UNIVERSIDADE DO VALE DO RIO DOS SINOS – UNISINOS
UNIDADE ACADÊMICA DE PESQUISA E PÓS-GRADUAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO DA EMPRESA E DOS NEGÓCIOS
NÍVEL MESTRADO PROFISSIONAL

RHAISSA SOUZA PROTO

Compliance de dados: elementos concretos de estruturação, implementação e execução de um programa efetivo

Porto Alegre
2022

RHAISSA SOUZA PROTO

Compliance de dados: elementos concretos de estruturação, implementação e execução de um programa efetivo

Dissertação apresentada como requisito parcial para obtenção do título de Mestre em Direito da Empresa e dos Negócios, pelo Programa de Pós-Graduação do Mestrado Profissional em Direito da Empresa e dos Negócios da Universidade do Vale do Rio dos Sinos (UNISINOS).

Orientador: Prof. Dr. Francis Rafael Beck

Porto Alegre
2022

P967c Proto, Rhaissa Souza.

Compliance de dados: elementos concretos de estruturação, implementação e execução de um programa efetivo / Rhaissa Souza Proto – 2022.

132 f. : il. color. ; 30 cm.

Dissertação (mestrado) – Universidade do Vale do Rio dos Sinos, Programa de Pós-Graduação em Direito da Empresa e dos Negócios, Porto Alegre, 2022.

"Orientador: Prof. Dr. Francis Rafael Beck."

1. Compliance de dados. 2. Proteção de dados. 3. Programas de compliance. 4. Avaliação de riscos. I. Título.

CDU 347.7

Dados Internacionais de Catalogação na Publicação (CIP)
(Bibliotecária: Bruna Sant'Anna – CRB 10/2360)

RHAISSA SOUZA PROTO

Compliance de dados: elementos concretos de estruturação, implementação e execução de um programa efetivo

Dissertação apresentada como requisito parcial para obtenção do título de Mestre em Direito da Empresa e dos Negócios, pelo Programa de Pós-Graduação em Direito da Empresa e dos Negócios da Universidade do Vale do Rio dos Sinos (UNISINOS).

Aprovado em 19 de janeiro de 2023.

BANCA EXAMINADORA

Dr. Manoel Gustavo Neubarth Trindade – UNISINOS (membro)

Dr. Fabiano Koff Coulon - UNISINOS (membro)

Dr. Ricardo Luiz Nicoli - UniRV (membro externo)

“Como sou pouco e sei pouco, faço o pouco que me cabe me dando por inteiro”

(Ariano Suassuna)

AGRADECIMENTOS

A Deus, por ser o ponto de partida inexorável neste momento, por sempre me iluminar e abençoar o caminho até aqui percorrido.

Aos meus pais e irmão, que merecem anotação destacada, por sempre me apoiarem a estudar e a lutar pelos meus sonhos, pelo amor incondicional e apoio irrestrito, vocês são minha fonte de energia.

Ao Professor Doutor Francis Rafael Beck, agradeço pelo profissionalismo demonstrado durante esses dois anos de convivência, que desde o contato inicial se revelou sempre disponível e solícito para debater, obrigada por todo o apoio, paciência, auxílio e esforços despendidos.

A todos os docentes do PPGD/UNISINOS, por todo conhecimento transmitido.

Aos amigos e colegas de mestrado, por terem tornado essa jornada leve, intensa e prazerosa.

A todos vocês, muito obrigado por fazerem parte dessa história.

RESUMO

O leque para aplicações de estratégias ou de implementação de programa de *compliance* se torna cada vez mais amplo. O enfoque que antes se dava especialmente nas áreas: empresarial, trabalhista, penal, tributária, pública, concorrencial, do terceiro setor e startups, agora apresenta grande destaque na proteção de dados. Especialmente depois da GDPR e da LGPD, é comum o surgimento de técnicas de *compliance* cada vez mais voltadas ao controle de riscos e de governança com enfoque na área de dados, tendo a proteção como seu grande objeto. Pensa-se, em verdade, na efetivação de direitos a partir do cumprimento de dever fundamental de autodeterminação informativa, porém sendo aplicado aos dados como um todo. Sob esta ótica, o presente estudo tem por objetivo entender como se caracteriza e funciona um programa de *compliance* de dados e a aplicação prática desse mecanismo com base nos pilares do programa de integridade, destacando a necessidade de adaptação à realidade de cada empresa. A metodologia adotada para o desenvolvimento da pesquisa bibliográfica restou amparada no método de abordagem indutiva, sistêmica-construtiva, dialético e a técnica de pesquisa na documentação indireta, especialmente bibliográfica. Já a abordagem se tratou da sistêmica-construtiva que utilizou da perspectiva atual para observar o problema da realidade e construiu resposta adequada ao problema identificado.

Palavras-chave: *compliance* de dados; pilares do programa de *compliance*; LGPD; programa de integridade; análise de risco; dados.

ABSTRACT

The fan for implementing strategies or implementing a compliance program is getting wider and wider. The focus that was previously given especially in the areas: business, labor, criminal, tax, public, competition, third sector and startups, now has great emphasis on data protection. Especially after the GDPR and the LGPD, it is common for the emergence of compliance techniques increasingly focused on risk control and governance with a focus on the data area, with protection as its main objective. One thinks, in fact, of the realization of rights from the fulfillment of the fundamental duty of informative self-determination, but being applied to the data as a whole. From this perspective, the present study aims to understand how a data compliance program is characterized and works and the practical application of this mechanism based on the pillars of the integrity program, highlighting the need to adapt to the reality of each company. The methodology adopted for the development of the bibliographical research remained supported by the inductive, systemic-constructive, dialectical method of approach and the research technique in indirect documentation, especially bibliographical. The approach was the systemic-constructive that used the current perspective to observe the problem of reality and built an adequate response to the identified problem.

Keywords: data compliance; pillars of the compliance program; GDPR; integrity program; risk assessment; data.

LISTA DE FIGURAS

LISTA DE SIGLAS

ANPD	Agência Nacional de Proteção de Dados
ANVIDA	Agência Nacional de Vigilância Sanitária
Art.	Artigo
CGU	Controladoria-Geral da União
COFINS	Contribuição para o Financiamento da Seguridade Social
COSO	*Committee of Sponsoring Organizations of the Treadway Commission*
DPO	Encarregado de Dados
ECA	Estatuto da Criança e do Adolescente
ENAP	Fundação Escola Nacional de Administração Pública
FOIA	*Freedom of Information Act*
GDPR	Regulamento Geral de Proteção de Dados
IBC	Internacional Benchmarking Clearinghouse
IIA	*The Institute os International Auditors*
ICP-BRASIL	Chave Pública
ISO	*International Organization for Standardization*
KPI´S	Indicador Chave desempenho
LGPD	Lei Geral de Proteção de Dados
MAPA	Ministério da Agricultura, Pecuária e Abastecimento
MEC	Ministério da Educação
OMS	Organização Mundial de Saúde
PASEP	Patrimônio do Servidor Público
PIS	Programas de Integração Social
SIF	Serviço de Inspeção Federal

SUMÁRIO

1 INTRODUÇÃO

Este estudo tem como tema principal o *compliance* de dados, especificamente quanto aos elementos concretos de estruturação, implementação e execução de um programa de integridade de dados efetivo. Nesse sentido a pesquisa busca compreender quais são os elementos concretos para implementação destes componentes.

Portanto, atentando-se à necessidade de adequação da empresa à LGPD, bem como às legislações que cada segmento empresarial deve vigilância, destacando ainda a importância da cibersegurança, a indispensabilidade da vigilância e mitigação de riscos dos dados como um todo, julga-se que a implementação do *compliance* como instrumento de inclusão para a proteção de dados é imprescindível em uma empresa.

Diante disso, a presente pesquisa possui como objetivo apresentar uma estrutura de implementação e execução de um programa de *compliance* de dados efetivo, baseado em elementos essencialmente práticos.

Após exposição dos principais conceitos que envolvem o tema (*compliance*, dados de maneira geral, *compliance* de dados, pilares do programa de integridade), centra-se a investigação em propor elementos concretos de estruturação, implementação e execução de um *compliance* de dados efetivo, que possam servir de parâmetro para as empresas interessadas em executar um programa de proteção de dados. Razão pela qual analisa-se a proteção de dados, com ênfase na necessidade e importância de sua vigilância e destacando as normatizações ligadas ao tema, explora-se o *compliance* de dados e toda a sua estrutura e, ainda, apresentou-se os elementos concretos de estruturação, implementação e execução de um programa de *compliance* de dados efetivo.

A proteção de dados se consubstancia, na atualidade, em um tema de extrema relevância, muito teorizado nas obras literárias, todavia, em pesquisa pessoal realizada sobre o assunto nota-se a escassez de ensinamentos práticos para efetivação do mecanismo em questão nas empresas.

O *compliance* surgiu como uma forma de lidar com os riscos da atividade empresarial, e tem a finalidade de evitar a ocorrência de eventos danosos que comprometam a credibilidade de um agente econômico, de uma organização pública e de empresas sem fins lucrativos. Para estes, se trata de uma forma de

autorregulação que o próprio mercado passou a exigir, visando sempre almejar a lucratividade, a expansão dos negócios e a otimização do modo de produção, mas se guiando por condutas éticas e princípios legais.

Já a Lei nº 13.709/2018, intitulada Lei Geral de Proteção de Dados Pessoais (LGPD), visa proteger a liberdade e a privacidade das pessoas naturais que, por qualquer motivo, forneçam seus dados a pessoa natural ou jurídica, de direito público ou privado. Se trata de um marco regulatório da atividade de tratamento de dados e, como dito, sua função primordial é proteger o cidadão. A Lei Geral de Proteção de Dados reconhece que a atividade de tratamento de dados possui riscos implícitos e indeterminados, que podem variar consideravelmente de acordo com as circunstâncias e prejudicar diferentes *stakeholders* (consumidores, investidores, fornecedores, comunidade local, mídia, governo, etc.), o que exige uma análise individualizada de cada a caso.

Nessa direção, a estrutura das instituições complexas também necessita de atenção e avaliações constantes e adequadas no que se refere ao tratamento de dados, que se dará pelo *compliance* de dados, sempre em sintonia com os ditames da Lei Geral de Proteção de Dados, porém buscando um olhar adiante da vigilância de dados pessoais.

Nesse diapasão, no que se refere ao problema a ser tratado no presente trabalho, este se consubstancia-se na indagação de quais são os elementos concretos para estruturação, implementação e execução de um programa de *compliance* de dados efetivo.

Assim sendo, a presente pesquisa tem como hipótese apresentar uma estrutura de implementação e execução de um programa de *compliance* de dados efetivo, baseado em elementos essencialmente práticos.

O primeiro capítulo tratará da proteção de dados, apresentando sua necessidade e importância como segurança e tecnologia da informação, bem como conceituações pertinentes referentes aos dados como ativo de valor e ainda acerca das normatizações e princípios utilizados nos tratamentos. Em seguida, investigar-se-á a origem da Lei Geral de Proteção de Dados, trazendo à baila assuntos pertinentes para a pesquisa sobre o tema.

O segundo capítulo abordará o *compliance* de dados, apresentando sua conceituação e principais discussões acerca do tema. Em continuação, adentrar-se-

á nos pilares do programa de integridade, discorrendo sobre cada um destes e destacando as principais ideias sobre o tema.

O terceiro capítulo discorrerá sobre os elementos concretos de estruturação, implementação e execução de um programa de *compliance* de dados de maneira efetiva, discorrendo, em cada dos pilares do programa de integridade, melhores práticas para se implementar na empresa (seja de qual porte for).

A escolha do tema se justifica pela atualidade, importância e centralidade do assunto. Inegavelmente, o desenvolvimento do presente trabalho trará inúmeros benefícios para os interessados na implementação do *compliance* de dados. Quanto ao primeiro aspecto, convém registrar serem poucos os estudos especificamente sobre o tema de *compliance* de dados, a ponto de não se ter identificado uma obra própria sequer na literatura especializada internacional que aborde o objeto com a exclusividade que aqui se propõe. No Brasil, as pesquisas tendem geralmente a discorrer sobre o assunto somente sob a perspectiva legal da lei geral de proteção de dados, não abordando o *compliance* e desconsiderando os outros dados atrelados ao negócio.

Quanto à importância da matéria, ressalta-se que, diante da escassa produção doutrinária atualmente disponível que efetivamente discorra sobre o *compliance* de dados, o trabalho acadêmico que se proponha a estudar o assunto de modo específico e metodologicamente válido será de extrema valia e preencherá uma lacuna constatada atualmente no direito.

No que pertine à centralidade do assunto, considerando-se que os dados atualmente se tratam do insumo mais valioso do mundo, não carece dúvidas de que a investigação do tema possa servir de parâmetro para as empresas interessadas em implementar um programa de proteção de dados fomentando a difusão, a facilitação e o acesso ao novo mecanismo de controle de riscos, com a finalidade de que o programa não fique restrito ao campo meramente documental, razão pela qual desenvolveu-se ferramentas e apresentação dos principais temas que proporcionem conhecimento inicial para a efetividade do programa.

A metodologia adotada para o desenvolvimento da investigação restou amparada no método de abordagem indutivo, já que irá partir de uma análise específica com o fito de impactar, de forma generalizada, as empresas na implementação do *compliance* de dados. Se amparou, ainda, no método de abordagem dialético e a técnica de pesquisa na documentação indireta,

especialmente bibliográfica. Já a abordagem se tratou da sistêmica-construtiva que utilizou da perspectiva atual para observar o problema da realidade e construiu resposta adequada ao problema identificado.

Ao final, a pesquisa se caracterizou como bibliográfica e objetivou-se a promover o aprofundamento prático do tema exposto. Paralelamente, desenvolveu um estudo documental verificando manuais disponíveis por outras empresas e benefícios trazidos a elas com a implementação do programa de integridade e conformidade, assim como os prejuízos provocados por sua ausência.

Com a dissertação apresentada, espera-se oferecer subsídios para contribuir com a construção e aperfeiçoamento dessa sistemática tão fundamental para as empresas que é o auxílio no entendimento para implementação de um programa de *compliance* de dados.

2 A PROTEÇÃO DE DADOS

A Lei Geral de Proteção e Dados Pessoais brasileira (Lei nº 13.709, de 14 de agosto de 2018, ou simplesmente LGPD[1]) que entrou em vigor no dia 18 de setembro de 2020, se tornou um assunto de grande relevância social e de interesse de toda sociedade, haja vista que com o aumento da utilização da internet os dados pessoais passaram a ficar expostos.

Desde seu advento, mesmo antes da sanção do governo, emergiu questionamentos acerca da quantidade e tipos de dados pessoais coletados, bem como a sua destinação posterior, já que seu uso deve seguir uma série de restrições legais. A Lei Geral de Proteção de Dados dispõe que para fins exclusivos de segurança pública, a lei não será aplicável para o tratamento de dados pessoais em cujos cenários deverão utilizar medidas proporcionais e especificamente necessárias ao atendimento do interesse público, implementando salvaguardas para proteção dos dados do usuário.

Porém, quando o assunto se trata de segurança de dados, o atendimento à Lei Geral de Proteção de Dados é apenas um pequeno percentual dentre uma gama de atenção que se deve ter, a qual, se for ignorada, traz inúmeros prejuízos às empresas (de direito público ou privado, com ou sem fins lucrativos), pessoas físicas e as organizações públicas.

Nesse sentido é sabido que a evolução tecnológica trouxe inúmeros benefícios e conveniências indiscutíveis para a sociedade. Porém, em outro viés, surgiram preocupações quanto à fiscalização e tratamento dos dados.

Com o surgimento de uma nova fronteira da hipercomunicação, que nas palavras de Manuel Castells[2], trata-se de uma nova ‘galáxia da Internet’, com a internet das coisas (*Internet of Things*, ou IoT) propiciada pelo 5G, o *blockchain*, os contratos inteligentes e os indivíduos estarão cada vez mais ameaçados de invasão da privacidade, de suas autodeterminações informativas.

---

[1] 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). Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 18 set. 2022.

[2] CASTELLS, Manuel. **The Internet galaxy**: reflections on the Internet, business, adn society. Oxford: Oxford University Press, 2001.

Conforme Manuel Castells[3], após 1970, houve o desenvolvimento de microprocessadores, o que resultou na existência de computadores mais funcionais; e de bens para que a telecomunicação tivesse progresso. Em decorrência destes constantes desenvolvimentos de bens foi possível a existência da sociedade em rede. Nesta linha, Antonia Espíndola Longoni Klee e Alexandre Nogueira Pereira Neto[4] ensinam que os meios digitais facilitaram a comunicação e o envio de informações de cunho pessoal, situação que reflete no fato de que o avanço da tecnologia aumenta o risco potencial da utilização abusiva dessas informações e, consequentemente eleva a vulnerabilidade do direito à privacidade.

Diante dessa nova realidade, as organizações necessitam buscar soluções preventivas de adequação à tecnologia, visando a mitigação de riscos que a empresa esteja suscetível a incorrer e todas as suas consequências. Por serem fundamentais nessa gestão, a implementação de um programa de *compliance* tem sido a medida mais adotada pelas empresas, seja para gerenciar todos os riscos relacionado ao direito de dados que envolvem as ações da empresa, seja para minimizar riscos de reputação.

2.1 Segurança e tecnologia da informação: necessidade e importância da proteção de dados

Inicialmente, destaca-se a conceituação de dado, que consoante os ensinamentos de Elucida Bergson Lopes Rêgo

> Os dados são a base de todo o processo para geração da sabedoria empresarial e o primeiro nível de estágio a ser atingido. Eles representam fatos através de textos, números, imagens, sons ou vídeos. Os dados não possuem qualquer significado relevante dentro de um contexto de negócio (dado sem contexto)[5].

[3] CASTELLS, Manuel. **Sociedade em rede**. Tradução de Roneide Venâncio Majer. 6. ed. São Paulo: Paz e Terra, 1999.

[4] KLEE, Antonia Espíndola Longoni; PEREIRA NETO, Alexandre Nogueira. A Lei Geral de Proteção de Dados (LGPD): uma visão panorâmica. *In:* THEMOTEO, Reinaldo J. (Coord.). **Proteção de dados pessoais**: privacidade versus avanço tecnológico. Rio de Janeiro: Fundação Konrad Adenauer, 2019.

[5] RÊGO, Bergson Lopes. **Gestão e governança de dados**: promovendo os dados como ativo de valor nas empresas. Rio de Janeiro: Brasport, 2013, p. 14.

Nesta seara, é importante, em um primeiro momento, compreender o conceito de dado e informação, já que se trata de termos utilizados de forma idêntica, sendo útil distinguir seus significados. Por essa perspectiva, Danilo Doneda leciona que:

> Em relação à utilização dos termos “dado” e “informação”, é necessário notar preliminarmente que o conteúdo de ambos de sobrepõe em várias circunstâncias, o que justifica uma certa promiscuidade na sua utilização. Ambos os termos servem a representar um fato, um determinado aspecto de uma realidade. Não obstante, cada um deles possui suas peculiaridades a serem levadas em conta.
> Assim, o “dado” apresenta conotação um pouco mais primitiva e fragmentada, como se observa em um autor que entende como uma informação em estado potencial, antes de ser transmitida. O dado, assim, estaria associado a uma espécia de “pré-informação”, anterior à interpretação e a um processo de elaboração. A informação, por sua vez, alude a algo além da representação contida no dado, chegando ao limiar da cognição. Mesmo sem aludir ao seus significado, na informação, já que se pressupõe a depuração do seu conteúdo – daí que a informação carrega em si também um sentido instrumental, no sentido da redução de um estado de incerteza [6].

Como bem destaca Felipe Nery Rodrigues Machado e Maurício Pereira de Abreu, o tratamento de informações origina vários tipos de dados, porém este registra apenas os aspectos relevantes daquele e, destaca, ainda, que a dificuldade em distinguir informação e dado traz consequências diretas na modelagem de um sistema [7].

Nesta seara, cumpre destacar que os dados são um ativo valioso e devem ser gerenciados conforme são transferidos em uma organização. À medida que as fontes de informações estão se tornando mais numerosas e diversificadas e as iniciativas de conformidade regulatória mais direcionadas, a necessidade de integrar e acessar informações dessas fontes diferentes de forma consistente, confiável e reutilizável também está se tornando essencial.

Nesse sentido, entende-se que a organização e transformação de dados nos direciona a informações valiosas, como leciona Danilo Doneda “uma considerável parcela das liberdades individuais hoje é concretamente exercida em estruturas ou

---

[6] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais** [livro eletrônico]: elementos da formação da lei geral de proteção de dados. 1. Ed. São Paulo: Thomson Reuters Brasil, 2019. P. RB-2.1

[7] MACHADO, Felipe Nery Rodrigues; ABREU, Maurício Pereira de. Projeto de banco de dados: uma visão prática. 17ª edição. Saraiva, p. 17

plataformas nas quais a comunicação e a informação possuem um papel relevante” [8].

Erroneamente, algumas empresas possuem o entendimento de que, por serem pequenas, não necessitam se adequar pois não irão realizar transferência de dados internacionais e, não possuem a pretensão de ter crescimento exponencial. Porém, se equivocam, no sentido de que a empresa de maior porte necessita realizar negócios com a pequena empresa e, se essa não se atentar para o atendimento das determinações, ficará desclassificada de seu rol de colaboradores.

Sem contar que o entendimento acima exposto consubstancia apenas no cumprimento da lei, devendo os empresários se atentarem ao fato de que o dado é um ativo de valor e a aplicação da medida de segurança (*compliance*) agrega pontos positivos à empresa[9].

Cumpre destacar a ressalva de que por segurança da informação entende-se por garantir a integridade e proteção das informações de uma empresa. Todavia, o conceito de segurança da informação não se baseia apenas na proteção dos dados ligada à tecnologia, dentro de um computador, mas inclui todo um sistema, desde o ambiente externo à infraestrutura da empresa[10].

Para proteção de dados necessário se faz preocupar-se com as medidas técnicas, administrativas[11] e físicas[12]. Destacando a última medida, verifica-se que a

---

[8] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais** [livro eletrônico]: elementos da formação da lei geral de proteção de dados. 1. Ed. São Paulo: Thomson Reuters Brasil, 2019. P. RB-2.1

[9] RÊGO, Bergson Lopes. **Gestão e governança de dados: promovendo os dados como ativo de valor nas empresas**/ Bergson Lopes Rêgo- Rio de Janeiro: Brasport, 2013, p. 14.

[10] CASTRO, Rita de C. C. de; SOUSA, Verônica L. Pimental de. **Segurança em cloud computing**: governança e gerenciamento de riscos de segurança. Disponível em: https://www.academia.edu/7520311/Seguran%C3%A7a_em_Cloud_Computing_Governan%C3%A7a_e_Gerenciamento_de_Riscos_de_Seguran%C3%A7a. Acesso em: 25 out. 2022.

[11] A LGPD explana em seu art. 46 que “os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito”.

[12] A própria expressão já diz, refere-se a cercas, portas, fechaduras e extintores, ou seja, controle que evita problemas físicos no âmbito da segurança da informação. No âmbito da proteção de dados, um controle físico pode evitar um problema de um vazamento de dados pessoais na internet, por exemplo, os dados estão armazenados em um servidor, o qual está em uma determinada sala do edifício da sede da empresa, possuindo uma porta que impede a entrada de pessoas não autorizadas, aqui já se tem uma medida física de proteção de dados para garantia da segurança da informação e consequentemente também para a proteção de dados. As legislações de proteção de dados pessoais não falam em medidas físicas apesar destas serem importantes, já que se você tem dados pessoais dos titulares é claro que você vai ter que tomar cuidado com as medidas físicas, você não vai deixar o servidor em uma sala, sem ar condicionado, por exemplo, podendo as máquinas aquecerem até seu determinado limite, gerando problemas. Conclui-se, portanto, que a medida física é um controle preventivo.

proteção de dados pessoais não faz menção a essa questão, pelo fato de que a empresa poderá sofrer uma sanção se não tiver implementado a devida medida técnica, mas curiosamente, a organização não sofrerá nenhum tipo de retaliação se não implantar medida física.

A esse assunto, acrescente-a o entendimento de Jean Miguel Dias, Rita de Cássia M.C. Rodrigues e Daniel Facciolo Pires[13]:

> Na criação de proteção para os dados utilizam-se dois métodos para o controle: os físicos e os lógicos. Basicamente, o controle físico é toda a infraestrutura similar a de um banco para proteger a informação, que vale mais que dinheiro. E os controles lógicos são todos os softwares que ficam responsáveis pelo firewall, pela criptografia, entre outros.

Inicialmente, acerca das medidas técnicas, destaca-se que estas se consubstanciam naquelas que se relacionam com as tecnologias e com os meios de controle que podem ser utilizados no que tange à segurança da informação, podendo-se citar, dentre elas, os mais comumente utilizados como o controle de acesso, a segurança dos dados pessoais armazenados e das comunicações e a manutenção de programa de gerenciamento de vulnerabilidade[14].

Ademais, no que se refere as medidas administrativas, estas se tratam daquelas relacionadas à política e procedimentos referentes à segurança da informação, sendo citada, a título de exemplo, as políticas dessa segurança, conscientização e treinamento e gerenciamento de contratos [15].

Em outro viés, cumpre mencionar que medida física é de extrema relevância, como as outras duas, pelo fato de que possuem o mesmo nível de importância.

---

[13] DIAS, Jean Miguel; RODRIGUES, Rita de Cássia M. C.; PIRES, Daniel Facciolo. A segurança de dados na computação em nuvens nas pequenas e médias empresas. **Revista Eletrônica de Sistemas de Informação e Gestão Tecnológica**, v. 2, n. 1, 2012. Disponível em: http://periodicos.unifacef.com.br/index.php/resiget/article/view/287/278. Acesso em: 18 jul. 2022.

