, incluindo Dados Pessoais, poderão ser coletados quando o cliente submete ou quando interage em Nossos Ambientes e Serviços, o que inclui:

A possibilidade de o cliente solicitar a confirmação da existência de tratamento de Dados Pessoais, além da exibição ou retificação de seus Dados Pessoais, diretamente ao Encarregado de Proteção de Dados Pessoais, através do e-mail quando o pedido estiver relacionado à confirmação de existência ou disponibilização de acesso aos dados pessoais, o Banco responderá a requisição em até 15 (quinze) dias corridos após a confirmação da identidade do titular.

Em relação a limitação, oposição e exclusão de dados. Pelos Canais de Atendimento, podendo o cliente também requerer: a) a limitação do uso de seus Dados Pessoais; b) manifestar sua oposição e/ou revogar o consentimento quanto ao uso de seus Dados Pessoais; ou c) solicitar a exclusão de seus Dados Pessoais que tenham sidos coletados no âmbito dos nossos Serviços.

Porém, restava claro que se o cliente retirar seu consentimento para finalidades fundamentais ao regular funcionamento dos Serviços e dos Nossos Ambientes, tais ambientes e serviços poderão ficar indisponíveis para ele.

Findos o prazo de manutenção e a necessidade legal, os Dados Pessoais serão excluídos com uso de métodos de descarte seguro, ou utilizados de forma anonimizada para fins estatísticos.

Com a promulgação de Lei de Proteção de Dados a implantação na instituição teve início com uma série de treinamentos voltados ao entendimento e aplicação da lei, tendo ocorrido por volta de 12 meses antes da mesma entrar em vigor, esses treinamentos trataram assuntos tais como:

- Política de Proteção de Dados
- Planos de ação referente a Política de Proteção de Dados
- Revisão e implantação da Política de Proteção de Dados
- Auditorias internas de Privacidade de Dados
- Análise de GAP de sistemas de Privacidade de Dados

A implantação da nova lei geral de proteção de dados foi dividida basicamente entre processos tecnológicos e processos administrativos.

3.1 Administrativos

- Análise GAP de privacidade de dados:

Essa analise consistiu em verificar os itens relevantes da lei, levantando o que a instituição possuía que atenderia a mesma e o que seria necessário implantar, desde soluções administrativas a tecnológicas.

- Criação da política de proteção de dados pessoais.

Nesse ponto foram levantados todos os requisitos impostos pela lei, e documentado de forma a criar uma Política de Proteção de Dados condizente com a estrutura organizacional da instituição e atendendo todas as demandas que a lei exigia.

- Divulgação e conscientização da Política de Proteção de dados pessoais.

Após a conclusão da política e reconhecimento da mesma pelo conselho administrativo da instituição, iniciou-se o trabalho de divulgação e conscientização da mesma, através de treinamentos aos colaboradores e partes interessadas a organização.

- Escolha do DPO ou encarregado de dados.

Conforme exigência da lei, foi definido um membro colaborador da instituição para ser o DPO, ou seja, o encarregado de dados e responsável em responder a ANPD (Agência

Nacional de Proteção de Dados) em qualquer das solicitações, também responsável em responder os titulares de dados em caso de solicitações por esses realizados.

- Levantamento do mapa de finalidades de dados.

Seguindo as exigências da Lei Geral de Proteção de Dados, foram efetuados o levantamento das finalidades de dados através de um mapeamento realizado junto aos setores chaves da instituição, setores esses que de alguma forma utilizam-se de dados pessoais dentro de qualquer uma das fases que a lei propõe (Coleta, Retenção, Processamento, Compartilhamento e Eliminação).

- Adequações contratuais entre controladores e operadores de dados.

Nessa fase foram levantados junto ao setor jurídico da instituição dos os contratos com controladores e operadores que de alguma forma manipulam dados pessoais em alguma das fases que a lei propõe. O objetivo desse trabalho foi adequar esses contratos através de clausulas que assegurem a correta manipulação e a privacidade de dados pessoais.

Nesse período foram levantados não somente os contratos envolvendo o ambiente tecnológico, mas também os de cunho administrativo.

- Analise de risco e de impactos relacionados a dados pessoais.

