UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO DE ARTES E COMUNICAÇÃO
DEPARTAMENTO DE CIÊNCIA DA INFORMAÇÃO
CURSO DE GESTÃO DA INFORMAÇÃO

JADSON FITIPALDI DE LIMA BEZERRA

CONTRIBUIÇÕES DA GESTÃO DA INFORMAÇÃO PARA A ADEQUAÇÃO DAS FACTORINGS À LGPD

RECIFE
2022

JADSON FITIPALDI DE LIMA BEZERRA

CONTRIBUIÇÕES DA GESTÃO DA INFORMAÇÃO PARA A ADEQUAÇÃO DAS FACTORINGS À LGPD

Trabalho de Conclusão de Curso apresentado ao Departamento de Ciência da Informação da Universidade Federal de Pernambuco como requisito parcial para obtenção do grau em Bacharel no curso de Gestão da Informação.

Orientador: Prof. Dr. Silvio Luiz de Paula

RECIFE

2022

Ficha de identificação da obra elaborada pelo autor,
através do programa de geração automática do SIB/UFPE

Bezerra, Jadson Fitipaldi de Lima.
Contribuições da gestão da informação para a adequação das factorings à LGPD / Jadson Fitipaldi de Lima Bezerra. - Recife, 2022.
64 p. : il.

Orientador(a): Silvio Luiz de Paula
Trabalho de Conclusão de Curso (Graduação) - Universidade Federal de Pernambuco, Centro de Artes e Comunicação, Gestão da Informação - Bacharelado, 2022.

1. Gestão da Informação. 2. Lei Geral de Proteção de Dados (LGPD). 3. Segurança da Informação. 4. Factorings. I. Paula, Silvio Luiz de . (Orientação). II. Título.

020 CDD (22.ed.)

Serviço Público Federal
Universidade Federal de Pernambuco
Centro de Artes e Comunicação
Departamento de Ciência da Informação

FOLHA DE APROVAÇÃO

Contribuições da gestão da informação para adequação das factorings à LGPD

Jadson Fitipaldi de Lima Bezerra

Trabalho de Conclusão de Curso submetido à Banca Examinadora, apresentado e aprovado de modo remoto (online), pelo Curso de Gestão da Informação, do Departamento de Ciência da Informação, da Universidade Federal de Pernambuco, como requisito parcial para obtenção do título de Bacharel em Gestão da Informação.

TCC aprovado 20 de Outubro de 2022.

Banca Examinadora:

Orientador – Prof. Dr. Sílvio Luiz de Paula.
DCI/Universidade Federal de Pernambuco.

Examinadora 1 – Profa. Dra. Márcia Ivo Braz.
DCI/Universidade Federal de Pernambuco.

Examinadora 2 – Profa. Dra. Claudinete de Fátima Silva Oliveira Santos.
GECNET – Administração e Serviços Ltda.

Dedico este trabalho a minha família e amigos. À instituição que me proporcionou diversas conquistas e experiências.

AGRADECIMENTOS

Venho por meio desse item, registrar meus agradecimentos, primeiramente, a minha mãe Sandra de Oliveira Fitipaldi, por todo suporte e dedicação. Ao meu companheiro Helder Wanderley de Freitas, pela paciência e parceria.. Dedico aqui a vocês meu amor e admiração.

Agradeço ao meu orientador, Silvio Luiz de Paula, pelas oportunidades ofertadas, orientações, conversas e por ser esse profissional e amigo admirável. Também agradeço a todos os professores e profissionais do Departamento, pelo esforço e trabalho exercido, sua dedicação contribuiu de forma essencial para minha formação.

Agradeço aos colegas de turma, do curso e dos projetos pelos momentos e conhecimentos partilhados, além do apoio e crescimento conjunto.

Aos meus familiares e amigos, que estiveram sempre dispostos e presentes, acompanhando meu desempenho e conquistas, incentivando-me a alcançar meus objetivos mesmo quando tudo parecia ser tão difícil. Meus sinceros agradecimentos.

"Nas grandes batalhas da vida, o primeiro passo para a vitória é o desejo de vencer.”

Mahatma Gandhi

RESUMO

O acesso à informação foi acelerado devido ao avanço das tecnologias, especialmente após o surgimento da internet, que é utilizada por grande parte da população mundial. Foi exatamente por este movimento crescente de trocas de informações pessoais, que se observou a necessidade de criar algumas garantias e direitos relacionados aos dados pessoais ou dados sensíveis, relativos aos usuários/clientes, pois existe um desequilíbrio de poderes entre os possuidores de dados pessoais e os titulares destes dados. Diante deste contexto o presente trabalho tem o objetivo de apresentar um modelo para o processo de adequação das empresas de factoring às regras da LGPD apresentando como a Gestão da informação pode ser uma aliada neste processo, garantindo segurança às informações coletadas e uma adequada governança de dados com as informações pessoais que são tratadas em suas bases de dados. Para alcançar os objetivos deste trabalho, foram feitas pesquisas sobre o conceito da atividade de *factoring*, os principais requisitos da LGPD com foco para as atividades de *factoring*, e requisitos da Gestão da Informação que possam auxiliar nesse processo. Com estes levantamentos foi possível apresentar um modelo de adequação das empresas de *factoring* à Lei 13.709/2018. Através das 07 etapas sugeridas neste trabalho é possivel garantir a segurança e a governança adequada das informações pessoais que rodeiam o ambiente do fomento mercantil, para empresas que não tenham acesso a consultorias especializadas.

Palavras-chave: Gestão da Informação. Lei Geral de Proteção de Dados (LGPD). Segurança da Informação. *Factorings*.

ABSTRACT

Access to information has been accelerated due to the advancement of technologies, especially after the emergence of the internet, which is used by a large part of the world's population. It was precisely because of this growing movement of exchanges of personal information, that the need to create some guarantees and rights related to personal data or sensitive data, related to users/customers, was observed, as there is an imbalance of powers between the holders of personal data and the holders of these data. Given this context, the present work aims to present a model for the process of adapting factoring companies to the rules of the LGPD, showing how Information Management can be an ally in this process, ensuring security to the information collected and adequate data governance. with the personal information that is processed in their databases. To achieve the objectives of this work, research was carried out on the concept of factoring activity, the main requirements of the LGPD with a focus on factoring activities, and Information Management requirements that can assist in this process. With these surveys, it was possible to present a model of suitability of factoring companies to Law 13.709/2018. Through the 07 steps suggested in this work, it is possible to guarantee the security and adequate governance of personal information that surround the market development environment, for companies that do not have access to specialized consultancies.

Keywords: Information management. General Data Privacy Regulation (GDPR). Information Security. Factoring.

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

ANFAC	Associação Nacional das *Factorings*
ANPD	Autoridade Nacional de Proteção de Dados
CI	Ciência da Informação
CID	Confidencialidade, Integridade e Disponibilidade
CPF	Cadastro Pessoa Física
DPO	Data Protection officer
DSI	Departamente de Segurança da Informação
ECS	Empresa de Crédito Simples
GDPR	General Data Protection Regulation
GI	Gestão da Informação
LGPD	Lei Geral de Proteção de Dados
PME	Pequenas e Médias Empresas
RG	Registro Geral
RGPD	Regulamento Geral sobre Proteção de Dados da União Europeia
SI	Segurança da Informação
SINFAC	Sindicato das Sociedades de Fomento Mercantil
TI	Tecnologia da Informação

SUMÁRIO

1 INTRODUÇÃO

O acesso à informação foi acelerado devido ao avanço das tecnologias, especialmente após o surgimento da internet, que é utilizada por grande parte da população mundial. Foi exatamente por este movimento crescente, que observou-se a necessidade de criar algumas garantias e direitos relacionados aos dados pessoais ou dados sensíveis, relativos aos usuários/clientes, pois existe um desequilíbrio de poderes entre os possuidores de dados pessoais e os titulares destes dados.

O direito da personalidade, alicerçado no Código Civil Brasileiro e na Constituição Federal, batalham pela proteção deste direito, abarcando a privacidade como direito essencial à qualidade de vida das pessoas, frente às perspectivas individuais e coletivas (BRASIL, 1998).

É neste contexto que a Lei Geral de Proteção de Dados (LGPD), surge por meio de um movimento mundial que representa o esforço da sociedade para que se tenha maior segurança sobre as informações e privacidade dos dados (SÁ, 2019).

A LGPD é uma norma brasileira que regula, principalmente, questões ligadas ao tratamento de dados pessoais. De acordo como esta Lei, os dados pessoais são informações capazes de identificar alguém e a maneira como o tratamento destes dados é realizado, representam qualquer operação que os envolvem, desde sua coleta e uso, até seu armazenamento e transmissão.

Com base no Regulamento Geral sobre a Proteção de Dados RGPD da União Europeia, foi aprovada no Brasil no dia 14 de agosto de 2018 a Lei nº 13.709 que dispõe:

> Sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou 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, sem paginação).

A LGPD (Lei nº 13.709) foi fundamentada nos princípios de respeito à privacidade, liberdade de expressão, de informação, de comunicação e de opinião; não violação da intimidade, honra e imagem; livre iniciativa, livre concorrência e defesa do consumidor e, principalmente, os direitos humanos.

Com o objetivo de permitir que o cidadão possa ter maior controle sobre o tratamento de suas informações pessoais, LGPD estabelece uma série de regras

para empresas e organizações que atuam no Brasil. Desde o dia 18 de setembro de 2020 que estas normas entraram em vigor, e a partir deste momento, todos os usuários passam a ter o direito de saber como as organizações coletam, armazenam e utilizam seus dados pessoais.

As empresas deverão definir responsáveis pelo tratamento de dados pessoais, sendo essa pessoa ou grupo de pessoas responsáveis por responder às solicitações de ordem pessoal ou governamental (BRASIL, 2018).

Os responsáveis pelo tratamento de dados, junto com a empresa, deverão formular novas políticas para se adequarem à Lei estabelecendo novas condições para a organização em relação ao seu regimento de funcionamento, procedimentos, incluindo termos para reclamação e petição de titulares de dados, além de implementações de normas de segurança, padrões técnicos, obrigações específicas para os envolvidos no tratamento de dados, ações educativas para seus empregados e supervisão de riscos de negócios e outros aspectos relacionados ao tratamento de dados pessoais (BRASIL, 2018).

Diante de todo este contexto apresentado, é possível perceber que as empresas precisam estar preparadas para atender ao marco regulatório da LGPD brasileira, e que todas elas necessitam de consideráveis modificações nos seus processos internos de coleta e armazenamento de dados, além de profundas alterações na gestão de dados e nas questões segurança da informação.

Diante deste cenário, é importante que as empresas iniciem a adequação à LGPD e demonstrem compromisso em estabelecer medidas que visem atender às normas, visto que ela é aplicável a todos os setores da economia, incluindo o fomento mercantil, realizado pelas empresas de *factoring*.

O *factoring* está presente no cenário econômico/financeiro do Brasil, e vem ao longo dos anos, gradativamente aumentando sua importância dentro deste contexto. Parte dessa relevância pode ser explicada pelo fato de que o fomento comercial traz facilidade e agilidade para alavancar o capital de giro dessas empresas (SINDICATO DAS SOCIEDADES DE FOMENTO MERCANTIL, 2022).

De acordo com a Associação Nacional das *Factorings* (ANFAC), a atividade de fomento comercial atende a uma clientela composta em sua grande maioria formada por PME´S (Pequenas e Médias Empresas), que comumente enfrentam dificuldades, dentre as quais, escassez de recursos, tanto para financiar o giro dos negócios, como também, para promover o ajuste do seu fluxo de caixa.

As operações convencionais de *factoring*, foram as que mais se destacaram, dominando a maior parcela deste setor, como algo em torno de 200 mil empresas clientes, dos mais variados tamanhos e setores econômicos. Se bem estruturadas e analisadas, observando seus custos, vantagens e desvantagens, o *factoring* se mostra como um importante mecanismo de apoio às pequenas e médias empresas. (ASSOCIAÇÃO NACIONAL DAS *FACTORINGS*, 2022).

No aspecto socioeconômico, o fomento comercial viabilizou transações nas diversas etapas das cadeias produtivas industriais, comerciais, agronegócios e serviços, contribuindo na manutenção de mais de 5 milhões de empregos diretos e indiretos (ASSOCIAÇÃO NACIONAL DAS *FACTORINGS*, 2022).

Stabile (2012), explica que o contrato de *Factoring* é aquele em que um comerciante cede ao outro os créditos, na totalidade, ou em parte, de suas vendas a terceiros, recebendo o primeiro do segundo o montante destes créditos, mediante o pagamento de uma remuneração.

> Tal contrato se caracteriza, por tanto, pela cessão de créditos, mediante remuneração de um comerciante a uma empresa de *factoring*, sendo que esta assume os riscos pelo inadimplemento dos referidos créditos. Por ser um contrato de cessão de crédito, o *factoring* representa ainda, verdadeira alienação ou venda do faturamento. (ARRIERO, 1999, p.30).

Diante do que foi exposto até o momento, percebem-se os impactos positivos e a importância do setor de fomento comercial para o desenvolvimento econômico das PMES e consequentemente para a economia do país. Por ter uma parcela importante de participação, e com a realização e milhares de operações, fica claro, que durante o processo operacional, muitos dados e informações são trocados entre as empresas, e boa parte desses dados são sensíveis e acabam por incidir diretamente com o propósito da LGPD.

Com a informação ganhando cada vez mais importância dentro deste novo conceito de sociedade e de mercado cada vez mais competitivos, a Informação, assim como os Recursos de Informação ganharam importância nas organizações em seus mais variados contextos, com destaque para a adequação à LGPD, mostrando a necessidade de se tratar melhor e de forma mais eficaz esse tipo de recurso.

Recursos de informação são os produtos, fornecedores, manipuladores e distribuidores, inclusive os suportes de informação. Estão incluídas as bibliotecas, centros de informação, os sistemas de informação, bancos de dados de computador,

arquivos e registros de escritório, recortes de jornais, gravações de som e filmes, correspondências, mensagens e outros estoques informacionais e variados formatos de mídia. (HORTON, 1974 apud MARTINS, 2014).

Neste contexto, a Gestão da Informação encontra papel de destaque, e identifica o Gestor da Informação como tendo as habilidades necessárias para exercer as atividades relacionadas à competência informacional acerca do papel de técnicas informacionais e das novas tecnologias como ferramenta de auxílio ao processo de adequação à LGPD, mitigando as possíveis dificuldades encontradas durante este processo.

Entenda-se que, a gestão da informação cuida dos processos intermediários, executados entre a origem e o uso da informação: a coleta, a organização, o armazenamento, a recuperação, os produtos e serviços de informação, a disseminação, uso, os efeitos do uso na vida dos usuários, das organizações e da sociedade e, ainda, o comportamento em informação das pessoas. (LE COADIC, 2004; DAVENPORT; PRUSAK, 1998; CHOO, 1998 apud RODRIGUES; BLATTMANN, 2014).

Com o advento das novas tecnologias, dos meios de comunicação e um montante de informações geradas, cada vez maior, a consolidação de uma equipe multidisciplinar torna-se necessária para que haja a atuação de profissionais que tenham formação e capacidade para trabalhar com este tipo de recurso.