[14] XAVIER, Fabio Correa. **Recomendações de medidas técnicas e administrativas de segurança da informação para municípios de pequeno porte na jornada de adequação à LGPD.** Tribunal de Contas do Estado de São Paulo. 2021. Disponível em < https://www.tce.sp.gov.br/sites/default/files/publicacoes/Artigo-Fabio%20Xavier%20-%20Recomenda%C3%A7%C3%B5es%20de%20medidas%20t%C3%A9cnicas%20e%20administrativas.pdf>. Acesso em 28 de dezembro de 2022.

[15] XAVIER, Fabio Correa. **Recomendações de medidas técnicas e administrativas de segurança da informação para municípios de pequeno porte na jornada de adequação à LGPD.** Tribunal de Contas do Estado de São Paulo. 2021. Disponível em < https://www.tce.sp.gov.br/sites/default/files/publicacoes/Artigo-Fabio%20Xavier%20-%20Recomenda%C3%A7%C3%B5es%20de%20medidas%20t%C3%A9cnicas%20e%20administrativas.pdf>. Acesso em 28 de dezembro de 2022.

Além disto, problemas físicos afetam o funcionamento correto das demais[16]. Cita-se, como exemplo[17], um superaquecimento do computador central, seja por uma inundação ou falta de resfriamento na sala, em que se não houver realizado o *backup*, haverá perda de dados, com consequente prejuízo monetário[18]. Percebe-se como a medida física é tão importante quanto as outras no âmbito da segurança da informação e da proteção de dados pessoais.

Superada esta questão, no que tange à proteção dos dados pessoais, sabe que a implementação de um sistema de gestão de proteção de dados vai gerar um custo para empresa, tanto é que, no corrente ano, houve a proposição do Projeto de Lei nº 4/2022[19] que prevê a alteração das Leis nºs 10.637/2002, 10.833/2003 e 10.865/2004, para permitir o desconto de créditos relativos a valores despendidos com investimentos em atividades de adequação e operacionalização da Lei nº 13.709/2018, da base de cálculo da Contribuição para os Programas de Integração Social (PIS) e de Formação do Patrimônio do Servidor Público (PASEP), da Contribuição para o Financiamento da Seguridade Social (COFINS), da Contribuição para os Programas de Integração Social e de Formação do Patrimônio do Servidor Público incidente na Importação de Produtos Estrangeiros ou Serviços (PIS/PASEP-Importação) e da Contribuição Social para o Financiamento da Seguridade Social

---

[16] PASSOS, Matheus. LGPD, Governança de Dados e Gestão de Metadados. Curso online. Data Science Academy. 2020. Realizado pelo link: https://www.datascienceacademy.com.br/course/lgpd-governanca-de-dados-e-gestao-de-metadados

[17] Pode-se ainda citar outras influências externas, tais como inundações, tempestades, neve, raios, incêndios, etc., os quais podem ameaçar a organização em função da sua localidade, qualidade de proteção dos equipamentos e do potencial destrutivo desses eventos em caso de sua ocorrência- ALMEIDA, Gláucio de Oliveira. NASCIMENTO, Pedro Carvalho; SEIXAS, Flávio Luiz. Pesquisa qualitativa das práticas de segurança nas empresas do setor do TI. Disponível em < https://app.uff.br/riuff/bitstream/handle/1/26255/04__VERSAO_FINAL_ARTIGO.pdf?sequence=1&isAllowed=y >. Acesso em 18 dez. 2022. P. 9.

[18] Acrescenta-se, ainda, outras ações a serem tomadas a fim de enquadrar na fiscalização da medida física: instalação e proteção de equipamentos, utilidades (ativos críticos devem ser capazes de continuar em operação mesmo quando se sucede falhas), manutenção dos equipamentos, segurança de equipamentos fora das dependências da organização, reutilização e alienação segura dos equipamentos, remoção de propriedade – ALMEIDA, Gláucio de Oliveira; NASCIMENTO, Pedro Carvalho; SEIXAS, Flávio Luiz. **Pesquisa qualitativa das práticas de segurança nas empresas do setor de TI.** Disponível em <https://app.uff.br/riuff/bitstream/handle/1/26255/04__VERSAO_FINAL_ARTIGO.pdf?sequence=1&isAllowed=y>. Acesso em 21 dez de 2022. p.15/16

[19] BRASIL. Senado Federal. **Projeto de Lei nº 4 de 2022**. Disponível em: https://www.congressonacional.leg.br/materias/materias-bicamerais/-/ver/pl-4-2022. Acesso em 20 de novembro de 2022.

devida pelo Importador de Bens Estrangeiros ou Serviços do Exterior (COFINS-Importação) [20].

Todavia, o olhar deve ser direcionado para o fato de que o cumprimento à vigilância dos dados, em seu caráter geral, vai além da visão de custos, mas de que se trata de um investimento. Para tanto, há estudos realizados que apresenta evidências empíricas de que o investimento em privacidade gera valor comercial como retorno para a empresa [21].

Harari[22] afirma que a questão da governança dos dados se define como o maior problema da atualidade, do qual depende o futuro da democracia e da humanidade. As questões a serem enfrentas vão além de optar pelo que o autor chama de um “nacionalismo isolacionista” ou uma “cooperação global”, uma vez que os dados serão também utilizados numa visão de empoderamento dos cidadãos, ou numa perspectiva um totalitarismo estatal, em que diversas iniciativas de estados ou do mercado (ou ambos de maneira combinada) possam utilizar os dados sem as devidas seguranças.[23]

Em um outro viés, a pesquisa realizada pela Cisco[24], concluiu que “em todos os entrevistados, a proporção média entre benefícios e gastos foi de 2,7, o que significa que para cada dólar de investimento, a empresa recebeu US$ 2,70 em benefícios[25]”.

Assim sendo, registra-se que os dados, além de se tratar de um dos bens mais valiosos e em abundância, possuem relevância financeira dentro do setor

---

[20] Inclusive, até a data de 27/11/2022 encontra-se aberto a consulta pública acerca do projeto de lei em questão, a qual pode ser acessada pelo sítio eletrônico https://www12.senado.leg.br/ecidadania/visualizacaomateria?id=151507.

[21] DA PRIVACIDADE ao lucro: como obter retornos positivos sobre investimentos em privacidade. Estudo comparativo de privacidade de dados. Cisco 2020. Disponível em: https://www.cisco.com/c/dam/global/pt_br/solutions/pdfs/2020-data-privacy-report-ptbr.pdf. Acesso em: 29 dez 2022.

[22] HARARI, Yuval Noah. **21 lições para o século 21**. Tradução de Paulo Geiger. São Paulo: Companhia das Letras, 2018.

[23] HARARI, Yuvah Noah. **In the battle against coronavirus**: humanity lacks leadership. 2020. Disponível em: https://time.com/5803225/yuval-noah-hararicoronavirus-humanity-leadership/. Acesso em: 17 set. 2021.

[24] A Cisco Systems, Inc. se trata de uma companhia transnacional estadunidense com sede em San José, Califórnia, com 47.000 empregados em todo o mundo e possui como atividade principal o oferecimento de soluções para redes e comunicações, na fabricação e venda e ainda na prestação de serviços por meio de suas subsidiárias. (SOBRE a Cisco. Disponível em: https://www.cisco.com/c/pt_br/about.html. Acesso: 2022).

[25] DA PRIVACIDADE ao lucro: como obter retornos positivos sobre investimentos em privacidade. Estudo comparativo de privacidade de dados. Cisco 2020. Disponível em https://www.cisco.com/c/dam/global/pt_br/solutions/pdfs/2020-data-privacy-report-ptbr.pdf. Acesso em: 15 nov. 2022.

empresarial, devendo ser olhando e tratado não como custo, mas sim como investimento.

Cumpre ressaltar a necessidade de se ter em mente que o dado, desde sua coleta, até a realização do seu descarte, passará por diversas etapas, podendo incorrer em transformações[26]. Nesse sentido, a ABNT NBR ISO/IEC 27002 define que “a informação tem um ciclo de vida natural, desde a sua criação e origem, armazenamento, processamento, uso e transmissão, até a sua eventual destruição ou obsolescência”[27]. Por essa razão a sua proteção é medida necessária e de extrema relevância.

2.2 Dados como ativo de valor: conceituação e principais apontamentos

Não se pretende abordar, de forma técnica, os elementos que compõe um banco de dados, apresentando toda sua contextualização e ramificações, pelo fato de que isso demandaria um conhecimento muito especializado de sistemas de informação.

Dessa forma, buscando compreender os dados como ativo de valor, inicialmente, destaca-se que, no entendimento de Thomas Davenport e Laurence Prusak, dado é compreendido como um componente da informação ainda não tratada, tratando-se de uma descrição exata de algo/algum acontecimento. Os dados empregados isoladamente, não têm propósito, relevância, consequentemente não transmitem conhecimento. A sua importância reside no fato de constituírem a matéria-prima essencial para a criação da informação[28].

Os dados atualmente são considerados o novo petróleo, conforme afirma Samuel Flender[29] na frase originalmente em inglês “*data is the new oil*”, inspiração atribuída ao especialista em ciência de dados Clive Humby em 2006 e que ainda perscruta discussões a respeito de realmente os dados serem ou não esse novo petróleo.

---

[26] AMARAL, Fernando. **Introdução à ciência de dados**. Rio de Janeiro: Alta Books, 2016. p.17

[27] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ABNT. NBR ISO/IEC 27002 – Tecnologia da Informação - Código de Prática para a Gestão de Segurança da Informação – 2013. Disponível em <https://profjefer.files.wordpress.com/2013/10/nbr_iso_27002-para-impressc3a3o.pdf>. Acesso 18 dez. 2022.

[28] DAVENPORT, Thomas H.; PRUSAK, Laurence. **Working knowledge**: how organizations manage what they know. [*S.l.*]: Harvard Business Press, 1998.

[29] FLENDER, Samuel. **Data is not the new oil.** 10 fev. 2019. Disponível em https://towardsdatascience.com/data-is-not-the-new-oil-bdb31f61bc2d. Acesso em: 05 maio 2022.

Ressalta-se que os dados correspondem a um ativo valioso que necessita ser gerenciado consoante é transferido dentro de uma empresa ou organização[30]. Percebe-se que, na medida em que as fontes de informações estão se tornando em maior número e diversificadas no que se refere à tomada de medidas para iniciativa mais assertivas, verifica-se ser essencial a implementação de meios para acessar os dados dessas fontes distintas de forma confiável, reutilizável e consistente, também está se tornando essencial[31].

A união de dados, somados, processados e analisados geram cenários que é conhecido como informação. A informação de qualidade deriva de dados qualificados, o que é uma característica essencial que determina a confiabilidade dos dados para a tomada de decisões [32].

Para Denis Rezende e Aline França[33], informação é todo o dado tratado, trabalhado, útil, com valor significativo ou agregado a ele e com um sentido natural e lógico para quem usa a informação. Acrescenta Yves-François Le Coadic[34] que "a informação é um significado que é transmitido através das mensagens inscrita por meio de signos".

Importante mencionar, como explicado por Jan Van Dijk[35], que a informação constitui a essência da sociedade contemporânea, e adquire formato a partir das estruturas organizacionais, podendo difundir efeitos e gerar danos na esfera jurídica. Para melhor contextualização, reporta-se à confidencialidade, que é aquilo revelado em segredo por dizer respeito a assunto íntimo de alguém.

Qualquer empresa que almeje o aprimoramento de seus recursos de gerenciamento de dados, precisa levar em conta alguns conceitos, dentre eles a

---

[30] FUNDAÇÃO ESCOLA NACIONAL DE ADMINISTRAÇÃO PÚBLICA. **Governança de dados- módulo 1:** contexto da governança de dados na administração pública. Brasília, 2019. Disponível em https://repositorio.enap.gov.br/bitstream/1/5008/1/M%C3%B3dulo%201%20-%20Contexto%20da%20Governan%C3%A7a%20de%20Dados%20na%20Administra%C3%A7%C3%A3o%20P%C3%BAblica.pdf. Acesso em: 25 nov. 2022, p. 13.

[31] FUNDAÇÃO ESCOLA NACIONAL DE ADMINISTRAÇÃO PÚBLICA. **Governança de dados- módulo 1:** contexto da governança de dados na administração pública. Brasília, 2019. Disponível em https://repositorio.enap.gov.br/bitstream/1/5008/1/M%C3%B3dulo%201%20-%20Contexto%20da%20Governan%C3%A7a%20de%20Dados%20na%20Administra%C3%A7%C3%A3o%20P%C3%BAblica.pdf. Acesso em: 25 nov. 2022, p. 13.

[32] PASSOS, Matheus. LGPD, Governança de Dados e Gestão de Metadados. Curso online. Data Science Academy. 2020. Realizado pelo link: https://www.datascienceacademy.com.br/course/lgpd-governanca-de-dados-e-gestao-de-metadados

[33] REZENDE, Denis Alcides; DE ABREU, Aline França. Planejamento estratégico da tecnologia de informação alinhado ao planejamento estratégico de empresas. **Revista de Administração Mackenzie**, v. 3, n. 2, 2008.

[34] LE COADIC, Yves-François. **A ciência da informação**. Brasília: Briquet de Lemos, 1996. P. 5

[35] DIJK, Jan Van. **The network society**. 2. ed. Londres: Sage, 2006, E-book, kindle, p. 138.

onipresença dos dados (referente ao fato de que quase todo processo organizacional consome ou cria dados, ou os dois respectivamente), o valor dos dados como um ativo, o rol de atividades da empresa e as funções envolvidas no gerenciamento de dados[36].

O crescimento do volume, número e da diversificação dos dados que podem ser combinados alcançou um rápido crescimento especialmente pelo uso intensivo da Internet de forma onipresente e ilimitada, elevando o risco de re-identificação dos dados mesmo após a anonimização ou pseudonimização de bases isoladas, cujas conceituações serão exploradas em momento posterior.[37] Registra-se ainda o fato de que no que se refere aos mercados que são abundantes em dados e rodeados por segredos quanto a aplicação de seus algoritmos, os quais são utilizados para propiciar uma vantagem concorrencial, são diversos os danos decorrentes dessa obscuridade [38].

Esses dados em comento, quando em número maior, integram-se aos tão notórios e falados *big datas*, que no entendimento de Gonzáles[39] referem-se a "[...] grandes quantidades e informação digital controlada por companhias, autoridades e outras organizações, sujeitas a uma análise extensa baseada em algoritmos". Registra-se que a utilização dos dados, por si só, não consegue causar danificações, com exceção de aplicação por terceiros sem o consentimento do manuseio das personalidades a eles interligados. Nesta seara, Faleiros Júnior[40] traz a conceituação de *big data* como sendo:

> [...] nada mais é que um enorme banco de dados no qual se armazena todo tipo de informação para que, posteriormente, se

---

[36] FUNDAÇÃO ESCOLA NACIONAL DE ADMINISTRAÇÃO PÚBLICA. **Governança de dados-módulo 2**: princípios, importância e desafios do gerenciamento de dados. Brasília, 2019. Disponível em: https://repositorio.enap.gov.br/bitstream/1/7092/2/M%C3%B3dulo%202%20-%20Princ%C3%ADpios%2C%20Import%C3%A2ncia%20e%20Desafios%20do%20Gerenciamento%20de%20Dados%2003-2021.pdf. Acesso em: 25 nov. 2022.

[37] MOONEY, S. J.; PEJAVER V. Big data in public health: terminology, machine learning, and privacy. **Annu Rev. Public Health**, n. 39, p. 95-112, 2018.

[38] FALEIROS JÚNIOR, José Luiz de Moura. **Administração pública digital**: proposições para o aperfeiçoamento do regime jurídico administrativo na sociedade da informação. São Paulo: Foco, 2020, p. 84.

[39] GONZÁLEZ, Elena Gil. **Big data**: privacidade y protección de dados. Madrid: Agencia Española de Protección de Datos, 2016. Disponível em: https://www.researchgate.net/publication/324831404_Big_data_privacidad_y_proteccion_de_datos. Acesso em: 27 set. 2021, p. 17.

[40] FALEIROS JÚNIOR, José Luiz de Moura. **Administração pública digital**: proposições para o aperfeiçoamento do regime jurídico administrativo na sociedade da informação. São Paulo: Foco, 2020, p. 289.

> trabalhe com esses bancos de dados, cruzando as informações coletadas através de algoritmos, oferecendo possibilidades variadas de previsão de eventos futuros e, ainda, condições de se identificar correlação de dados a partir de causalidades complexas, oferece possibilidades de análises estatísticas infindáveis, normalmente se valendo de amostragens. Quanto maior o banco de dados, maior é a sua confiabilidade e, consequentemente, mais precisa será a aferição obtida pelo algoritmo utilizado na testagem proposta.

No que tange aos dados pessoais, em uma definição mais restrita, conceitua-se apenas aquelas informações que se relacionam a uma pessoa identificada, específica, isto é, o vínculo entre a pessoa e o dado a quem está vinculado é estabelecido de forma direta e imediata[41].

Por outro lado, em uma definição ampla, dado pessoal abrange também os que potencialmente outorguem a identificação do titular da informação. Em outras palavras, um dado será considerado pessoal se a partir dele exista a possibilidade de singularizar a pessoa a quem ele se atribui, mesmo que de forma indireta[42]. Nessa seara, o conceito de dado pessoal pode ser entendido como as comunicações, informações, fatos e ações que se destinem a um indivíduo identificado ou identificável[43].

Mesmo antes do surgimento da tecnologia da informação, a informação e o conhecimento foram fundamentais para a vantagem competitiva. As organizações que possuem informações confiáveis e de alta qualidade sobre seus usuário, produtos, serviços e operações podem tomar melhores decisões do que aquelas sem dados (ou com dados não confiáveis). Porém, produzir dados de alta qualidade e gerenciá-los de maneiras que permitam que sejam utilizados com eficiência não é um processo simples [44].

Ainda, a conceituação de metadados é de extrema relevância para o contexto. A Enap- Fundação Escola Nacional de Administração Pública afirma que:

---

[41] BIONI, Bruno R. Xeque-mate: o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil. **Privacidade e Vigilância**, São Paulo, 2015, p. 17.

[42] MACHADO, Diego; DONEDA, Danilo. Proteção de dados pessoais e criptografia: tecnologias criptográficas entre anonimização e pseudonimização de dados. **Revista dos Tribunais**, São Paulo, v. 998, p. 99-128, 2018, Caderno Especial, p. 106.

[43] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 55-56.

[44] PASSOS, Matheus. LGPD, Governança de Dados e Gestão de Metadados. Curso online. Data Science Academy. 2020. Realizado pelo link: https://www.datascienceacademy.com.br/course/lgpd-governanca-de-dados-e-gestao-de-metadados

> A definição mais comum de metadados – "dados sobre dados" – é aparentemente simples. Para alguns, infelizmente, é uma fonte de confusão e não de esclarecimento, porque muitos tipos de informações podem ser classificados como metadados e não existe uma linha clara entre "dados" e "metadados". Em vez de tentar traçar essa linha, descreveremos como os metadados são usados e por que são tão importantes[45].

Em outras palavras os metadados são dados para identificar dados e, portanto, de um dado se refere a outro dado que se relaciona a outro dado, que se destina a um titular de dados, se tratando de uma corrente em que um leva à outro. Vale mencionar, a título de exemplo, uma foto registrada no celular de uma pessoa, imagem que armazena eventualmente e, dependendo das configurações, pode armazenar a localização, a hora do registro e outras informações diversas. Seguindo esse raciocínio, a localização, a data e o horário do registro da foto corresponde a um metadado. Se tratam, pois, de informações que levam a uma pessoa identificável, motivo pelo qual entende-se o metadado também como dado pessoal.

As alterações jurídicas trazem respaldo legal que proporciona confiança da sociedade, de maneira geral, na lisura dos sistemas informáticos que trabalham com informações sigilosas, colocando, assim, o Brasil em uma posição mais vantajosa perante o setor internacional, pelo fato de que diversos países se preocupam com a segurança da informação, posterior a escândalos de vazamento de informações confidenciais e espionagem. Inovações estas que viabilizam maior atuação das empresas brasileiras em diversas áreas da computação, como por exemplo, no mercado internacional, o *big data* [46].

Apresentado os dados como um ativo de valor, ressalta-se a sua complexidade e tamanha dimensão, destacando que se trata de uma fonte inesgotável e que em cada combinação pode gerar uma nova informação, com novo dado.

---

[45] FUNDAÇÃO ESCOLA NACIONAL DE ADMINISTRAÇÃO PÚBLICA. **Governança de dados**- módulo 4: gerenciamento de metadados e da qualidade de dados. Brasília, 2019. Disponível em: https://repositorio.enap.gov.br/bitstream/1/5008/4/M%C3%B3dulo%204%20-%20Gerenciamento%20de%20Metadados%20e%20da%20qualidade%20de%20Dados.pdf. Acesso em: 25 nov. 2022, p. 5.

[46] ALMEIDA, Gláucio de Oliveira. NASCIMENTO, Pedro Carvalho; SEIXAS, Flávio Luiz. **Pesquisa qualitativa das práticas de segurança nas empresas do setor do TI.** Disponível em < https://app.uff.br/riuff/bitstream/handle/1/26255/04__VERSAO_FINAL_ARTIGO.pdf?sequence=1&isAllowed=y >. Acesso em 18 dez. 2022. P. 12/13.

2.3 Normatizações e princípios utilizados no tratamento de dados

As normatizações a serem utilizadas no tratamento de dados, dependerão de qual ramo a empresa se aloca. Para isso, um levantamento inicial referente aos relacionamentos com terceiros, quais são as suas principais atividades e quais são os riscos iniciais detectáveis, são de extrema importância. Imagine-se que se a implementação de tratamento de dados se dê em uma organização de produção de alimentos, ela deverá ter relações com agentes públicos diversos (MAPA, ANVISA, registro em SIF e na AFFA) para que possa assegurar a qualidade dos produtos produzidos e entregues ao mercado. Ainda, necessária emissão de licenças junto aos órgãos ambientais federais/estaduais/municipais, com as empresas de produção de energia, corpo de bombeiros, entre outros. Se tratar de uma empresa de grande porte, ainda está sujeita aos órgãos reguladores de outros países em que opera, sendo necessária a autorização das entidades de fiscalização sanitária para comercialização naquela localidade.

Portanto, não se trata apenas de fiscalização de uma lei específica. O que se observa, ainda, nesse caso, é a necessidade de verdadeiro diálogo de fontes[47] entre a Lei Geral de Proteção de Dados Pessoais (mais específica) e o Código de Defesa do Consumidor (mais generalista) em relação à tutela dos temas relativos à proteção do ciberconsumidor; e, igualmente, diálogo entre a lei geral de proteção de dados e o Código Civil e/ou o Marco Civil da Internet para a tutela de outras ofensas geradoras de danos (quando não forem relações consumeristas), bem como pela Lei nº 13.787/2018 e a própria Constituição da República.

Cumpre-se realizar uma ressalva acerca da teoria do diálogo das fontes, que diferentemente dos métodos tradicionais da hermenêutica, que rogam pela prevalência de uma norma superior à outra[48], mas se propondo a uma intersecção e complementação das normas, adotando uma coordenação ao invés de monossolução[49].

---

[47] Sobre o tema, confira-se: MARQUES, Claudia Lima. Superação das antinomias pelo diálogo das fontes. **Revista de Direito do Consumidor**, São Paulo, v. 51, p. 34-67, jul./set. 2004.

[48] BOBBIO, Norberto. **Teoria do ordenamento jurídico.** São Paulo/Brasília: Pollis/Universidade de Brasília, 1990.

[49] MARQUES, Claudia Lima. Superação das antinomias pelo diálogo das fontes. **Revista de Direito do Consumidor**, São Paulo, v. 51, p. 34-67, jul./set. 2004, p.25.

Não obstante, no que se refere aos princípios, o artigo 6º da Lei Geral de Proteção de Dados[50], elenca os da boa-fé, finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas. A análise dos princípios revela a preocupação do legislador do indivíduo participar do fluxo de suas informações.

De forma simplificada, pelo princípio da boa-fé entende-se como instituição de padrão ético de conduta pautado nos ideais de lealdade, lisura e honestidade, com o fito de garantir a legitima expectativa e confiança [51]. Somado a este, o princípio da finalidade destaca que a utilização dos dados se proceda nos exatos moldes que haviam sido discriminados no momento do recolhimento, com legítima finalidade, em consonância com as normas que regulamentam o tratamento de dados em todo seu ciclo [52].

Pelos princípios da adequação e necessidade, entende-se que os dados armazenados precisam condizer com a realidade e a motivação condizer com a informação solicitada, assim a coleta e tratamento devem ser feitos de modo adequado com cuidado, de forma específica quanto a sua necessidade, com a correção e devida atualização que vier a ser necessária[53].

Já no que se refere no princípio do livre acesso, destaca-se que este viabiliza que o titular possa, de forma constante, acompanhar o fluxo informacional que lhe diga respeito, devendo ter o direito de solicitar descarte de dados, incorretos ou desatualizados, que sejam fora do contexto ou então ilícitos. Aliado encontra-se o princípio da qualidade dos dados, que define a essencialidade para o tratamento,

---

[50] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). 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: 18 set. 2022.

[51] SILVA, Michael César; SANTOS, Wellington Fonseca. O direito do consumidor nas relações de consumo virtuais. **Revista da Faculdade Mineira de Direito**, v.15, n. 30, jul./dez. 2012 – ISSN 1808-9429. Disponível em < http://periodicos.pucminas.br/index.php/Direito/article/view/P.2318-7999.2012v15n30p119>. Acesso em 17 dez. 2022. p.128.

[52] GEDIEL, José Antônio Peres; CORRÊA, Adriana Espíndola, p.146. Proteção jurídica de dados pessoais: a intimidade sitiada entre o Estado e o mercado. **Revista da Faculdade de Direito** UFPR, v. 47, 2008. p. 147

[53] VIDOR, Daniel Martins. Os princípios da Lei Geral de Proteção de Dados e aplicabilidade. Blog Mercury. 27 de março de 2019. Disponível em <https://pt.linkedin.com/pulse/os-princ%C3%ADpios-da-lei-geral-de-prote%C3%A7%C3%A3o-dados-e-daniel-martins-vidor>. Acesso em 12 de dez. de 2022.

pois somente através das informações confiáveis e atualizadas será possível proteger os direitos do titular [54].