A realização da análise de risco em privacidade de dados veio com o objetivo de fazer uma análise dos impactos relacionados a manipulação dos dados e garantia da privacidade diante da nova lei. Essa análise levou em consideração as vulnerabilidades e ameaças encontradas, gerando assim os possíveis impactos para a instituição em caso da não atendimento correto a lei.

- Revisão das demais políticas da instituição que se interligam com as propostas da Lei Geral de Proteção de Dados.

Além da Política de Proteção de Dados, a instituição conta com outras políticas que de alguma forma também auxiliam na proteção e privacidade de dados, tais como:

- Política de Segurança da Informação
- Política de Segurança da Informação para Fornecedores
- Política de Classificação da Informação
- Política de Segurança Cibernética

3.2 Tecnológicas

- Revisão dos sistemas e contratos que tratam dados pessoais.

Assim como nos contratos administrativos e de negócios, os contratos de tecnologias precisaram de revisão e quando necessário, inclusões de clausulas de confidencialidade e privacidade de dados pessoais.

- Implantação de sistema para registro e tratamento de logs, DLP.

O tratamento de logs veio da importância de rastreabilidade imposta pela Lei Geral de Proteção de Dados, tanto para atendimento direto a ANPD quanto a solicitação de Titulares de Dados. Nesse quesito foi importante a implantação de sistema próprio para esse tipo de guarda e amostragem de informação.

- Implantação de sistema para controle de fluxo de dados pessoais, tanto para sistemas locais quanto para e-mails, DLP.

Em conjunto com a necessidade de rastreabilidade, a segurança através do controle de entrada e saída de dados também teve sua importância revelada com a nova Lei Geral de Proteção de Dados. Nesse fundamento foram utilizadas tecnologias de controle de fluxo de dados, objetivando além dos registros das informações de saída e entrada, como também o bloqueio das mesmas em caso de não cumprimento dos papeis relacionados a Política de Proteção de Dados.

- Auditorias internas em sistemas que tratam dados pessoais.

Em conjunto a implementação de uma Política de Proteção de Dados, vem a necessidade de assegurar o cumprimento das diretrizes impostas na mesma, para esse fim foram definidos períodos analises de auditoria interna na instituição, afim de encontrar possíveis apontamentos que de alguma forma estejam em desacordo com a Política proposta, e consequentemente em desconformidade com a Lei Geral de Proteção de Dados.

3.3 Entrevista

Pois bem à análise dos dados, se utiliza a pesquisa qualitativa. O método qualitativo, de acordo com Richardson (1999) é utilizado para estudar cenários complexos e rigorosamente específicos, possibilitando descrever um problema de difícil compreensão, analisar a relação entre variáveis e, abstrair, além de classificar, processos vividos por grupos sociais. Desta forma, os dados obtidos junto departamento de TI com auxílio do chefe de setor, partiram da análise qualitativa e permitiram identificar os pontos positivos que possam identificar alguma ausência na manutenção da segurança da informação dos dados armazenados.

No que se diz respeito aos objetivos, o estudo defendido como descrito, para Gil (2002), tem como finalidade principal descrever as particularidades de uma determinada população ou, a formação de relações entre variáveis. Com este trabalho emprega são ilustradas as características da instituição sobre atual gerencia proteção de dados de seus associados por meio de seus colaboradores.

Entretanto no que se refere a coleta de dados, foi efetuado um estudo a partir de um levantamento feito junto ao setor de TI com aplicação de um questionário ao chefe de setor, neste questionário foram descritas todas as respostas e transcritas no trabalho. Segundo Gil (2002), a pesquisa na forma de levantamento, se caracteriza pela interrogação direta das pessoas das quais a conduta se deseja conhecer. O método estudo de caso consiste na análise de um ou poucos objetos, para que seja possível ter o conhecimento maior e mais detalhado acerca de um determinado assunto.

3.4 Resultados

- Quais profissionais tem acesso total aos dados pessoais da cooperativa?

Setor TI tem acesso liberado a pasta, documentos e ao sistema em geral.

- Dentre essas pessoas que acessam, existe um rastreio?