Neste contexto, o gestor da informação surge então como sujeito essencial para tornar mais eficaz a utilização dos recursos informacionais dentro do contexto de adequação às normas da LGPD, facilitando o caminho das organizações para atingir tal feito.

Desta forma, a valorização por parte das organizações, do gestor da informação, trabalhado em conjunto com os profissionais de outras áreas, pode garantir maior segurança e qualidade, na questão de tratamento de dados, com o intuito de adequar-se às regras da LGPD e assim evitar possíveis sanções previstas na Lei. É dentro desta realdade que o presente trabalho questiona: Como crirar um modelo de adequação à LGPD aplicável às *factorings* com suporte das técnicas e ferramentas da Gestão da Informação?

1.1 Objetivos

1.1.1 Objetivo geral

De acordo com o exposto até o momento, este trabalho tem como objetivo geral: Apresentar um modelo para o processo de adequação das empresas de *factoring* às regras da LGPD.

1.1.1 Objetivos específicos

a) Explorar conceitos sobre a LGPD e identificar os principais requisitos necessários de adequação à Lei com um olhar voltado para as empresas de *factoring*.

b) Identificar ferramentas e conceitos da Gestão da informação, que são necessários para adequação das empresas à LGPD;

1.2 Justificativa

Este trabalho pretende contribuir para ampliar o conhecimento sobre as discussões acerca da LGPD, e como suas diretrizes podem impactar diretamente no funcionamento de todas as organizações do país, com atenção especial para as pequenas e médias empresas, que podem encontrar maiores obstáculos neste processo de adequação. A LGPD já se encontra em vigor desde agosto de 2021, demonstrando a urgência em definir as ações necessárias para que estas empresas não venham a sofrer com as sansões previstas em Lei.

Segundo Donini (2004 apud WIENHAGE; SOUZA; TOLEDO FILHO, 2009), uma grande parte dos empregos gerados no país, são oriundos das pequenas e médias empresas que apesar de contribuir para o desenvolvimento econômico, apresentam algumas barreiras como limitações de recursos, para o giro e manutenção do seu empreendimento - que ocorre em grande parte, devido à falta de assistência dos órgãos fomentadores. Neste sentido, as *factorings* atuam como instrumento fundamental no suporte financeiro e administrativo dessas empresas.

Nos anos de 2018 e 2019, a Associação Nacional das *Factorings* (ANFAC), realizou um levantamento estatístico que apontou o valor do giro das operações

realizadas pelos seus associados, em suas distintas estruturas empresariais de *factoring*, fundos de investimentos em direitos creditórios, securitizadoras e Empresas de Créditos Simples (ECS), que foi algo em torno de R$150 bilhões anuais. (ASSOCIAÇÃO NACIONAL DAS *FACTORINGS*, 2022).

A ANFAC enfatiza a importância desse tipo de empresa, afirmando que só no ano de 2016, as *factoring* somavam um total de mais de 1.100 empresas no Brasil. (ASSOCIAÇÃO NACIONAL DAS *FACTORINGS*, 2022).

A abordagem da LGPD voltada para as *factorings* se justifica exatamente pela relevância que estas organizações têm para o crescimento de empresas brasileiras, e por ainda ser muito pouco conhecido e muitas vezes até confundido com agiotagem ou instituição financeira. Sendo o fomento mercantil uma opção de crédito, especialmente para pequenas e médias empresas, oferecendo um trabalho de parceria com seus clientes, deveria ser mais conhecido e até reconhecido por sua importância econômica, pois ainda existem muitos empresários que desconhecem todo o suporte que uma factoring pode oferecer.

O estudo sobre o factoring torna-se importante, de acordo com Amaral (2000 apud STABILE, 2012), pelo fato das empresas de faturização se distinguirem das instituições financeiras porque estas não realizam operações especulativas e sim operações de crédito, enquanto as empresas de faturização realizam operações de risco. Esta questão ainda não é de conhecimento geral para muitos pequenos e médios empresários e seu entendimento teria maior esclarecimento no instante em que estes empreendedores estão em busca de capital de giro para suas empresas.

Este trabalho pode vir a servir como mais um meio, em que empresas de pequeno e médio porte, especialmente as factorings, possam encontrar caminhos e guias de como utilizar a gestão da informação como ferramenta para se adequar às exigências da LGPD.

2 REFERENCIAL TEÓRICO

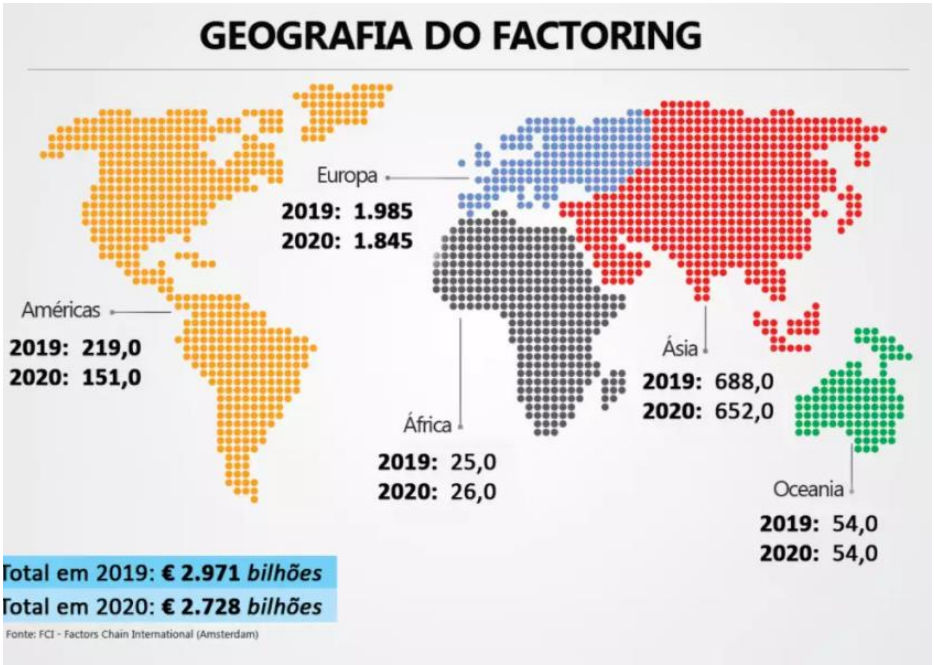
2.1 A atividade de *Factoring*

De acordo com Leite (2004), a atividade de fomento mercantil ou *factoring*, é descrita como uma atividade comercial que estabelece uma prestação de serviços contínua, envolvendo a compra de créditos oriundas das empresas-clientes, referente às suas vendas mercantis ou de prestação de serviços, realizadas à prazo.

Dentro do contexto brasileiro, segundo Wolf (2008), o *factoring* se apresenta como um mecanismo da iniciativa privada, que independente do governo, mira na contribuição para o desenvolvimento econômico, modernização do parque industrial, aumento da produção e geração de empregos de forma direta e indireta.

Na imagem a seguir, disponibilizada pela ANFAC, podemos observar a importância desta atividade não apenas no Brasil, como no mundo, o que enfatiza a sua relevância no mercado mundial.

Figura 1 – A Geografia do Factoring



Fonte: Associação Nacional das Factorings (2022).

Apesar de ser uma palavra inglesa, tem sua origem no latim, do verbo *facere* (fazer), de onde é proveniente o substantivo *factor* (caso normativo), factoris (caso genitivo), com o significado de aquele que faz, e que para os romanos representava

um agente comercial, ou intermediário de comerciantes nas trocas de produtos em locais afastados ou distantes. Já o sufixo *ing* deriva do inglês. Acoplado a factor, significa "fazendo" ou "agindo" (RIZZARDO, 1997 apud STABILE, 2012).

O termo *factoring*, cuja tradução para "faturização" foi proposta por Fábio K. Comparado, e que passou a ser adotada pela doutrina brasileira, vem significando basicamente, a operação já descrita (BULGARELLI, 1998).

Leite (2011) explica que a necessidade de desenvolvimento do comércio estimulou os comerciantes a buscar por mecanismos que possibilitassem a venda de suas mercadorias para outros mercados, o que está ligado às origens do *factoring* com as atividades mercantis. Ainda de acordo com o autor, a venda de mercadorias ou ativos tem como finalidade obter os recursos necessários para o comerciante e também para que se possa girar seus negócios posteriormente.

Há certa dificuldade envolvendo a origem precisa das práticas do *factoring*, assim como o período exato da história em que se deu o início da atividade, mas Leite (2011), remonta sua origem à cultura neo-babilônica e do "Código de Hamurabi", há aproximadamente 2000 a.c., em uma atividade onde comissários garantiam a comitentes, a cobrança dos créditos a que estes teriam direito, sendo cobrado sobre o serviço, uma taxa: a comissão.

A atividade de *factoring* foi desenvolvida há alguns séculos para auxiliar os produtores a trocar suas mercadorias em lugares geograficamente distantes, sendo que agregou características financeiras com o surgimento da moeda. Alguns anos depois, surgiu a venda de créditos originados pela venda dos bens, pelos produtores ou fornecedores, que por meio dos *factors* adquiriam o direito de cobrá-los como seus legítimos proprietários (LEITE, 2011).

De acordo com a ANFAC, a história do *factoring* remete a figura do "factor", que surge no Império Romano e foi utilizado no século XVIII, no período de colonização inglesa, para representar na América os interesses da metrópole Londres. Ou seja, visava desenvolver a economia local da colônia, priorizando a nascente indústria têxtil e o comércio doméstico. Os comerciantes locais incubiam a alguns de seus agentes, os *factors*, a obrigação de guarda e venda de suas mercadorias.

A disseminação do *factoring* ocorreu com o comércio de têxteis exportados pela Inglaterra para sua colônia americana. Devido a dificuldade da distância, os comerciante ingleses tomaram como prática comum a intercessão de agentes na

qual transportavam e vendiam seus produtos na América (ROCHA, 2000).

> O sistema apresentava características especiais nos Estados Unidos, ainda colônia inglesa, onde os factors não apenas administravam os estoques de produtos (principalmente têxteis, roupas e outras mercadorias) para os seus proprietários na Europa e os vendiam, mas também garantiam o pagamento como agentes del credere. Com o tempo, os factors prosperaram, passaram a pagar a vista aos seus fornecedores o valor das vendas por estes efetuadas, antes mesmo de os compradores fazê-lo. O factor, a par dos serviços prestados, substituiu o comprador, pagando a vista ao fornecedor, melhorando o padrão de crédito e efetuando a cobrança junto ao comprador final daquela mercadoria. (LEITE, 1994 apud ROCHA, 2000, p.3).

O *factoring* como se pratica na atualidade se caracterizou no século XVI na Inglaterra, e junto com o desenvolvimento do Novo Mundo foi levado aos Estados Unidos ainda como colônia dos ingleses:

> Durante os séculos XVII e XVIII, o factoring adquiriu grande importância na América anglo-saxônica, onde os factors representavam e trabalhavam para interesses britânicos, recebendo e distribuindo as mercadorias importadas, efetuando as cobranças das mesmas e ainda efetuando antecipação ou adiantamento aos exportadores ingleses (DONINI, 2002, apud WIENHAGE; SOUZA; TOLEDO FILHO, 2009, p.14).

De acordo com Rizzardo (2004), a primeira *factoring* foi constituída nos Estados Unidos em 1808. Na primeira metade do século XX, segundo Donini (2002 apud WIENHAGE; SOUZA; TOLEDO FILHO, 2009), as atividades de fomento estavam atuando exclusivamente com as manufaturas de algodão e de lã, atingindo seu ponto mais alto em conexão com as indústrias têxteis americanas. O autor explica ainda que, foi em torno dos anos 60, quando o comércio entrou em uma nova fase de normalidade e que os grandes bancos americanos irromperam na atividade do *factoring*, que se registrou sua introdução nos países da Europa industrializada.

No Brasil, de acordo com a ANFAC, a atividade de fomento comercial começou a ser desenvolvida a partir de 11 de fevereiro de 1982, quando foi criada a Associação Nacional das *Factorings* (ANFAC), tendo seu reconhecimento legal em 1988, pela circular 1359 do Banco Central, definindo sua atividade como sendo de natureza mercantil.

Assim, surgiu o sentido moderno do *factoring*, ou seja, com a venda dos créditos oriundos da venda dos bens, pelos produtores ou fornecedores, os *factors* adquirem o direito de cobrá-los, como seus legítimos proprietários. O *factor*, que no seu sentido primitivo prestava serviços de comercialização, distribuição e

administração, agregou a função de fornecedor de recursos (LEITE, 2011).

Constata-se então que, a definição de *factoring* se transformou de um simples contrato de custódia de mercadorias, com objetivo de comercialização, para uma abordagem mais ampla, oferecendo também serviços de gestão de crédito, administração de contas, seleção de riscos, análise de clientes, assessoria contábil e cobrança de dívidas, além de compra de créditos das vendas mercantis.

Em acordo com tudo que foi exposto, pode-se considerar que empresas de *factoring*, especialmente as que seguem as diretrizes da ANFAC, lidam com dados pessoais em seu cotidiano, uma vez que é comum o trabalho com avalistas, empresas sacadas, em que muitos deles atuam também como pessoas físicas. Desta forma, podemos considerar que as empresas que trabalham com fomento mercantil, são controladoras de dados, ou seja, elas que decidem sobre o tratamento, e para que fins serão utilizados os dados pessoais que coletam, e por isso a LGPD é aplicável a estas empresas.

2.2 Lei Geral de Proteção de Dados (LGPD)

Diante do avanço da tecnologia e sua presença cada vez mais marcante na vida das pessoas, o fluxo de dados circulando pelas redes tomaram grandes proporções. Nos últimos vinte anos, ao redor do mundo, o número de usuários com acesso à internet e a quantidade de informações disponíveis nas redes aumentaram de forma exponencial.

O contexto, então, sinaliza que se vive uma era de expansão informacional complexa, veloz, volumosa e variada, como propões o conceito de Big Data, que diz respeito ao conjunto de dados que precisam ser geridos com a devida atenção ao seu processamento, armazenamento e segurança. Isto vai de encontro ao que se prevê para a boa gestão da informação e do conhecimento (OLIVEIRA; PANISSET; SILVA, 2019).

Essas informações parecem ser acertadas quando percebe-se que no mercado atual, dados impulsionam cada vez mais os negócios, desde os gigantes da indústria até as pequenas empresas do varejo e serviços, atingindo, inevitavelmente o setor de fomento mercantil.

Amorim e Tomáel (2011, p. 2), ratificam essa compreensão, ao afirmarem que "na sociedade contemporânea, a informação e o conhecimento estão sendo

considerados fundamentais para as organizações que se encontram em ambiente ambíguos e de extrema incerteza".

De acordo com matéria do canal G1, a BBC News em 20 de março de 2018 noticiou que desde o escândalo mundial que veio a tona envolvendo a empresa Cambridge Analytica, acusada de extrair milhões de dados de seus usuários sem a devida autorização de seus proprietários - o debate sobre o uso de dados pessoais no mundo foi aprofundado. Esta mesma empresa foi acusada também de utilizar dados pessoais para influenciar resultados de processos eleitorais do Brexit e também a eleição norte-americana de 2016. (ENTENDA.., 2018).