Consoante explica César Pereira Viana, no que se refere ao princípios da transparência de que as questões “estão novamente em vigor nas regulamentações processuais, incluindo a promoção de uma cultura de transparência e disponibilização de dados em línguas acessíveis sem barreiras técnicas” [55].

Pelo princípio da segurança entende-se a imposição ao responsável pelos dados a obrigação de utilização das medidas técnicas e administrativas (já explanadas anteriormente) eficientes à proteção de dados. Ligado ainda ao princípio da prevenção, é imposto que as medidas sejam realizadas de modo qualitativo com a finalidade de evitar eventuais danos decorrentes do tratamento dos dados [56].

Já o princípio da não-discriminação, como já retratado pelo seu próprio nome, trata-se do fato de que os dados, em seu tratamento, não podem ser realizados para finalidades discriminatórias ilícitas ou abusivas, podendo citar como exemplo, a negativa de vaga de emprego em razão da religião ou doença de titular[57].

Quanto ao princípio da responsabilização e da prestação de contas, Adriane Garcel, Sergio Fernando Moro, José Laurindo de Souza Netto e Karen Paiva Hippertt destacam que:

> Caso o uso acarrete prejuízo ou viole quaisquer regras do ordenamento jurídico, ensejará responsabilização civil, nos termos do

---

[54] MACHADO, Luciana Cristina Pinto; MARCONI, Licia Pimentel. Estudos preliminares sobre os princípios aplicados ao tratamento de dados pessoais na Lei nº 13.709/2018- LGPD.**Enepe-Encontro Nacional de Ensino, Pesquisa e Extensão- Inteligência emocional e autodesenvolvimento**. Unoeste, 2020. Disponível em < https://www.unoeste.br/Areas/Eventos/Content/documentos/EventosAnais/564/anais/Sociais%20Aplicadas/Direito.pdf#page=190>. Acesso em 30 dez. 2022.

[55] VIANA, César Pereira. O Princípio Constitucional Da Transparência e a sua relação com o modelo de excelência em Gestão Pública. IV Congresso Consad. Disponível em <https://www.administracao.go.gov.br/noticias/311-gest%C3%A3o/modernizacao/banco-de-boas-praticas-de-gestao/gestao-e-planejamento/15522-o-principio-constitucional-da-transparencia-e-a-sua-relacao-com-o-modelo-de-excelencia-em-gestao-publica.html>. Acesso em: 15 dez. 2022. p.7

[56] GARCEL, Adriane; MORO, Sergio Fernando; SOUZA NETTO, José Laurindo de; HIPPERTT, Karen Paiva. Lei geral de proteção de dados: diretrizes e implicações para uma sociedade pandêmica. Coletâneas de artigosjurídicos: em homenagem ao Professor José Laurindo de Souza Netto. Viviane C. de S. K., Adriane G., José L. de S. N. 1.ed., Curitiba: Clássica Editora, 2020. ISBN 978-65-87965-03-1. Disponível em <https://www.tjpr.jus.br/documents/18319/47149551/42.+Artigo+Lei+Geral+de+Prote%C3%A7%C3%A3o+de+Dados.pdf/f4e4281e-2318-9799-39a8-f394a68230b3>. Acesso em 20 dez. 2022. p. 11

[57] MACHADO, Luciana Cristina Pinto; MARCONI, Licia Pimentel. Estudos preliminares sobre os princípios aplicados ao tratamento de dados pessoais na Lei nº 13.709/2018- LGPD.**Enepe-Encontro Nacional de Ensino, Pesquisa e Extensão- Inteligência emocional e autodesenvolvimento**. Unoeste, 2020. Disponível em < https://www.unoeste.br/Areas/Eventos/Content/documentos/EventosAnais/564/anais/Sociais%20Aplicadas/Direito.pdf#page=190>. Acesso em 30 dez. 2022.

> princípio da responsabilização que exige ainda, o acompanhamento pelas autoridades competentes do processamento dos dados impondo sanções quando houver descumprimento da lei. Paralelamente, o princípio da prestação de contas trata da necessidade de comprovação da adoção das medidas adequadas[58].

Verifica-se, no caso, que são normas de direcionamento e não processos que necessita ser implementados pelas empresas. Em que pese os princípios serem definidos na Lei Geral de Proteção de Dados e o presente trabalho possuir um escopo mais abrangente, esses norteadores são aplicáveis ao tratamento de dados de maneira geral.

Já no que se refere aplicação desse diálogo das fontes, deve ainda ser evitado que a legislação não engesse novos modelos de negócios, especialmente na atualidade em que a internet das coisas, a inteligência artificial, *blockchain*, *bitcoin*, *fintechs*, entre outros, estão cada vez mais presentes na realidade e que se utilizam de dados para gerar valor a todas as empresas [59].

Todo esse universo normativo se consolida em verdadeiro microssistema voltado à preservação das relações jurídicas que envolvam dados, aplicado pela conjugação de cada norma.

2.4 Lei Geral de Proteção de Dados: conceito, contextualização histórica, penalidades decorrentes da não vigilância e o direito fundamental à proteção de dados pessoais

Traduzida por alguns como “privatividade”[60], denotando sua origem advinda daquilo que é “privativo” e indicando o imperativo de tutela contra a perturbação externa, que garante a proteção da intimidade no âmbito individual[61], cumpre ressaltar que a privacidade sempre foi encarada como um contraponto à exposição.

---

[58] GARCEL, Adriane; MORO, Sergio Fernando; SOUZA NETTO, José Laurindo de; HIPPERTT, Karen Paiva. Lei geral de proteção de dados: diretrizes e implicações para uma sociedade pandêmica. Coletâneas de artigosjurídicos: em homenagem ao Professor José Laurindo de Souza Netto. Viviane C. de S. K., Adriane G., José L. de S. N. 1.ed., Curitiba: Clássica Editora, 2020. ISBN 978-65-87965-03-1. Disponível em <https://www.tjpr.jus.br/documents/18319/47149551/42.+Artigo+Lei+Geral+de+Prote%C3%A7%C3%A3o+de+Dados.pdf/f4e4281e-2318-9799-39a8-f394a68230b3>. Acesso em 20 dez. 2022. p. 11

[59] BLUM, Renato; VAINZOF, Rony; MORAES, Henrique. **Data Protection Officer*:*** teoria e prática de acordo com a LGPD e GDPR. São Paulo: Thomson Reuters Brasil, 2020.

[60] COSTA JÚNIOR, Paulo José da. **O direito de estar só**: tutela penal da intimidade. São Paulo: Revista dos Tribunais, 1995, p. 25.

[61] FERNANDES, Milton. **Proteção civil da intimidade**. São Paulo: Saraiva, 1977, p. 90.

Por essa razão, seus efeitos transcendem ordenamentos e se perpetuam no tempo, sendo objeto recorrente de proteção.

Destaca-se, inicialmente, as informações apresentadas por Rodrigo Bisso no sentido de que, em 2018, no setor bancário, especificamente referente ao Banco Inter, conforme investigação realizada pelo Ministério Público, foram vazados dados de vinte mil clientes, e quase um ano depois, por uma falha de segurança na mesma empresa, os dados de mais de um milhão e quatrocentos clientes. Em outro viés, no setor educacional, noticiou-se que sessenta colégios e faculdades americanas deixaram vazar dados de alunos, em decorrência de vulnerabilidades nos sistemas operacionais computacionais. Ainda, na área de rede social, em 2019, houve quinhentos e quarenta milhões de vazamentos de registros de usuários da plataforma facebook. Destaca-se, ainda que no setor médico, sete milhões e setecentos mil dados de pacientes vazaram da empresa *LabCorp* [62].

A proteção de dados não é algo que está surgindo agora, sua existência já se estende por algum tempo. O primeiro momento em que se verifica a defesa do direito à privacidade se dá em 1890, quando os advogados norte-americanos Samuel D. Warren e Louis Brandeis, escreveram o artigo *The Right to Privacy*[63], onde defenderam o direito a ser “deixado sozinho”, definição que davam para a privacidade, no fim do século XIX, indicando, então que esta corresponderia ao direito que uma pessoa tem a ser deixada sozinha.

A partir daí começa-se uma evolução desta proteção de dados, não apenas em declarações, que não têm força vinculativa, ou seja, são mais uma visão de princípios e ideal a ser feito, mas também em legislações específicas à proteção da privacidade individual. Em 1967 o *Freedom of Information Act* (FOIA)[64] nos Estados Unidos, que trata do direito do cidadão de ter acesso ao que agências governamentais têm sobre ele.

Após, em 1980, surgem as diretrizes, orientações da *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (OECD), ou seja, é o

---

[62] BISSO, Rodrigo et al. Vazamentos de dados: histórico, impacto socioeconômico e as novas leis de proteção de dados. **Revista Eletrônica Argentina-Brasil de Tecnologias da Informação e da Comunicação**, v. 3, n. 1, mar. 2020, p. 1-3.

[63] WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. **Harvard Law Review**, v. 4, n. 5, p. 193-220, dez. 1890. Disponível em: http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html. Acesso em 25 out. 2022.

[64] FREEDOM OF INFORMATION ACT. **[Site]**. Disponível em: https://www.foia.gov/. Acesso em: 04 out. 2022.

primeiro documento europeu que trata especificamente do fluxo internacional de dados pessoais, contendo princípios muito semelhantes ao do atual regulamento europeu[65].

Em 1981, tem destaque a publicação pelo Conselho da Europa, da chamada *Convention for the Protection of Individuals with regard to Automatic Processing os Personal Data* (Convenção 108)[66]. Trata-se de um documento juridicamente vinculante, que obriga os signatários a que os dados pessoais sejam devidamente protegidos, devendo criar legislação interna nesse sentido[67]. É um documento relevante, que ainda está válido e do qual vários países são signatários, não apenas europeus, mas também de outros continentes como a América, sendo exemplos, o Uruguai, a Argentina e o México.

Depois disto e agora entramos mais especificamente no contexto europeu, temos em 1995 a Diretiva 95/46/CE[68] que foi o primeiro documento jurídico, em âmbito europeu, para a proteção de dados pessoais. Essa Diretiva 95/46/CE teve um marco importante por ser a primeira legislação, em âmbito europeu, para a proteção de dados pessoais, também chamada de DPD (Diretiva de Proteção de Dados) o que significou dizer, portanto, que a partir de 1995 todos os Estados-membros da Comunidade Europeia eram obrigados a ter uma legislação de proteção de dados que seguia este modelo criado pelo Parlamento Europeu que era a Diretiva 95/46. Razão pela qual, pode-se dizer, que desde 1995 existia nos estados-membros da União Europeia legislação de proteção de dados[69].

---

[65] MORGADO, L. F. O cenário internacional de proteção de dados pessoais. Necessitamos de um Código Brasileiro?. **Âmbito Jurídico**, Rio Grande, v. 12, n. 65, jun. 2009. Disponível em: http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=6336. Acesso em: 19 nov. 2021.

[66] COUNCIL OF EUROPE. **Convention for the protection of individuals with regard to automatic processing of personal data**. Strasbourg, 1981. Disponível em: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108. Acesso em: 20 abr. 2021.

[67] Cumpre destacar que se trata de um documento válido, mas que necessita que cada país crie sua legislação interna para cumprir com os ordenamentos presentes na Convenção 108, diferentemente da Diretiva. Antes cada país membro da União Europeia necessitava da edição de normas internas de aplicação, se tratando de um direcionamento, de instrução, que dificultava a harmonia e adequação interna das legislações com os países. ARMELIN, Ruth Maria Guerreiro da Fonseca; TEIXEIRA, Tarcisio. **Lei geral de proteção de dados pessoais comentada artigo por artigo.** Salvador: Juspodim, 2019, p. 20.

[68] DIRECTIVA 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046. Acesso em: 2022.

[69] MOSHELL, Ryan. And there was one: the outlook for a self-regulatory United States amidst a global trend toward comprehensive data protection. **Texas Tech Law Review**, v. 37, p. 366-367, 2005.

Avançando, em termos de contextualização, tem-se outros dois marcos. Em 2002 surgiu a Diretiva ePrivacy (Europa)[70] de grande relevância porque regula o *marketing* na Europa em relação aos dados, disciplina os *cookies* em sites, na medida em que contêm dados pessoais, regulando como os sites devem apresenta-los e pedir o consentimento dos titulares. Essa diretiva abrange comunicações de maneira geral, trazendo recomendações não apenas sobre *marketing* direto (e-mail, por exemplo), mas também por outros meios como ligações telefônicas e correios.

Outro marco, em 2016, foi a aprovação do Regulamento Geral sobre a Proteção de Dados ("RGPD" ou "GDPR") pelo Parlamento Europeu. Sobre o regulamento, explana Pedro Alexandre Brandão Mendes que:

> O RGPD já é de uma complexidade significante com grandes mudanças e impactos nos negócios, e como se trata de um regulamento, para além de ter que ser cumprido de igual forma em todos os países da União Europeia, a sua implementação é obrigatória também nos países membros. O cumprimento com este regulamento tem como princípio fundamental a gestão de riscos para os dados pessoais dos titulares dos dados, e implica que as organizações necessitem de realizar análises de risco aos seus processos que tratem dados pessoais e às suas atividades que os processam [71].

Com base na GDPR, criou-se a Lei Geral de Proteção de Dados, cuja norma tem como objetivo dispor as regras de tratamento de dados pessoais, seja em ambientes físicos ou virtuais, por pessoas jurídicas ou físicas, tanto de direito público como de direito privado, com o intento de assegurar o livre desenvolvimento da pessoa natural; bem como de fazer o direito fundamental à privacidade ter eficiência e efetividade [72]. Se trata de um marco regulatório da atividade de tratamento de dados e, como dito, sua função primordial é proteger o cidadão.

---

[70] COSTA, Marta Maia Campos. **O sistema de vigilância na União Europeia**: a conservação de dados pessoais gerados no contexto das comunicações eletrónicas e a violação da carta dos direitos fundamentais da União Europeia. 2016. Dissertação (Mestrado em Direito Público, Internacional e Europeu) – Escola de Direito, Universidade Portuguesa, Porto, 2016. Disponível em: https://repositorio.ucp.pt/bitstream/10400.14/21981/1/Disserta%C3%A7%C3%A3o%20Marta%20Campos%20Costa%20-%202016%20.pdf. Acesso em: 25 nov. 2022.

[71] MENDES, Pedro Alexandre Brandão. **Análise de Risco no GDPR.** 2018. Disponível em < https://repositorio.ul.pt/bitstream/10451/35494/1/ulfc124806_tm_Pedro_Mendes.pdf>. Acesso em 20 dez. 2022.

[72] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). 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: 18 set. 2022.

Antonia Espíndola Longoni Klee e Alexandre Nogueira Pereira Neto[73] argumenta que o processo de tratamento de dados pessoais, tanto por agentes privados quanto pelo poder público, independentemente do local de sede e do ramo de atuação, terá irradiação da lei geral de proteção de dados:

> [...] desde que: a operação de tratamento seja realizada no território nacional; a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

Os fundamentos que justificam a intervenção do Estado na atividade econômica a partir da lei geral de proteção de dados[74], e que também norteiam a aplicação deste marco regulatório, estão elencados na própria lei:

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

Se nota que o legislador buscou inspiração nos mais caros valores da democracia liberal, como autodeterminação, liberdade de expressão, respeito à privacidade e à livre inciativa, dentre outros, para “demonstrar o nível de seriedade e importância do país na proteção das liberdades, de modo a servir como instrumento a permear relações mais transparentes e menos abusivas”[75].

---

[73] KLEE, Antonia Espíndola Longoni; PEREIRA NETO, Alexandre Nogueira. A Lei Geral de Proteção de Dados (LGPD): uma visão panorâmica. *In:* THEMOTEO, Reinaldo J. (Coord.). **Proteção de dados pessoais**: privacidade versus avanço tecnológico. Rio de Janeiro: Fundação Konrad Adenauer, 2019, p. 17.

[74] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). 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: 18 set. 2022.

[75] SILVA, Daniela Juliano. Govtech à Brasileira: o plano nacional de internet das coisas e o cadastro base do cidadão. *In:* LEAL, Fernando; MENDOÇA, José Vicente Santos de (Org.). **Transformações do direito administrativo:** liberdades econômicas e regulação. Rio de Janeiro: FGV Direito Rio, 2019, p. 117.

A preocupação com a autodeterminação do indivíduo fica evidente no artigo 11, inciso I, da lei geral de proteção de dados que taxa como indispensável o consentimento do titular (ou seu responsável) que fornece dados para tratamento, que deve ocorrer “de forma específica e destacada, para finalidades específicas” [76].

A Lei Geral de Proteção de Dados[77] também definiu no artigo 5º diversos conceitos essenciais para se compreender a atividade de tratamento de dados[78], dentre os quais podem ser destacadas as definições sobre os principais atores do tratamento de dados

> V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
> 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;
> VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);
> IX - agentes de tratamento: o controlador e o operador;

Além de diferenciar dados pessoais de dados pessoais sensíveis e definir regras especiais para tratamento de dados de crianças e adolescentes, a Lei Geral de Proteção de Dados[79] traz ainda as hipóteses em que o tratamento de dados de cada uma destas modalidades pode ser realizado, além de definir os direitos do titular dos dados e outras questões.

---

[76] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). 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: 18 set. 2022.

[77] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). 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: 18 set. 2022.

[78] DONDA, Daniel. **Guia prático da implementação da LGPD**: tudo o que sua empresa precisa saber para estar em conformidade. São Paulo: Labrador, 2020. e-Book, p. 19.

[79] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). 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: 18 set. 2022.

A Lei Geral de Proteção de Dados[80] obriga no artigo 37 que o controlador e o operador mantenham o registro das operações de tratamento de dados que realizarem, belo exemplo da preocupação do legislador com a transparência nos processos de tratamento de dados. Sobre esse assunto Daniel Donda explica que

> De acordo com a lei, temos que prever os riscos relacionados a um acidente se ele ocorrer e descrever quais foram as medidas adotadas para reverter os efeitos do prejuízo. Todo esse tema, na verdade, é muito amplo, e talvez seja necessária a contratação de profissionais da segurança da informação para ajudar no processo de análise e avaliação de seus ativos [81].

A Lei Geral de Proteção de Dados[82] também exige, no artigo 41, que o controlador indique formalmente a pessoa que será a encarregada de tratamento de dados, que internacionalmente é conhecido por *Data Protection Officer* (DPO), cujos dados devem ser públicos e acessíveis.

O encarregado de tratamento de dados, ou DPO, tem suas funções definidas no parágrafo segundo do referido artigo, sendo que o parágrafo terceiro permite ainda que a autoridade nacional crie normas complementares sobre *"a definição e as atribuições do encarregado"*. É oportuno transcrever o que a lei entende como atividades do encarregado de tratamento

> § 2º As atividades do encarregado consistem em:
> I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
> II - receber comunicações da autoridade nacional e adotar providências;
> III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e
> IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares[83].

---

[80] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). 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: 18 set. 2022.

[81] DONDA, Daniel. **Guia prático da implementação da LGPD**: tudo o que sua empresa precisa saber para estar em conformidade. São Paulo: Labrador, 2020. e-Book, p. 83.

[82] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). 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: 18 set. 2022.

[83] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). 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: 18 set. 2022.

Como visto, o DPO, ou encarregado, é o canal de relacionamento entre os agentes de tratamento de dados e a sociedade – e daí vem a preocupação com a publicidade de sua identificação precisa –, mas quem efetivamente procede ao tratamento dos dados pessoais constantes dos bancos de dados da instituição é o controlador (aquele que toma decisões) e o operador (aquele que realiza a análise dos dados).

Diogo Silva Marzzoco destaca que, tendo em vista a importância do papel do encarregado, que necessita ser exercido com responsabilidade e profissionalismo e, embora não conste na Lei Geral de Proteção de Dados é recomendável que o profissional tenha conhecimento jurídico e regulatório, tendo em vista a necessidade de harmonização das leis e outras regulações setoriais [84].

Portanto, são os agentes de tratamento de dados aqueles que devem estar mais atentos às boas práticas do *compliance* digital e com as regras da Lei geral de proteção de dados, e por isso mesmo são os que podem ser responsabilizados por danos acarretados na atividade de tratamento de dados.

Conforme dispõe o artigo 42 da lei geral de proteção de dados[85],

> O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.

A responsabilidade civil ainda poderá ser solidária entre os agentes de tratamento nas hipóteses dos incisos do artigo 42, § 1º, da LGPD[86], que se verificam quando o operador descumprir a lei ou as instruções lícitas do controlador; ou quando este também estiver envolvido no tratamento de dados que gerou danos ao(s) titular(es).

---

[84] MARZZOCO, Diogo Silva. A figura do encarregado pela proteção de dados pessoais. In: **Lei Geral de Proteção de Dados: estudos sobre um novo cenário de Governança Corporativa/** coordenado por Rodrigo Pironti. Belo Horizonte: Fórum, 2020. p. 235

[85] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). 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: 18 set. 2022.

[86] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). 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: 18 set. 2022.

Embora seja matéria nova no ordenamento jurídico brasileiro (e nos nossos tribunais), a doutrina já se debruça sobre a responsabilidade civil dos agentes de tratamento de dados, sendo que Walter Aranha Capanema traça critérios a serem seguidos para a mensuração do quantum indenizatório em caso de responsabilização civil dos agentes de tratamento de dados, e também da aplicação das sanções administrativas que serão vistas adiante:

> a) a quantidade de dados pessoais afetados; b) a natureza dos dados pessoais afetados: o vazamento de dados pessoais sensíveis, por exemplo, determinará uma indenização maior, especialmente se se tratar de dados biométricos, que não podem ser substituídos; c) a reincidência da conduta; d) a omissão em tomar medidas de segurança e técnicas para minorar o dano ou em colaborar com a Autoridade Nacional de Proteção de Dados; e) a ausência de notificação dos usuários da ocorrência do incidente; f) a comprovada utilização dos dados pessoais vazados de titulares por terceiros [87].

Como dito, a Lei Geral de Proteção de Dados prescreve no artigo 52 sanções administrativas aos agentes de tratamento que causarem danos por descumprimento da lei, que vão de advertência a multa que pode chegar a cinquenta milhões de reais, além da publicização da infração, bloqueio ou eliminação dos dados pessoais a que se refere a infração, suspensão parcial do funcionamento do banco de dados a que se refere a infração e até mesmo proibição total ou parcial do exercício de operações que envolvam tratamento de dados[88].

Tem-se, portanto, que as medidas a serem tomadas pelos agentes de tratamento de dados são nada mais que cuidados para que os dados pessoais constantes dos bancos de dados das instituições não sejam vazados, causando prejuízos à privacidade de terceiros.

Importante destacar que a Lei Geral de Proteção de Dados dita regras para que as instituições criem seus planos de *compliance* digital, pois é trabalhada em todo um estímulo de autorregulação, o que se reflete na verdade numa corregulação[89].

---

[87] CAPANEMA, Walter Aranha**.** A responsabilidade civil na Lei Geral de Proteção de Dados. **Cadernos Jurídicos**, São Paulo, v. 21, n. 53, p. 163-170, 2020, p. 168.

[88] REIS, Luciano Elias; LIPPMANN, Rafael Knorr. A administração pública na lei geral de proteção de dados. In: **Lei Geral de Proteção de Dados: estudos sobre um novo cenário de Governança Corporativa/** coordenado por Rodrigo Pironti. Belo Horizonte: Fórum, 2020. P. 176

[89] LÓSSIO, Claudio Joel Brito. **Proteção de Dados e *Compliance* Digital**. São Paulo: Almedina, 2021, p. 20.

2.5 Autoderminação Informativa

Sendo a informação a substância essencial da composição dessa nova morfologia estruturante da sociedade, "os dados pessoais chegam a fazer às vezes da própria pessoa em uma série de circunstâncias nas quais a sua presença física seria outrora indispensável"[90], motivo pelo qual o tratamento de tais dados adquire notável relevância, a ponto de se definir a proteção constitucional para as informações e para os dados pessoais [91].

No que concerne à almejada proteção do livre desenvolvimento da personalidade é que reside a proposta defendida, dentre outros, por Bruno Bioni, no sentido de que: o enquadramento da proteção de dados como categoria autônoma dos direitos da personalidade é visualizada como liberdade positiva, em contraposição ao direito à privacidade, visto como liberdade negativa [92]. É a partir dessa concepção que se desenvolve o lastro teórico de um direito fundamental autônomo.

Nesta seara, importante destacar a decisão do Supremo Tribunal Federal (STF) em foram referendadas medidas cautelares autorizadas pela ministra Rosa Weber em cinco Ações Diretas de Inconstitucionalidade (ADIs) ajuizadas contra a Medida Provisória (MP) 954/2020 que se refere ao compartilhamento de dados pessoais entre operadoras de telefonia e o Instituto Brasileiro de Geografia e Estatística (IBGE), para firmar o entendimento de que o compartilhamento previsto na referida MP viola o direito constitucional à intimidade, à vida privada e ao sigilo de dados. Os ministros do STF destacaram a higidez do IBGE, bem como o seu caráter de instituição pública de pesquisa, porém não esconderam sua desconfiança em relação aos objetivos da coleta do nome, endereço e número de telefone de milhões de brasileiros (artigo 2º da MP 954/20) [93].

---

[90] DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico**, Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011, p. 92.

[91] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 169. E, nesse contexto, a autora sustenta que: “[...] a vitalidade e a continuidade da Constituição dependem da sua capacidade de se adaptar às novas transformações sociais e históricas, possibilitando uma proteção dos cidadãos contra novas formas de poder que surgem na sociedade”.

[92] BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020.