Todo e qualquer movimentação feita proveniente no sistema ou pastas são gerados logs com usuário que as modificou, podendo assim ser solicitados relatórios, dentre esses sistemas o (DLP) Data Loss Prevenion é nova ferramenta que ajuda a prevenção do dado, ele identifica o dado pessoal e critico prevenido de acessos indevidos e mostra aonde esses dados está circulando.

- Levando em consideração os colaboradores de outros setores como funciona os acessos?

Cada setor possui determinado acesso, aplicado a grupos e políticas da empresa.

- Como funciona as políticas de acesso?

Funcionário em questão tende a criar uma senha na qual precisa informar números, letras Maiúsculas e minúsculas e um caractere especial, para que possa ingressar no seu ambiente de trabalho contudo esta senha precisa ser atualizada dentre 30 dias, após ingressar o usuário tende a abrir o sistema no qual passa a utilizar autenticações de 2 fatores com seu celular devidamente instalado, e o sistema de desbloqueio liberado conforme feita liberação do departamento de TI, essa autenticação equivale para quase todos acessos pessoais do colaborador afim de deixar ainda mais robusto o sistema de tais invasões. Essas políticas geralmente são impostas ao setor de TI, que faz a instalação dos sistemas e nessas mesmas políticas são criada as GPOs dentro do servidor que como exemplo, permitem o acesso ao usuário somente em dias da semana com horário estabelecido conforme a carga horária de trabalho dentre as demais citadas anteriores, a maioria é configurada dentro do servidor da empresa e aplicada.

Os envios de e-mails são rotulados de acordo com o conteúdo, isso ajuda aplicar politicas a cada envio de e-mail, no qual são configurados por cada instituição levando em

consideração recomendações de ordens superiores. Um anexo como um arquivo pessoal não estando ligado a cooperativa, pode bloquear seu envio como também rotulagem do e-mail para tal destinatário.

- Quais garantias estão aplicadas, não havendo assim um ataque cibernético?

São utilizados Antivírus renomeados no mercado, programas totalmente licenciados, firewall robusto no bloqueio de acesso dos colaboradores tanto em meio físico como em navegação na rede, rede de internet privada somente conexão estática, como rede wifi somente interna, rede pública para acesso em agencia para utilização de wifi.

- Como é a segurança no meio físico?

A documentação por fim que pode ser acessada pessoalmente e tê-la em mãos são armazenadas em locais aonde somente com senhas, tanto de alarme como de abertura do local são exigidas, ficando impossibilitado qualquer acesso, além do mais as instalações possuírem cadeados a qual interrompem qualquer acesso primário.

- Dentre a Instituição, a alguma espécie de fiscalização para que a empresa trabalhe da forma correta?

Todos os anos são feitas auditorias internas de ordens superiores do Banco que realizam tarefas afim de apontarem alguma fragilidade ou erro de operação.

- Há alguma espécie de treinamento aos funcionários? Garantido que não haja evasão dos dados?

São realizados dois treinamentos anualmente envolvendo LGPD e (PSI) Política de Segurança da Informação, que são ministradas pelo chefe de setor de TI, além do mais cada funcionário que entra para o banco precisa passar por esse treinamento.

- Em relação a disponibilidade da informação?

A informação está disponível em que a mesma for necessária.

- Quais ferramentas são utilizadas para integridade da informação?

Os backups em nuvem e físico estão disponíveis a qualquer momento se necessidade de perca de informação.

- Como os dados são coletados?

Quando cliente submete ou interage em nossos ambientes e serviços.

- Como funciona a troca de informações pessoais na instituição?

A instituição não promove a troca de informações por ligações, para isso a empresa utiliza de forma presencial, um ambiente interativo como um WhatsApp Web que possui controle total sobre o setor de TI e por meio dos canais digitais, a qual só irão pedir informações de acordo como o associado ou pessoa deseja realizar alguma operação, pois isso faz com que haja proteção na identificação da pessoa física ou jurídica.

Em relação a melhorias que podem serem adotas, fica clara a fiscalização para que os mesmos erros acontecido anteriores não ocorram novamente, dente eles atualização frequente de dados, softwares, meios físicos, acompanhamento e mudança das leis imposta da LGPD, PSI da segurança da informação.