Outros escândalos em torno dos vazamentos de dados por empresas como *Facebook, Netshoes e Uber*, também acabaram expondo dados pessoais como nomes, endereços, números de cartões de crédito, e colocaram em evidência os efeitos devastadores que a falta de rigor com a segurança no tratamento de dados pessoais podem causar. Identificou-se então uma grande necessidade de adotar mecanismos eficazes para minimizar os riscos de possíveis vazamentos e assim garantir a segurança dos dados armazenados (FERNANDES, 2019).

Com estes tipos de eventos criminosos ocorrendo pelo mundo, onde dados pessoais são utilizados sem o devido consentimento de seus donos, os países democráticos passam a se preocupar com questões que ultrapassam somente o lucro, mas que podem inclusive ferir a soberania das nações.

De acordo com Rapôso et al. (2019), na Europa após os relatórios de espionagem e violação de dados de clientes envolvendo a Cambridge Analytica e o Facebook, deu-se início a discussões sobre a regulamentação para tratar de segurança de dados. Foram essas regulamentações que acabaram por inspirar a formulação do Regulamento Geral de Proteção de Dados (RGPD) que regulamenta a união Europeia e impôs medidas para aprovar a legislação sobre a segurança de dados pessoais.

No Brasil também ocorreram alguns escândalos sobre a venda ilegal de dados. O jornal Correio Brasiliense, em 16 de julho de 2018, publicou a seguinte manchete: "Dados pessoais de brasileiros são negociados livremente na internet - enquanto o Legislativo e o Executivo discutem proteção de dados pessoais, informações de milhares de brasileiros são negociados ilegalmente na internet, a preços irrisórios" (SOUZA, 2018, sem paginação).

Inspirada pela RGPD foi criada no Brasil a Lei Geral de Proteção de Dados

(LGPD), surgindo então um novo paradigma, que envolve a alteração da maneira como as empresas passam a ter que lidar com dados pessoais de pessoas físicas nos meios online e *offline* e passam a ter a função de proteger os direitos fundamentais de liberdade e privacidade em qualquer relacionamento que venha a envolver a utilização de dados pessoais (SÁ, 2019).

Neste sentido, o Brasil, no ano de 2018, publicou a sua Lei Geral de Proteção de Dados (LGPD), outros países também caminham no mesmo sentido da proteção dos dados pessoais dos indivíduos e publicaram suas legislações, com a União Europeia (de onde o Brasil se inspirou para produzir a sua Lei), Estados Unidos e México. (OLIVEIRA; PANISSET; SILVA, 2019).

Para entender o que é a LGPD, em seu art. 1º encontra-se a sua definição:

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

A LGPD está fundamentada nos direitos fundamentais de liberdade e de privacidade, como livre iniciativa e o desenvolvimento econômico e tecnológico do país, de acordo com o artº 2 da Lei 13.709, de 14 de agosto de 2018.

Percebe-se então que, no contexto atual de mercado e sociedade, a importância atribuída pelo direito brasileiro aos dados pessoais pode ser equiparada ao do direito fundamental. Como o próprio dispositivo indica, o principal objetivo da Lei é regulamentar a forma com que os dados pessoais são tratados (operacionalizados), para assegurar que os titulares (donos dos dados) tenham sua privacidade respeitada.

A LGPD é o instrumento normativo que disciplina a proteção e o tratamento de dados pessoais no Brasil e entrou em vigor desde 14 de agosto de 2020. O tratamento de dados pessoais com a o qual a LGPD se envolve, de acordo com o seu artigo 5°, refere-se a:

> [...] toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (BRASIL, 2018, sem paginação).

Anteriormente a LGPD, o Brasil já possuía algumas diretrizes e Leis que tratam a respeito da proteção e privacidade de dados – como o marco civil da

internet, código civil do consumidor e Lei Carolina Dieckman. Todas essas Leis e regulamentos, acabava por criar um cenário com diversas legislações atuando simultaneamente, gerando uma estrutura legal complexa. A LGPD vem para substituir esse cenário multicomplexo, com diversas Leis, e traz uma regulamentação específica para o adequado uso, proteção e transferência de dados pessoais no Brasil (PONTICELLI, 2018).

A LGPD altera o Marco Civil da Internet no Brasil, que agora inclui o termo privacidade em seu sistema legal (SÁ, 2019).

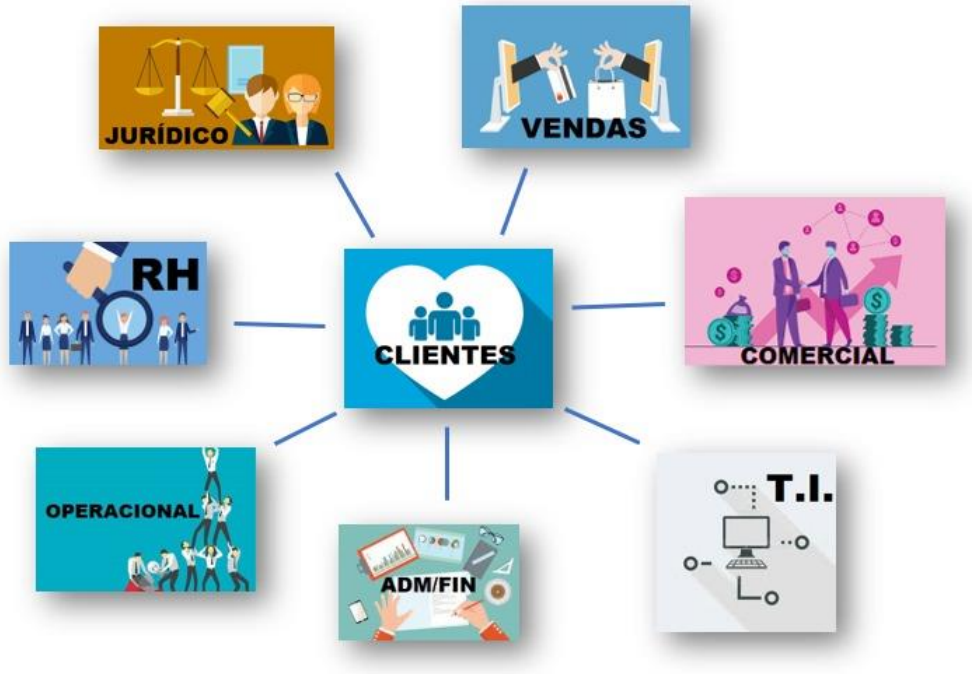
A LGPD foi sancionada pelo ex-presidente Michel Temer, e está em vigência desde o dia 16 de agosto de 2020, com o objetivo de regular as atividades referentes ao tratamento dos dados pessoais no Brasil.

Dados todos os casos de vazamentos apresentados e os consideráveis aumentos de concorrência entre empresas. Raposô (2019) apontou a importância das empresas ajustarem suas tecnologias de modo a se adequar à LGPD, e consequentemente garantir aos seus clientes/usuários a plena consciência sobre a forma que seus dados estão sendo coletados, armazenados e utilizados.

Percebe-se que toda empresa deve sim, adequar-se à LGPD, mesmo que não atue com dados sensíveis, não atenda diretamente pessoas físicas, nem seja do ramo tecnológico. A Lei aplica-se ao tratamento de qualquer dado pessoal, mesmo que seja apenas um e-mail, endereço ou CPF, de qualquer pessoa física, mesmo que ela represente uma empresa. Então, se uma instituição capta, armazena e compartilha dados pessoais, ela deve se adequar à LGPD, e isso inclui o ramo de atividade das *factorings.*

A LGPD veio para mudar de forma significativa a cultura no tratamento de dados de pessoais e, consequentemente, na maneira como as empresas coletam, armazenam e compartilham dados pessoais de seus clientes e colaboradores. Na Figura 2, apresentada abaixo, é possível ver todas as áreas de uma empresa que são afetadas pela nova legislação em questão:

Figura 2 – Áreas de uma empresa afetadas pela LGPD

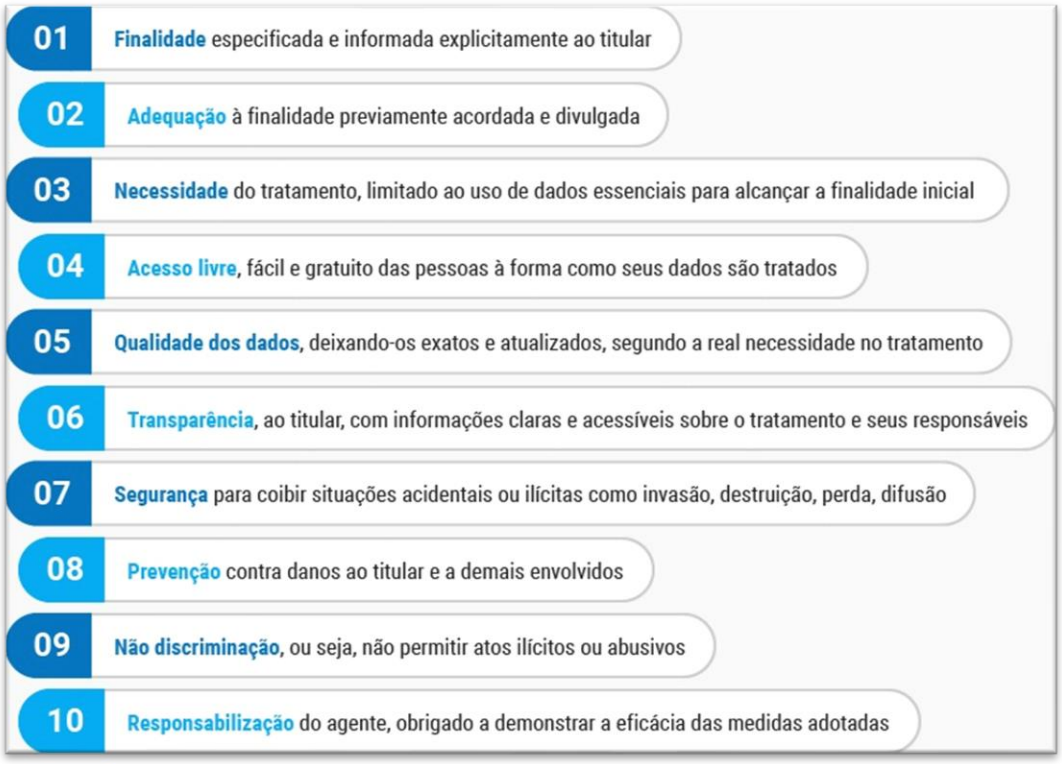


Fonte: Elaborado pelo autor (2022).

Como forma de garantir os direitos dos titulares de dados pessoais, a LGPD baseia-se em alguns princípios que a norteiam, todos eles previstos no art. 6º e os quais, quando bem compreendidos podem auxiliar a entender os direitos e deveres dos titulares de dados.

O art. 6º da LGPD traz em sua composição 10 princípios apresentados na Figura 3, a seguir:

Figura 3 – Príncipios da LGPD



Fonte: Serviço Federal de Processamento de Dados (2022a).

Outro ponto abordado pela Lei importante de ser compreendido é sobre o que deve ser considerado um dado pessoal. Segundo a LGPD, dado pessoal é toda “informação relacionada à pessoa natural identificada ou identificável”, ou seja, sempre que a informação que se tenha permitir identificar uma pessoa (vale lembrar que se trata de pessoa natural, ou seja, pessoa física), essa informação é um dado pessoal (BRASIL, 2018).

Alguns dados pessoais são facilmente identificados, como o nome de alguém, o CPF e o RG – e alguns outros são identificados em decorrência de sua relação direta com o titular, como endereços, e-mails, números de telefone, endereços IP, dados de consumo, entre outros. Não existe uma lista específica e objetiva – na prática, todo dado que, isoladamente ou em conjunto com outras informações, direta ou indiretamente, possa levar a identificação de alguém, será considerado um dado pessoal. (SERVIÇO FEDERAL DE PROCESSAMENTO DE DADOS, 2022b).

Assim, podem também ser considerados dados pessoais uma foto, um vídeo, a placa de um veículo, um número de matrícula, ou até mesmo os dados bancários de um titular.

Visando explicar quem são os responsáveis pelo tratamento destes dados, a

Lei 13.709, de 14 de agosto de 2018, traz em art. 5º, inciso VIII, a definição do que ela chama de “agente de tratamento” – aqueles atuantes nas operações de tratamento de dados pessoais, classificados em dois atores: o Controlador e o Operador (BRASIL, 2018).

Ainda de acordo com o art. 5º da LGPD, seus incisos VI e VII trazem as definições sobre controlador e operador:

> [...] VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais; VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador (BRASIL, 2018, sem paginação).

Ou seja, o controlador é o responsável pela tomada de decisões relativas ao tratamento de dados pessoais, como quando realiza-la, o porquê de fazê-lo, mantê-los ou exclui-los e ainda por determinar o destino dos dados em todo o seu ciclo de vida. É o exemplo de uma *factoring* que coleta dados de seus clientes em um cadastro, ou até mesmo para emissão de uma nota fiscal.

Já o operador é aquele que é contratado pelo controlador e atua no tratamento de dados em nome e por conta deste. É normalmente, alguém subcontratado para executar uma função, um papel ou uma atividade de tratamento de dados pessoais em razão de sua especificidade, formação ou expertise. Um exemplo de operadores podem ser escritórios de contabilidade ou de advocacia, que em suas relações com pessoas jurídicas apenas executam as diretrizes impostas pelo controlador.

A LGPD deixa evidente que o controlador é o principal decisor e possuidor do maior poder de controle sobre as finalidades, ações, processos e procedimentos utilizados para o tratamento de dados pessoais. Cabe também ao Controlador as responsabilidades em relação aos dados em tratamento sob sua supervisão e de quaisquer violações da LGPD durante este processo.

Além de representar uma figura central na proteção dos direitos dos titulares de dados pessoais, os agentes precisam observar a legislação para garantir que as ações de tratamento são realizadas por outros agentes sejam conformes o que é estabelecido pela Lei.

A LGPD prevê, em seu artigo 37º que o controlador tem o dever de elaborar relatórios de impacto à proteção de dados pessoais e a nomeação de um encarregado pelo tratamento, este que irá atuar como uma ponte de comunicação

entre o controlador e a Autoridade Nacional e entre controlador e os titulares dos dados pessoais sob seu tratamento.

Mesmo que o exercício da função de operador se restrinja em atuar em nome de seu controlador e de acordo como o que é decidido por ele, é comum que lhe seja concedido certo grau de discricionariedade e liberdade sobre o processo de tratamento dos dados. Desta maneira, o operador tem o direito de exercer um determinado controle sobre as ações de tratamento e tem a permissão de decidir a maneira que os dados serão tratados. Isso condiz aos aspectos técnicos relativos à forma que um serviço de tratamento será prestado.

Outro ator destacado pela Lei, descrito no art. 5º, inciso VIII, é o encarregado de dados, que é a pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). (BRASIL, 2018).

O encarregado de dados, também conhecido como Data Protection Officer (DPO), é o profissional indicado pelo controlados e será o responsável de cuidar de todas questões referentes à proteção dos dados dentro da empresa.

É possível que o encarregado seja um empregado da corporação (pessoa natural) ou um terceiro prestador de serviços (pessoa física ou jurídica). Além disso, apesar da LGPD não trazer exigências específicas quanto a qualificação desse profissional, é sugerido que este de preferência, agregue profundos conhecimentos de Tecnologia da Informação (TI) e bases sólidas sobre direito regulatório.