[93] BRASIL. Supremo Tribunal Federal. **STF suspende compartilhamento de dados de usuários de telefônicas com IBGE**. 2020. Disponível em:

No Brasil, o tema se tornou de tamanha relevância que o Congresso Nacional sinalizou, anteriormente, a consagração da proteção de dados pessoais como direito fundamenta (através da Proposta de Emenda à Constituição 17/2019, que visava incluir a proteção de dados pessoais entre os direitos e garantias fundamentais do cidadão, inserindo o inciso XII-A ao rol do artigo 5º da Constituição)[94], devidamente aprovada e alterada para emenda constitucional nº 115 de 10/02/2022 [95].

Referida decisão acatou uma preocupação generalizada no que se refere a iniciativas de monitoramento no período da quarentena, decorrentes do período pandêmico e a ameaça de um Estado em vigilância, já que, até aquele momento, não ocorreu a entrada em vigor da lei geral de proteção de dados, não existindo, assim, a figura de um fiscalizador, reconhecendo que a Constituição Federal contém elementos basilares da proteção de dados (como o direito à honra, imagem, intimidade, vida privada e dignidade), pronunciando, de forma explícita, o princípio de autodeterminação informacional [96].

O conceito de autodeterminação informativa teve origem na República Federal da Alemanha, reconhecido, originalmente, como direito fundamental, em 1983, em uma decisão histórica de um caso paradigmático da autodeterminação informativa declarada pelo Tribunal Constitucional Federal Alemão (TCFA) sobre a Lei do Censo [97]. De acordo com Danilo Doneda:

> O direito à autodeterminação informativa surgiu basicamente como uma extensão das liberdades presentes nas leis de segunda geração, e são várias as mudanças específicas neste sentido que podem ser identificadas na estrutura destas novas leis. O tratamento de dados pessoais era visto como um processo, que não se encerrava na simples permissão ou na da pessoa à utilização de seus dados pessoais, porém procurava incluí-la em fases sucessivas do processo de tratamento e utilização de sua própria informação por

---

http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=442902. Acesso em: 03 jan. 2020.

[94] BRASIL. Senado Federal. **Proposta de Emenda à Constituição nº 17, de 2019.** 2019. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/135594Acesso em: 20 dez. 2020.

[95] "Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais"- (BRASIL. Senado Federal. **Proposta de Emenda à Constituição nº 17, de 2019.** 2019. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/135594Acesso em: 20 dez. 2020).

[96] BRASIL. Senado Federal. **Proposta de Emenda à Constituição nº 17, de 2019.** 2019. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/135594Acesso em: 20 dez. 2022.

[97] MARTÍNEZ, Ricard. ***El derecho fundamental a la protección de datos: perspectivas***. Revista Internet, Derecho y Política, nº 5, 2007. Disponível em <https://www.researchgate.net/publication/28178556_El_derecho_fundamental_a_la_proteccion_de_datos_perspectivas>. Acesso em: 20 dez. 2022.

> terceiros, além de compreender algumas garantias, com o dever de informação [98].

Nesta seara, cumpre destacar que autodeterminação informativa, conhecida como a “liberdade informática” [99], significa dizer que, se forma singular, aos titulares de dados é concedido o direito de determinar o que sobre si deve e possui vontade de ser divulgado à terceiros [100].

Consoante elucida Ingo Wolfgang Sarlet, no que se refere a distinção da autodeterminação informativa em relação à proteção de dados:

> O que se pode afirmar, sem temos de incorrer em erro, é que seja na literatura jurídica, seja na legislação e jurisprudência, o direito à proteção de dados vai além da tutela da privacidade, cuidando-se, de tal sorte, de um direito fundamental autônomo, diretamente vinculado à proteção da personalidade [101]

Verifica-se, portanto, que o direito à autodeterminação informativa possui como pretensão assegurar uma ampla proteção de dados pessoais, por meio da participação ativa do cidadão, em todo o processo de coleta, tratamento, armazenamento e compartilhamento de tais dados [102].

2.6 Tecnologia da informação e comunicação: importância e melhores práticas de segurança no tratamento de dados

Toda empresa deveria ter, em sua generalidade, uma preocupação no sentido de aplicação de melhores práticas de segurança no que se refere ao tratamento de dados, instituindo até mesmo softwares, sejam estes públicos ou privados, a fim de garantir, tanto aos clientes, fornecedores e aos colaboradores o olhar desta garantia.

---

[98] DONEDA. Danilo. Princípios da proteção de dados pessoais. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira Pereira de (Coord.). *Direito e Internet III*. Marco Civil da Internet. Lei nº 12.965/2014. Tomo I. São Paulo: Quartier Latin, 2015, p. 373.

[99] PÉREZ LUÑO, Antonio Enrique. ***Manual de informática y derecho***. Barcelona: Ariel, 1996, p. 44.

[100] CUEVA, Pablo. ***Informática y Protección de Datos Personales. Revista Chilena de Derecho Informático***. 2011. Disponível em <https://www.researchgate.net/publication/314947621_Informatica_y_Proteccion_de_Datos_Personales>. Acesso em: 20 dez. 2022.

[101] SARLET, Ingo Wolfgang. **Proteção de dados pessoais como direito fundamental na Constituição Federal de 19881: contributo para a construção de uma dogmática constitucionalmente adequada**. Direitos e Fundamentos & Justiça, Belo Horizonte, ano 14, n. 42, p. 179-218.

[102] SANTOS JÚNIOR, Belisário dos, SANTOS, Juliana Vieira dos. Autodeterminação informativa: surge um novo direito fundamental. **Aspectos relevantes da lei geral de proteção de dados**/ (organizadores) Gustavo Marinho (et al.). 1 ed. São Paulo: Editora Contracorrente, 2021, p. 23.

Nas palavras de Ricardo Albuquerque[103] “é impossível obter um sistema seguro em um ambiente inseguro”

Tem-se, assim, que a segurança de dados se trata de um dos grandes desafios deste século e a tendência é o aumento dos danos causados [104]. Nesse sentido, Paulo Henrique de Souza Oliveira e Alencar Machado destaca que:

> Diante do atual cenário da internet, onde ataques a sites de organizações públicas e privadas estão cada vez mais comuns, é fundamental que os profissionais da áreas de tecnologia implantem rigorosas políticas de segurança, não só para o cumprimento do usuário final, como também o próprio desenvolvimento, estudando e corrigindo riscos que possam ser explorados por pessoas e *softwares* mal intencionados [105].

Sobre esse ponto, quando já acometido com o problema de vazamento da segurança dos dados, em seu tratamento, os responsáveis pela empresa devem realizar um levantamento de vulnerabilidades, como o objetivo de adotar medidas cabíveis ao fortalecimento para apurar os níveis de segurança internamente, a fim de que mitigue as possibilidades de novas ocorrências [106].

No que se refere ao tratamento de dados, é sabido que se torna imperioso a implementação das políticas de privacidade, incluindo ferramentas, treinamento e disseminação, antes do acometimento de problemas. Esses mecanismos que se darão através da aplicação do programa de *compliance*, devem incluir ferramentas que facilitem as tomadas de decisões dentro das organizações relativas ao uso

---

[103] ALBUQUERQUE, Ricardo. **Segurança no desenvolvimento de software: como garantir a segurança do sistema para seu cliente usando a ISSO/IEC**. Ricardo Albuquerque, Bruno Ribeiro Imprenta. Rio de Janeiro: Campus, 2002. p.5.

[104] BATISTA, Lucas Oliveira, SILVA, Gabriel Adriano de; ARAÚJO, Vanessa Souza; ARAÚJO, Viníciu Jonathan Silva; REZENDE, Thiago Silva, GUIMARÃES, Augusto Junio; SOUZA, Paulo Vitor de Campos. **Utilização de Redes Neurais Nebulosas para criação de um Sistema Especialista em Invasões Cibernéticas**. Icofcs, 2018, p. 1. Disponível em <http://icofcs.org/2018/ICoFCS-2018-002.pdf>. Acesso em 18 dez. 2022.

[105] OLIVEIRA, Paulo Henrique de Souza; MACHADO, Alencar. **Uso de boas práticas de segurança no tratamento das principais vulnerabilidades de software no desenvolvimento para web**. Disponível em < https://publicacoeseventos.unijui.edu.br/index.php/salaoconhecimento/article/view/16694/15376>. Acesso em 25 dez. 2022.

[106] PASSOS, Matheus. LGPD, Governança de Dados e Gestão de Metadados. Curso online. Data Science Academy. 2020. Realizado pelo link: https://www.datascienceacademy.com.br/course/lgpd-governanca-de-dados-e-gestao-de-metadados.

apropriado de dados, proteção e capacitação, bem como para com terceiros que se relacionam com a empresa [107].

Noutro giro, no que se refere a importância da segurança no tratamento de dados, cumpre ressaltar que, os custos despendidos para a implantação de uma política de *compliance* na empresa se dividem em: custos de manutenção (despesas para executar e promover essa política, assim como custo de pessoal, treinamento, comunicação) e custos de governança (manutenção e despesas da diretoria e dos comitês, despesas legais e jurídicas, contratação de auditoria externa ou criação de uma auditoria interna). Não aderindo ao Programa de Conformidade, a empresa/empresário poderá sofrer as penalidades, multas e tributos de imposições por violação às leis, custo de remediação, perda da receita, interrupção dos negócios e perda da produtividade, impacto no capital, danos à reputação com produção de imagem negativa de seus empregados e da marca, despesas com custas judiciais e valor/hora da alta administração[108].

Expõe Coelho[109] que a tentativa de identificação prévia dos riscos pela empresa e posteriormente afastá-los ou mitigá-los, faz com que aumente sua credibilidade econômica, financeira e social.

Acrescenta-se a esse ponto a extrema importância da tomada de práticas para segurança do tratamento de dados destinado para as pequenas e médias empresas, isso porque se tratam de empresas em crescimento, e qualquer equívoco com o tratamento dos dados (sejam eles pessoais de terceiros, sejam eles estratégicos para o negócio) pode acarretar em perdas extremas, comprometendo toda a organização e seu desempenho [110].

Sucede-se, ainda, que diante do aumento de consumidores atentos, que procuram não somente os bens de consumo propriamente dito, mas também

---

[107] SCATOLIN, Carolina Lanzini. Uso da Tecnologia *blockchain* no *compliance* de dados: uma análise da possibilidade e entraves a serem resolvidos. **Revista de Economia, Empresas e Empreendedores na CPLP.** Volume 08, número 01| 10.29073/e3.v8i1.611. Disponível em <https://revistas.ponteditora.org/index.php/e3/article/view/611/418>. Acesso em 19 dez. 2022.

[108] COIMBRA, Marcelo de Aguiar; MANZI, Vanessa Alessi (Org.). **Manual de compliance**: preservando a boa governança e a integridade das organizações. São Paulo: Atlas, 2010, p. 106

[109] COELHO, Cláudio Carneiro Bezerra Pinto. **Compliance na Administração Pública**: uma necessidade para o Brasil. 2016. Disponível em:<https://www.researchgate.net/publication/323352076_O_COMPLIANCE_NA_ADMINISTRACAO_PUBLICA_E_A_LEI_1330316>. Acesso em: 06 fev. 2022.

[110] PASSOS, Matheus. LGPD, Governança de Dados e Gestão de Metadados. Curso online. Data Science Academy. 2020. Realizado pelo link: https://www.datascienceacademy.com.br/course/lgpd-governanca-de-dados-e-gestao-de-metadados.

averiguam o comportamento das organizações de acordo com esses valores, o tratamento de dados converte-se em vantagem competitiva[111].

Portanto investir na segurança do tratamento de dados vai além de criar a proteção, proporciona lucros para a empresa. Trata-se de uma vantagem competitiva e fundamental em que as organizações, a alta administração e os colaboradores devem abraçar a transparência e a responsabilidade da maneira como gerenciam dados. Assim sendo, qualquer perspectiva regulatória para a proteção dos dados necessita levar em conta a existência de uma economia de vigilância.

[111] PASSOS, Matheus. LGPD, **Governança de Dados e Gestão de Metadados**. Curso online. Data Science Academy. 2020. Realizado pelo link: https://www.datascienceacademy.com.br/course/lgpd-governanca-de-dados-e-gestao-de-metadados.

3 O *COMPLIANCE* DE DADOS

Dentre as preocupações dos líderes empresariais, as ameaças cibernéticas têm ganhado maior notoriedade devido ao aumento significativo das violações dos dados nos últimos tempos [112]. O surgimento dessas ameaças, que inicialmente não eram normatizadas, no passar do tempo se tornou um risco à empresa, fato este que exigiu uma forte conscientização coletiva dos empresários e que acabou atraindo atenções da legislação para penalização das condutas neste segmento.

Tendo-se em conta que os dados passaram a constituir um *commodity* de alto valor para a era digital[113], a matéria concernente à sua proteção abarca constantes desafios, decorrentes da insurgência contínua de situações inéditas. Destarte, com o crescimento da importância de vigilância de dados, as normatizações sobre o assunto passaram a ganhar destaque.

As organizações precisam gerenciar seus dados difundidos na organização, visto que o avanço da tecnologia expandiu o escopo da necessidade de fiscalização. Quase todos os processos de negócios - desde a criação de clientes, transações de compras, contato com clientes para *feedback* e serviços - usam dados como entrada e produzem dados como saída. Esses dados podem ser armazenados, manipulados, integrados e agregados para diferentes utilizações; incluindo inteligência artificial e análise preditiva. Esse gerenciamento também fornece evidências de conformidade (ou falta) com a legislação vigente e regulamentos internos [114].

Argumenta José Luiz de Moura Faleiros Júnior [115] que “na medida em que o tratamento de dados acirra riscos, o *compliance* surge como salvaguarda para que

---

[112] KLINCZAK. Marjori. Uso da inteligência na detecção de ameaças cibernéticas. ***The eleventh International Conference on forensic computer Science na cyber law.*** São Paulo, Brasil. Novembro, 2019. Disponível em <http://icofcs.org/2019/ICoFCS2019-002.pdf>. Acesso em 19 dez. 2022.

[113] FERREIRA, Luciene Braz; RAMOS, Anatália Saraiva Martins. Tecnologia da informação: commodity ou ferramenta estratégica? **Revista de Gestão da Tecnologia e Sistemas de Informação *Journal of Information Systems and Technology Management.*** Vol. 2, nº 1- 2005, pp. 69-79, **P**.76. Disponível em <>. Acesso em 19 dez. 2022.

[114] MACHADO, Felipe Nery Rodrigues; ABREU, Maurício Pereira de. **Projeto de banco de dados: uma visão prática**. 17ª edição. Saraiva, p. 27

[115] FALEIROS JÚNIOR, José Luiz de Moura. **Administração pública digital**: proposições para o aperfeiçoamento do Regime Jurídico Administrativo na sociedade da informação. Indaiatuba, SP. Foco, 2020, p. 202.

se tenha o devido respeito à transparência e, em último grau, para assegurar a *accountability*[116] pública em todos os seus níveis".

Com isso, responder às expectativas e demandas, bem como buscar adequação por parte do ramo público ou privado às diversas instâncias de normatividade e de institucionalidade, requer acessibilidade e manuseio qualificado de informações precisas e constantemente atualizadas e, o instituto do *compliance*, em seus vários segmentos, cumpre a função de tornar compreensíveis as normas e processos aos quais suas atividades precisam se conformar [117].

Nesse ínterim, verifica-se, que a aplicação do *compliance* de dados, não apenas se trata de medidas para adequação à lei geral de proteção de dados, mas, por outro giro, se trata de uma proteção de uma gama maior dos dados, se sobressaindo apenas à vigilância dos dados pessoais.

3.1 *Compliance* como instrumento de inclusão: considerações sobre a origem, contextualização, pilares, conteúdo sobre o programa e o *compliance* digital

O termo *compliance* emana do verbo inglês "*to comply*" que conforme Coimbra a definição consiste em satisfazer, cumprir e estar em conformidade com a imposição, sendo entendida como, no âmbito empresarial, a conduta de cumprir princípios éticos e regulamentos internos e externos, com o fito de reduzir o risco de violação dessas respectivas regras[118]. Castro acrescenta que conceituar *compliance* como estar em "*compliance* a" é banalizar o tema que possui inúmeros pilares, não podendo deixar que caia no senso comum com fórmulas genéricas e teóricas [119].

O *compliance* integra um sistema complexo e organizado de procedimentos de controle de riscos e a preservação dos valores e princípios de uma empresa.

---

[116] Na definição de Faleiros Júnior, *accountability* é o "Processo pelo qual as entidades e os gestores públicos são responsabilizados pelas próprias decisões e ações, contemplando o trato com recursos públicos e todos os aspectos de desempenho". (FALEIROS JÚNIOR, José Luiz de Moura. **Administração pública digital**: proposições para o aperfeiçoamento do Regime Jurídico Administrativo na sociedade da informação. Indaiatuba, SP. Foco, 2020, p. 131).

[117] LÓSSIO, Claudio Joel Brito. **Proteção de Dados e *Compliance* Digital**. São Paulo: Almedina, 2021, p. 23.

[118] COIMBRA, Marcelo de Aguiar; MANZI, Vanessa Alessi (Org.). **Manual de compliance**: preservando a boa governança e a integridade das organizações. São Paulo: Atlas, 2010, p. 2.

[119] CASTRO, Rodrigo Pironti Aguirre de. **Compliance**: repensando o [obvio, para não cair no senso comum. Disponível em: https://www.cafecompliance.com.br/?area=autores&a=10. Acesso em: 28 out. 2022.

Agrega também o compromisso efetivo de sua liderança e, como elemento, a estratégia que a empresa usará para criar um ambiente de segurança jurídica e confiança [120]. Esses elementos são indispensáveis para uma tomada de decisões.

Augusto Martinez Perez Filho[121] traz que a intenção, com a aplicação do *compliance,* é tornar o controle mais preventivo, objetivando a promoção de inteligência corporativa, por meio de análise de dados em sinergia com as estratégias de gestão.

A exigência para uma conduta íntegra e responsável por parte das organizações se deu a partir da maior circulação de informação que provocou um significativo aumento da transparência das organizações. De modo consequente, houve um aumento das expectativas da sociedade no que tange ao seu comprometimento ético [122].

Nesse segmento, direcionando o presente estudo aos objetivos que a aplicação do programa de *compliance* proporciona à empresa, mister destacar que o sucesso das organizações é extremamente dependente da admiração e da confiança pública que terceiros depositam nela. Isso se reflete no valor de suas marcas, em sua reputação nos negócios, na capacidade de atrair e fidelizar clientes, investidores e até funcionários. Pode ser demonstrado através de estudos que as empresas que apresentam uma estrutura sólida de preceitos éticos e de atuação responsável estão em um patamar elevado em detrimento das demais que atuam de forma diversa. Mas é preciso ir além, para não permitir que o tema seja mais um, dentre tantos outros, a cair no chamado “conhecimento vulgar”[123].

Edmo Colnaghi Neves[124] apresenta oito motivos para implementar e manter um programa de *compliance* nas empresas, sendo eles: diminui os riscos de cometer violações das legislações; reduz a pena caso a empresa incorra em descumprimento e sofra alguma sanção; promove atitude fiscalizadora dos

---

[120] CARVALHO, André Castro (Coord.); ALVIM, Tiago Cripa (Coord.); BERTOCCELLI Rodrigo (Coord.); VENTURINI, Otavio (Coord.). **Manual de compliance**. 2. ed. Rio de Janeiro: Forense, 2020. p. 47

[121] PEREZ FILHO, Augusto Martinez. **O compliance na administração pública**: combate à corrupção e efetivação do direito à boa administração. São Paulo: JH Mizuno, 2019.

[122] CARVALHO, André Castro (Coord.); ALVIM, Tiago Cripa (Coord.); BERTOCCELLI Rodrigo (Coord.); VENTURINI, Otavio (Coord.). **Manual de compliance**. 2. ed. Rio de Janeiro: Forense, 2020. p. 48

[123] CASTRO, Rodrigo Pironti Aguirre de. ***Compliance*: repensando o óbvio para não cair no senso comum.** Consultor jurídico, 2018. Disponível em < https://www.conjur.com.br/2018-jul-14/rodrigo-pironti-repensando-obvio-compliance>. Acesso em 18 dez. 2022.

[124] NEVES, Edmo Colnaghi. **Compliance empresarial**: o tom da liderança: estrutura e benefícios do programa. São Paulo: Trevisan, 2018. 500 Mb; ePUB.

administradores, prevenindo que a empresa e os funcionários/servidores venham a cometer violação das normas; reduz a perda de receitas em decorrência de compras de bens e serviços que estejam superfaturados; proporciona a boa reputação da empresa por ser ética; possibilita mais acesso a créditos de investimentos dada a maior avaliação da empresa por possuir programa de integridade; apresenta diferencial competitivo; e, por fim, estimula o orgulho do colaborador em laborar em um local que segue a integridade e honestidade como princípios norteadores do seu negócio.

Necessário fazer alusão ao tratamento dado pela norma aos mecanismos e procedimentos que devem ser internalizados e praticados pelas empresas, com vistas à garantia da efetividade dos chamados "programas de *compliance*". Apesar de, nos termos do art. 7º, inciso VIII da lei anticorrupção, a presença dessas ferramentas poder ser vista e considerada como simples e singular elemento apto a atenuar as sanções administrativas, a questão da integridade empresarial já adquiriu e consolidou uma nova dimensão nos últimos anos[125].

Os incentivos diretos para que organizações empresariais adotem um conjunto de boas práticas em suas estruturas internas e no relacionamento com o Poder Público decorrem da própria natureza repressiva e inibitória da Lei Anticorrupção. Da análise daquele diploma legal, verifica-se que, ao criar um sistema voltado exclusivamente à responsabilização de pessoas jurídicas, lastreado em critérios objetivos para a aplicação de duras penalidades, as regras e princípios advindos da norma acabam por gerar estímulos à implantação e contínuo aperfeiçoamento dos programas de *compliance*, com vistas à prevenção da prática de atos considerados ilícitos. A escolha – ou omissão – empresarial que siga em direção oposta a esse caminho pode resultar na desvalorização da organização no mercado, elevados riscos reputacionais e dificuldades para a realização de parcerias de negócios[126].

A KPMG[127] define *compliance*, no âmbito institucional e corporativo, como o conjunto de disciplinas para fazer cumprir as normas legais e regulamentares, as

---

[125] COIMBRA, Marcelo de Aguiar; MANZI, Vanessa Alessi (Orgs.). **Manual de Compliance: preservando a boa governança e a integridade das organizações**. São Paulo: Atlas, 2010, p. 87

[126] COIMBRA, Marcelo de Aguiar; MANZI, Vanessa Alessi (Orgs.). **Manual de Compliance: preservando a boa governança e a integridade das organizações**. São Paulo: Atlas, 2010, p. 88.

[127] AGRO + integridade selo agro: integridade empresas do agronegócio. KPMG Consultoria, 2017. Disponível em: https://www.legiscompliance.com.br/images/pdf/br_selo_agro_integridade.pdf. Acesso em: 20 de out de 2022.

diretrizes e políticas e as definidas para o segmento da empresa, bem como detectar, mitigar, evitar e buscar a solução de qualquer desvio ou inconformidade que possa ocorrer. Atualmente este termo não significa só cumprir as normas, um programa de perdura para que a empresa crie procedimentos capazes de evitar a prática de atos ilícitos.

De forma mais recente, o *compliance* passou a integrar diversos diplomas legais internacionais, entre as quais: Lei Anticorrupção do Reino Unido (*UK Bribery Act*, de 2011), Lei Mexicana de Combate à Corrupção (*Ley Federal Anticorrupción em Contrataciones Publicas*, de 2012) e a Comissão de Valores Imobiliários dos Estados Unidos (*US Securities & Exchange Comission* - SEC). Há também outras convenções internacionais, como a: Convenção de Combate à Corrupção de Funcionários Públicos e Estrangeiros em Transações Comerciais Internacionais, de 1995, a Organização para a Cooperação do Desenvolvimento Econômico (OCDE), de 1997, e a Convenção das Nações Unidas Contra a Corrupção, aprovada em 2005[128].

A União Europeia também teve iniciativa de igual teor, quando, em 26 de maio de 1997, em Bruxelas, aprovou a Convenção Relativa à Luta contra a Corrupção dos Funcionários das Comunidades Europeias ou dos Estados-Membros da União Europeia. A União Africana também estabeleceu a Convenção sobre a Prevenção e a Luta contra a Corrupção da União Africana (UA), entrando em vigor em 2006 e abrigando 34 países africanos[129].

Na conjuntura global, casos como os atos terroristas nos Estados Unidos, em 2001, os escândalos de governança, como, por exemplo, os relacionados ao Banco Barings, Enron, WordCom e Parmalat e a crise global de 2008, além da descoberta de casos de corrupção envolvendo autoridades públicas, chamaram a atenção para a maior necessidade de conformidade a padrões legais e éticos de conduta impostos, ampliando a abrangência do *compliance* para novos modelos desejáveis de comportamento a serem seguidos" [130].

---

[128] SILVA, Daniel Calvacante; COVAC, José Roberto. **Compliance como boa prática de gestão de ensino superior privado.** São Paulo: Saraiva, 2015, p. 4-5.

[129] CASTRO, Leonardo Bellini de. **Lei anticorrupção:** impactos sistêmicos e transversais. Leme, SP: JH Mizuno, 2019.

[130] COIMBRA, Marcelo de Aguiar; MANZI, Vanessa Alessi (Org.). **Manual de compliance**: preservando a boa governança e a integridade das organizações. São Paulo: Atlas, 2010, p. 1-2.

No Brasil, o *compliance* chega com maior efetividade por meio da Lei nº 12.846/2013[131], conhecida como Lei Anticorrupção ou Lei da Empresa Limpa. Ela foi a responsável por instituir, no Brasil, a responsabilização objetiva (tanto a administrativa, quanto a civil) das pessoas jurídicas pela prática de atos lesivos que sejam cometidos contra a Administração Pública nacional ou estrangeira. Com a Lei aprovada, o advento desse diploma legal alterou substancialmente o cenário de enfrentamento à corrupção empresarial no Brasil, ao estabelecer um novo paradigma de normas e princípios para a responsabilização de pessoas jurídicas envolvidas em atos ilícitos[132]. A criação do microssistema jurídico da Lei nº 12.846/13[133] também fez com que as questões relacionadas à integridade empresarial se desdobrassem em outras vertentes. Exemplo disso é a tendência nacional de que Estados e Municípios passem a exigir a presença de mecanismos e procedimentos internos de integridade em contratações públicas[134].