3.5 ANÁLISE DO ESTUDO DE CASO

Após esse estudo de caso no banco Alpha e entrevista realizada, podemos concluir a instituição frente a Lei Geral de Proteção de Dados está trabalhando em um conjunto com a lei desde que ela entrou em vigor, de acordo com os dados do questionário aplicado, visitas de vistorias que apontam problemas as cooperativas que integram a rede da instituição são feitas anualmente sendo assim, caso estejam trabalhando de forma incorreta em alguns pontos as mesmas são apontadas, desta forma foi analisado e encontrado algumas irregularidades em uma fechadura do CPD (Centro de Processamentos de Dados) a qual não apresentava logs de entrada e saídas, outro problema apontado foi uma irregularidade no sistema de uma suposta colaboradora que ainda estava ativa sendo que já tinha deixado a instituição, entretanto o descaso foi por conta do setor de Recurso Humanos que não informou a TI que a mesma tinha sido desligada do Banco. Todos esses problemas vão contra a LGPD podendo causar danos maiores tanto a instituição como também ao associado que possuem seus dados armazenados, tendo em vista esses problemas o setor de Tecnologia prontamente regularizou tudo, ficando alinhada com a Lei a Cooperativa.

CONCLUSÃO

Na era da informação, é a internet a disseminadora de dados, que são compartilhados de maneira instantânea neste ciberespaço, mas a acentuada difusão dessas informações acaba por comprometer a privacidade das pessoas que tiveram fatos expostos em na rede.

O advento da internet constitui em um dos mais importantes marcos da humanidade, ocasionando mudanças nas relações econômicas, sociais e culturais existentes, beneficiando o consumo, que passou a ter mais comodidade para que os clientes adquirissem seus produtos e/ou serviços de maneira online.

Entretanto, essa modalidade trouxe consigo sérias fragilidades no tocante a segurança, indo desde fraudes a coleta indevida de dados pessoais. Deste modo, os diversos casos de vazamentos de dados pessoais colocam em evidência a segurança no meio digital, haja vista o consumidor não possuir noção do procedimento realizado em face do tratamento dos seus dados fornecidos.

Esse problema demandou a necessidade de criação de regulamentação a fim de coibir essas violações, a fim de trazer segurança jurídica para todos, já que a inserção diária de dados em páginas eletrônicas passou a ser algo comum e necessário.

Desta maneira, a Lei Geral de Proteção de Dados, que entrou em vigor em agosto de 2021 protege o titular de dados, oferecendo controle acerca destes, pois o consentimento e a transparência são os pilares da lei. Portanto, pode-se concluir que o estudo da proteção de dados pessoais no Brasil torna-se cada vez mais importante, devido aos diversos riscos que podem advir do tratamento de dados.

Dita análise é ainda mais gritante no comércio eletrônico, por conta da vulnerabilidade do consumidor, sendo necessário das empresas a adoção de compliance para evitar irregularidades e as consequentes sanções impostas pela lei.

Por certo que a LGPD pode ser considerada um avanço para o país, pois a sociedade está em constante mutação e o direito visa acompanhar e regular estas mudanças.

No que se refere às instituições financeiras elas lidam com consultas e análises de dados o tempo todo. Parte dessas análises é solicitada por outras empresas, e a outra parte pelos próprios clientes. Naturalmente, essas informações ficam registradas na base das instituições e podem ser utilizadas no futuro para a oferta de serviços e produtos,

Com vigência da LGPD, o cliente passa a ter o direito de solicitar a retirada de suas informações das bases de dados das financeiras. Se a empresa não tiver uma justificativa válida para manter os dados, é o direito do cliente que prevalece.

Por conta disso a adequação à nova legislação exige que a empresa tenha uma forma segura de armazenamento e tratamento dos dados dos clientes. Caso contrário, as informações podem ser colocadas em risco, prejudicando o consumidor e a empresa.

Em relação ao banco estudado acredita-se que ele vem atuando de maneira satisfatória ao cumprimento da Lei e segurança da informação e quesito proteção de dados de seus clientes. Porém, a segurança cibernética é fator que precisa estar sempre em constância, mutação e evolução, sob pena de ficar defasada.