Sua identidade e as informações de contato devem estar divulgadas publicamente de forma clara e objetiva, preferencialmente no endereço eletrônico do controlador e obrigatoriamente na política de privacidade. Suas funções são devidamente descritas na LGPD, no art. 41, parágrafo 2º, incisos I a IV, que são:

> I - Aceitar reclamações e comunicações dos titulares de dados, prestar esclarecimentos e adotar providências; II - Receber as comunicações da ANPD e adotar providências; (vale ressaltar que ele também deverá responder aos demais órgãos de fiscalização); III - Orientar os funcionários e os contratados da entidade a respeito das boas práticas a serem tomadas em relação à proteção e dados pessoais; IV - Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares. (BRASIL, 2018, sem paginação).

O compartilhamento de dados pessoais sob a guarda do Controlador pode ocorrer desde que observados os deveres de informação e de transparência em relação ao titular dos dados pessoais. Para que esse compartilhamento seja

legítimo, é necessário que o titular de dados seja previamente comunicado acerca da possibilidade de compartilhamento, bem como de sua finalidade – ou seja, que se outorgue o consentimento claro, específico e destacado para tal fim – conforme os termos do 5º ou 7º art. da LGPD. Com a LGPD, todas as organizações brasileiras, independente de seu porte, devem investir em segurança tecnológica para impedir violações de dados pessoais.

É necessário que se observe os requisitos de segurança da informação para a realização operacional do compartilhamento, de modo que as boas práticas e os controles relevantes para o tratamento dos dados pessoais estejam assegurados, em especial garantindo uma transmissão segura entre emissor e receptor.

A maneira para legitimar o tratamento de dados é através das bases legais, que são as condições que autorizam o tratamento de dados pessoais pela LGPD. Importante destacar que a forma de interpretar a regulamentação é analisar se naquele fluxo específico para aquela determinada finalidade é possível enquadrar o tratamento em uma das bases legais previstas na Lei.

Os direitos dos titulares de dados estão todos previstos nos artigos 8º, 9º e 18º da LGPD e podem ser solicitados ao controlador a qualquer tempo, mediante requisição. São eles:

> I – Confirmação da existência de tratamento; II – Acesso aos dados; III – Correção da existência de tratamento; IV – Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na Lei. V – Portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação legal da autoridade nacional; VI – Eliminação dos dados pessoais tratados com o consentimento do titular, exceto em hipóteses previstas na Lei; VII – Informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; VIII – Informação sobre a possibilidade de não oferecer consentimento e sobre as consequências da negativa; IX – Revogação do consentimento, nos termos previstos na Lei (BRASIL, 2018, sem paginação).

Percebe-se então que o compartilhamento de dados sob a guarda do controlador é possível, desde que observados os deveres de informação e de transparência em relação ao titular de dados pessoais.

De acordo com a LGPD, em seu art. 7º apresentam-se as bases legais para o tratamento de dados pessoais, que são condições que autorizam o tratamento desses dados. São elas:

> I - Quando o titular autorizar expressamente o consentimento, sendo importante registrar e manter a sua devida concessão; II. Para a elaboração

> ou cumprimento de um contrato junto ao titular de dados; III - Para utilização em um possível processo judicial, administrativo ou arbitral; IV - Para o cumprimento de obrigações legais ou regulatórias; V - Para finalidades de proteção ao crédito; VI - Para a realização de estudos por órgãos de pesquisa, garantida sempre que possível a anonimização dos dados pessoais; VII - Para a proteção da integridade física do titular dos dados ou de outra pessoa; VIII -Quando em atendimento de serviços de saúde; IX -Quando necessários com base no legítimo interesse do controlador ou mesmo de um terceiro. (BRASIL, 2018, sem paginação).

Vale destacar que a maneira de interpretar a regulamentação é analisar se no fluxo de dados envolvido para uma determinada finalidade é possível de se enquadrar em uma das bases previstas na Lei.

Em seus artigos 49º ao 51º a LGPD traz explicações sobre como devem ser a estruturação dos sistemas de tratamento de dados:

> Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares. (BRASIL, 2018, sem paginação).

Com a promulgação da LGPD e a então necessidade de sua fiscalização, foi criada a Autoridade Nacional de Proteção de Dados (ANPD), sendo sua competência estabelecida pelo art. 55º, com suas principais funções sendo o zelo pela aplicação da Lei, fiscalização, comunicação com os controladores e fixação de sanções caso sejam verificadas irregularidades. (BRASIL, 2018).

Boas práticas de governança visam disseminar e promover a multiplicação do conhecimento entre controladores e todos os envolvidos com o objetivo de mitigar os riscos e trazer clareza nas informações dadas aos titulares de dados. Um alto nível de documentação facilita a prestação de informações para a ANPD e órgãos fiscalizadores (BRASIL, 2018).

Se mesmo seguindo todas as normas e boas práticas exigidas pela LGPD, caso ocorra algum incidente com risco ou dano relevante ao titular de dados, a empresa deve imediatamente: acionar o encarregado de dados (DPO) e o comitê de segurança; registrar de maneira detalhada a natureza dos dados afetados e indicar o que está sendo feito para reverter ou amenizar os efeitos; informar todos os riscos envolvidos a todos os titulares envolvidos no incidente; indicar as medidas técnicas e de segurança utilizadas na proteção de dados; e após todo o levantamento, documentos tudo no relatório de incidente de dados, e se for necessário, reportar a ANPD (BRASIL, 2018).

Por ser um órgão da administração pública federal, a ANPD é dotada de

autonomia técnica e decisória. Então em caso de vazamento a LGPD prevê, desde agosto de 2021, algumas sanções, dispostas em seu art. 52º, aplicáveis pelo órgão regulatório:

> I - Advertência, com a indicação de prazo para adoção de medidas corretivas; II - Multa simples de até 2% do faturamento limitada a 50 milhões de reais por infração; III - Multa diária, observado o limite total a que se refere o inciso anterior; IV - Publicidade da infração, após apuração e confirmação; V - Bloqueio dos dados pessoais a que ser refere a infração até sua regularização; VI - Eliminação dos dados pessoais a que se refere a infração. (BRASIL, 2018, sem paginação).

Todas as sanções mencionadas só serão aplicadas após procedimento administrativo que assegure a ampla defesa do acusado. Desta maneira, serão consideradas as particularidades de cada caso em específico, assim, a Lei traz alguns parâmetros e critérios para avaliação daquilo que será aplicado no caso concreto, tais como: a gravidade e a natureza das infrações e dos direitos pessoais afetados, boa-fé, reincidência, o grau de danos causados, cooperação do infrator, condição econômica, vantagem auferida ou pretendida pelo infrator, adoção de política de boas práticas e governança, adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, adoção de medidas corretivas e a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

Importante destacar que algumas das penalidades acima podem inviabilizar a continuidade do negócio.

Percebe-se então a necessidade da devida adequação da empresa à LGPD, de maneira a garantir proteção, organização e maior gerenciamento dos dados pessoais – além de garantir segurança para seus clientes, funcionários e colaboradores.

Neste contexto, a Gestão da Informação (GI) apresenta-se como uma ferramenta importante para tornar mais eficaz a utilização dos recursos informacionais e garantir mais segurança e qualidade no tratamento de dados realizados dentro das organizações, e assim minimizar a ocorrência de possíveis sanções previstas na LGPD.

Na seção a seguir, serão apresentados os fundamentos teóricos que validam a GI como um importante e essencial ator dentro de um processo de adequação de uma empresa à LGPD.

2.3 Gestão da Informação

Com a informação ganhando cada vez mais importância dentro deste novo conceito de sociedade e de mercado cada vez mais competitivos e regulamentados. Os recursos informacionais ganharam destaque nas organizações em seus mais variados contextos, com destaque para adequação à LGPD, observando a necessidade de tratar melhor e de forma mais eficaz esse tipo de recurso.

Como apresentado por Porém, Santos e Belluzzo (2012, p.187) a gestão da informação pode ser explicada como um "conjunto de conceitos, princípios, métodos e técnicas utilizados na prática administrativa e colocados em execução pela liderança de uma organização para atingir a missão e objetivos fixados".

A informação não é apenas um conjunto de dados que se encaixam em certo contexto. Do ponto de vista da crescente interação social, as organizações tendem a perceber a informação como um ativo, este devendo ser armazenado e compartilhado, trabalhado e gerenciado, sendo uma fonte confiável e estruturada e que possa ser consultada nas tomadas de decisão e auxiliar nos ambientes de incertezas (BRAGA, 2000).

Sobre os pontos analisados Drucker (1993 apud BRAGA, 2000, p. 2) assume defender o:

> [...] primado da informação como a base para um novo tipo de gestão, em que em curto prazo se perspectiva a troca do binômio capital/trabalho pelo binômio informação/conhecimento como fatores determinantes no sucesso empresarial.

Ainda neste sentido, Porém, Santos e Belluzzo (2012) estabelecem uma relação entre as novas tecnologias e o trato com as informações geradas, assim dizendo que:

> A informação é considerada, a cada dia, um recurso estratégico e de valor agregado para a percepção e absorção de novas tecnologias. Portanto, a tecnologia e a informação são afetadas e impactadas ao mesmo tempo, e processos provenientes delas tendem a se tornar mais dinâmicos. A gestão da informação procura justamente alinhar esses processos por meio de um conjunto de atividades e padrões que os estruturem em uma dinâmica inteligente para a geração do conhecimento. (PORÉM, SANTOS E BELLUZZO, 2012, p.15).

Outro aspecto importante da gestão da informação é a cultura da informação. A gestão e os fluxos de informação se desenvolvem e sofrem interferência em conformidade ao ambiente em que se encontram. E a liderança organizacional

interfere nesta cultura, que influência nos fluxos de informação. Tais fluxos informacionais se estabelecem como canais: tangíveis ou intangíveis; formais ou informais; permanentes ou esporádicos; constantes ou intermitente (RODRIGUES; BLATTMANN, 2014).

De acordo com Barbosa, Sepulveda e Costa (2009), a obtenção e uso da informação são fatores de transformações sociais e econômicas. Os autores defendem a necessidade de uma perspectiva integradora da gestão da informação e do conhecimento nos ambientes organizacionais. Contribuindo, assim, para a competitividade dessa organização.

> Pacheco e Valentim (2010), explicam que as empresas precisam atentar para a importância da informação e do conhecimento como um recurso gerencial estratégico, a partir do reconhecimento das fontes de informação. Molina (2010) corrobora e percebe a informação como insumo para inovação da competitividade, e expõe a necessidade da realização da gestão da informação útil e seu uso de forma estratégica, afirmando ser o homem o "recurso" mais importante nesse processo. (RODRIGUES; BLATTMANN, 2014, p.8).

Vital, Floriani e Varvakis (2010 apud RODRIGUES; BLATTMANN, 2014), em um resgate da literatura na área de gestão da informação, fazem inferências, das quais se destacam que o gerenciamento da informação em organizações passa por um processo contínuo de etapas estruturadas, organizadas e sistematizadas (fluxo de informação), com pessoas atuantes no processo e responsáveis por tal gestão, além do uso otimizado das fontes de informação.

Esse gerenciamento realiza-se por meio do mapeamento dos fluxos, tornando-se possível reconhecer as etapas pelas quais as informações perpassam e verificar os aspectos falhos do processo. É preciso conhecer as necessidades de uso e os usuários da informação para mapear as fontes de informações pertinentes ao contexto.

No que diz respeito aos objetivos da Gestão da Informação, Tarapanoff (2001) explica que o alvo é detectar e intensificar os recursos informacionais de uma organização e sua capacidade de informação. E ainda ensiná-la a aprender e adaptar-se às mudanças ambientais.

No que se refere às ações, Valentim (2002) explica que a GI atua no conhecimento explícito, ou seja, aquele que está materializado em algum suporte ou veículo de comunicação, tangível e formal. Esse processo dialógico em que o conhecimento explícito se torna uma informação permite que sua gestão se torne

possível, pois é passível de gerenciar sua organização, armazenamento e disseminação, facilitando o uso por meio de produtos e serviços.

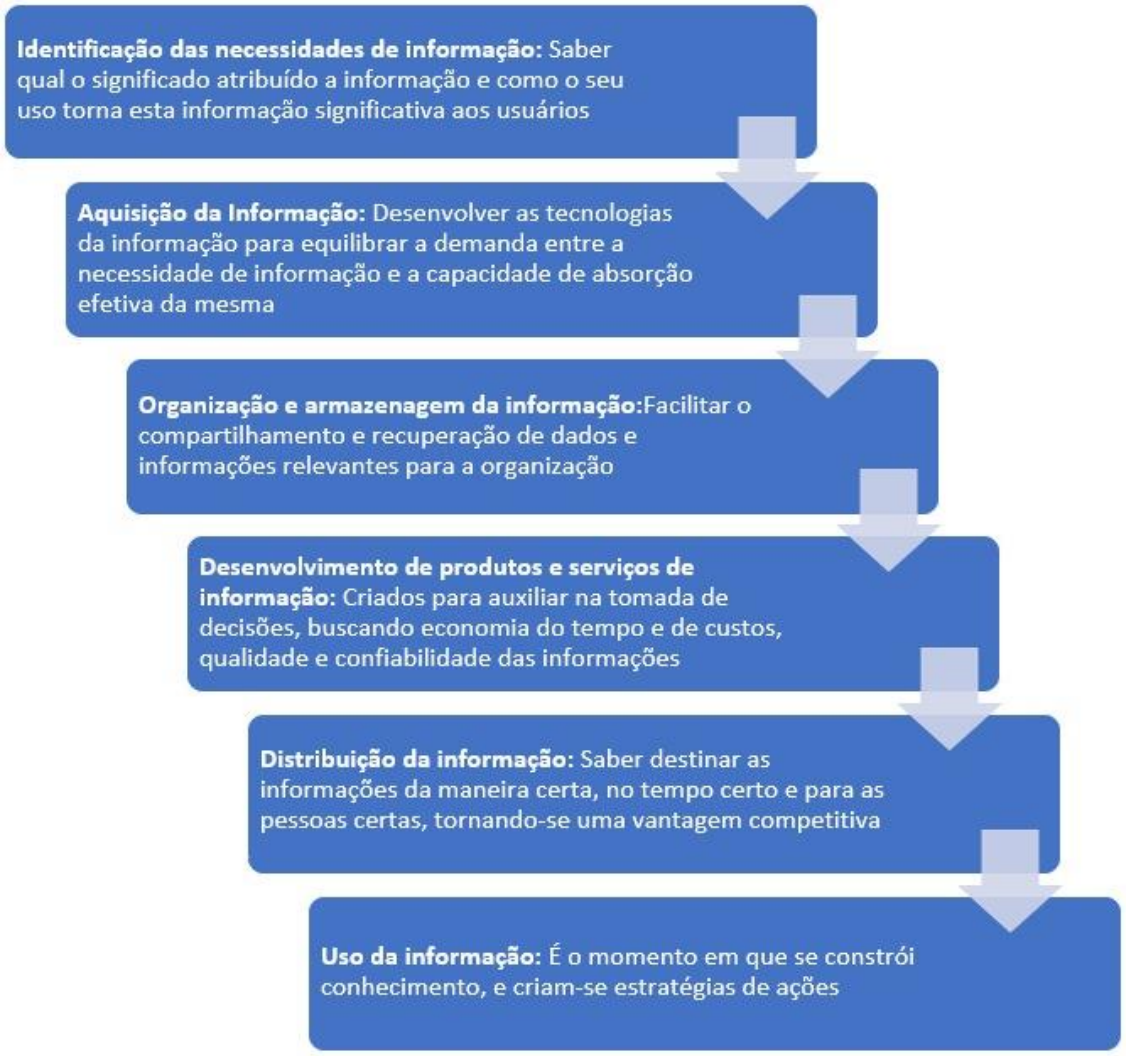
Apresentando os pressupostos de Davenport e Prusak (2003), podemos destacar as etapas trazidas por ele para a GI. De acordo com os autores, são quatro etapas a seguir: "determinação das exigências informacionais, obtenção da informação, distribuição da informação e utilização da informação". No entanto, destacam que se pode definir o processo de GI de diferentes maneiras.