Diante dessa nova realidade, as organizações necessitam buscar soluções preventivas de adequação à tecnologia, visando a mitigação de riscos que a empresa esteja suscetível a incorrer e todas as suas consequências. Por serem fundamentais nessa gestão, a implementação de um programa de *compliance* tem sido a medida mais adotada pelas empresas, seja para minimizar riscos de reputação, seja para gerenciar todos os riscos relacionado ao direito digital que envolvem suas ações da empresa[135].

Block[136] elenca exemplos de empresas que possuem alto risco de reputação que incorreram na falha ou falta de atenção na segurança da informação (tratamento dos dados pessoais), quais sejam: (i) British Airways- utilização de medidas técnicas e organizacionais insuficientes que não garantiram a segurança da informação de

---

131 BRASIL. **Lei nº 12.846, de 1º de agosto de 2013**. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2013/Lei/L12846.htm. Acesso em: 21 jan. 2021.

132 CONTROLADORIA GERAL DA UNIÃO. **Programa de integridade:** diretrizes para empresas privadas. set. 2015. Disponível em: https://www.legiscompliance.com.br/images/pdf/programa_integridade_diretrizes_para_empresas_privadas_cgu.pdf. Acesso em: 21 jan. 2022.

133 BRASIL. **Lei nº 12.846, de 1º de agosto de 2013**. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2013/Lei/L12846.htm. Acesso em: 21 jan. 2021.

134 CONTROLADORIA GERAL DA UNIÃO. **Coleção integridade em contratações públicas.** Volume I. Brasília, agosto de 2021. Disponível em < https://repositorio.cgu.gov.br/bitstream/1/66646/7/Informativo_Colecao_Integridade_em_Contratacoes_Publicas_2021_V1.pdf>. Acesso em 119 dez. 2022.

135 COIMBRA, Marcelo de Aguiar; MANZI, Vanessa Alessi (Org.). **Manual de compliance: preservando a boa governança e a integridade das organizações**. São Paulo: Atlas, 2010.

136 BLOK, Marcella. **Compliance e governança corporativa**. 3. ed. Rio de Janeiro: Freitas Bastos, 2020, p. 216.

seus usuários, culminou em uma multa de EUR 204,6 milhões, (ii) Marriot International Inc. do Reino Unido com multas de EUR 50 milhões por diversas violações legais; (iv) Austrian Post, da Áustria multada em EUR 18 milhões por possuir base jurídica insuficiente para o devido processamento de dados e; (v) Deutsche Wohnen SE, na Alemanha com multas de EUR 14,5 milhões pela falta de conformidade com os princípios gerais de *data processing*.[137]

O instituto do *compliance* pode ser dividido em dois campos de atuação: o primeiro refere-se à ordem subjetiva, compreendendo regulamentos internos e implementação de mecanismos de conformidade com a legislação que rege a sua área de atuação, a fim de prevenir ou minimizar riscos. Já o segundo campo é o de ordem objetiva, obrigado por lei [138].

Com isso, uma empresa que adota um programa consistente de *compliance* tem sua reputação positivamente impactada. Isso porque a mídia confere maior atenção aos atos de infrações existentes e o maior impacto que este fato causa é na reputação da empresa[139].

Explica André Castro Carvalho que o *compliance* integra um sistema complexo e organizado de procedimentos de controle de riscos e preservação dos valores e princípios de uma empresa, como também o compromisso efetivo de sua liderança e a estratégia que a empresa usará para criar um ambiente de segurança jurídica e confiança, elementos indispensáveis para a tomada de decisões [140]. Na visão de Marcelo de Aguiar Coimbra e Vanessa Alessi Manzi a modificação de exigência de uma conduta íntegra e responsável das organizações se deu a partir da maior circulação de informação, provocando um significante aumento da transparência das organizações e, de modo consequente, das expectativas da sociedade no que tange ao seu comprometimento ético.[141]

---

[137] STATISTICS: fines imposed over time. Disponível em: https://www.enforcementtracker.com/?insights. Acesso em: 2022.

[138] GABARDO, Emerson; CASTELLA, Gabriel Morettini e. A nova lei anticorrupção e a importância do compliance para as empresas que se relacionam com a Administração Pública. **Revista de Direiro Administrativo e Constitucional**, Belo Horizonte, v. 15, n. 60, p. 129-147, abr./jun. 2015. Disponível em: https://www.editoraforum.com.br/wp-content/uploads/2015/08/lei-anticorrupcao-compliance.pdf. Acesso em: 18 fev. 2020.

[139] MENDES, Francisco Schertel; CARVALHO, Vinicius Marques de. **Compliance:** concorrência e combate à corrupção. São Paulo: Trevisan, 2017. 15 Mb; ePUB.

[140] CARVALHO, André Castro *et al.* (Coord.). **Manual de compliance.** 2. ed. Rio de Janeiro: Forense, 2020, l. 1270.

[141] COIMBRA, Marcelo de Aguiar; MANZI, Vanessa Alessi (Org.). **Manual de compliance**: preservando a boa governança e a integridade das organizações. São Paulo: Atlas, 2010, p. 11.

O principal objetivo é consolidar as relações de confiança no mercado com os *stakeholders*[142] que a empresa de relaciona, motivo pelo qual as mudanças no âmbito da empresa se justificam[143].

O desenvolvimento de um programa de *compliance* se relaciona a um sistema de atividades de forma contínua e, na maioria dos casos, organizado em três fases, mas que estão em sinergia e alternam ciclicamente, quais sejam, *establishment* ("estabelecimento"), *embedment* ("incorporação"- à cultura organizacional) e *enforcement* ("aplicação"). Referido programa, portanto, não "se compra", mas deve ser incorporado como padrão comportamental e valorativo de uma empresa, capaz de refletir nas atitudes de todos os colaboradores, tornando o programa parte integrante de seu negócio[144].

Logo, se mostra de grande importância a implementação de um programa de *compliance*, mecanismo que possui diversas ramificações (trabalhista, ambiental, tributário, de dados - utilizados por alguns doutrinadores como digital-), administrativo, empresarial, penal, entre outros), sendo na presente pesquisa o estudo realizado na ramificação do direito de dados.

Nesse diapasão, o *compliance* de dados surge como um forte aliado para a valorização da imagem organizacional das empresas diante de seus *stakeholders* [145], já que se trata da união de estar em conformidade com as leis e com o uso da tecnologia da informação. Com isso, o *compliance* de dados se trata de um conjunto de protocolos e práticas de segurança que visa proteger as informações sigilosas, dados pessoais, de ataques criminosos ou até mesmo de uma errôneo tratamento, com o objetivo mitigar os riscos e as decorrentes consequências, adotando medidas

---

[142] As partes interessadas são chamadas de *stakeholders*, que faz menção ao grupo que abrange todas as pessoas ou entidades que podem vir a afetar ou que são afetadas pela atividade de uma organização. Eles podem ser: consumidores, investidores, fornecedores, comunidade local, mídia, governo e etc.- COIMBRA, Marcelo de Aguiar; MANZI, Vanessa Alessi (Org.). **Manual de compliance**: preservando a boa governança e a integridade das organizações. São Paulo: Atlas, 2010, p. 2.

[143] CARNEIRO, Claúdio. **Compliance em tempos de pós-covid-19**. 08 jun. 2020. Disponível em: https://www.editorajc.com.br/18814-2/. Acesso em: 22 ago. 2022.

[144] CARVALHO, André Castro *et al.* (Coord.). **Manual de compliance.** 2. ed. Rio de Janeiro: Forense, 2020, I. 1270-1284.

[145] Adota-se o conceito denominado Stakeholder Capitalism, cuja essência pode ser verificada, entre outras fontes, em: SCHWAB, Klaus; VANHAM, Peter. Stakeholder Capitalism: ***A Global Economy that Works for Progress, People and Planet***. John Wiley & Sons: New Jersey, 2021, P. 198.

preventivas para a adequação da organização e às regras aplicáveis às tecnologias da informação[146].

Cumpre trazer à baila, o entendimento de Block[147], consubstanciado nas medidas comumente mais praticadas e relevantes para aplicação de um programa de *compliance* de dados, quais sejam: (i) auditoria prévia a fim de verificar a administração das soluções em tecnologia adotadas pelas empresas com o fim de pesquisa de gestão identificar eventuais falhas e reformular seu uso para que sirvam como fatores de segurança e desempenho, mitigando riscos; (ii) análise de licenças contratadas, verificando-se se estão adequadas ao número de usuários capacitados para o seu uso com o objetivo de preservação da segurança de dados dos clientes, de ataques cibernéticos e furtos de informações; (iii) adequação da política de privacidade, políticas de condutas e termo de uso em conformidade com o Marco Civil da Internet, a lei geral de proteção de dados e demais leis impostas ao direito digital e; (iv) normas internas de gestão através dos seus regulamentos voltados à gestão dos recursos da tecnologia da informação e políticas internas a fim de evitar ocorrência de riscos, abusos, práticas antiéticas e ilegais que podem colocar em risco toda a atividade da empresa e a sua reputação, já que o objetivo final é fortalecer a relação com *stakeholders* e aumentar a credibilidade da empresa.

Em razão disto, necessário se faz a adoção de rotinas de auditoria a fim de verificar a vulnerabilidade dos seus sistemas de segurança digital, bem como da fiscalização referente ao comportamento dos funcionários em como tratar essas informações, com a finalidade de evitar danos aos usuários e as suas consequências no meio empresarial. Todavia, mister destacar que embora controles dessa natureza sejam altamente eficientes para os chefes tanto do departamento de *compliance* quanto para o DPO (*Data Protection Officer*), conhecer os parâmetros com os quais podem ser utilizados é essencial para que se dissemine em toda a empresa a prática desses atos, bem como que ela atue dentro da legalidade sem cometer excessos. Com isso, as discussões que levaram à criação da Lei nº 13.079, a Lei Geral da Proteção de Dados brasileira, se inserem nesse contexto.

---

[146] BLUM, Renato Opice. MALDONADO, Viviane. **Comentários ao GDPR: Regulamento Geral de Proteção de Dados da União Européia**. São Paulo. Thomson Reuters Brasil. 2018. pag.13

[147] BLOCK, Marcella. **Compliance e governança corporativa**: atualizado de acordo com a Lei Anticorrupção Brasileira (Lei 12.846) e Decreto-Lei 8.421/2015. Rio de Janeiro: Freitas Bastos, 2017, p. 216.

Na visão de Luiz Eduardo Lanzini o *compliance* de dados suporta três situações: valor da informação, qualidade da informação e valores para o negócio. Quando combinadas possibilitam a governança digital e, com essas condições, um programa de *compliance* de dados deve fornecer normas, diretrizes e controles para as empresas garantirem valor e sucesso neste novo ambiente informacional [148].

Compliance de dados é, portanto, uma derivação do ramo do *compliance*, que surge de forma natural quando as relações passam para o meio digital, momento em que se precisam criar métodos de conformidade dentro das instituições. Nesse diapasão, o *compliance* de dados é o melhor caminho para a valorização da imagem organizacional das empresas diante de *stakeholders* e *shareholders*, já que se trata da adoção de boas práticas pelo agente processador de dados, evitando responsabilidades criminais, civis e administrativas [149].

Partindo desta conceituação, destaca-se que a lei geral de proteção de dados trouxe uma noção ampla de tratamento de dados pessoais e, se trata de uma nova exigência que todos os agentes econômicos estarão sujeitos aos riscos de implementação na realização de suas atividades. Ocorre que, esses riscos não são determinados e podem variar consideravelmente entre uma ação ou outra e entre diferentes *stakeholders* (qualquer terceiro que tenha relação com a empresa), o que exige uma análise individualizada de caso a caso[150]. Nessa direção, a estrutura e toda a complexidade de uma empresa, também necessita de um atendimento e avaliação constante e adequado do uso de dados, que se dará pelo *compliance* de dados [151].

3.2 *Compliance* como espécie da governança corporativa

[148] LANZINI, Luiz Eduardo. **Governança corporativa e compliance**: global trading. Curitiba: Contentus, 2020, p. 117.
[149] LÓSSIO, Claudio Joel Brito. **Proteção de Dados e *Compliance* Digital**. São Paulo: Almedina, 2021, p. 23.
[150] SARLET, Gabrielle Bezerra Sales; RUARO, Regina Linden. **LGPD na prática** [recurso eletrônico]. Editora Fundação Fênix, 2022. Disponível em < https://www.fundarfenix.com.br/_files/ugd/9b34d5_ff82cbbab20042838363bb45a74051da.pdf#page=41>. Acesso em 18 dez. 2022.
[151] RODRIGUES, Luís Augusto Antunes. A importância do *compliance* como instrumento de combate aos crimes cibernéticos. **Revista Pan-americana de direito**. Disponível em < https://periodicosfapad.emnuvens.com.br/rtpj/article/view/60/56>. Acesso em 17 dez. 2022.

Por governança, entende-se como gestão da gestão[152]. Refere-se, em suma, na forma em que as decisões são tomadas nas empresas, envolvendo definição de políticas, responsabilidades, procedimentos e autoridades com o fito de traçar as diretrizes e objetivos [153].

Adriana Andrade e José Paschoal Rosetti[154] exemplificam a governança corporativa sendo esta observada como uma estrutura de poder dentro das companhias:

> Como a governança corporativa nasceu do divórcio entre a propriedade e a gestão das empresas, seu foco é a definição de uma estrutura de governo que maximize a relação entre o retorno dos acionistas e os benefícios auferidos pelos executivos. Nesse sentido, envolve a estratégia das corporações, as operações, a geração de valor e a destinação de resultados.

O Instituto Brasileiro de Governança Corporativa (IBGC)[155] define a governança corporativa como sendo o sistema através do qual as organizações são dirigidas, incentivadas e monitoradas, envolvendo as práticas entre os empresários, conselho da administração, órgãos de controle e a diretoria. Ainda, apresenta as linhas mestras das boas práticas de governança em seu Código das Melhores Práticas de Governança Corporativa, oportunidade em que relaciona 4 vertentes:

> Transparência – Consiste no desejo de disponibilizar para as partes interessadas as informações que sejam de seu interesse e não apenas aquelas impostas por disposições de leis ou regulamentos. Não deve restringir-se ao desempenho econômico-financeiro, contemplando também os demais fatores (inclusive intangíveis) que norteiam a ação gerencial e que conduzem à preservação e à otimização do valor da organização;
> Equidade – Caracteriza-se pelo tratamento justo e isonômico de todos os sócios e demais partes interessadas (stakeholders), levando em consideração seus direitos, deveres, necessidades, interesses e expectativas;
> Prestação de contas (accountability) – Os agentes de governança devem prestar contas de sua atuação de modo claro, conciso, compreensível e tempestivo, assumindo integralmente as

---

[152] FONTES, Edson; **Políticas e normas para a segurança da informação.** Editora Brasport, 1ª Edição, 2021.
[153] BLOK, Marcella. ***Compliance* e governança corporativa**. 3. ed. Rio de Janeiro: Freitas Bastos, 2020.p. 17
[154] ANDRADE, Adriana; ROSSETTI, José Paschoal. **Governança corporativa**: fundamentos, desenvolvimento e tendências. 4. ed. São Paulo: Atlas, 2009, p. 139.
[155] INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. **Governança corporativa.** Disponível em: https://www.ibgc.org.br/conhecimento/governanca-corporativa. Acesso em: 2022.

> consequências de seus atos e omissões e atuando com diligência e responsabilidade no âmbito dos seus papéis;
> Responsabilidade corporativa – Os agentes de governança devem zelar pela viabilidade econômico-financeira das organizações, reduzir as externalidades negativas de seus negócios e suas operações e aumentar as positivas, levando em consideração, no seu modelo de negócios, os diversos capitais (financeiro, manufaturado, intelectual, humano, social, ambiental, reputacional, etc.) no curto, médio e longo prazos [156].

Consoante conceituação acima, o *compliance* encontra-se como um dos pilares da governança corporativa, se enquadrando na responsabilidade corporativa, ao garantir a conformidade com leis, normas, leis e políticas da organização (interna e externa), bem como ao fortalecer o ambiente ético através de controles internos e visibilidade da transparência. Assim, "certamente não se pode falar em governança corporativa e sustentabilidade sem se referir à ética e consequentemente considerar a importância de *compliance*" [157].

Nessa seara, a governança Corporativa possui como objetivo, consoante disposto pelo IBGC[158], criar mecanismos eficazes e eficientes, em relação a incentivos quanto de monitoramento, para garantir que o comportamento dos administradores sempre se mantenha condizente com a missão da empresa.

Governança de dados, bem como a política de dados tratam de tópicos emergentes quando se trata de políticas públicas. A política de dados trata de escolhas coletivas, mirando em regras e princípios gerais (aqui se conceitua a governança) que orientam os responsáveis pela coleta, armazenamento, processamento e posterior compartilhamento de dados, a fim de garantir que seu uso tenha sido de maneira adequada, motivo pela qual ela abarca ações para a qualificação, acesso às informações, a segurança, a privacidade e as possibilidades de aplicações tecnológicas que enfocam o uso de dados em políticas e serviços. Já a governança de dados, por sua vez, se consubstancia em distribuir e redistribuir

---

156 INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. **Governança corporativa.** Disponível em: https://www.ibgc.org.br/conhecimento/governanca-corporativa. Acesso em: 2022

157 MANZI, Vanessa Alessi. **Compliance no Brasil**: consolidação e perspectivas. São Paulo: Saint Paul, 2008, p. 123.

158 INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. **Governança corporativa.** Disponível em: https://www.ibgc.org.br/conhecimento/governanca-corporativa. Acesso em: 2022

recursos, assim como normas de caráter operacional, criando responsabilidades e requerendo a aplicação de *compliance* com relação a princípios e normas[159].

Pelo exposto, verifica-se a necessidade de ação integrada da Governança corporativa e o *compliance* visando o sucesso das empresas, em busca de eficiência e transparência, obtendo resultados para avanço da empresa [160].

3.3 Pilares do programa de *compliance*

Um programa de *compliance* robusto com a finalidade de gerar eficiência econômica e sustentabilidade para a empresa, vai muito além de controle de fraudes no âmbito interno, há uma complexidade e pilares que devem ser atendidos. O instrumento em questão é também valioso para defesa dos gestores da organização, apresentando maior segurança em suas ações, já que haverá a possibilidade de comprovação de tomada das providências necessárias pela empresa que eram possíveis no caso concreto[161].

Os pilares de um programa de *compliance* mais adotados pelas instituições são os embasados no suporte e comprometimento da alta administração (*tone from the top*), avaliação de riscos (*risk assessment*), código de ética e conduta, políticas e procedimentos, controles internos, treinamento e comunicação, canais de denúncia, investigações internas e medidas disciplinares, *due diligence* de integridade, auditoria e monitoramento contínuo [162].

No mesmo sentido, os pilares mais utilizados para implementação de um programa de *compliance*, conforme Matheus Lourenço Rodrigues Cunha e Márcio el

---

[159] FIGUEIRAS, Fernando; SILVA, Bárbara. Desenhando políticas e governança de dados para cidades inteligentes: ensaio teórico com o uso da IAD Framework para analisar políticas orientadas por dados. **Revista de Administração Pública**, 2022. Disponível em: https://www.scielo.br/j/rap/a/fNVvVDxzNdD6bvczcjWdvLB/?lang=pt&format=pdf. Acesso em: 29 nov. 2022.

[160] BLOK, Marcella. ***Compliance* e governança corporativa**. 3. ed. Rio de Janeiro: Freitas Bastos, 2020.p. 316.

[161] i, Rodrigo Pironti. **A due diligence**: instrumento de compliance à serviço da governança e da segurança jurídica nas relações empresariais em PPP´s. Disponível em: https://www.cafecompliance.com.br/?area=artigo&c=819280cbb9e37d853ccaa9f3632cf1b8. Acesso em: 19 ago. 2022.

[162] CASTRO, Rodrigo Pironti Aguirre de. **A due diligence**: instrumento de compliance à serviço da governança e da segurança jurídica nas relações empresariais em PPP´s. Disponível em: https://www.cafecompliance.com.br/?area=artigo&c=819280cbb9e37d853ccaa9f3632cf1b8. Acesso em: 19 ago. 2022.

Kalay[163], são: 1) *tone from the top*: comprometimento e suporte da alta administração; 2) *risk assessment*: metodologia de análise de riscos para a conformidade legal; 3) Código de ética e de conduta, políticas e procedimentos: os documentos normativos relacionados ao programa de integridade da empresa; 4) controles internos; 5) comunicação e treinamento: difundir a cultura de integridade; 6) canais de comunicação; 7) investigações internas e medidas disciplinares; 8) *due diligence*: pesquisa de gestão de risco de terceiros e; 9) monitoramento e auditoria. Não há um programa de *compliance* efetivo sem a aplicação desses pilares e para isso necessário que se dê de forma contínua, pois a cada transação, há nova possibilidade de ocorrência de um risco.

A LEC (*Legal Etichs Compliance)* conta ainda com o 10º pilar que é intitulado como diversidade e inclusão, destacando que "não há *compliance* sem respeito e igualdade" [164]. Porém, para continuação do presente trabalho será adotada a metodologia baseada apenas nos nove pilares que serão abaixo detalhados, haja vista que, neste caso, o décimo pilar se enquadra como uma espécie do pilar de treinamento.

Entende-se por *the tone from the top* ou *the tone at the top* como o tom da liderança, representando o grau de comprometimento da empresa em implementar, manter e desenvolver a ética em todos os seus negócios, fazendo a liderança através do exemplo[165].

Esse contexto reflete o sentido que dentre as missões de uma empresa deve-se constar a necessidade de demonstrar sua disposição e capacidade para ser responsável, a fim de responder por suas práticas em relação a dados perante todos os envolvidos com sua organização. O descumprimento dos deveres de cuidado no tratamento dos dados pessoais é a alavanca para ser imputada à empresa como um todo a responsabilidade criminal, administrativa e civil, inclusive de cunho patrimonial, que pode se estender à suspensão de suas atividades, proibição definitiva de atuação em território brasileiro ou, em alguns casos, se a imputação for de relevante quantia financeira, poderá inviabilizar a continuidade das atividades da

---

[163] CUNHA, Matheus Lourenço Rodrigues; EL KALAY, Márcio. **Manual de compliance***:* compliance mastermind. São Paulo: LEC, 2019, v. 1.

[164] OS 10 PILARES de um programa de compliance. Disponível em: https://lec.com.br/os-10-pilares-de-um-programa-de-compliance/. Acesso em: 2022.

[165] NEVES, Edmo Colnaghi. **Compliance empresarial**: o tom da liderança: estrutura e benefícios do programa. São Paulo: Trevisan, 2018. 500 Mb; ePUB, p. 30.

empresa. Nesse sentido, estabelecem Itamar Carvalho e Bruno Cesar Almeida Abreu que [166]:

> A referida área deve ser dotada de independência funcional, financeira e estrutural, sobretudo com a criação de cargo que esteja horizontalmente integrado com as áreas operacionais e de estrutura da corporação, de forma a evitar assédios externos. Mas para que se possa garantir a implementação e o cumprimento das normas procedimentais do Programa de Integridade, essa mesma área deverá estar condicionada verticalmente com a Alta Direção, para que esta última possa exercer a adequada fiscalização.

Com a utilização efetiva do programa de *compliance*, os administradores resguardam a si e a todos os envolvidos na organização. Para melhor contextualização o Guia de Programa de Integridade para Empresas Privadas, da Controladoria Geral da União[167] elucida que:

> O comprometimento da alta direção da empresa com a integridade nas relações público-privadas e, consequentemente, com o Programa de Integridade é a base para a criação de uma cultura organizacional em que funcionários e terceiros efetivamente prezem por uma conduta ética. Possui pouco ou nenhum valor prático um Programa que não seja respaldado pela alta direção. A falta de compromisso da alta direção resulta no descompromisso dos demais funcionários, fazendo o Programa de Integridade existir apenas “no papel”.

Tomada a decisão pela alta direção da pessoa jurídica sobre a criação de um programa de *compliance*, será preciso, a constituição de uma área específica que ficará responsável pela implementação, fiscalização e atualização do programa ou, em caso de pequenas empresas, a definição de quem será o responsável pelo controle.

Nos dias de hoje, quando se trata de organizações de grandes portes, essa área específica é ocupada por um *compliance officer*[168] e estruturada por meio de

---

[166] CARVALHO, Itamar; ABREU, Bruno Cesar Almeida. Programas de compliance: o programa de integridade. *In:* CARVALHO, André Castro *et al.* **Manual de compliance**. 2. ed. Rio de Janeiro: Forense, 2020, p. 67.

[167] CONTROLADORIA GERAL DA UNIÃO. **Programa de integridade:** diretrizes para empresas privadas. set. 2015. Disponível em: https://www.legiscompliance.com.br/images/pdf/programa_integridade_diretrizes_para_empresas_privadas_cgu.pdf. Acesso em: 21 jan. 2022, p. 8.

[168] Nas palavras de Pedro Augusto Amaral Dassan P.11 trata-se de “pessoas delegadas pelo empresário para cumprir tal função”. (DASSAN, Pedro Augusto Amaral. **A posição de garante no contexto empresarial**: contributo ao estudo da responsabilidade do Compliance Officer. 2017.

comitês compostos por pessoas de outras áreas da empresa (RH, auditoria interna, jurídico etc.), em que serão analisadas e julgadas todas as ocorrências, ainda que a fiscalização e a instrução dos processos sejam conduzidas por colaboradores alocados especificamente na área *compliance* [169].