À medida que as empresas de serviços financeiros precisam evoluir para garantir a prestação de serviços de qualidade ao cliente, também precisam assegurar que suas soluções de segurança da informação sejam realmente capazes de proteger os dados confidenciais que capturam e transmitem. Assim, é por meio do uso de tecnologias de segurança que as instituições asseguram que os dados trafegados nas transações não corram riscos durante as operações.

E os bancos são os mais adiantados na corrida para o cumprimento da LGPD. O principal motivo está no fato de ser um setor muito regulamentado.

Tendo em vista esta pesquisa, acredito como a lei começou a vigorar a pouco tempo, muitas empresas nem se quer se movimentaram com tanta ênfase neste assunto, neste caso novas pesquisas em outros nichos empresarias levando em conta todos aspectos explorados em torno desse conteúdo devem ser feitas, ficando aberto para novos estudos a LGPD visando identificar pontos invulneráveis e até mesmo pontos fortes a serem seguidos e tomados como exemplo quais forem áreas e segmentos, de forma de tornar e propor métodos de conscientização voltados a segurança dos dados pessoais.

REFERÊNCIAS

AGOSTINELLI, J. **A importância da lei geral de proteção de dados pessoais no ambiente onlin**e. Etic, Presidente Prudente, v. 14, n. 14, 2018.

ALLEASY; MANO, Janini Nogueira D'Alessandro; BARONOVSKY, Thainá. **Como garantir segurança de dados em instituições financeiras**. 2021. Disponível em: https://www.alleasy.com.br/2019/01/07/como-garantir-seguranca-de-dados-em-instituicoes-financeiras/. Acesso em: 11 jan. 2022.

ALVES, Larissa Brito. **As práticas abusivas nas relações de consumo**. 2018. Disponível em:https://repositorio.animaeducacao.com.br/bitstream/ANIMA/15667/1/TCC%20Alex%20Coelho%20atualizado%20.pdf, Acesso em: 23 de novembro de 2021.

ANDREOTTI Tüchumantel Hackerott, Nadia. et al. Título: **Aspectos jurídico do e-commerce:** Como surgiu o comércio eletrônico? Edição 2021. Editora, Revista dos Tribunais.

BRASIL. **Constituição da República Federativa do Brasil**. Brasília, DF: Senado Federal, 1988.

BARRETO FILHO, Marcelo Vandré Ribeiro. **Os Contornos Jurídicos da Lei Geral de Proteção de Dados Frente ao Consumo no Ambiente Virtual**. 2019. 51 f. TCC (Graduação) - Curso de Direito, Universidade Federal da Paraíba, Santa Rita, 2019.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoas** – A Função e os Limites do Consentimento. São Paulo: Editora Forense, 2018.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais:** a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020.

BORGES, Fernando Augusto de Vita. **Manual da LGPD** - lei geral da proteção de dados - lei 13.709/2018 devidamente atualizada com a lei 13.853/2019. JH Mizuno, 2020.

BRASIL. Lei n. 12.965, de 23 de abril de 2014. **Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil**. Diário Oficial da República Federativa do Brasil. Brasília, DF, 23 abr. 2014. Disponível em: https://www.tjdft.jus.br/institucional/imprensa/campanhas-e-produtos/direito-facil/edicao-semanal/marco-civil-da-internet#:~:text=Lei%20n%C2%BA%2012.965%2C%20de%2023,Munic%C3%ADpios%20em%20rela%C3%A7%C3%A3o%20%C3%A0%20mat%C3%A9ria. Acesso em: 05 de dezembro. 2021.

BRASIL. Lei Carolina Dieckmann, Lei n° 12.737. **Dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências**. Brasília, Distrito Federal, Brasil. 2014.

BRASIL. Marco Civil da internet, Lei nº 12.965. **Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília**, Distrito Federal, Brasil. 2014. Tribunal de Justiça - RS. Apelação Civil 70057245193 RS.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965**, de 23 de abril de 2014 (Marco Civil da Internet). Brasília, 2018.