A Gestão da Informação, nas ideias defendidas pelo professor Chun Wei Choo (2003), é retratada por meio de um modelo em etapas. Para que uma gestão da informação seja eficiente é preciso garantir a execução de seis atividades processuais e interdependentes, apresentadas a seguir: identificação das necessidades de informação, aquisição da informação, organização e armazenagem da informação, desenvolvimento de produtos e serviços de informação, distribuição da informação e uso da informação.

O modelo de Choo contempla a presença do comportamento adaptativo, que não se faz explícito em Davenport e Prusak (2003), mas que é pertinente no que se refere a identificação e a correção de eventuais falhas, importante para o aprimoramento dos serviços prestados.

É neste sentido que apresenta-se, na Figura 4, as etapas do ciclo informacional de Choo.

Figura 4 – Etapas do Ciclo informacional



Fonte: Adaptação de Choo (2003).

Cada atividade descrita assume um papel determinante e através da interação delas, a gestão da informação pode causar impactos positivos e decisivos às organizações contemporâneas nas quais o conhecimento, como fonte de inovação e vantagens competitivas, torna-se cada dia elementar e imprescindível aos seus negócios. (PORÉM; BELLUZZO; SANTOS, 2012).

Analisando o modelo apresentado, entende-se que, para identificar as necessidades de informação, primeiro deve-se buscar compreender o contexto em que está inserido cada indivíduo e o contexto da organização, para identificar quais informações o rodeiam.

Choo (2003) observa que cada usuário tem características próprias e uma

maneira diferente de encarar determinado problema. O problema é mutável à medida que o indivíduo utiliza a informação e adquire nova percepção. Para tanto, deve-se identificar os problemas vividos por eles.

Depois de compreender o ambiente organizacional, parte-se para a etapa de aquisição da informação. Nesta etapa, ocorre uma peculiaridade: devido ao fato de a organização possuir muitas necessidades informacionais, há de se ter o equilíbrio entre a quantidade de informações e a qualidade da informação.

Ter um variedade de informações ajuda a enxergar novas possibilidades, novas ideias, ao passo que a redução da variedade permite o aprofundamento da questão, contribuindo para a eficiência do processo. Daí, também, a importância de se ter uma equipe com o maior número de pessoas, o uso estruturado da tecnologia, e ter a disposição os conhecimentos de um profissional especializado como o gestor da informação para integrar os dois fatores (CHOO, 2003).

Na etapa de organização e armazenamento, a prioridade se dá para a memória organizacional, para que possa preservá-la e utilizá-la para futuras necessidades. Ao tomar determinada decisão e armazená-la, a informação ficará disponível para ser consultada em outro momento, caso estejam em situação semelhante. Vale destacar que um indivíduo, ao sair da organização, leva consigo todo o seu arcabouço de conhecimento, e ter um sistema que possa manter “tal conhecimento” solidifica o crescimento da instituição com um todo.

Ainda de acordo com Choo (2003), os produtos e serviços de informação precisam, além de identificar os potenciais problemas e disseminá-los ao tomador de decisão, mostrar-lhes as possibilidades para solucionar estes problemas. O autor fala que a GI precisa agregar valor aos seus produtos e serviços, dando-lhe qualidade por meio de: facilidade de uso da informação; redução de ruído por meio da exclusão de informações indesejáveis e trabalho de indexação; qualidade por meio de informações confiáveis e cobertura completa do assunto; adaptabilidade que atendam às necessidades específicas dos usuários; e economia de tempo e de custo, com serviços e produtos precisos em tempo hábil e economizando dinheiro ao usuário.

A etapa de disseminação da informação, de acordo com Choo (2003), envolve a maneira como a informação será repassada aos usuários certos, de acordo com suas necessidades e preferências específicas, em tempo hábil, por meio de formatos certos, e delimitação de canais de compartilhamento que permitam a

eles a apropriação da informação para tomar decisões e construírem conhecimento.

O uso da informação é a implementação de todo o trabalho feito anteriormente e que levará ao resultado e a resposta no que diz respeito aos processos desenvolvidos na gestão da informação. É uma etapa muito dependente do usuário, pois ele a usa paralelamente à sua cognição, suas experiências prévias, e sua intuição, seu *feeling.* Tudo isso vai variar de acordo com a interpretação que o sujeito fez das informações destinadas a ele. Por isso então, devem ser pensados métodos e processos que deem flexibilidade na representação das informações (CHOO, 2003).

Todo esse processo descrito vem culminar através do comportamento adaptativo, que permite ao gestor da informação identificar os acertos, as falhas, as necessidades informacionais, tendo um *feedback* dos usuários do sistema.

Para gerir esse sistema descrito no modelo, deve ter um profissional com competências suficientes para lidar com toda a massa informacional existente dentro e fora da organização, acerca dos objetivos estabelecidos.

Segundo Reis (1993 apud BRAGA, 2000, p.3), a eficácia no processo de gestão das informações está associado à necessidade de se:

> [...] estabelecer um conjunto de políticas coerentes que possibilitem o fornecimento de informação relevante, com qualidade suficiente, precisa, transmitida para o local certo, no tempo correto, com um custo apropriado e facilidades de acesso por parte dos utilizadores autorizados.

Este processo de gestão só se torna viável ao aproximar pessoas à competência em informação e desta forma transformar este ativo em inteligência. Para tal é necessário uma estruturação e alinhamento da realidade presente em cada organização, assim o "conhecimento sobre determinado assunto ou contexto podem se tornar palpáveis, além de nortear as ações de tomadas de decisões atuais e mesmo futuras", (PORÉM; BELLUZZO; SANTOS, 2012, p.191).

Neste aspecto, encontramos a figura do profissional da informação, mais especificamente o gestor da informação, como o mediador entre a informação e o usuário, gerindo para dar estrutura ao processo de busca, armazenamento, organização e disseminação dessas informações, por meio de serviços informacionais.

No atual contexto, o gestor da informação encontra-se em um momento único de sua história, inserindo-se no rol de profissionais da informação. Em consonância

com as teorias discutidas na esfera de Ciência da Informação (CI), os profissionais pertencentes à GI percebem que o mercado mostra-se como um leque abrangente de ocupações para absorvê-los, e que as empresas passam a dar-lhes um reconhecimento que outrora não ocorrera.

Souto (2005, p. 50) ratifica esta afirmação e complementa esse cenário dizendo que “a abertura do mercado empresarial para os profissionais da informação tem como principal causa de aumento das informações e da necessidade de seu domínio/conhecimento para a tomada de decisão”. O autor ressalta ainda que, devido à grande competitividade, as empresas estão investindo de forma considerável em estruturas que possam gerir o seu capital intelectual e monitorar o ambiente interno e externo da organização.

Por se tratar de estruturas que trabalham essencialmente com informação, mais precisamente com a sua gestão, a presença de um profissional qualificado é exigida para dar suporte aos trabalhos que serão desenvolvidos. O gestor da informação, profissional cujo insumo de trabalho é a informação, hoje se desprende do estereotipo de trabalhar com as informações registradas apenas em papeis e livros. Passa a ser o mediador entre informação (em diferentes suportes), e usuário.

As transformações e revoluções do mundo acabaram por exigir um perfil profissional mais generalista e/ou polivalente, que ultrapassa a formação técnica de sua profissão, e que saiba buscar um entendimento de todas as etapas do processo produtivo. Essas mudanças acabaram por exigir também que as instituições formadoras adequassem seus currículos para contemplar disciplinas que visam desenvolver tais características em sua grade.

Buscando tal escopo, as escolas formadoras do campo da CI têm adequado seus currículos para a formação de profissionais com características que permitem ao profissional se inserir em vários segmentos no mercado de trabalho.

Essas mudanças podem ser observadas nas palavras de Guimarães (2004) ao tratar das Diretrizes Curriculares em Ciência da Informação, referindo-se a mudança de concepção, na Lei de Diretrizes e Bases voltada às competências e habilidades necessárias aos profissionais e não mais exclusivamente nos conteúdos.

Outro ponto a ser enfatizado é que deve partir do próprio profissional o entendimento de sua nova definição profissional. Ele precisa, fundamentalmente, "[...] ter consciência do papel estratégico da informação para o desenvolvimento socioeconômico das empresas e do país”. (VALENTIM, 2002, p. 127).

O profissional da informação, por possuir competências que permeiam os processos de busca, organização, disseminação da informação, ele basicamente atuará como gestor de informação independente do setor e independente dos produtos e serviços que a organização desenvolve.

Valentim (2000, p. 150) confirma tal afirmação, destacando que “o profissional da informação pode e deve trabalhar a informação como fator de competitividade organizacional, quer se trate de organização pública quer de uma organização privada”.

O que deve ser levado em consideração, porém, são as especificidades de cada área e a clara compreensão das rotinas da organização, de modo a compreender em um primeiro momento seu fluxo informacional, para então pensar em um sistema que o gerencie e atenda as necessidades de seus usuários.

Esta afirmação está diretamente ligada ao perfil do profissional da informação e de acordo com Guimarães (2004), a literatura vem discutindo tais questões e mostrando a importância dada à formação do profissional em consonância com as exigências do mercado. Em suas palavras, a dimensão do profissional frente ao novo se dá por elementos como a criatividade, capacidade de se adaptar, conhecimento das tecnologias e como usá-las para o seu trabalho, conhecimento das especificidades das áreas, fazer uso eficaz dos instrumentos de trabalho disponíveis e o profissionalismo frente ao seu ambiente.

Pelo fato de se discutir na literatura assuntos como os expostos acima, inevitavelmente eles passam a fazer parte das práticas profissionais, tendo em vista que a prática decorre da teoria, pois essa a fundamenta. Ao buscar o entendimento da importância de se compreender as especificidades do ambiente organizacional, observa-se uma linha muito tênue entre a quantidade de informação existente e a informação que cada organização possui para sua atuação frente ao mercado, de acordo com seus objetivos.

O profissional precisa ter a clareza de que em um mercado baseado em informação sempre vai ocorrer desvantagens de acesso e posse dessa informação, pois cada organização defende seus interesses e se protege escondendo-as para não se expor às investidas dos concorrentes. Também se considera o uso que é feito com essas informações. É nesse ponto que está o diferencial e um dos fatores decisivos para o sucesso das estratégias organizacionais e para a atuação do profissional da informação.

É neste contexto que atualmente a GI vem atuando nas organizações, gerenciando os mais diversos tipos e formatos de dados e informações. Por isso diretamente ligada à gestão da informação, temos a governança de dados, uma área que tem alcançado cada vez mais espaço e notoriedade dentro das organizações devido a sua grande importância.

2.4 Segurança da Informação

De acordo com Campos (2007), o elemento essencial para todos os processos de negócios da organização é a informação. A definição para a segurança da informação está diretamente ligada em proteger dados de propriedade das organizações e ou sob sua guarda, podendo ser de pessoa física e jurídica, nas quais requerem esforços para garantir a mitigação de riscos e a continuidade das operações. O ato de aplicar a segurança da informação a qualquer tipo de dado está envolvido em utilizar processos de governança empresarial, que envolva recursos humanos, de infraestrutura e lógicos (computacionais).

A segurança da informação (SI) aparece como um tema amplamente discutido em salas de aula, redes sociais e diversos outros meios de comunicação como sendo um tema que trata de assegurar informações pessoais e corporativas, que caso, vazadas ou acessadas por terceiros não autorizados poderão ocasionar transtornos diretos e/ou indiretos às vítimas.

Para os estudiosos e pesquisadores da área, há inúmeras definições de Segurança da Informação (SI), são vários os autores que discorrem sobre o assunto e a seguir serão citados os conceitos de alguns deles alinhados aos objetivos deste trabalho. A SI “visa proteger a informação de forma a garantir a continuidade dos negócios, minimizando os danos e maximizando o retorno dos investimento e as oportunidades de negócios”. (ALVES, 2006, p.15).

Também existe um sistema especializado para padronização mundial, formado pela ISO (International Organization for Standardization) e IEC (International Electronichnical Commision) e definem Segurança da Informação: “como uma proteção das informações contra uma ampla gama de ameaças para assegurar a continuidade dos negócios, minimizar prejuízos e maximizar o retorno de investimentos e oportunidades comerciais”.

De acordo com a norma IDO/IEC 27001 NBR, segurança da informação é a

preservação da confidencialidade, integridade e disponibilidade da informação. Também estão relacionadas com outras propriedades como autenticidade, responsabilidade, não repúdio e confiabilidade. (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2013).

Sêmola (2003, p.9) define SI como “uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade”.

Para Ferreira (2003), a Segurança da Informação:

> Protege a informação de diversos tipos de ataques que surgem no ambiente organizacional, garante a continuidade dos negócios, reduz as perdas e maximiza o retorno dos investimentos e das oportunidades.

Diante do contexto apresentado, a informação se apresenta como um ativo muito desejado e valioso tanto para uma pessoa física como para uma organização, devendo obrigatoriamente estar protegido de acessos não autorizados.

Ao resgatar a história, no período da Revolução Industrial, pouco se pensava sobre segurança da informação e, se pensavam, o problema era facilmente solucionado, porque as informações que circulavam em uma empresa eram feitas em formulários, apresentadas em papel, e eram arquivadas em armários com chaves.

Ao longo dos anos, chegando no século XX, foram introduzidos em pequenos bancos de dados e armazenadas no próprio computador com acesso ainda bastante restrito, porque poucas pessoas manipulavam a máquina. Mais adiante, com a chegada da internet, é que esse quadro foi modificando, no final do século XX o processo chamado de Globalização trouxe drásticas mudanças na administração dos negócios, as informações já não podiam circular facilmente pelos computadores em discos flexíveis sem maiores preocupações, pois os sistemas caminhavam pelas redes de computadores, correndo o risco de acessos não autorizados.

Hoje, a dependência pelos sistemas informatizados é gigante, a sobrevivência de muitas organizações depende exclusivamente desses ambientes, tornando esses ativos ainda mais valiosos e cobiçados, pois passaram a integrar todos os processos da organização, ou seja, nesses sistemas armazenam-se processam-se e transmitem-se dados corporativos, tornando os processos mais rápidos e eficientes, no entanto, se usado inadequadamente, tem o poder de inviabilizar resultados satisfatórios.

Em relação as funções do departamento de segurança de informação de uma empresa, suas atividades basicamente envolvem a criação, implementação, controle e monitoramento de políticas que buscam assegurar os ativos de informações de uma empresa ou pessoa.