Toda criação de um programa eficiente e robusto, em seu primeiro passo, necessariamente toma como premissa a análise de riscos envolvidos na atividade a ser desenvolvida pela empresa. Essa etapa também é conhecida como "*risk assessment*", e considera as circunstâncias individuais da empresa, pontualmente os riscos prováveis relacionados às atividades que ali são desenvolvidas, sendo o mapeamento dos riscos identificados alocados em uma matriz de risco [170].

Conforme preceitua Beatriz Miranda Batisti um programa ideal e robusto de *compliance* deve ser adaptado e levar em conta a realidade da empresa, o nível de segurança das informações, o nível de autonomia que cada funcionário possui, o grau de controle efetivamente praticado sobre os atos dos funcionários em diferentes níveis hierárquicos, bem como a tolerância com o não seguimento das diretrizes internas. Ele deve ser sempre aprimorado de forma a garantir sua efetividade. Para isso, é necessária uma análise de risco que leve em conta as circunstâncias individuais de cada empresa e, pontualmente, os riscos que a mesma pode sofrer. Esses riscos são alocados em uma matriz de risco [171].

O entendimento de Nelson Ricardo Fernandes[172] é consubstanciado no fato de que o risco se trata de uma potencial perda existente em determinada ação (ou na ausência desta), sendo incerta a sua ocorrência, porém sucede quando uma ameaça encontra alguma vulnerabilidade nos sistemas de proteção, autorizando a

---

Dissertação (Mestrado) – Faculdade de Direito, Universidade de Coimbra. Disponível em: https://estudogeral.sib.uc.pt/bitstream/10316/84041/1/Texto_final.pdf. Acesso em: 2022).

[169] DASSAN, Pedro Augusto Amaral. **A posição de garante no contexto empresarial**: contributo ao estudo da responsabilidade do Compliance Officer. 2017, p. 11.

[170] BATISTI, Beatriz Miranda; KEMPFER, Marlene. Parâmetros de compliance por meio da metodologia de análise de risco para a mitigação da responsabilidade objetiva diante da lei anticorrupção (12.846/2013) em face de negócios públicos. **Revista Brasileira de Direito Empresarial**, v. 2, n. 1, p. 184-200, 2016. Disponível em: https://www.indexlw.org/index.php/direitoempresarial/article/view/1019. Acesso em: 05 fev. 2022, p. 190.

[171] BATISTI, Beatriz Miranda; KEMPFER, Marlene. Parâmetros de compliance por meio da metodologia de análise de risco para a mitigação da responsabilidade objetiva diante da lei anticorrupção (12.846/2013) em face de negócios públicos. **Revista Brasileira de Direito Empresarial**, v. 2, n. 1, p. 184-200, 2016. Disponível em: https://www.indexlw.org/index.php/direitoempresarial/article/view/1019. Acesso em: 05 fev. 2022, p. 190.

[172] FERNANDES, Nelson Ricardo. **Análise de risco parametrizada**: manual prático do planejamento e gestão de riscos. [*S.l.*]: Editora Clube do Autor, 2015, p. 16.

concretização do risco, destacando, no caso, que o risco não é confundido como mera vulnerabilidade.

Não há risco se não existir uma vulnerabilidade e uma ameaça devidamente associada, sendo necessário conhecer o risco e procurar entendimento se o que está associado a ele se trata de um ativo que possui valor para a empresa (dados e informações, servidores, *softwares*, pessoas e estações de trabalho, por exemplo) [173].

A definição de risco pode ser construída a partir de sua diferenciação no tocante à oportunidade. Em termos gerais, segundo o COSO[174], os eventos que se relacionam a uma entidade podem ter impacto negativo, positivo ou ambos, em que aqueles com impacto negativo representam os riscos, que podem impedir a criação de valor ou desgastar o valor existente, e aqueles com impacto positivo podem compensar impactos negativos ou representar oportunidades, que afetam positivamente a realização de objetivos, apoiando a criação ou preservação de valor.

Importante destacar que no ambiente corporativo, público ou privado, há uma série de espécies ou grupo de riscos que se estabelecem, como riscos financeiros, estratégicos, operacionais, de *compliance* e lei geral de proteção de dados.

A etapa de análise do risco permite um aprofundamento sobre os riscos, envolve as causas e fontes de risco, suas consequências positivas e negativas, assim como sua probabilidade de ocorrência. Nessa etapa a organização deverá analisar todos os riscos identificados na etapa anterior, verificando quais são as consequências e probabilidades dos riscos [175].

De acordo com a ISO 31000[176]:

---

[173] DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico**, Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011, p. 84

[174] O COSO- *Committee of Sponsoring Organizations of the Treadway Commission*- é um comitê, sem fins lucrativos, dedicado à melhoria dos relatórios financeiros por meio da ética, efetividade dos controles internos e governança corporativa e surgiu com a finalidade de criar estruturas sistemáticas que dessem conta do novo cenário apresentado pelas corporações. É formado por algumas das principais associações de classe de profissionais da área financeira e contábil nos EUA. (COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION. **[Site]**. Disponnível em: https://www.coso.org/SitePages/Home.aspx. Acesso em: 2022).

[175] CUNHA, Matheus Lourenço Rodrigues da; CASTRO, Rodrigo Pironti Aguirre de. *Compliance risk assessment*: análise de caso de participação em licitações e contratos públicos. In: CUNHA, Matheus Lourenço Rodrigues; EL KALAY, Mário. **Manual de *compliance: compliance mastermind***. São Paulo: LEC, 2019. P. 138

[176] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT/CEE-063**: Projeto de revisão ABNT NBR ISO 31000: 2018. Disponível em: https://drive.google.com/file/d/1fdNcTyTZ3Qs7LpGYf_g4-a054fVtiC6b/view. Acesso em: 2022.

> O propósito da análise de riscos é compreender a natureza do risco e suas características, incluindo o nível de risco, onde apropriado. A análise de riscos envolve a consideração detalhada de incertezas, fontes de risco, consequências, probabilidade, eventos, cenários, controles e sua eficácia. Um evento pode ter múltiplas causas e consequências e pode afetar múltiplos objetivos. A análise de riscos pode ser realizada com vários graus de detalhamento e complexidade, dependendo do propósito da análise, da disponibilidade, e confiabilidade da informação, e dos recursos disponíveis. As técnicas da análise podem ser qualitativas, quantitativas ou uma combinação destas, dependendo das circunstâncias e do uso pretendido.

Importante destacar os f*rameworks*[177], que são direcionais relacionados à gestão de riscos. Os mais utilizados são o COSO, ISO 31.000 e as três linhas de defesa[178]. Não existe uma maneira mais ou menos adequada de se gerir riscos, existe a melhor maneira que melhor se encaixa na necessidade e complexidade da empresa.

Dentre as missões de uma empresa deve constar a necessidade de demonstrar sua disposição e capacidade para ser responsável, a fim de responder por suas práticas em relação a dados perante todos os envolvidos. Para isso, devem ser criados programas e políticas de condutas ligadas a critérios externos (leis e regulamentos, como por exemplo) e projetados para fornecer ao indivíduo com quem mantém relação comercial uma proteção de privacidade efetiva, através de implantação de mecanismos para atuar sobre essas políticas e monitorá-las [179].

Compliance não se trata de uma forma genérica em que se cria um modelo e aplica-se a todas as empresas, é necessário estudo sobre a gestão de riscos em

---

[177] De acordo com Cambridge Dictionary, "*framework* é uma estrutura que serve de suporte em torno da qual algo pode ser construído". (FRAMEWORK. *In*: CAMBRIDGE dictionary. Disponível em: https://dictionary.cambridge.org/us/. Acesso em: 2022).

[178] As três linhas de defesa foi uma metodologia criada pelo IIA (*Institute of Internal Audits*). Este modelo é uma "forma simples e eficaz de melhorar a comunicação do gerenciamento de riscos e controles por meio do esclarecimento dos papéis e responsabilidades essenciais", apresentando "um novo ponto de vista sobre as operações, ajudando a garantir o sucesso contínuo das iniciativas de gerenciamento de riscos, e é aplicável a qualquer organização, não importando seu tamanho ou sua complexidade". ELETROBRAS. **Política Anticorrupção das Empresas.** Rio de Janeiro, 2018. Disponível em < https://www.eletronuclear.gov.br/Canais-de-Negocios/Documents/Etica%20e%20Compliance/Pol%C3%ADtica%20Anticorrup%C3%A7%C3%A3o%20das%20Empresas%20Eletrobras.pdf>. Acesso 19 dez 2022.

[179] LOOSLI, Marilia Zulini da Costa; IKO, Massamitsu Alberto. Código de ética e de conduta, políticas e procedimentos: os documentos normativos relacionados ao programa de integridade da empresa. *In*: CUNHA, Matheus Lourenço Rodrigues; EL KALAY, Mário. **Manual de compliance***:* compliance mastermind. São Paulo: LEC, 2019, p. 162.

todo o contexto em que se situa a organização, a fim de que sejam detectados e apontadas quais as melhores medidas para estar em conformidade[180].

A gestão de riscos proposta pela metodologia do Pacto Global[181] compreende três passos principais:

> (i) identificação de situações de risco, mapeamento de situações ou fatores que possam facilitar, camuflar ou contribuir para prática de atos lesivos contra a administração pública, nacional ou estrangeira.
> (ii) Criação de políticas para mitigar os riscos com base nesse levantamento, desenvolver políticas com o objetivo de aumentar o controle sobre as situações de risco e diminuir as chances de ocorrência de atos lesivos.
> (iii) (Análise periódica de riscos e atualização das políticas, mudanças no cenário de risco podem trazer a necessidade de adaptações e, até mesmo, reformulações nas políticas e controles estabelecidos pela empresa.

Para se determinar a análise de riscos, utiliza-se a análise entre a probabilidade x impacto. Matrizes de probabilidade e impacto (MPI), comumente chamadas de matrizes de riscos, consubstanciam-se em ferramentas mais simples para análise e identificação de risco, através de um gráfico, apresentado em duas dimensões, probabilidade e impacto [182]. Nesse sentido, Gustavo Lucena[183] esclarece que:

> Uma matriz de impacto x probabilidade, como o próprio nome induz, irá aquilatar e conjugar dois critérios para a obtenção do nível de riscos: um critério de impacto e outro de probabilidade. A conjugação destes dois critérios em um diagrama de cálculo de riscos, permitirá a confirmação do nível de risco da atividade verificada e, a depender do apetite de riscos da Entidade, determinará sua correção ou aceitação.

Em uma matriz 3x3, como a abaixo apresentada na imagem de análise de risco qualitativa, o impacto e a probabilidade recebem valores classificados como alto, médio e baixo:

---

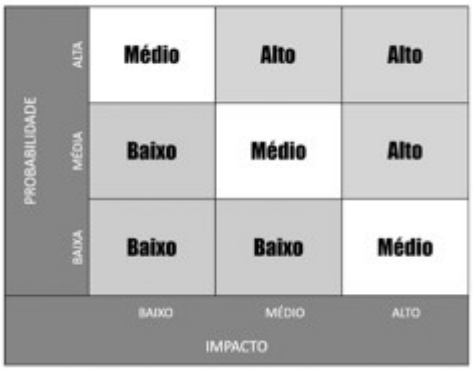
[180] COMPLIANCE: repensando o óbvio para não cair no senso comum. 12 mar. 2019. Disponível em: https://cafe.jmlgrupo.com.br/compliance-repensando-o-obvio-para-nao-cair-no-senso-comum/. Acesso em: 2022

[181] THE GLOBAL COMPACT. **Guia de avaliação de risco de corrupção**. 2013. Disponível em: https://www.gov.br/dnit/pt-br/assuntos/integridade/coordenacao-geral-de-integridade/legislacao-basica/guia-de-avaliacao-de-risco-de-corrupcao.pdf. Acesso em: 25 jun. 2022.

[182] MARKOWSKI, A.; MANNAN, S. Fuzzy risk matrix. **Journal of Hazardous Materials**, v. 159, n. 1, p. 152-157, 2008.

[183] LUCENA, Gustavo. Pilar 2- Risk Assessment: metodologia de análise de riscos para conformidade legal *In*: CUNHA, Matheus Lourenço Rodrigues; EL KALAY, Mário. **Manual de compliance***:* compliance mastermind. São Paulo: LEC, 2019.

Figura 1 - Matriz de risco probabilidade x impacto- 3x3



Fonte: Doneda [184]

A linha de impacto, que é a responsável por definir o grau de afetação do evento de risco no objetivo da empresa, pode se dar de maneira qualitativa ou quantitativa, a depender do interesse da organização e do nível de maturidade que a empresa se encontra nas suas análises de risco.

Em linhas conclusivas deste pilar, à luz da gestão de riscos, ISO 31.000 e COSO, verifica-se que matriz de risco é probabilidade de impacto, a partir do qual é identificado o nível de risco, e este, por fim, vai determinar o plano de gerenciamento de riscos [185].

Concomitante à criação do programa de integridade a pessoa jurídica deve estabelecer claramente um código de ética e um código de conduta, incorporando, expressa ou implicitamente, que todos os empregados e colaboradores devem cumprir as normas de condutas internas e toda legislação aplicável à empresa. A esse respeito, Antônio Cesar Amaru Maximiano e Irene Patrícia Nohara referem que:

> [...] as atividades de nível estratégico relacionam-se com a viabilização continuada de operações da organização. Nesse nível, a gestão de pessoas olha para o futuro e para o ambiente, estudando as tendências sociais, competitivas, tecnológicas etc., procurando determinar quais as competências serão necessárias para fazer face às ameaças e oportunidades, de quantas pessoas a organização precisará e que programas deverão ser colocados em prática para atraí-las, desenvolvê-las e mantê-las. O mais importante das atividades de nível estratégico é

[184] DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico**, Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011, p. 84.

[185] PASSOS, Matheus. LGPD, Governança de Dados e Gestão de Metadados. Curso online. Data Science Academy. 2020. Realizado pelo link: https://www.datascienceacademy.com.br/course/lgpd-governanca-de-dados-e-gestao-de-metadados

> participar do processo de definir a estratégia corporativa e definir políticas de gestão de pessoas para toda a organização, realizar programas de desenvolvimento organizacional, desenhar carreiras e planos de competências e implementar programas e projetos inovadores[186].

Importa destacar também a necessidade de a pessoa jurídica criar políticas e procedimentos operacionais padrões disciplinando material e procedimentalmente as diversas esferas de ação[187].

O sucesso de um programa de *compliance* e da cultura depende da ampla comunicação interna sobre o tema. *Compliance* e sua importância devem estar diariamente presentes na vida dos empregados e dos colaboradores da pessoa jurídica, seja por meio da disponibilização de todo material em sistema de intranet ou alocados em áreas de acesso comum da estrutura física, como salas de reunião, espaços de sociabilidade, refeitórios e outros[188].

Para isso, deve ser criado programas e políticas de condutas ligadas a critérios externos (leis e regulamentos, como por exemplo) e projetados para fornecer ao indivíduo com quem mantém relação comercial uma proteção de privacidade efetiva, através de implantação de mecanismos para atuar sobre essas políticas e monitorá-las [189].

Assim, incluir o tema *compliance* em tão relevante situação faz com que ele seja visto com a mesma importância que a realização dos negócios [190]. Mais ainda, que no futuro somente haverá espaço para empresas que realizem suas atividades empresariais pautadas em condutas éticas.

Em continuidade, a aplicação de um programa efetivo, em um possível processo de violação do código de conduta, necessário se faz identificar quais serão os procedimentos utilizados para detectar e investigar tal prática, através do canal

---

[186] MAXIMIANO, Antonio Cesar Amaru; NOHARA, Irene Patrícia. **Gestão Pública**: abordagem integrada da administração e do direito administrativo. São Paulo: Atlas, 2017, p.330.

[187] LOOSLI, Marilia Zulini da Costa; IKO, Massamitsu Alberto. Código de ética e de conduta, políticas e procedimentos: os documentos normativos relacionados ao programa de integridade da empresa. *In*: CUNHA, Matheus Lourenço Rodrigues; EL KALAY, Mário. **Manual de compliance***:* compliance mastermind. São Paulo: LEC, 2019, p. 163.

[188] FARIA, Felipe. Comunicação e treinamento de *compliance:* difundindo a cultura da integridade. *In*: CUNHA, Matheus Lourenço Rodrigues; EL KALAY, Mário. **Manual de compliance***:* compliance mastermind. São Paulo: LEC, 2019, p. 210.

[189] LOOSLI, Marilia Zulini da Costa; IKO, Massamitsu Alberto. Código de ética e de conduta, políticas e procedimentos: os documentos normativos relacionados ao programa de integridade da empresa. *In*: CUNHA, Matheus Lourenço Rodrigues; EL KALAY, Mário. **Manual de compliance***:* compliance mastermind. São Paulo: LEC, 2019, p. 163.

[190] FARIA, Felipe. Comunicação e treinamento de *compliance:* difundindo a cultura da integridade. *In*: CUNHA, Matheus Lourenço Rodrigues; EL KALAY, Mário. **Manual de compliance***:* compliance mastermind. São Paulo: LEC, 2019, p. 210.

de denúncia, assegurada a confidencialidade dos denunciantes (*whistleblowing*) a fim de garantir o efeito dissuasório para detectar a funcionalidade da percepção. Ao mesmo passo, como a empresa se comportará frente à violações, independentemente de caracterizarem delito, mas também infrações administrativas ao código, para se buscarem as causas-raízes (*root-causes*) do problema.[191]

Nesse diapasão, consagra Coutinho que apenas adotar o programa de conformidade não garantirá a purificação total da empresa, de modo que não haja nenhuma violação, porém, por outro lado, casos os desvios ocorram, o programa permite a identificação e consequente correção do problema internamente [192].

Ainda de forma tão importante é o quinto pilar, que trata da comunicação e treinamento de *compliance* para difundir a cultura de integridade. De início, cumpre destacar o conceito de cultura organizacional consagrado por Edgar H. Schein como:

> modelo de pressupostos básicos que um grupo assimilou na medida em que resolveu os seus problemas de adaptação externa e integração interna e que, por ter sido suficientemente eficaz, foi considerado válido e repassado aos demais novos membros como a maneira correta de perceber, pensar, sentir em relação a estes problemas.[193]

O sistema de treinamento deve ser adequado para cada estrutura empresarial, podendo ser um modelo simples por meio de respostas a questionamentos e pontuação, como sistemas mais sofisticados com a disponibilização de aplicações de tecnologia da informação em que haja a interação do empregado com situações do dia a dia. Contudo, o diferencial e aspecto mais importante para a empresa será a frequência com que se realiza o treinamento [194].

Os treinamentos, ainda que realizados de forma simplificada, devem colocar o colaborador diante de situações de clara distinção entre o “certo” e o “errado”, e

---

[191] COUTINHO, Doris Terezinha Pinto Cordeiro de Miranda. **Finanças públicas**: travessia entre o passado e o futuro. São Paulo: Blucher, 2018. Disponível em: https://www.editoraforum.com.br/wp-content/uploads/2015/08/lei-anticorrupcao-compliance.pdf. Acesso em: 16 fev. 2022. p. 184.

[192] COUTINHO, Doris Terezinha Pinto Cordeiro de Miranda. **Finanças públicas**: travessia entre o passado e o futuro. São Paulo: Blucher, 2018. Disponível em: https://www.editoraforum.com.br/wp-content/uploads/2015/08/lei-anticorrupcao-compliance.pdf. Acesso em: 16 fev. 2022, p. 163

[193] SCHEIN, Edgar H. **Cultura organizacional e liderança**. SãoPaulo: Atlas, 2009, p. 16.

[194] FARIA, Felipe. Comunicação e treinamento de *compliance:* difundindo a cultura da integridade. *In*: CUNHA, Matheus Lourenço Rodrigues; EL KALAY, Mário. **Manual de compliance***:* compliance mastermind. São Paulo: LEC, 2019, p. 212.

apresentar aquelas que se encontram em zona cinzenta. Isso se deve para que a pessoa jurídica possa realmente analisar qual a referência inicial que o colaborador tem acerca de condutas lícitas e ilícitas, sendo submetidos a treinamentos sistemáticos e contínuos até que incorporem, segundos os padrões legais, as condutas éticas[195].

Todos os planos e políticas, antes de serem colocados em prática, devem ser examinados e aprovados pelos participantes do topo da administração da empresa e os que forem rejeitados devem ser visíveis a todos os integrantes dos níveis mais altos da organização. Isso se dá para que haja o comprometimento de que a implementação de políticas não seja subordinada a prioridades de outra organização. Para que seja efetivo necessário se faz a disseminação de cultura de cumprimento entre os funcionários, a fim de quem todos possam demonstrar o compromisso em executar as normas impostas[196].

Para isso alguns mecanismos para implementação das políticas de privacidade, incluindo ferramentas, treinamento e disseminação se tornam imperiosos. Esses mecanismos que se darão através da aplicação do programa de *compliance*, devem incluir ferramentas que facilitam as tomadas de decisões dentro das organizações sobre as atitudes relativas ao uso apropriado de dados, proteção, capacitação para o uso, bem como para com terceiros que se relacionam com a empresa. Essas ferramentas não podem ser opcionais, mas sim obrigatórias, a fim de que haja uma disseminação em sua aplicação[197].

Destacam-se alguns pontos que elencam a necessidade de tratamento, como a título de exemplo, os possíveis ataques cibernéticos demandam maior vigilância dos dados. Nesses casos, elucida Miguel Moura Silva que por serem utilizados sistemas e plataformas digitais que envolvem a colheita ou armazenagem de dados, ou possivelmente o compartilhamento de tecnologias, será necessária a observância

---

[195] FARIA, Felipe. Comunicação e treinamento de *compliance:* difundindo a cultura da integridade. *In*: CUNHA, Matheus Lourenço Rodrigues; EL KALAY, Mário. **Manual de compliance***:* compliance mastermind. São Paulo: LEC, 2019, p. 214.

[196] PASSOS, Matheus. LGPD, Governança de Dados e Gestão de Metadados. Curso online. Data Science Academy. 2020. Realizado pelo link: https://www.datascienceacademy.com.br/course/lgpd-governanca-de-dados-e-gestao-de-metadados.

[197] FARIA, Felipe. Comunicação e treinamento de *compliance:* difundindo a cultura da integridade. *In*: CUNHA, Matheus Lourenço Rodrigues; EL KALAY, Mário. **Manual de compliance***:* compliance mastermind. São Paulo: LEC, 2019, p. 215.

de tratamento[198]. Diante dessa viabilidade, necessário discutir-se sobre a implementação de tecnologias para efetivação do programa de *compliance* de dados.

Para efetividade do programa os canais de comunicação são de extrema relevância. Apesar da previsão de atividades e ações em políticas e procedimentos internos que possam facilitar a fiscalização pela empresa sobre eventual ato ilícito ou irregularidade, deve ser considerada como modelo de ampliação do controle interno a adoção de canais de denúncias [199].

A pessoa jurídica deve avaliar, também com base em sua estrutura, qual o melhor modelo a ser adotado, se via telefone, e-mail corporativo e específico, outros canais de denúncias online, não sendo tais canais excludentes, mas sim complementares. Neste sentido, a pessoa jurídica poderá, inclusive, criar prêmios e incentivos para que o empregado ou terceiro de boa-fé realize denúncia sobre a existência de determinado ato ilícito praticado por colaborador. Nesse caso, também será fundamental preservar a identidade do denunciante. Ademais, para a efetividade dos canais de denúncias, a empresa deve se preocupar em preservar a integridade moral do denunciante, sobretudo preservando sua identidade perante os demais empregados[200].

E merecendo um destaque, para efetivar a aplicação do programa de *compliance*[201], deve-se, ainda, investir em um sistema de monitoramento cuja finalidade é detectar a prática de violação nos padrões da conduta ética estabelecidos pela instituição, para que se possa ter, quando tal violação ocorrer, a previsibilidade, a contundência e a certeza da sanção a ser aplicada.

---

[198] SILVA, Miguel Moura e. **Inovação transferência de tecnologia e concorrência**: estudo comparado do direito da concorrência dos Estados Unidos e da União Européia. Coimbra: Almedina, 2003, p. 112-113.

[199] LOOSLI, Marilia Zulini da Costa; IKO, Massamitsu Alberto; CUNHA, Matheus Lourenço Rodrigues da. Canais de comunicação com o programa de *compliance*. *In*: CUNHA, Matheus Lourenço Rodrigues; EL KALAY, Mário. **Manual de compliance***:* compliance mastermind. São Paulo: LEC, 2019, p. 233.

[200] LOOSLI, Marilia Zulini da Costa; IKO, Massamitsu Alberto; CUNHA, Matheus Lourenço Rodrigues da. Canais de comunicação com o programa de *compliance*. *In*: CUNHA, Matheus Lourenço Rodrigues; EL KALAY, Mário. **Manual de compliance***:* compliance mastermind. São Paulo: LEC, 2019, p. 235.

[201] Consoante define Carole Basri: “Compliance programs are formal systems of policiesand procedures adopted by corporations and other organizations that are designed todetect and prevent violations of law by employees and other agents and to promoteethical business cultures” (BASRI, Carole. **Corporate compliance**. [*S.l.*]: Carolina Academic Press, 2017. Edição do Kindle, p. 4)

Dentre várias conceituações, a de auditoria interna com maior aceitação é a dada pela organização IIA (*The Institute os International Auditors*), com sede nos Estados Unidos, segundo a qual:

> A auditoria interna é uma atividade de avaliação e consultoria independente e objetiva, desenvolvida para agregar valor e melhorar as operações de uma organização. Ele ajuda uma organização a atingir seus objetivos, trazendo uma abordagem sistemática e disciplinada para avaliar e melhorar a eficácia dos processos de gerenciamento de riscos, controle e governança[202].