BULLA, B. (14 de outubro de 2017). **STJ proíbe compartilhamento de dados de cartão**. Acesso em 1 de dezembro de 2021, disponível em Estadão: https://economia.estadao.com.br/noticias/geral,stj-proibe-compartilhamento-dedados-de-cartao,70002043404
2017, COTS, Márcio; OLIVEIRA, Ricardo. **Lei Geral de Proteção de Dados Pessoais Comentada**. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

CASTRO, Dayane Marciano de Oliveira; MANO, Janini Nogueira D'Alessandro; BARONOVSKY, Thainá. **Dados pessoais bancários e financeiros são considerados dados sensíveis para a LGPD?** a criticidade dos dados bancários: riscos e danos aos titulares. A criticidade dos dados bancários: riscos e danos aos titulares. 2021. Disponível em: https://www.migalhas.com.br/depeso/350335/dados-pessoais-bancarios-sao-considerados-dados-sensiveis-para-a-lgpd. Acesso em: 11 jan. 2022.

DONEDA, Danilo. **Princípios da proteção de dados pessoais**. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cintia Rosa Pereira de (Coords.). Direito & Internet III – Tomo I: Marco Civil da Internet (Lei n.12.965/2014). São Paulo: Quartier Latin, 2015.

IMPERVA; MANO, Janini Nogueira D'Alessandro; BARONOVSKY, Thainá. **Data Governance:** what is data governance? a data governance definition. What is Data Governance? A Data Governance Definition. 2021. Disponível em: https://www.imperva.com/learn/data-security/data-governance/. Acesso em: 11 jan. 2022.

JESUS, Damásio de; MILAGRE, José Antonio. **Marco Civil da Internet**: Comentário à Lei 12.965/14. 1. ed. São Paulo: Saraiva, 2014.

KLEE, Antonia Espíndola Longoni. **Comércio eletrônico**. São Paulo: Revista dos Tribunais, 2014.

LINS, Bernardo Felipe Estellita. **A evolução da internet: uma perspectiva histórica**. Página 16. Janeiro / Abril de 2013. disponível em: http://www.belins.eng.br/ac01/papers/aslegis48_art01_hist_internet.pdf Acesso em 1 de dezembro de 2021.

PACETE, L. G. (21 de Maio de 2018). **"A GDPR terá um efeito viral**". Acesso em 4 de Janeiro de 2022, disponível em Meio & Mensagem: https://www.meioemensagem.com.br/home/midia/2018/05/21/a-gdpr-tera-um-efeito-viral.html#:~:text=Na%20pr%C3%B3xima%20sexta%2Dfeira%2C%2025,lei%20de%20prote%C3%A7%C3%A3o%20de%20dados.

PAESANI, Liliana Minardi. **Direito e Internet**: liberdade de informação, privacidade e responsabilidade civil / Liliana Minardi Paesani. – 7. ed. – São Paulo : Atlas, 2014.

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

PITNEYBOWE. **Mantendo o comércio fluindo**. Disponível em: https://www.pitneybowes.com/br. Acesso em 7 de Janeiro de 2022.

SOBHIE, Amir Ayoub; OLIVEIRA, Deymes Cachoeira de. **Proteção do consumidor no comércio eletrônico**: Inovações relevantes para as vendas on-line no Brasil a partir do Decreto Federal nº. 7962/2013. Revista Eletrônica de Iniciação Científica. Itajaí, Centro de Ciências Sociais e Jurídicas da UNIVALI. v. 4, n.4, p. 84- 107, 4º Trimestre de 2013. Disponível em: www.univali.br/ricc - ISSN 2236-5044. Acesso em: dezembro de 2021.

SOUZA, Thiago Pinheiro Vieira de. **A proteção de dados pessoais como direito fundamental e a incivilidade do uso de cookies**. 2018. 65 f. Monografia (Bacharelado em Direito) – Curso de Graduação em Direito, Universidade Federal de Uberlândia, Uberlândia, 2018.

VENTURA, Luiz Henrique**. Comércio e contratos eletrônicos**: aspectos jurídicos. 2. ed. Bauru: Edipro, 2010.

VENTURA, Ivan. **Dados Digitais**: O novo ouro?. Consumidor Moderno. Disponível em: https://digital.consumidormoderno.com.br/dados-digitais-o-novo-ouro-ed251/.Acesso em: 10 de janeiro de 2022.

RICHARDSON, Roberto Jarry. **Pesquisa social:** métodos e técnicas. 3. ed. São Paulo: Atlas, 1999.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa.** 4. ed. São Paulo: Atlas, 2002. 175 p.