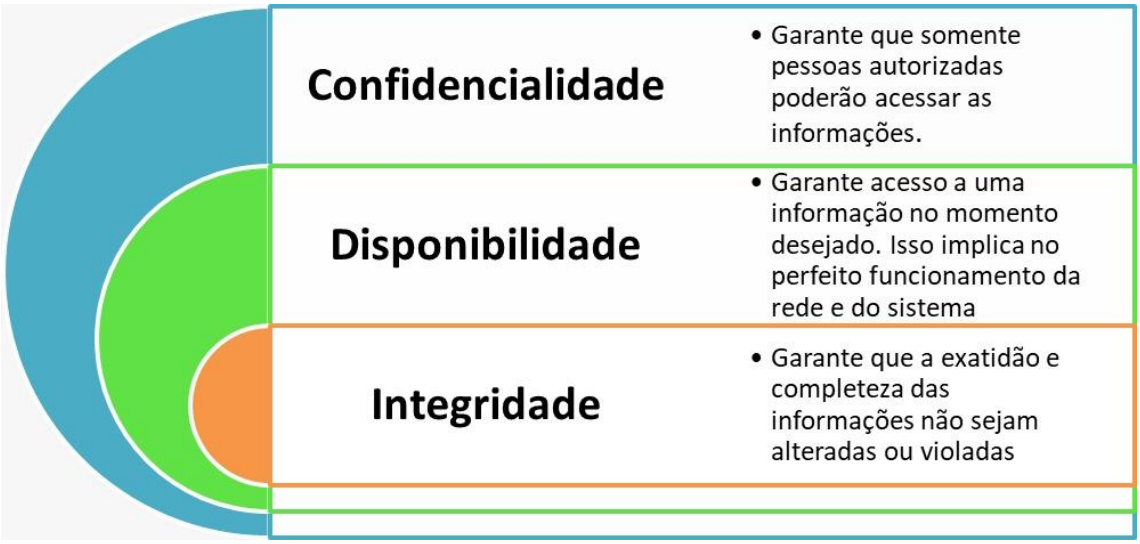
As áreas de negócios são seu foco, especialmente para os setores que utilizam as tecnologias para o desenvolvimento de trabalhos, sendo um recurso indispensável aos processos de produção da atualidade.

É importante que haja sinergia entre o Departamento de Segurança de Informação (DSI) e os demais departamentos da organização, devendo atuar de forma coordenada. Caso ocorra fragmento dentro da organização, o gerenciamento do negócio pode torna-se inviável e qualquer implementação de segurança da informação estará fadada ao fracasso, trazendo prejuízos para toda a organização.

Por isso, que para existir essa tão importante segurança da informação, que foram estabelecidos alguns princípios como pode observar a seguir.

De acordo com a descrição feita pela norma ISO/IEC 17799, a proteção da informação é vital, sendo caracterizadas pela trilogia CID: Confidencialidade, Integridade e Disponibilidade. (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2001). No figura a seguir, segue uma descrição desta trilogia:

Figura 5 – Princípios da Segurança da Informação



Fonte: Elaborado pelo autor (2022).

Além da trilogia CID, citadas acima, Sêmola (2003) acrescenta outros aspectos da segurança da informação, são eles:

a) Legalidade: Garantia de que a informação foi produzida em conformidade com a Lei;
b) Autenticidade: garantia de que em um processo de comunicação os remetentes sejam exatamente o que dizem ser e que a mensagem ou informação não foi alterada após o seu envio para validação.

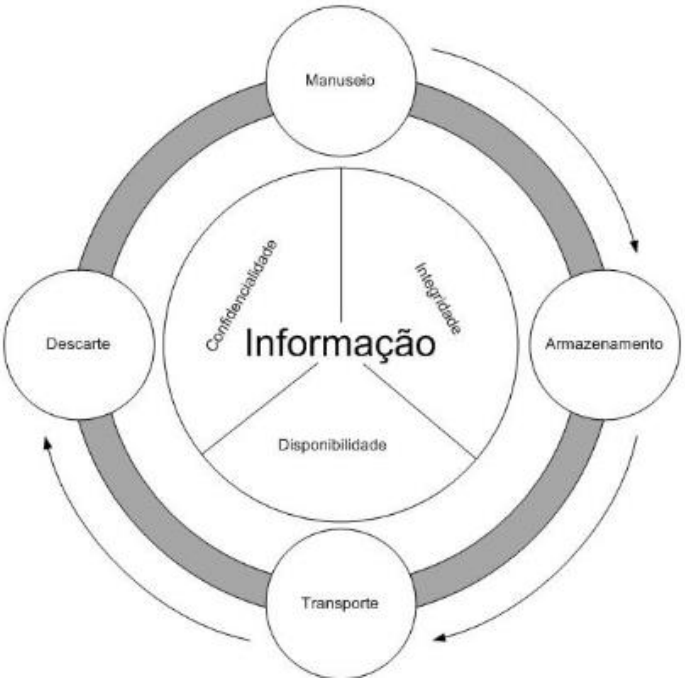
Acima de tudo, segurança da informação diz respeito a como as pessoas e empresas usam as informações que chegam até elas. E não há dúvida quanto a isso: seja um e-mail particular ou um relatório sobre uma grande venda, nada pode escapar do ecossistema de proteção criado pela organização.

Como observado, a segurança da informação apresenta-se como um item fundamental na proteção dos ativos de um usuário ou organização. Estruturada por pilares chave como confidencialidade, integridade e disponibilidade, a informação exige mecanismos de segurança, sejam físicos ou lógicos, que reduzam a vulnerabilidade dos sistemas e inibam eventuais ataques aos dados. Além disso, devem garantir um ciclo de vida seguro da informação, desde sua criação até o seu descarte.

Para entender o objeto da segurança da informação é importante conhecer os momentos que fazem parte do ciclo de vida da informação.

De acordo com Sêmola (2003), o ciclo de vida da informação é composto e identificado pelos momentos vividos pela informação e que as colocam em risco. Esses momentos compõem ativos físicos, humanos e tecnológicos que fazem uso, alteram ou descartam a informação.

Figura 6 – Ciclo de vida da informação



Fonte: Adaptado de Sêmola (2003, p.11).

As quatro etapas do ciclo de vida da informação, segundo Sêmola (2003) são: manuseio, armazenamento, transporte e descarte. Todo o cuidado com a segurança está focado nestes quatro momentos, para que não haja comprometimento da confidencialidade, integralidade e disponibilidade.

Sêmola (2014), explica que o manuseio é o momento em que a informação é criada – que pode ser escrevendo ou digitando informações, folheando documentos ou utilizando uma senha de acesso. O armazenamento acontece quando a informação é armazenada, seja em um banco de dados, mídias digitais como CD´s, DVD´s e pendrives. O transporte é a etapa que a informação é transportada, ocorre quando se envia um email, fala ao telefone ou realiza uma transferência bancária. Já o descarte ocorre quando a informação é descartada, ou seja é eliminada.

A fase de descarte, de acordo com Beal (2012 apud MIRANDA et al., 2019), deve ocorrer quando esta se torna obsoleta ou perde a utilidade para a organização, seguindo neste processo, as normas legais, políticas operacionais e exigências internas.

De acordo com Galvão (2015), em cada etapa do ciclo de vida da informação é necessário garantir confidencialidade, integridade, autenticidade, disponibilidade e também legalidade aos dados de maneira eficaz.

Em tempo, destaca-se a importância de todos os conceitos apresentados como alicerce aos temas que englobam a segurança da informação. Estes conceitos aplicados devem prever os diversos tipos de ataques e frustrar a quebra de confidencialidade da informação.

Pensando nisso, o presente trabalho criou um modelo que pode servir como guia para que as empresas possam ter o mínimo de garantia à segurança dos dados e informações, que será apresentado no capitulo a seguir.

3 PROCEDIMENTOS METODOLÓGICOS

De acordo com Zanella (2013, p. 24), “a ciência e a pesquisa andam de mãos dadas e uma não pode existir sem a outra”. Segundo a autora, só de faz ciência e se produz conhecimento fazendo pesquisa.

A investigação científica depende de um “conjunto de procedimentos intelectuais e técnicos” (GIL, 1999, p. 26) para que seus objetivos sejam atingidos: os métodos científicos.

Método científico é o conjunto de processos ou operações mentais que se devem empregar na investigação. É a linha de raciocínio escolhida no processo de pesquisa (GIL, 1999; LAKATOS; MARCONI, 1993).

Segundo Gil (2007), as pesquisas científicas podem ser classificadas quanto aos objetivos, à abordagem e aos procedimentos.

Ainda de acordo com Gil (2007), a pesquisa exploratória tem como finalidade aumentar o conhecimento sobre um determinado fenômeno. Esse tipo de pesquisa explora a realidade em busca de conhecimento para então planejar uma pesquisa descritiva – que pode ser entendida como uma procura por conhecer a realidade estudada, suas características e seus problemas.

Desta maneira, de acordo com os seus objetivos esta pesquisa pode ser considerada como exploratória e descritiva já que sua principal intenção é realizar um prévio conhecimento sobre o tema, com o intuito de criar um maior entendimento sobre a LGPD e seu impacto nas empresas de fomento mercantil e de pequeno porte.

Segundo Vieira (1996), a pesquisa qualitativa se define como a que se fundamenta principalmente em análises qualitativas, onde a principio não se utiliza de instrumentos estatísticos para análise de dados. Essa abordagem de pesquisa utiliza por base conhecimentos teórico-empíricos que permitem atribui-lhe cientificidade.

Ratificando esta definição sobre pesquisa com abordagem qualitativa, para Silva e Menezes (2005, p. 20) a interpretação dos fenômenos e a atribuição de significados são básicas no processo de pesquisa qualitativa. O ambiente natural é a fonte direta para a coleta de dados e o pesquisador é o “instrumento-chave”. Ela é descritiva e os pesquisadores tendem a analisar seus dados indutivamente – o processo e seu significado são os focos principais de abordagem.

Como observado, esta pesquisa adotou uma abordagem qualitativa visando compreender o fenômeno objeto de estudo com base em suas motivações, propósitos e aplicabilidade, e assim, inspirar novas ideias e futuras pesquisas.

Do ponto de vista dos procedimentos técnicos, de acordo com Gil (1999), este trabalho pode ser considerado como uma pesquisa bibliográfica, por ter sido elaborada a partir de materiais já publicados constituído principalmente de livros, artigos de periódicos e com materiais disponibilizados na internet, bem como conteúdo de palestras, cursos e seminários relacionados à Lei e as empresas de fomento mercantil. Ainda do ponto de vista dos procedimentos, essa pesquisa pode ser classifica como documental.

Esta pesquisa observa o atual contexto da informação e seu caráter imprescindível no exercício das atividades dentro das organizações, especialmente as *factorings*. O trabalho ainda relaciona com as atuais práticas de governança da informação, segurança da informação e como se dá suas relações com a nova legislação brasileira sobre a proteção no que se refere ao tratamento de dados pessoais.

Para isso, foram realizadas pesquisas sobre o uso contemporâneo da informação e sua importância, apresentando conceitos básicos sobre gestão da informação, governança de dados, segurança da informação bem como conceitos básicos e importantes sobre as atividades de fomento comercial.

Foram analisadas as orientações da Lei Geral de Proteção de Dados (LGPD) para tratamento de dados nas organizações procurando sempre relacioná-las aos conceitos de Segurança da Informação e as principais medidas técnicas da área para a proteção de dados pessoais e informações e às praticas de governança de dados.

Dado o contexto atual e importante do tema abordado neste trabalho, todas as pesquisas realizadas tiveram como principal objetivo contribuir para lançar luz sobre como as empresas do setor de fomento mercantil, como as *factorings*, podem adequar-se às exigências da LGPD e compreender como a Gestão da informação pode ser uma grande aliada neste processo - garantindo segurança às informações coletadas e tratadas em suas bases de dados.

O levantamento inicial foi realizado através das legislações vigentes no Brasil e no exterior, mais especificamente na Europa onde o Brasil se inspirou para criar sua Lei de proteção de dados. Posteriormente foram realizadas buscas referentes ao

processo de implementação da LGPD com foco para o ambiente das pequenas empresas, mais especificamente para o fomento comercial.

Para alcançar os objetivos propostos e responder à pergunta de pesquisa, o presente trabalho, inicialmente, realizou pesquisas em veículos de comunicação digitais sobre como os dados e informações são utilizadas na nova era da informação: a Era digital, e os impactos que são causados nas organizações, com foco especial para as *factorings*.

Para coletar os artigos, teses, livros e todo o material utilizado na bibliografia, foram utilizados através dos meios digitais, pesquisas no Google Acadêmico, SciElo, nos repositórios da UFPE, UFRS, UFRJ, CAPES, sites jornalísticos, entre outros.

Para realizar as pesquisas, foram utilizadas palavras-chave como: “Adequação à LGPD”, “Gestão da Informação”, “Fomento Comercial/*Factoring*”, “Governança de Dados”, Segurança da Informação”, “compartilhamento de dados”, “tratamento de dados”, “recursos da informação”, entre outras.

A pesquisa se baseia na importância dos trabalhos e autores que foram escolhidos a respeito da legislação, da gestão das informações e na segurança dessas informações – a literatura encontrada de norte sobre temas como a privacidade, proteção de dados pessoais e a responsabilidade envolvida no processo de tratamento de dados.

A apresentação dos resultados tem como parâmetro os trabalhos elaborados pelos autores escolhidos, com foco para a sugestão de uma modelo sobre como as *factorings* podem utilizar-se da Gestão da Informação para adequar-se minimamente às exigências da LGPD. Por fim, após analise da Lei, verifica-se alguns principais artigos que se aplicam à segurança da informação e à governança de dados, destacando a relação entre essas áreas e a Lei – identificando as principais alterações que precisam ocorrer dentro das organizações, adotando práticas mais modernas e medidas técnicas e administrativas para adequação à Lei.

4 MODELO SUGERIDO PARA ADEQUAÇÃO DAS FACTORINS À LGPD

De acordo com a ANFAC, as empresas de *factoring* lidam com dados pessoais em seu dia-a-dia, uma vez que é comum o trabalho com avalistas, empresas sacadas, em que muitos deles atuam também como pessoas físicas. Desta forma podemos classifica-las como Controladoras de Dados, ou seja, elas que decidem sobre o tratamento e para que fim serão utilizados os dados pessoais que coleta.