Além das disposições supracitadas, cumpre ressaltar a responsabilidade para a empresa independente de culpa. Diante disso, em caso de ocorrências de ilegalidades por funcionários, não poderá a empresa argumentar apenas que medidas internas foram tomadas, fato que deve dar atenção especial às práticas de *due diligence*, destinadas a conhecer o passado e o presente das organizações parceiras, reunindo todas as informações sobre proprietários/administradores, bem como a identificação de possíveis alertas vermelhos (*red flags*) [203].

Entende-se por *due diligence* como um processo que visa buscar informações sobre pessoas (sejam elas físicas ou jurídicas), com as quais a empresa se relaciona ou tem a intenção de se relacionar para concretização de negócios, tais como a contratação de fornecedores ou patrocinadores, prestação de serviços, demanda que envolva terceiros, contratação de agentes intermediários, dentre outros casos [204].

---

[202] No texto original: “Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.” (THE INSTITUTE OS INTERNAL AUDITORS. **Definition of internal auditing***,* 2019. Disponível em https://www.theiia.org/en/standards/what-are-the-standards/definition-of-internal-audit/. Acesso em 28 out. 2022).

[203] COUTINHO, Doris Terezinha Pinto Cordeiro de Miranda. **Finanças públicas**: travessia entre o passado e o futuro. São Paulo: Blucher, 2018. Disponível em: https://www.editoraforum.com.br/wp-content/uploads/2015/08/lei-anticorrupcao-compliance.pdf. Acesso em: 16 fev. 2022. p. 182.

[204] CASTRO, Rodrigo Pironti Aguirre de. **A due diligence**: instrumento de compliance à serviço da governança e da segurança jurídica nas relações empresariais em PPP´s. Disponível em: https://www.cafecompliance.com.br/?area=artigo&c=819280cbb9e37d853ccaa9f3632cf1b8. Acesso em: 19 ago. 2022.

Durante o processo da *due diligence*, investigam-se dentre vários escopos as informações reputacionais, financeiras, regulatórias, jurídicas. Essas pesquisas se dão por meio de diversas bases de dados[205].

Por fim, em atenção ao pilar do monitoramento e auditoria de *compliance*, Cíntia Rose Pereira de Lima e Kelvin Peroli[206], destacam que:

> [...] (i) o nexo estrutural (*structural nexus*), entendido como o desenvolvimento de políticas e procedimentos na própria empresa capazes de promover a cultura de conformidade, em seu âmago; (ii) o fluxo de informações (*information flow*) da empresa necessita ser eficiente, no sentido de que o *compliance* deve ser implantado no fluxo de informações do alto comando até os empregados do chão de fábrica, para garantir que a comunicação entre todos, de todos níveis hierárquicos, seja rápida e eficaz; (iii) monitoramento e vigilância (*monitoring and suveillance*), sendo também função do *compliance* o monitoramento do comportamento dos empregados, a fim de garantir a sua adesão às políticas e procedimentos da empresa, o que gera, consequentemente, a vigilância, que deve ser minimizada e utilizada apenas para os fins corporativos; (iv) o *enforcement* das políticas, procedimentos e normas de direito, que devem ser direcionados tanto para as atividades que oferecem maior risco de não-conformidade, quanto para as que menos risco oferecem, o que pressupõe, em verdade, a análise e o gerenciamento de riscos efetivos pela empresa.

Aliando aos outros pilares, a auditoria é o responsável por confirmar que a empresa se encontra em *compliance*, sendo nessas avaliações que se verificará se há o cumprimento das determinações e em quais pontos a organização precisa de melhorias para que possa ter diferenciais competitivos.

3.4 *Compliance* de dados como medida de segurança: proteção de dados guiados pelos pilares do programa de integridade

Nas palavras de Ricardo Villas Bôas Cueva “um programa de fachada, que não preencha os requisitos mínimos ou que os preencha apenas formalmente, pode

---

[205] CASTRO, Rodrigo Pironti Aguirre de. **A due diligence**: instrumento de compliance à serviço da governança e da segurança jurídica nas relações empresariais em PPP´s. Disponível em: https://www.cafecompliance.com.br/?area=artigo&c=819280cbb9e37d853ccaa9f3632cf1b8. Acesso em: 19 ago. 2022.

[206] LIMA, Cíntia Rosa Pereira de; PEROLI, Kelvin. **Direito digital**: compliance, regulação e governança. São Paulo: Quartier Latin, 2019, p. 136

de fato resultar em penalidades maiores do que aquelas que seriam aplicáveis em sua ausência” [207].

O objetivo do presente tópico é explanar acerca da implementação de um sistema geral de proteção de dados, através do *compliance* de dados, com o propósito de preparar a empresa para proteger a privacidade de seus dados como um todo (desde os dados negociais, empresariais, bem como os dados pessoais dos titulares envolvidos no negócio). Para tanto, as informações aqui explanadas se referirem à implementação de um sistema em uma empresa como esboço de um projeto interno referente a essa proteção de dados.

Como primeiro passo, se parte da análise de requerimentos e das necessidades de proteção de dados que impactam a organização, coletando, assim, as leis relevantes, padrões e regulamentos relacionados àquela realidade. Isso se dá pelo fato de que, partindo do pressuposto, a título de exemplo, que a empresa que irá implementar o referido programa seja da área de educação, a organização não deve vigilância apenas à lei geral de proteção de dados, porém se alguns dos usuários dos serviços prestados forem crianças ou adolescentes, necessário será o atendimento ao ECA ou, ainda, se exigirá a atenção às normas emitidas pelo Ministério da Educação (MEC) [208]. Essa fase inicial de levantamento de dados é de extrema importância para que se possa planejar e posteriormente colocar em prática o programa com eficiência.

Outro exemplo que cumpre destacar, no que se refere não apenas a vigilância da lei geral de proteção de dados, é referente a área da saúde, é o fato de que coincidentemente, no mesmo período de proposição da Medida Provisória nº 983/2020 (que altera a lei geral de proteção de dados), veio à tona a Lei nº 13.787/2018 (Lei dos Prontuários Eletrônicos), que prevê a digitalização e a existência de um conceito específico para documento digitalizado, o qual é atípico e tem um tratamento específico nessa lei. Isso gera uma grande discussão sobre o

---

[207] CUEVA, Ricardo Villas Bôas. Funções e Finalidades dos Programas de *Compliance*. In: LAMACHIA, Claudio; PETRARCA, Carolina (org.). ***Compliance*: essência e efetividade**. Brasília: OAB, Conselho Federal, 2018. p. 215-224. p. 219.

[208] PASSOS, Matheus. LGPD, Governança de Dados e Gestão de Metadados. Curso online. Data Science Academy. 2020. Realizado pelo link: https://www.datascienceacademy.com.br/course/lgpd-governanca-de-dados-e-gestao-de-metadados

assunto, porque os prontuários passaram a ser digitais e há uma obrigação por força da lei de prontuários médicos de que estes sejam armazenados por vinte anos[209].

Ao mesmo passo, enfrentava-se, dificuldades quanto à autenticação de documentos eletrônicos. Diante disso, Antonia Espíndola Longoni Klee explica que:

> O problema que surgiu com as novas mídias, principalmente as eletrônicas e digitais, foi a dificuldade de colocar sobre os documentos eletrônicos a subscrição (assinatura) exigida pelo nosso sistema legal para a existência do formulário (pelo menos se a assinatura é ligada ao movimento da mão feita com a caneta sobre o papel). Foi aí que se desenvolveu a técnica da assinatura digital. Quando se almeja a celebração de um contrato por computador, um dos requisitos relevantes é certificar-se de que a pessoa que está do outro lado é realmente quem diz ser para que se possa alcançar uma efetiva eficácia probatória do contrato digital.[210]

Diante da necessidade de simplificar e evitar contato entre indivíduos no período incerto de pandemia, bem como proporcionar segurança jurídica diante dos atos, foi proposta a Medida Provisória nº 983/2020, que no dia 24 de setembro de 2020 resultou na Lei nº 14.063, sancionada pelo presidente Jair Bolsonaro que desburocratizou as assinaturas eletrônicas de documentos para ampliar o acesso a serviços públicos digitais. Essa nova lei criou novos tipos de assinatura eletrônica em comunicações com entes públicos e em questões de saúde: a assinatura digital simples, qualificada e a avançada[211], o que aplicado ao presente trabalho, demonstra que a fiscalização não se dá apenas aos dados pessoais em si do paciente, mas também no que se refere a chave de assinaturas.

Para melhor entendimento, inicialmente a Medida Provisória nº 2.200-2/2001 (que institui a Infra-Estrutura de Chaves Públicas Brasileiras – ICP Brasil) adotava

---

[209] PASSOS, Matheus. LGPD, Governança de Dados e Gestão de Metadados. Curso online. Data Science Academy. 2020. Realizado pelo link: https://www.datascienceacademy.com.br/course/lgpd-governanca-de-dados-e-gestao-de-metadados

[210] Antonia Espíndola Longoni Klee, denominado "Comércio Eletrônico" – (KLEE, Antonia Espíndola Longoni; PEREIRA NETO, Alexandre Nogueira. A Lei Geral de Proteção de Dados (LGPD): uma visão panorâmica. *In:* THEMOTEO, Reinaldo J. (Coord.). **Proteção de dados pessoais**: privacidade versus avanço tecnológico. Rio de Janeiro: Fundação Konrad Adenauer, 2019).

[211] BRASIL. **Lei nº 14.063 de 23 de setembro de 2020.** Dispõe sobre o uso de assinaturas eletrônicas em interações com entes públicos, em atos de pessoas jurídicas e em questões de saúde e sobre as licenças de softwares desenvolvidos por entes públicos; e altera a Lei nº 9.096, de 19 de setembro de 1995, a Lei nº 5.991, de 17 de dezembro de 1973, e a Medida Provisória nº 2.200-2, de 24 de agosto de 2001. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/L14063.htm. Acesso em: 25 jul. 2022.

dois tipos de assinaturas eletrônicas[212]. A primeira, a partir da previsão do §1º do artigo 10[213] do referido dispositivo legal, equiparou a assinatura manuscrita com a denominada ICP-Brasil, o que implicava em decifrar a presunção de autoria ligada apenas a esse tipo de assinatura digital (ICP-Brasil) [214], já o segundo tipo possui previsão no §2º[215] do mesmo dispositivo legal que facultou a utilização de outro tipo de assinatura em documentos eletrônicos, mas desde que aceitos pelas partes ou a pessoa oposta à emissão do documento.

A exteriorização lícita dos dados pessoais do paciente, contraposta à exposição ilícita, assimilando como àquela informação não autorizada e obtida sem qualquer justa causa jurídica, podendo ocasionar em dano indenizável. É exatamente no âmbito das exposições lícitas e ilícitas que a autodeterminação informativa cresce em importância por ser a protetora da confiança do paciente no médico.[216]

Nesse diapasão, no que se refere aos dois exemplos acima expostos, verifica-se que cada área de atuação empresarial (escolar e área da saúde, como apresentado), necessita de vigilância quanto as determinações daquele setor em específico.

Essa razão verifica a necessidade e importância de que uma empresa realize o *compliance* de dados e não apenas a adequação da empresa nos moldes da lei geral de proteção de dados, já que o enfoque não está apenas nos dados pessoais para garantir a sua integridade. Dados de empresas não são protegidos pelas legislações de proteções de dados, como a lei geral de proteção de dados, motivo pelo qual necessita da vigilância através do *compliance*.

---

[212] BRASIL. **Medida Provisória nº 2.200-2 de 24 de agosto de 2001.** Disponível em: http://www.planalto.gov.br/ccivil_03/MPV/Antigas_2001/2200-2.htm. Acesso em: 25 set. 2022.

[213] Importante mencionar o trecho: “Art. 10. Consideram-se documentos públicos ou particulares, para todos os fins legais, os documentos eletrônicos de que trata esta Medida Provisória. §1º As declarações constantes dos documentos em forma eletrônica produzidos com a utilização de processo de certificação disponibilizado pela ICP-Brasil presumem-se verdadeiros em relação aos signatários”.

[214] Neste sentido, cumpre mencionar “Art. 219. As declarações constantes de documentos assinados presumem-se verdadeiras em relação aos signatários”.

[215] “ § 2º O disposto nesta Medida Provisória não obsta a utilização de outro meio de comprovação da autoria e integridade de documentos em forma eletrônica, inclusive os que utilizem certificados não emitidos pela ICP-Brasil, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento.”

[216] MAIA, Maurilo Casas. Telemedicina, prontuário eletrônico e atualização do código de defesa do consumidor- a tutela da hipervulnerabilidade eletrônica do paciente e de sua personalidade virtual. **Revista de Direito do Consumidor**, v. 89, p. 303-319, set./out. 2013.

Cumpre destacar que a atividade de tratamento de dados, deve ser realizada de forma individualizada para cada dado, cada informação que a empresa lida. Motivo pelo qual, o primeiro passo de levantamento das principais atividades exercidas pela empresa é de extrema relevância. Da mesma forma, que sejam documentadas todas as fases, visando cumprir com o princípio da responsabilização e prestação de contas [217].

Destaca-se que as atividades de tratamento elencadas na empresa precisarão ser atualizadas, eventualmente e até mesmo constantemente, pelo fato de que a cada novo dia a organização tem, ou pode ter, uma nova operação de tratamento que precise ser incluída neste documento ou até ser alterada. Essas atualizações afetam também os relatórios de avaliações de impactos sobre a proteção de dados[218].

Sabe-se ainda, que algumas empresas possuem a tendência de não querer atender as exigências da lei geral de proteção de dados bem como ao *compliance*, porém esquecem de se atentar que cada vez mais se trata de um caráter obrigatório e que, em alguns casos, ainda mais em um futuro próximo, as empresas que não se adequarem ficarão excluídas de negócios [219].

Na verdade, já há a ocorrência desses fatos. Empresas que possuem um programa de *compliance* efetivo, quando da realização da *due diligence*, não se relacionam com empresas que não comprovam a implementação do programa [220]. O mesmo acontece com as determinações de atendimento a Lei Geral de Proteção de Dados.

---

[217] Princípio explanado no artigo 6º, inciso X da LGP, *in verbis* “Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas”.

[218] PASSOS, Matheus. LGPD, **Governança de Dados e Gestão de Metadados**. Curso online. Data Science Academy. 2020. Realizado pelo link: https://www.datascienceacademy.com.br/course/lgpd-governanca-de-dados-e-gestao-de-metadados.

[219] PASSOS, Matheus. LGPD, **Governança de Dados e Gestão de Metadados**. Curso online. Data Science Academy. 2020. Realizado pelo link: https://www.datascienceacademy.com.br/course/lgpd-governanca-de-dados-e-gestao-de-metadados

[220] CASTRO, Rodrigo Pironti Aguirre de. **A due diligence**: instrumento de compliance à serviço da governança e da segurança jurídica nas relações empresariais em PPP´s. Disponível em: https://www.cafecompliance.com.br/?area=artigo&c=819280cbb9e37d853ccaa9f3632cf1b8. Acesso em: 19 ago. 2022.

Nesse interim, verifica-se que a implementação de um programa de c*ompliance* de dados guiados pelos pilares do programa de integridade, é o meio eficiente para utilização de medida de segurança.

4 ELEMENTOS CONCRETOS DE ESTRUTURAÇÃO, IMPLEMENTAÇÃO E EXECUÇÃO DE UM PROGRAMA DE *COMPLIANCE* DE DADOS EFETIVO

Compliance não se define somente pelos valores e em ter que estar arraigado na empresa e na Administração Pública. Não se trata apenas de políticas e procedimentos. *Compliance* refere-se a uma metodologia complexa que pressupõe inúmeras fases, desde a análise de maturidade e questionários de *compliance*, análise da gestão de risco com a posterior elaboração da matriz de risco e averiguação das políticas e procedimentos de integridade. Não se trata somente do código de conduta e de ética, trata-se da política de consequência, da *due diligence*, bem como de relacionamento com o poder público. Há ainda a necessidade de criação de canais de denúncia, independente e autônomo, realização de monitoramento contínuo com KPI'S, que basicamente são indicadores de chaves de desempenho, e constante treinamento com os colaboradores [221].

Destaca-se que há a existência de vários pilares de *compliance*, não podendo o tema se restringir apenas ao conceito de estar em conformidade. Por esse motivo, apresentaremos *insights* para elaboração de um programa de integridade voltado para a proteção de dados de um aspecto geral.

4.1 Proposta de estruturação, implementação e execução de um programa de *compliance* de dados detalhado

Em deliberação à parte prática, levando-se em consideração que a alta administração precisa mostrar empenho desde o acolhimento da ideia, enquanto na atividade de tratamento de dados, de forma assertiva Carolina Gazoni[222] apresenta

[221] PASSOS, Matheus. LGPD, Governança de Dados e Gestão de Metadados. Curso online. Data Science Academy. 2020. Realizado pelo link: https://www.datascienceacademy.com.br/course/lgpd-governanca-de-dados-e-gestao-de-metadados.

[222] GAZONI, Carolina. Pilar 1- Tone from the top- comprometimento e suporte da Alta Administração *In:* CUNHA, Matheus Lourenço Rodrigues; EL KALAY, Mário. **Manual de compliance***:* compliance mastermind. São Paulo: LEC, 2019, v. 1, p. 113.

um *check list* de verificações da evolução, bem como da comprovação do real comprometimento e apoio da alta administração, que segue abaixo.

Figura 2 - *Check list* da Alta Administração

APOIO E COMPROMETIMENTO DA ALTA ADMINISTRAÇÃO	NÃO DEFINIDO	DEFI-NIDO	IMPLE-MENTADO	PARCIAL-MENTE EFETIVO	EFETIVO
O conselho de administração e a alta direção estabelecem e defendem os valores fundamentais da organização?					
O conselho de administração e a alta direção asseguram que os objetivos e apolítica do Programa de Compliance sejam estabelecidos e consistentes com os valores, objetivos e direcionamento estratégico da organização ?					
O conselho de administração e a alta direção asseguram que as políticas, procedimentos e processos sejam desenvolvidos e implementados para atingir os objetivos de compliance?					
O conselho de administração e a alta direção asseguram que os recursos necessários para o Programa de Compliance estejam disponíveis, reservados e atribuídos?					
O conselho de administração e a alta direção asseguram a integração dos requisitos do Programa de Compliance aos processos do negócio da organização?					
O conselho de administração e a alta direção comunica a importância de um Programa de Compliance eficaz e a importância da conformidade dos requisitos do SGC?					
O conselho de administração e a alta direção dirige e apoia as pessoas que contribuem para a eficácia do Programa de Compliance?					
O conselho de administração e a alta direção apoia outros papéis de gestão pertinentes para demonstrar a sua liderança como se aplicam as suas áreas de responsabilidade de compliance?					
O conselho de administração e a alta direção asseguram o alinhamento entre as metas operacionais e as obrigações de compliance?					
O conselho de administração e a alta direção estabelece e mantém mecanismos de responsabilização por prestar contas, incluindo relato tempestivo sobre assuntos de compliance, incluindo o não cumprimento?					
O conselho de administração e a alta direção assegura que o Programa de Compliance atinja o seu resultado pretendido?					
A alta direção assegura que as responsabilidades e autoridades dos papéis pertinentes sejam atribuídas e comunicadas dentro da organização?					
O conselho de administração e a alta direção atribuem a responsabilidade e a autoridade para a função de compliance para relatar o desempenho do Programa de Compliance para o órgão regulamentador e a Alta Administração?					
O Conselho de Administração e a Alta Administração promove a melhoria contínua do Programa de Compliance?					

Fonte: Gazoni [223]

Após certificado o apoio pela alta administração, antes de iniciar qualquer análise de risco, necessário se faz, em um primeiro momento, descrever a atividade de tratamento, a qual deve se dar de forma sistemática e constar a finalidade do procedimento em questão. A situação deve ser descrita em todo seu fluxo, em todo seu ciclo de vida (inicia naquela situação, coleta os dados e se finda, onde os dados

[223] GAZONI, Carolina. Pilar 1- Tone from the top- comprometimento e suporte da Alta Administração *In:* CUNHA, Matheus Lourenço Rodrigues; EL KALAY, Mário. **Manual de compliance***:* compliance mastermind. São Paulo: LEC, 2019, v. 1, p. 113.

serão apagados). Ato contínuo, necessário se faz realizar a avaliação da necessidade e proporcionalidade das operações de tratamento em relação aos objetivos [224].

Exemplificando, supondo que a empresa que esteja buscando a implementação do presente programa tenha uma *landing page*[225] com o fito de coleta de e-mails para encaminhamento posterior de *marketing*, na seara do risco, será necessário avaliar quais os pontos prejudiciais aquela instituição irá incorrer em caso de vazamento de dados.

Para análise do risco será necessário verificar, em momento anterior, qual a finalidade, o objetivo e interesse da instituição na coleta de e-mails, bem como quais dados são realmente necessários para realizar a atividade proposta. Após, levando-se em consideração esses pontos, posteriormente à coleta realizada, caso a base de dados seja violada e esses e-mails forem divulgados na Internet, de maneira ilícita, para cada titular, individualmente, o risco é baixo, assim será caracterizado.

Porém, o controlador precisa se lembrar do fato de que muitos indivíduos utilizam o mesmo e-mail para vários serviços, o que já começa a elevar o nível de risco, o qual passa a ser caracterizado como médio. Utilizando a tabela de matriz de risco o resultado do último exemplo se caracterizou como médio diante da baixa probabilidade de acontecer, mas caso ocorra, se trata de um impacto alto. A figura abaixo exemplifica a presente explanação.

Figura 3 - Matriz de risco probabilidade x impacto- 3x3- com resultado alto

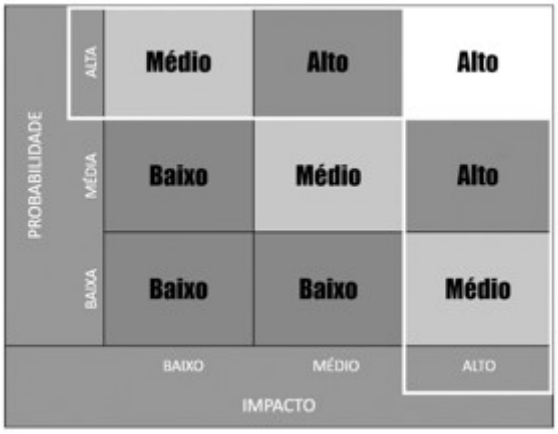
[224] PASSOS, Matheus. LGPD, Governança de Dados e Gestão de Metadados. Curso online. Data Science Academy. 2020. Realizado pelo link: https://www.datascienceacademy.com.br/course/lgpd-governanca-de-dados-e-gestao-de-metadados.

[225] Explica Daniara Regina Citadin o conceito de landing page: “são páginas que possuem um objetivo bem específico em um site. Diferente da página inicial, a página sobre a empresa, ou páginas de produtos, elas se diferem por influenciarem que o usuário tenha uma única ação naquela página. Seja baixar um ebook de conteúdo sobre o produto ou sobre a área de negócio para capturar leads, sejam webinars gratuitos e divulgados por email, blogs de conteúdo, entre outros. Para cada uma dessas ações, desenvolve-se uma página de destino (landing page) com o objetivo de atrair visitantes e transformá-los em leads. Em suma, estas páginas são então portas de entrada para um site”. (CITADIN, Daniara Regina. **Redesign de interface de landing page**: um estudo de caso do site sienge. 2017. Trabalho de Conclusão de Curso (Graduação em Design) – Universidade do Sul de Santa Catarina, Florianópolis, 2017. Disponível em: https://repositorio.animaeducacao.com.br/bitstream/ANIMA/7791/1/TCC%203%20-%20Daniara%20Citadin.pdf. Acesso em: 5 mar. 2022).

Fonte: Doneda.[226]

Em outros casos, se tratasse de um caso que tanto a probabilidade de acontecer seja alta, bem como o impacto também, haverá risco alto. Utilizando a mesma situação hipotética anteriormente apresentada, se trataria, exemplificando, de coleta não apenas do e-mail, mas de CPF, RG e outros dados que podem trazer danos incalculáveis para o titular e consequentemente, para empresa, tanto em relação às sanções que poderá sofrer quanto em razão, da perda da imagem positiva. A figura abaixo represente esse cálculo.

Figura 4 - Matriz de risco probabilidade x impacto- 3x3- com resultado alto



Fonte: Doneda.[227]

Realizado a análise, levando ainda em consideração o exemplo acima explanado, necessário se faz definir quais são as medidas que a empresa tem para

[226] DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico**, Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011, p. 84.
[227] DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico**, Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011, p. 84.

mitigar esse risco médio. Como solução, pode-se realizar a criptografia[228], em que só três funcionários da empresa, a título de exemplo, terão acesso à base de dados da forma originária. A partir do momento em que a organização define essa limitação, há uma medida administrativa/interna que auxilia a reduzir o risco, pelo fato também de que se algum dia houver vazamento dessa base de dados, provavelmente um dos três colaboradores pode estar envolvido.

Essa medidase tratou de uma mitigação do risco. Problema diferente seria se na base de dados estivesse disponível o código da criptografia, no drive da intranet da empresa disponível para todos os colaboradores, contendo a chave privada para descriptografar.

Pelo exemplo apresentado, verifica-se que uma análise de risco se trata de quando a empresa/controlador indica qual é o risco e o responsável direciona os direitos e liberdades dos titulares e, ao mesmo tempo, indica quais são as medidas que devem ser colocadas em prática com o fito de que esses riscos sejam investigados e, consequentemente, seja indicado quais medidas serão aplicadas para mitigar esses riscos. Nesses casos, o controlador tem uma avaliação de impactos sobre a proteção de dados completa e, a depender do resultado, poderá dar início à atividade de tratamento, mas se o risco for elevado e não houver possibilidade de mitigá-los, a atividade não poderá ocorrer[229].