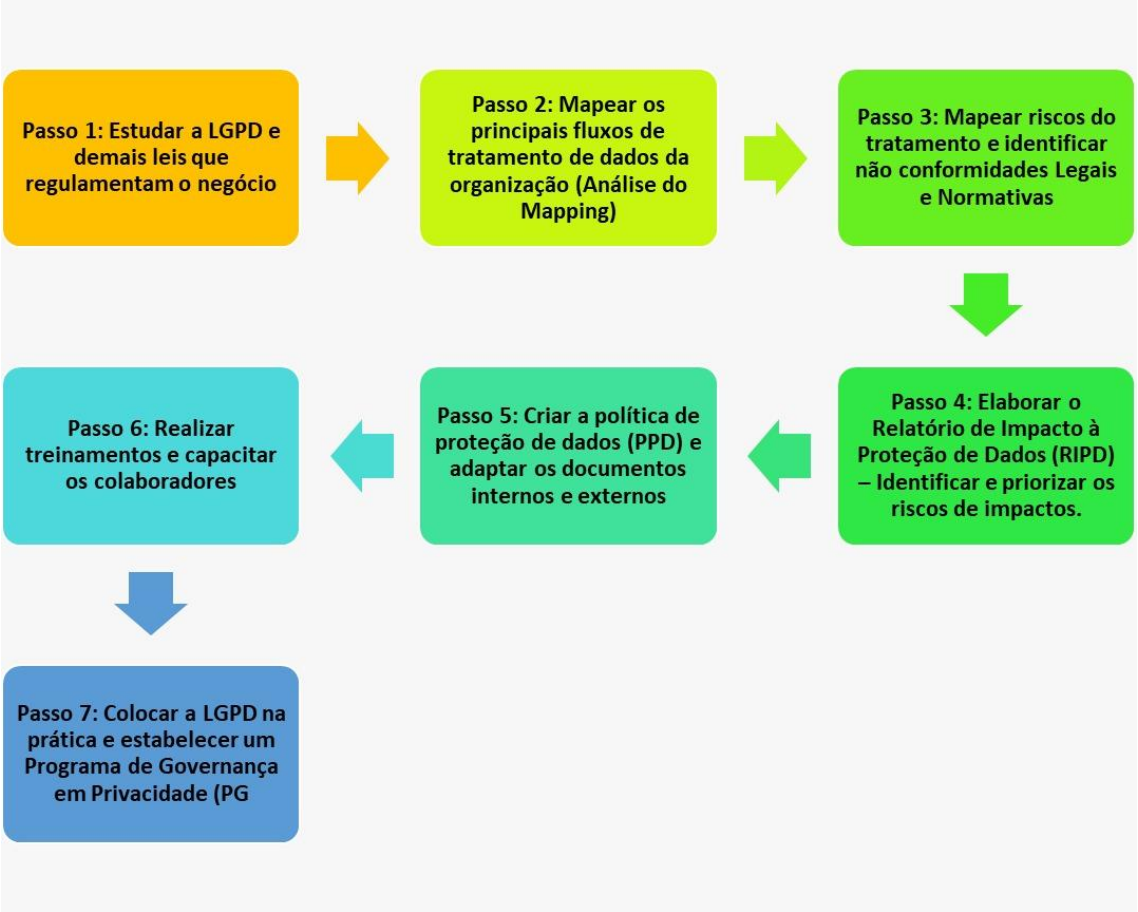
Além da mitigação de riscos e sanções, a conformidade das empresas com a LGPD eleva a reputação da empresa perante o mercado, seus concorrentes e clientes. Adequar-se a Lei, permite a construção de uma cultura ética de proteção de dados para a empresa.

Saber como implementar a LGPD na prática das atividades de uma *factoring* é uma necessidade que atinge todas as empresas desse seguimento e a adequação à Lei com o funcionamento dos controles exigidos pela legislação está longe de ser um processo simples e rápido.

A implementação da LGPD exige uma série de ajustes para a correta adoção de medidas para proteger os dados dos titulares (colaboradores, usuários e clientes), assim como o próprio negócio. Para tanto, convém criar um comitê responsável pelo processo. Algo que pode ou não contar com a orientação de especialistas terceirizados.

A seguir é possível acompanhar o modelo sugerido, elaborado a partir de todas as informações apresentadas neste trabalho, as etapas do processo para a adequação das *factorings* à LGPD:

Figura 7 - Modelo Sugerido para Adequação das Factorins à LGPD



Fonte: Elaborado pelo autor (2022).

4.1 Passo 1: Estudar a LGPD e demais Leis que regulamentam o negócio

O primeiro passo é conhecer o texto integral da LGPD, assim como de outras Leis que regulamentam a atuação da empresa. É imprescindível conhecer com profundidade o contexto da organização, o segmento de atuação no mercado, juntamente com todas as suas particularidades e exigências, considerar a organização interna em termos de procedimentos de trabalho, bem como, a definição de papeis e responsabilidades dos colaboradores.

É importante que todos da empresa se informem e sejam treinados para estar melhor habilitado a lidar com dados pessoais no dia-a-dia. Conceitos básicos sobre proteção de dados, categorização de dados, direito dos titulares e hipóteses de tratamento, importância da alta gestão e sanções da Lei e responsabilidade do encarregado de dados devem ser pontos enfatizados e compartilhado com todos.

Recomenda-se que todo o processo de entendimento do contexto da

organização seja documentado, com a apresentação e guarda de evidências para posterior rastreabilidade e/ou recuperação dos achados desta etapa.

4.2 Passo 2: Mapear os principais fluxos de tratamento de dados da organização (Análise do *Mapping*)

Este é o passo mais importante para colocar a LGPD na prática, e, provavelmente o um dos mais complexos e desgastantes de todo o processo de adequação da *factoring* à LGPD. Não é um processo fácil mapear corretamente os fluxos de tratamento de dados, tarefa que demanda organização, conhecimento, engajamento de todas as áreas da empresa e o estabelecimento de um esforço cooperativo, contando com a participação efetiva de muitas partes distintas.

Primeiro faz-se necessário identificar os principais processos de negócio da empresa, mapeando os fluxos de tratamento de dados pessoais que são realizados a partir dos processos de negócio previamente identificados.

Durante o mapeamento, devemos identificar com clareza, objetividade e precisão:

a) Os agentes de tratamento envolvidos no fluxo de dados: controladores, operadores e o encarregado de dados;
b) O fluxo de tratamento de dados pessoais: uma descrição sucinta do tratamento que está sendo mapeado, levando em conta as atividades de coleta, compartilhamento, armazenamento e exclusão de dados;
c) O inventário de dados pessoais que estão sendo tratados, bem como, a finalidade que justifica o tratamento, e a hipótese legal que autoriza aquele tratamento de dados;
d) Os meios pelos quais os dados pessoais são coletados, e quais pessoas, documentos ou sistemas participam da coleta;
e) Como os dados pessoais são armazenados, com a definição do período de retenção, e quais pessoas, documentos ou sistemas participam do armazenamento;
f) Com quem os dados pessoais são compartilhados e por qual motivo, e quais pessoas, documentos ou sistemas participam do compartilhamento;
g) Como e quando os dados pessoais são eliminados, e quais pessoas,

documentos ou sistemas participam da eliminação;

h) Quais medidas técnicas e administrativas de segurança da informação são empregadas durante o tratamento.

Com base na documentação dos fluxos de tratamento de dados pessoais, você deve elaborar e manter atualizado os registros de tratamento de operações de dados pessoais (RoPA), conforme determinação do art. 37 da LGPD.

Para isso, é importante fazer um esforço para não deixar nada de fora; mapeando a entrada de dados de usuários, clientes e outros *stakeholders*.

4.3 Passo 3: Mapear riscos do tratamento e identificar não conformidades Legais e Normativas

Ao mapear as operações de tratamento de dados pessoais, deve-se avaliar se estas atividades desempenhadas pela organização, estão de acordo com os requisitos legais estabelecidos pela LGPD, e também, por normas internacionais como é o caso do grupo de normas ISO 27000 – 27001, 27002, 27005, 27701 (normas relacionadas à segurança da informação e proteção de dados).

Para a implementação da LGPD também é necessário avaliar o ciclo de vida dos dados coletados, assim como eventuais falhas no processo. O objetivo é identificar possíveis riscos de vazamento de dados, uma vez que é responsabilidade da empresa garantir a proteção dessas informações e a privacidade de seus usuários e clientes.

4.4 Passo 4: Elaborar o Relatório de Impacto à Proteção de Dados (RIPD) – Identificar e priorizar os riscos de impactos.

O Relatório de Impacto à Proteção de Dados Pessoais (RIPD) é uma das exigências do processo de implementação da LGPD. Trata-se de um documento a ser elaborado pelo controlador dos dados — no caso, a empresa de *factoring* — sempre que for identificado algum risco possível decorrente do processo de tratamento de dados.

Após mapear os fluxos de tratamento de dados pessoais e apontar as principais não-conformidades legais e normativas, deve-se identificar e priorizar os riscos encontrados.

A LGPD determina de maneira explicita em seu art. 50, que as empresas devem estabelecer um programa de governança em privacidade, baseado numa gestão de riscos efetiva. Por isso, recomenda-se que seja utilizada uma boa metodologia para a gestão de riscos, preferencialmente, baseada em normas internacionais ou nas melhores práticas de mercado, com o é o caso da ISO 31000, ou o COSO.

É importante que todos os passos estejam devidamente documentos, visando a geração de provas positivas e a comprovação de boa-fé da empresa (art. 6 da LGPD). Assim, é necessário manter registros claros de como a avaliação dos riscos foi realizada, bem como, quais critérios foram utilizados, indicando com objetividade o método empregado para priorizar os riscos.

4.5 Passo 5: Criar a política de proteção de dados (PPD) e adaptar os documentos internos e externos

Para implementar a LGPD a empresa precisa estabelecer regras a normas a serem seguidas pela organização como um todo. Assim, se faz necessário a criação de uma PPD.

A política de proteção de dados é o documento mais importante em relação a proteção de dados, é por meio desse documento que se dá transparência para os titulares de dados em relação a quais dados são coletados e como de dá todo o seu tratamento.

Abaixo seguem algumas considerações importantes para a elaboração deste documento:

a) Definir quais tipos de dados são coletados e documentar os motivos para o tratamento destes dados;
b) Criar documentação que indiquem como se dá a segurança no armazenamento desses dados;
c) Apresentar as bases legais utilizadas para tratamento dos dados;
d) Informar se ocorre o compartilhamento de dados com outras empresas e justificar tais compartilhamentos;
e) Indicar um contato para que os titulares possam tirar dúvidas sobre a política de privacidade;
f) Informar os direitos que os titulares possuem e indicar como ele pode

exercer tais direitos.

Essas diretrizes, assim como outros documentos oficiais que contenham normas da empresa, precisam ser revisadas pelo departamento jurídico ou por uma consultoria especializada. O objetivo é assegurar que toda documentação esteja em conformidade com a Lei Geral de Proteção de Dados e, assim, guie a empresa no caminho correto.

4.6 Passo 6: Realizar treinamentos e capacitar os colaboradores

Para manter a organização em conformidade com a LGPD de forma continuada – o que certamente demanda atenção e apoio de todas as equipes, e alterações na cultura organizacional.

Todos os envolvidos na atividade da empresa como os colaboradores, prestadores de serviços e parceiros comerciais precisam entender os fundamentos da LGPD, incorporando à pratica da proteção de dados pessoais no dia-a-dia, em todas as atividade em que estiverem envolvidos.

Para tanto, sugere-se que os agentes de tratamento de pequeno porte conscientizem os colaboradores por meio de treinamento e campanhas de conscientização sobre suas obrigações e responsabilidades relacionadas ao tratamento de dados pessoais.

Algumas informações úteis que podem ser passadas aos colaboradores são: como utilizar controles de segurança dos sistemas de TI relacionados ao trabalho diário; como evitar se tornar vítima de incidentes de segurança corriqueiros como a contaminação por vírus através de links suspeitos; manter documentos físicos que contenham dados pessoais dentro de gavetas, e não sobre mesas; não compartilhar logins e senhas de acesso das estações de trabalho; bloquear os computadores quando se afastar para evitar acesso de terceiros; seguir as orientações de politica de privacidade.

É importante criar um ambiente organizacional que incentive usuários de sistemas da empresa, tanto clientes quanto funcionários, a informar incidentes e vulnerabilidades detectadas – é importante trazer o aprendizado para o debate interno, e assim, gerar as condições para que a cultura de proteção de dados seja incorporada à organização de forma definitiva.

4.7 Passo 7: Colocar a LGPD na prática e estabelecer um Programa de Governança em Privacidade (PGP)

Após criar as principais medidas de adequação, é preciso implementar um PGP efetivo, por meio da adoção de controles que possam ser devidamente acompanhados e monitorados. Por este motivo é recomendado não apenas a adoção de políticas e processos, mas, principalmente, a designação de um DPO (Data Protection Officer) que é o profissional responsável por atuar como um canal de comunicação entre o controlador, os titulares de dados e a Autoridade Nacional de Proteção de Dados (ANPD).

De acordo com o art. 41 da LGPD, compete ao Encarregado de Dados Pessoais:

a) Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
b) Receber comunicações da autoridade nacional e adotar providências;
c) Orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e
d) Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

Por isso, o Encarregado pelo Tratamento de Dados Pessoais torna-se imprescindível para colocar a LGPD na prática e implementar um Programa de Governança em Privacidade efetivo e duradouro. Função essa que como vimos ao longo do trabalho, pode ser exercida por um Gestor da Informação – que possui as competências necessárias para atuar neste processo.

Este presente modelo proposto foi desenvolvido com o objetivo de disseminar boas práticas e medidas básicas de segurança da informação para apoiar os agentes de tratamento de pequeno porte, com as *factorings*, no desenvolvimento de suas atividades de governança de dados em um ambiente institucional mais seguro no que se refere ao tratamento de dados pessoais.

É importante lembrar que não existe um caminho fácil que leve a adequação perante a Lei – uma avaliação profunda de operação, customizada, que pondere tanto os aspectos técnicos quanto os organizacionais, certamente refletirá em um robusto plano de ações que certamente mitigará de forma eficaz os principais riscos de não conformidade.

Espera-se que essas medidas possam contribuir para estabelecer um ecossistema de proteção de dados pessoais mais seguro e que possam ser entendidas com um guia de boas práticas que deverá ser atualizado e aperfeiçoado sempre que necessário.

5 CONSIDERAÇÕES FINAIS

De acordo com o que foi apresentado durante este trabalho, acabamos por entender que no atual contexto de nossa sociedade, o processamento de dados pessoais acontece de forma ininterrupta, realizado por diversos agentes do mercado que buscam obter vantagens competitivas frente aos seus concorrentes.

É dentro deste contexto da Era da Informação, que toda a sociedade está inserida, o que não deixaria de fora as empresas de *factoring*, que na realização de suas atividades operacionais, comerciais e trabalhistas acabam realizando o processamento de diversos dados pessoais.

Com o intuito de entender mais sobre a atividade de fomento mercantil, no primeiro capítulo deste trabalho foram apresentados os principais conceitos relativos à atividade - indicando sua origem e observando sua importância dentro do mercado. Foi possível compreender que a atividade realiza bastante tratamento de dados pessoais em suas operações.

Durante muitos anos, o direito à privacidade, estabelecido no artº 5º, X, da Constituição Federal foi suficiente para proteger o titular de dados de possíveis tratamentos abusivos. Contudo à medida que os interesses mercadológicos começaram a conflitar com os direitos fundamentais das pessoas, a sociedade acabou percebendo a necessidade de uma lei mais especifica para tratar deste tema.

Foi neste contexto que a Lei Geral de Proteção de Dados Pessoais – LGPD, foi editada como uma norma brasileira apta a regular o tratamento de dados pessoais em território brasileiro, ou ainda, em território internacional. A Lei estabeleceu todos os princípios que devem ser observados por toda e qualquer pessoa ou empresa que realiza tratamento de dados pessoais de modo a garantir sua efetividade no tempo.

Em seu segundo capítulo, este trabalho trouxe os principais conceitos encontrados sobre a Lei, e tentou identificar os principais requisitos necessários para que as *factoring* possam adequar-se corretamente à Lei.

Na seção 2.2 sobre a LGPD, foi verificado que o consentimento por parte do titular de dados é a principal base legal para fundamentar o tratamento de dados pessoais. O consentimento vai permitir que o tratamento destes dados seja realizados de acordo com os princípios da LGPD.

A Lei veio para auxiliar as organizações e trouxe em seu texto importantes conceitos como dados pessoais, tratamento de dados, dados anonimizados, consentimento, os agentes de tratamento de dados, e vários outros conceitos para evitar qualquer dificuldade de entendimento.

Foi possível observar que a LGPD estabelece uma gama de exigências relacionadas à boa prática de governança de dados com foco na segurança da informação que devem ser cumpridas pelas empresas: como conhecer o seu ativo e fluxo informacional, revisar políticas de proteção e segurança, adotar medidas técnicas de proteção dessas informações, adequar seus contratos e termos e preparar seus colaboradores com conhecimentos e responsabilidades.

Para ajudar a entender como a Gestão da Informação pode ser um grande aliado para ajudar as empresas de *factoring* na adequação à Lei, foi visto na seção 2.3 deste trabalho, as principais ferramentas e conceitos sobre o tema.

Percebe-se que todo o gerenciamento acaba sendo realizado através do mapeamento dos fluxos, conhecendo as necessidades de uso e mapeando todas as fontes de informações pertinentes a cada contexto organizacional.

Por se tratar de estruturas que trabalham essencialmente com informação, mais precisamente com a sua gestão, a presença de um profissional qualificado é exigida para dar suporte aos trabalhos que serão desenvolvidos. O gestor da informação, profissional cujo insumo de trabalho é a informação, hoje se desprende do estereotipo de trabalhar com as informações registradas apenas em papeis e livros. Passa a ser o mediador entre informação (em diferentes suportes), e usuário.

Neste contexto a Gestão da Informação encontra papel de destaque, e coloca o gestor da informação como adequado por ter as habilidades necessárias para exercer atividades relacionadas à Competência Informacional acerca do papel das novas tecnologias como ferramentas de adequação à LGPD, mitigando as dificuldades encontradas durante o processo.

O trabalho mostrou ainda, os principais aspectos da área da segurança da informação, apresentando as medidas técnicas de proteção à informação, que devem ser apresentados de acordo com os contextos nos quais as organizações estão posicionadas.

Foi possível concluir que a própria legislação estabeleceu um vínculo entre a segurança da informação e a governança de dados, e as duas áreas têm se ocupado em buscar um equilíbrio entre a proteção e a utilidade desses elementos

nas organizações.

Com a inclusão das novas tecnologias, dos meios de comunicações e o montante de informações geradas, cada vez maior, a consolidação de uma equipe multidisciplinar torna-se necessária, para que haja uma atuação de profissionais com formação e capacitação necessárias para trabalhar com estes novos recursos.

Com o intuito de ajudar as empresas de *factoring* a encontrarem um caminho que possa auxiliá-los no processo de adequação à LGPD foi apresentado em seu capítulo 4, um modelo criado pelo autor, com alguns passos essenciais para sua devida adequação.

Por fim conclui-se que o objetivo geral deste trabalho foi alcançado, visto que conseguiu lançar luz sobre como as empresas do setor de fomento mercantil, como as *factorings*, podem adequar-se às exigências da LGPD e entender como a Gestão da informação pode ser uma grande aliada neste processo - garantindo segurança às informações coletadas e tratadas em suas bases de dados. E ainda criando um modelo que pode servir como uma espécie de guia informacional para auxiliar empresas de *factoring* que necessitem de algum caminho a seguir.

Não se busca com este trabalho o esgotamento das medidas necessárias à adequação e a conformidade com a Lei Geral de Proteção de Dados (LGPD), mas sim os aspectos mais essenciais para sua implementação. Como observado ao longo do texto, a realidade operacional de cada organização é item essencial de análise para melhor compreensão e suas necessidades. Além de que, não basta uma adequação estrita do ponto de vista jurídico, ou do ponto de vista técnico – é necessária a implementação de medidas tanto técnicas quanto organizacionais para fim de conformidade.

REFERÊNCIAS

ALVES, G. A. **Segurança da informação**: uma visão inovadora da gestão. Rio de Janeiro: Ciência Moderna Ltda, 2006.

AMORIM, F. B.; TOMAÉL, M. I. Gestão da informação e gestão do conhecimento na prática organizacional: análise de estudos de casos. **Revista Digital de Biblioteconomia & Ciência da Informação**, v. 9, n. 1, p. 1-22, 2011. Acesso em: 16 jul. 2022.

ARRIERO, M. A. S**. Mecanismos de apoio à pequena empresa: a polêmica factoring x agiotagem**. 1999. 62 f. Trabalho de Conclusão de Curso (Graduação em Administração Financeira e Bancária) - Centro Universitário Ibero-Americano, 1999. Disponível em: http://www.administradores.com.br/_resources/files/_modules/academics/academics_2517_201002281827118c26.pdf. Acesso em: 25 mai. 2022.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 17799**: Tecnologia da informação: código de prática para a gestão da segurança da informação. Rio de Janeiro: ABNT, 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR NBRISO/IEC27001**: Tecnologia da informação: técnicas de segurança: sistemas de gestão da segurança da informação: requisitos. Rio de Janeiro: ABNT, 2001.

ASSOCIAÇÃO NACIONAL DAS FACTORINGS. **Estatísticas do mercado.** 2022. Disponível em: https://anfac.com.br/estatisticas-do-mercado/. Acesso em: 16 jul. 2022.

BARBOSA, R. R.; SEPULVEDA, M. I. M.; COSTA, M. U. P. da. Gestão da informação e do conhecimento na era do compartilhamento e da colaboração. **Informação & Sociedade**: Estudos, João Pessoa, v. 19, n. 2, p. 13-24, 2009.

BRAGA, A. A gestão da informação. **Millenium,** v. 19, 2000.

BRASIL. **Constituição da República Federativa do Brasil**. Brasília, DF: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 25 mai. 2022.

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, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 25 mai. 2022.

BULGARELLI, W. **Contratos mercantis.** 10 Ed. São Paulo: Atlas, 1998.

CAMPOS, A. **Sistema de segurança da informação**. 2 ed. Florianópolis: Visual Books, 2007.

CHOO, C. W. **A organização do conhecimento:** como as organizações usam a informação para criar significado, construir conhecimento e tomar decisões. São Paulo: Senac, 2003.

DAVENPORT, T. H.; PRUSAK, L. **Conhecimento empresarial**: como as organizações gerenciam o seu capital intelectual. Rio de Janeiro: Elsevier, 2003

ENTENDA o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades. **G1 Globo**, São Paulo, 20 mar. 2018. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/entenda-o-escandalo-de-uso-politico-de-dados-que-derrubou-valor-do-facebook-e-o-colocou-na-mira-de-autoridades.ghtml. Acesso em: 10 ago. 2022.

FERNADES, A. V. **Efeitos do vazamento de dados segundo a LGPD**. 2019. Disponível em: https://4s.adv.br/blog/efeitos-do-vazamento-de-dados-segundo-lgpd/.Acesso em: 10 ago. 2022.

FERREIRA, F. N. F. **Segurança da informação**. Rio de Janeiro: Ciência Moderna. 2003.

GALVÃO, M. da C. **Fundamentos em segurança da informação**. São Paulo: Person, 2015.

GIL, A. C. **Métodos e técnicas de pesquisa social.** 5. ed. São Paulo: Atlas, 2007.

GIL, A. C.. **Métodos e técnicas de pesquisa social.** São Paulo: Atlas, 1999.

GUIMARÃES, J. A. Profissional da informação: desafios e perspectivas para sua formação. In: BAPTISTA, S. G.; MUELLER, S. P. M. (Org). **Profissional da informação: o espaço de trabalho**. Brasília: Thesaurus, 2004. p. 87-104.

LAKATOS, E. M.; MARCONI, M. A. **Fundamento de metodologia científica.** São Paulo: Atlas, 1993.

Leite, L. L. **Factoring no Brasil.** 12. ed. São Paulo, Atlas, 2011.

Leite, L. L. **Factoring no Brasil**. São Paulo: Atlas, 2004.

Martins, S. de C. **Gestão da Informação**: estudo comparativo de modelos sob a ótica integrativa dos recursos de informação. 2014. Dissertação (Mestrado em Ciência da Informação) – Programa de Pós-Graduação em Ciência da Informação, Universidade Federal Fluminense, 2014 . Disponível em: https://app.uff.br/riuff/bitstream/handle/1/10725/DISSERTA%C7%C3O_SERGIO%20MARTINS.pdf;jsessionid=A567C835649ACCD454CD7E7E525A0559?sequence=1. Acesso em: 10 ago. 2022

MIRANDA, M. A. S. de et al. Ciclo de vida da informação no suporte ao processo de inovação: uma proposta de modelo interativo. **Revista Gestão e Planejamento**, Salvador, v. 20, p. 581-599, 2019. Disponível em: https://revistas.unifacs.br/index.php/rgb/article/download/6007/3844. Acesso em: 25 mai. 2022

OLIVEIRA, L. M. V. de.; PANISSET, B. T. C.; SILVA, J. A. da. Horizonte sobre dados pessoais no Brasil: a lei geral de proteção de dados e a autoridade nacional de dados em questão. *In:* ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO, 20., 2019, Florianópolis. **Anais** [...], Florianópolis: UFSC, 2019. Disponível em: https://conferencias.ufsc.br/index.php/enancib/2019/schedConf/presentations. Acesso em: 23 mar. 2021.

PONTICELLI, M. M. **O direito fundamental à privacidade no âmbito da rede mundial de computadores com o advento da lei geral de proteção de dados**. 2018. 57 f. Trabalho de Conclusão do Curso (Graduação em Direito) - Universidade do Sul de Santa Catarina, Tubarão, 2018. Disponível em: https://repositorio.animaeducacao.com.br/bitstream/ANIMA/6124/1/TCC%20Murilo%20Assinado.pdf. Acesso em: 10 ago. 2022.

PORÉM, M. E.; BELLUZZO, R. C.; SANTOS, V. C. dos. Vantagem competitiva nas empresas contemporâneas: a informação e a inteligência competitiva na tomada de decisões estratégicas. **InTexto**, Porto Alegre, v. 27, n. 1, p. 183–199, 2012.

RAPÔSO, C. F. L et al. LGPD - lei geral de proteção de dados pessoais em tecnologia da informação: revisão Sistemática. **RACERevista da Administração**, v. 4, p. 58-67, 2019.

RIZZARDO, Arnaldo. **Factoring.** 3. ed. São Paulo. Revista dos Tribunais, 2004.

RIZZARDO, Arnaldo. **Factoring**. São Paulo: Revista dosTribunais, 1997.

ROCHA, M. H. da. Estudo sobre o contrato de factoring. **Revista Jus Navigandi**, Teresina, v. 5, n. 42, 2000. Disponível em: https://jus.com.br/artigos/634. Acesso em: 22 junho. 2022.

RODRIGUES, C.; BLATTMANN, U. Gestão da informação e a importância do uso de fontes de informação para geração de conhecimento. **Perspectivas em Ciência da Informação,** v. 19, n. 3, p. 4-29, 2012. Disponível em: https://doi.org/10.1590/1981-5344/1515. Acesso em: 10 ago. 2022.

SÁ, M. D. de. **Análise do impacto da nova Lei de Proteção de Dados Pessoais nas aplicações de Internet das coisas**: aplicações mobile do governo. 2019. 39 f. Trabalho de Conclusão de Curso (Especialização em Informática) - Universidade Federal de Minas Gerais, Brasília, 2019. Disponível em: https://repositorio.ufmg.br/bitstream/1843/32040/1/MarceloDiasDeSa.pdf. Acesso em: 10 junho 2022.

SÊMOLA, M. **Gestão da segurança da Informação:** uma visão executiva. Rio de Janeiro: Campus, 2003.

SÊMOLA, M. **Gestão da segurança da informação**: uma visão executiva. 2. ed. Rio de Janeiro: Elsevier, 2014.

SERVIÇO FEDERAL DE PROCESSAMENTO DE DADOS. **Conheça os princípios e as bases legais que dão suporte à Lei Geral de Proteção de Dados Pessoais**. Brasília: SERPRO, 2022a. Disponível em:

https://www.serpro.gov.br/lgpd/menu/tratamento-dos-dados/principios-da-lgpd Acesso em: 10 ago. 2022.

SERVIÇO FEDERAL DE PROCESSAMENTO DE DADOS. **O que são dados pessoais, segundo a LGPD.** Brasília: SERPRO, 2022b. Disponível em: https://www.serpro.gov.br/lgpd/menu/protecao-de-dados/dados-pessoais-lgpd. Acesso em: 10 ago. 2022.

SILVA, E. L.; MENEZES, E. M. **Metodologia da pesquisa e elaboração de dissertação.** 4. ed. Florianópolis, SC: UFSC, 2005.

SINDICATO DAS SOCIEDADES DE FOMENTO MERCANTIL. **Sobre factoring**. 2022. Disponível em: http://www.sinfacpe.com.br/entenda-melhor/index.asp. Acesso em: 10 junho 2022.

SOUTO, L. F. **O profissional da informação em tempos de mudanças.** Campinas: Alínea, 2005.

SOUZA, Renato. Dados pessoais de brasileiros são negociados livremente na internet. **Correio Braziliense**, Brasília, 16 jun. 2018. Disponível em: https://www.correiobraziliense.com.br/app/noticia/brasil/2018/07/16/interna-brasil,695136/dados-pessoais-de-milhares-de-brasileiros-sao-negociados-na-internet.shtml. Acesso em: 10 ago. 2022

STABILE, H. H. Factoring: um estudo desse mecanismo de apoio às pequenas e médias empresas. **Caderno de Administração**, v. 20, n. 2, 2012.

TARAPANOFF, K. (Org.). **Inteligência organizacional e competitiva.** Brasília: UnB, 2001.

VALENTIM, M. L. P. (Org.). **Formação do profissional da informação**. São Paulo: Polis, 2002.

VALENTIM, M. L. P. **O profissional da informação: formação, perfil e atuação profissional**. São Paulo: Polis, 2000.

VIEIRA, M. M. F. V. **A comparative study on quality managemant in the brazilian and the Scottish prison service.** 1996. Tese (Doutorado PhD on Business Studies) – Scotland, University of Edinburg, Edimburgo, 1996.

WIENHAGE, P.; SOUZA; R. P. S. de; TOLEDO FILHO, J. R. As empresas de fomento mercantil e o risco jurídico: um estudo sobre as principais causas e prevenções de litígios judiciais. **Sociais e Humanas**: revista do Centro de Ciências Sociais e Humanas, v. 23, n. ja/ju 2010, p. 33-45, 2010. Disponível em: https://periodicos.ufsm.br/sociaisehumanas/article/view/2098/1281. Acesso em: 20 jun. 2022.

WOLF, Fernando Machado. **As práticas de análise para concessão de crédito numa empresa de fomento mercantil (*factoring*).** 2008. 64 f. Trabalho de Conclusão de Curso (Graduação em Ciências Contábeis) - Universidade Federal de Santa Catarina, Florianópolis, 2008.

ZANELLA, Liane Carly Hermes. **Metodologia de pesquisa.** 2. ed. Florianópolis: Departamento de Ciências em Administração/UFSC, 2013.