Analisado o risco, passa-se à etapa de resolução dos que foram encontrados durante essas avaliações, em que as organizações devem implementar um procedimento para avaliar os problemas identificados, possíveis processos alternativos para mitigar os riscos e monitorar como as ações de mitigação de risco escolhidas são implementadas. Exemplificando, a empresa tem um determinado processo “x” qualquer para proteger dados e, ao analisar esta operação a fim de averiguar se efetivamente está protegendo dados pessoais, conclui que o procedimento em questão não protege os dados, motivo pelo qual, identificado o

---

[228] Explica Routo Terada que “Algoritmos criptográficos basicamente objetivam “esconder” informações sigilosas de qualquer pessoa desautorizada a lê-las, isto é, de qualquer pessoa que não conheça a chamada chave secreta de criptografia”. (TERADA, Routo. **Segurança de dados:** criptografia em redes de computador. São Paulo: Blucher, 2008, p. 18).

[229] PASSOS, Matheus. LGPD, Governança de Dados e Gestão de Metadados. Curso online. Data Science Academy. 2020. Realizado pelo link: https://www.datascienceacademy.com.br/course/lgpd-governanca-de-dados-e-gestao-de-metadados.

risco, há de se procurar um procedimento alternativo, para substituir o antigo de modo a garantir essa proteção de dados[230].

Na fase final, reportam-se as análises e resultados dos riscos à proteção de dados para quem é de direito. Pode-se remeter para as autoridades de controle (ANPD), quando for requerido, e ainda pode-se divulgar, eventualmente, a colaboradores, de modo em que esses grupos estejam cientes dos riscos de privacidade antes do lançamento de um novo produto, programa, sistema, processo ou para realocação de dados [231].

A empresa tem a possibilidade de contratar uma parte externa para realizar os relatórios de impacto sobre a proteção de dados (tanto os dados pessoais quanto os de segredo do negócio), caso isso implique uma análise de risco mais aprofundada, realizada em situações em que o nível deste seja elevado e quando possui uma atividade de tratamento em larga escala, ou então quando se trata de uma atividade que envolve dados sensíveis, ou ainda quando se trata da possibilidade de monitoramento de um número elevado de titulares, situações que trazem uma atividade de tratamento com risco elevado e tornam necessário realizar a contratação de um externo para realizar a análise. A organização pode definir que uma avaliação será executada por um provedor de serviço externo e, posteriormente, validada a conformidade diante das políticas de privacidade internas da empresa.

Em outro viés, quando se trata da mitigação do risco quando da implementação de *compliance* de dados pessoais, a manutenção dos avisos de privacidade aos titulares sobre como os seus dados são coletados, usados, mantidos, retidos e divulgados, são de extrema relevância. Nesse caso, verifica-se se em todos os pontos de coleta de dados pessoais[232] existem avisos de

---

[230] PASSOS, Matheus. LGPD, Governança de Dados e Gestão de Metadados. Curso online. Data Science Academy. 2020. Realizado pelo link: https://www.datascienceacademy.com.br/course/lgpd-governanca-de-dados-e-gestao-de-metadados.

[231] BROTTO, Natália; CAMARGO, Pedro Henrique Dalgallo. Autoridade Nacional de Proteção de Dados, aspectos pendentes de regulação e cultura de proteção de dados. *In:* In: **Lei Geral de Proteção de Dados: estudos sobre um novo cenário de Governança Corporativa/** coordenado por Rodrigo Pironti. Belo Horizonte: Fórum, 2020. p. 93.

[232] No que se refere aos pontos de coleta podemos citar como exemplo: a empresa possui um próprio site que já se trata de um desses pontos, porque o site provavelmente usa cookies estes tratam dados pessoais, portanto a empresa necessita ter um aviso de cookies indicando quais são estes, quais os motivos deles estarem ali presentes e como os dados são tratados via cookies. Ainda, esse próprio site pode ter outros pontos de coleta, como por exemplo, um formulário de contato. Em outro contexto, imagine a empresa que tem lá um local físico onde fica a sua sede e que na portaria daquele local há a solicitação de preenchimento de um formulário toda vez que um visitante entra

privacidade, sendo necessário que a empresa verifique se está sendo efetivo, ou seja, que estão à disposição do titular no momento correto (antes ou até o momento da coleta dos dados). Realizando essa ação, estará mitigando um risco e garantindo a implementação do programa de *compliance* de proteção de dados no que se refere ao cumprimento dos deveres de informação e transparência que toda empresa tem para com o titular por meio desses avisos de privacidade.

Cumpre destacar o entendimento de Rodrigo Pironti Aguirre de Castro[233]:

> Aqui uma primeira grande questão: tais programas não se resumem ao estabelecimento e publicação de códigos de ética ou de conduta, ou ainda, produtos de prateleira e soluções caseiras como softwares ou sistemas de gestão de informação para integridade que não guardam a mínima relação com a atividade desenvolvida pela empresa. Receitas genéricas não combinam com *Compliance.*

Merece também referência que há inúmeras *red flags*[234] para os profissionais da área da saúde, por exemplo, em que a implementação do programa começa pela busca de riscos (e esse mapeamento não é estático, devendo existir durante todo o ciclo de vida do dado[235]) e todas as ações que necessitem do dever de guarda e proteção dos dados. E aqui entram os prontuários digitalizados, devendo ser lembrado que não se deve proteger apenas os dados digitais, mas os em meio físico também, principalmente quando digitalizado for. Então, a conformidade não pode se limitar a banco de dados e arquivos digitais, menosprezando arquivos físicos.

---

na empresa, razão pela qual ali deve existir um aviso de privacidade. Outro viés é o caso das empresas que utilizam câmeras de vigilância, ou seja naquele local temos um outro ponto de coleta de dados pessoais que se trata das imagens das pessoas, portanto em todos esses cenários criados, é obrigatório que a empresa possua os avisos de privacidade corretos e atualizados, encontrando-se na sua versão mais recente e devem, efetivamente, passar informação para o titular a respeito daquela atividade de tratamento de dados pessoais a qual será realizada com base nos dados coletados naquele ponto de coleta.

233 COMPLIANCE: repensando o óbvio para não cair no senso comum. 12 mar. 2019. Disponível em: https://cafe.jmlgrupo.com.br/compliance-repensando-o-obvio-para-nao-cair-no-senso-comum/. Acesso em: 2022.

234 alertas vermelhos

235 A título da menção, importante destacar que a MP/983 (agora lei 14.063), deu legalidade a assinatura avançada (que não é de padrão ICP-BRASIL). Contudo o §2º da lei da digitalização (13.787/2018) não foi revogado. “Art. 2º. O processo de digitalização de prontuário de paciente será realizado de forma a assegurar a integridade, a autenticidade e a confidenciabilidade do documento digital.§2º. No processo de digitalização será utilizado certificado digital emitido no âmbito da Infraestrutura de Chaves Públicas Brasileiras (ICP-Brasil) ou outro padrão legalmente aceito”. Esse fato ilustra a necessidade quanto a necessidade da aplicação do *compliance* se dar de forma contínua. Isso porque, atualmente, nos prontuários médicos por não ter sido revogado tal dispositivo, recomenda-se a continuidade do uso da assinatura pelo ICP-BRASIL.

Em linhas conclusivas do presente pilar, registra-se que a atividade de tratamento se realizará para cada perigo detectado e toda a análise deverá ser documentada, para que posteriormente possa realizar a comprovação do trabalho realizado pelo operador e, consequentemente, comprovar que realizou a deliberação.

A materialização das regras do programa de *compliance* de dados desenvolvidas a partir do levantamento de riscos e, ainda, somadas às demais regulações normativas que a organização deve seguir, criam cenário fértil para desenvolver estruturas de controle interno, as quais devem estar consolidadas em um código, que define normas para todos os funcionários e colaboradores daquela instituição. Renata Machado Saraiva explana que "trata-se, assim, de uma declaração expressa das políticas, dos valores, da ética e das diretrizes" [236].

Em linhas gerais, os códigos de condutas devem expor, em um primeiro momento, todos os valores e princípios éticos que as atividades desenvolvidas naquela organização estão sendo baseadas.

Posteriormente, deve-se expor as principais exigências quanto à postura que os colaboradores devem tomar, a título de exemplo, requerer o zelo ao patrimônio da empresa, solicitar o sigilo de informações perante terceiros (além dos que estão alheios à empresa, em caso de definição de nível entre os trabalhadores, deve-se guardar a informação entre eles).

Registra-se que a elaboração do código deve ser vista como uma mensagem da alta administração a todos os colaboradores e trabalhadores, que refletirá, inclusive, em toda a sociedade, motivo pelo qual é de extrema importância que membros da alta administração aprovem o Código de Conduta a ser elaborado e se comprometam com o cumprimento em rigor das diretrizes ali estabelecidas [237].

De igual importância, destaca-se a necessidade de que o código defina as medidas disciplinares e sancionatórias caso venha a descumprir as normas vigentes, de modo que o código não fique apenas como mero documento elaborado pela empresa[238].

---

[236] SARAIVA, Renata Machado. **Criminal compliance como instrumento de tutela ambiental**: a propósito da responsabilidade penal das empresas. São Paulo: LiberArs, 2018, p. 85.

[237] JÚNIOR, Filipa Marques; MEDEIROS, João. A elaboração de programas de compliance. *In*: SOUSA MENDES, Paulo de; PALMA, Maria Fernanda; SILVA DIAS, Augusto. **Estudos sobre law** enforcement, compliance e direito penal. Lisboa: Almedina, 2018, p. 140.

[238] SARAIVA, Renata Machado. **Criminal compliance como instrumento de tutela ambiental**: a propósito da responsabilidade penal das empresas. São Paulo: LiberArs, 2018, p. 90.

Além disso, criação de documentos que facilitam o entendimento do colaborador é de extrema importância. Nesta seara, indica-se que os códigos de conduta e políticas de *compliance* se atentem à utilização de mecanismos que facilitem a visualização do documento e que sejam fixadas pelo colaborador. Para isso, dentre os mecanismos existentes, usar *nudges*[239] é um uma excelente ferramenta apresentada pelos economistas comportamentais como auxílio no entendimento da funcionalidade, eis que se trata de uma arquitetura de escolha e paternalismo libertário [240].

Explicando mais sobre o recurso, *nudge* tem a sua tradução estrita como sendo um "empurrão", e se trata de um novo enquadramento de escolhas, o qual é gerado com a finalidade de superar as tendências inconscientes e fazendo com que indivíduos adotem decisões consideradas irracionais [241]. O termo trata de ferramentas utilizadas para auxiliar nas decisões a serem tomadas, destacando o atendimento a liberdade de escolhas, de preferência na direção correta[242].

Não se trata de manipulação, já que não altera os incentivos econômicos existentes previamente, bem como não obriga um indivíduo a seguir a direção específica de quem determina. Pode ser, na verdade um alerta, *defaults* (que são as escolhas padrão) ou requerimentos de divulgação de informações ao público de maneira direta e clara[243].

É o caso, por exemplo, da disposição de alimentos mais saudáveis em um supermercado, com a finalidade de induzir o consumidor a preferir aqueles ao invés de outros de menor qualidade. Cita-se ainda que para o combate à pandemia, houve

---

[239] Felix Kessler apresenta como "o segundo conceito importante é o da Arquitetura da Escolha. Esse é o nome dado ao processo de elaboração do método a ser utilizado para que melhores decisões sejam tomadas por parte daqueles que enfrentam uma situação de escolha. Porém, é importante deixar claro que só se pode considerar um nudge aquelas intervenções onde a liberdade de escolha é mantida. Em outras palavras, não se deve induzir alguém a tomar uma atitude sem que este possa arbitrar a priori ante as possibilidades. Este ainda é um assunto muito polêmico, pois a autonomia individual é algo considerado sagrado no mundo ocidental". (KESSLER, Felix. **Empurrõezinhos e nossos processos cerebrais**. Disponível em: http://www.economiacomportamental.org/nacionais/empurroezinhos-e-nossos-processos-cerebrais/. Acesso em: 25 ago. 2022).

[240] THALER, Richard H; SUSTEIN, Cass R. **Nudge**: improving decisions about health, wealth and happiness. London: Penguin, 2009.

[241] NERY, P. F. **Errar é humano**: economia comportamental aplicada à aposentadoria. Brasília: Núcleo de Estudos e Pesquisas/CONLEG/ Senado, 2016. Texto para Discussão n. 188. Disponível em: www.senado.leg.br/estudos. Acesso em: 15 fev. 2022.

[242] KESSLER, Felix. **Empurrõezinhos e nossos processos cerebrais**. Disponível em: http://www.economiacomportamental.org/nacionais/empurroezinhos-e-nossos-processos-cerebrais/. Acesso em: 25 ago. 2022.

[243] THALER, Richard H; SUSTEIN, Cass R. **Nudge**: improving decisions about health, wealth and happiness. London: Penguin, 2009, p. 108-111.

aplicação de *nudges* importantes para evitar a disseminação da doença, como quando utilizados alertas para conscientizar o público em geral. Outro exemplo clássico é o GPS, que sempre sugere a melhor rota em termos de distância ficando na conveniência do usuário se adere ou não [244].

No caso da criação do código de ética pode ser utilizado ícones para auxiliar na visualização do documento e dar maior atenção ao tópico, como o caso das imagens de perigo, setas indicando a atenção, entre outros [245].

Ultrapassada a criação de códigos de conduta, agora passa-se para a criação da política de *compliance*. Nesse momento, dá-se início à implementação das práticas para o gerenciamento de dados na empresa, que trata-se de documentos (termo utilizado no plural diante da necessidade de criação de várias políticas em cada determinado assunto) em que toda organização deve apresentar os ideais e procedimentos específicos a serem utilizados em determinadas situações. Trata-se de criação de termos, um documento estratégico de uma organização, que diz respeito à estruturação daquilo que a organização entende como sendo a sua estratégia. Por exemplo, no que se refere a uma política de senha a empresa utiliza o entendimento de que a senha seja trocada todo mês e que não possa ser reutilizada pelo menos as três últimas. Nesse caso o procedimento é indicar para o colaborador como se dará a criação de nova senha (quantidade de caracteres, números, letras, etc).

Em termos da criação de política principal, apresentar os principais conceitos relacionados à proteção de dados é de extrema importância[246]. Poderá no caso definir os comportamentos e procedimentos que o colaborador deve seguir na coleta de dados, bem como em casos que não constem na política de procedimento, procure o DPO da empresa antes da tomada de novas atitudes.

Na aplicação deste pilar, ao definir a tomada de atitudes para o colaborador ao se deparar com alguma atividade específica, pode-se apresentar o caminho a ser perscrutado pelo colaborador, apresentando os modelos de respostas, as decisões

---

[244] BHARATH, B. S. **The nudge theory**: a stellar strategy for a better outcome. Disponível em: https://uxdesign.cc/nudge-theory-a-stellar-strategy-for-a-better-outcome-8504d5f7af74. Acesso em: 05 out. 2022.

[245] PASSOS, Matheus. LGPD**, Governança de Dados e Gestão de Metadados**. Curso online. Data Science Academy. 2020. Realizado pelo link: https://www.datascienceacademy.com.br/course/lgpd-governanca-de-dados-e-gestao-de-metadados.

[246] Pode-se alguns indagar se há na lei a definição qual a necessidade de descrever no documento de políticas de *compliance*, a necessidade se dá pelo fato de que os colaboradores não são obrigados conhecer as leis, bem como para facilitar o entendimento do trabalhador.

automatizadas a serem utilizadas e procedimentos específicos a depender de cada caso[247].

Importante destacar que os procedimentos aqui apresentados são aplicados para empresas de todo o porte (desde a pequena até as organizações maiores) devendo se adaptar cada uma a sua realidade. Trata-se de *insights* para a implementação do programa na empresa.

Os auditores devem realizar entrevistas com o fito de averiguar as possíveis ameaças existentes ou apenas para certificar se o tratamento está sendo devidamente realizado. Pode-se proceder através de pesquisas, desde em relação quem ocupa o cargo da mais alta administração até o trabalhador da ponta, um operador funcional[248].

Importante sempre o controlador lembra-se que é de extrema necessidade a documentação de toda a investigação realizada, haja vista que, em eventuais certificações e investigações em níveis externos, será exigida a comprovação da auditoria na empresa realizada em tempos pretéritos[249].

As investigações internas irão garantir que o programa de *compliance* se comprove como efetivo naquela organização. Porém, necessário que seja visto com olhares de terceiros sobre a empresa, isso porque a necessidade de certificação é importante e projeta na empresa conceitos positivos.

Ademais, em que pese haver toda a documentação da auditoria interna, os auditores que realizam o procedimento, podem ser questionados acerca de suas certificações[250], se não possuírem, poderão ser desacreditados quanto ao programa [251].

No que se refere as certificações, estas se consubstanciam em ferramentas fundamentais para as organizações que pretendem se ampliarem e alocar-se com

---

[247] PASSOS, Matheus. LGPD, Governança de Dados e Gestão de Metadados. Curso online. Data Science Academy. 2020. Realizado pelo link: https://www.datascienceacademy.com.br/course/lgpd-governanca-de-dados-e-gestao-de-metadados.

[248] PASSOS, Matheus. LGPD, **Governança de Dados e Gestão de Metadados**. Curso online. Data Science Academy. 2020. Realizado pelo link: https://www.datascienceacademy.com.br/course/lgpd-governanca-de-dados-e-gestao-de-metadados

[249] PASSOS, Matheus. LGPD, **Governança de Dados e Gestão de Metadados**. Curso online. Data Science Academy. 2020. Realizado pelo link: https://www.datascienceacademy.com.br/course/lgpd-governanca-de-dados-e-gestao-de-metadados

[250] Há diversas certificações relevantes, mas, como parte relacionada ao tema deste trabalho de pesquisa, citam-se: ISO 19600 – Sistemas de Gestão da Conformidade ISO - 26000 – Da ética à responsabilidade social; ISO 31000 – Gestão de Riscos – Princípios e Diretrizes e; ISO 31010 – Gestão de Riscos - Técnicas para o Processo de Avaliação de Riscos

[251] No sítio eletrônico da ABNT-ISO há inúmeros cursos para preparar a equipe da auditoria interna.

destaque no mercado em que estão inseridas, criando um diferencial competitivo frente às concorrentes. Se trata de uma forma de mostrar-se organizado, de apresentar-se de maneira sistêmica. Entre as variadas certificações existentes, destaca-se as normas ISO (*International Organization for Standardization*) como parâmetro, uma organização internacional, formada por países diversos, com o fito de definir normas técnicas no âmbito internacional [252].

Caso não seja do interesse da empresa a certificação, o programa Pró-Ética que iniciou-se o Cadastro Pró-Ética, em 2010, criado pelo Instituto Ethos de Empresas e Responsabilidade Social (Instituto Ethos[253]) e pela então Controladoria-Geral da União (CGU) é outro excelente meio para demonstrar a busca pela conformidade. De acordo com o Instituto Ethos[254], a corrupção é um mal que tem origem nos diversos setores da sociedade e precisa ser mitigado de forma colaborativa. Nesse sentido, a parceria com a CGU teria surgido para "reagir contra o alto custo social, político e econômico gerado pela corrupção, e pago, de uma maneira ou de outra, por empresas, governos e cidadãos" [255].

Diferentemente da ISO, a pró-etica não se trata de uma certificação, mas de um meio de fomento. A ideia é que, ao se encaminhar toda a extensa ficha de informações requeridas na plataforma, será gerado um resultado informando se a empresa se encontra ou não atendendo àqueles ditames. Caso não atenda, é uma experiência válida, já que os resultados poderão auxiliar o controlador a realizar mudanças nos déficits da empresa [256].

As empresas que coletam e usam informações pessoais, através da gestão de análise de risco, devem monitorar e medir se as políticas que tenham adotado e

---

[252] AZEVEDO, Mateus Miranda de Azevedo; CARDOSO, Antônio Almeida; DARTE, Jairo Gonçalves; FEREICO, Bianca Ellen; LIMA, Marco Antônio Ferreira. O *compliance* e a gestão de riscos nos processos organizacionais. Disponível em < http://www.fics.edu.br/index.php/rpgm/article/view/507/555>. Acesso em 30 dez. 2022.

[253] "O Instituto Ethos trata-se de uma organização da sociedade civil de interesse público (Oscip) criada em 1998 e sediada em São Paulo. Sua missão é mobilizar, sensibilizar e auxiliar as empresas a gerirem seus negócios de modo socialmente responsável, fazendo delas parceiras na construção de uma sociedade justa e sustentável". (INSTITUTO ETHOS. **Sobre o Instituto**. Disponível em: https://www3.ethos.org.br/conteudo/sobre-o-instituto/#.WSm7B2jyvIV . Acesso em: 27 maio 2022).

[254] INSTITUTO ETHOS. **Sobre o Instituto**. Disponível em: https://www3.ethos.org.br/conteudo/sobre-o-instituto/#.WSm7B2jyvIV . Acesso em: 27 maio 2022

[255] INSTITUTO ETHOS. **Empresa pro-ética.** 2016. Disponível em: https://www.ethos.org.br/conteudo/projetos/integridade/empresa_pro_etica/#.WSnRlmjyvIU. Acesso em: 27 maio 2022.

[256] INSTITUTO ETHOS. **Empresa pro-ética.** 2016. Disponível em: https://www.ethos.org.br/conteudo/projetos/integridade/empresa_pro_etica/#.WSnRlmjyvIU. Acesso em: 27 dez. 2022.

implementado realmente protegem, asseguram as informações e estão efetivamente em funcionamento. Essa atitude através dos sistemas de monitoramento de desempenho com base em suas próprias culturas de negócio são que tornam as empresas mais eficazes e mais seguras diante do público externo. E para que isso ocorra, a empresa deve estabelecer programas de *compliance* que visam garantir que os mecanismos sejam utilizados adequadamente por funcionários que tomam decisões sobre o gerenciamento de informações, sendo feita sua análise quanto ao cumprimento de forma contínua e periódica [257].

Mesmo com o código de conduta interno devidamente elaborado e entregue aos colaboradores, é importante ressaltar que o programa de *compliance* não será eficaz se os setores responsáveis pela gestão e disseminação das regras de integridade não praticarem esforços para transmitirem aos seus funcionários as nefastas consequências provocadas pela violação das normas e não vigilância da proteção de dados [258].

É importante que o treinamento dos trabalhadores/colaboradores trate de atos contínuos, destacando sempre a necessidade de demonstrar os riscos particulares vinculados a cada grupo, cada departamento. É sabido que os treinamentos são a chave para que seja concretizado o *compliance* na empresa [259].

O treinamento deve destacar o cuidado que o colaborador precisa ter com abertura de e-mails suspeitos, que podem gerar ataques maliciosos por agentes que se fundamentam na inocência do colaborador. Em suma, pequenas questões que se atentadas ao colaborador poderão mitigar inúmeros riscos [260].

O controlador/operador, após a indicação aos seus colaboradores para nunca abrirem ou responderem a e-mail suspeito, como a título de exemplo, pode criar um

---

[257] FARIA, Felipe. Comunicação e treinamento de compliance: difundindo a cultura da integridade. In: CUNHA, Matheus Lourenço Rodrigues; EL KALAY, Mário. **Manual de *compliance: compliance mastermind***. São Paulo: LEC, 2019. p. 219.

[258] LOOSLI, Marilia Zulini da Costa; IKO, Massamitsu Alberto. Código de ética e de conduta, políticas e procedimentos: os documentos normativos relacionados ao programa de integridade da empresa. In: CUNHA, Matheus Lourenço Rodrigues; EL KALAY, Mário. **Manual de *compliance: compliance mastermind***. São Paulo: LEC, 2019, p. 162.

[259] FARIA, Felipe. Comunicação e treinamento de compliance: difundindo a cultura da integridade. In: CUNHA, Matheus Lourenço Rodrigues; EL KALAY, Mário. **Manual de *compliance: compliance mastermind***. São Paulo: LEC, 2019. p. 219.

[260] FARIA, Felipe. Comunicação e treinamento de compliance: difundindo a cultura da integridade. In: CUNHA, Matheus Lourenço Rodrigues; EL KALAY, Mário. **Manual de *compliance: compliance mastermind***. São Paulo: LEC, 2019. p. 220.

e-mail *phishing*[261] (e-mail falso), com a finalidade de testar o seu colaborador, porém quando este entrar, cairá em uma página da própria empresa, podendo colocar uma informação alertando ao colaborador.

Outro exemplo se consubstancia no fato de que a empresa entende factível que os colaboradores conheçam as diretrizes da lei geral de proteção de dados, pelo que, caso seja viável, indica-se o treinamento a ser direcionado às pessoas que precisam ter um conhecimento mais aprofundado sobre o que que a lei exige.

Para que os processos de monitoração das irregularidades levantadas sejam desenvolvidos de forma eficiente, o que se recomenda é que seja elaborado, no âmbito interno da empresa, canais de comunicação que permitam aprimorar a metodologia de recebimento de denúncias internas, para qualificar as investigações a serem realizadas.

Esses mecanismos podem ser criados, a partir do desenvolvimento de um canal de denúncia online em uma plataforma terceirizada que garanta o sigilo e a imparcialidade, utilizando de *login* e senha padrão (mesmo *login* e senha para todos). Outra sugestão é deixar "caixas de sugestão" na empresa[262], medidas estas que garantem que o denunciante está resguardado de qualquer tipo de retaliação.

É de suma importância que as informações necessárias estejam disponíveis ao colaborador para que não tenha necessidade ou sinta-se reprimido em procurar saber como realizar a denúncia. Nos treinamentos, no código de postura, sempre deve ser deixado claro onde estarão os locais para recebimento da denúncia. Se tratar-se de um site online, são convenientes *qr codes* ou o *link* de acesso disponíveis para o colaborador [263].

Recebida a denúncia, o responsável deve encaminhar para ser realizada a investigação interna, com base no pilar anteriormente explanado, momento em que

---

[261] Daniel Donda conceitua *phishing* como "é o tipo de golpe em que um atacante tenta obter dados pessoais e financeiros de um usuário pela utilização combinada de meios técnicos e engenharia social usando e-mails falsos de grandes empresas com links maliciosos." (DONDA, Daniel. **Guia prático da implementação da LGPD**: tudo o que sua empresa precisa saber para estar em conformidade. São Paulo: Labrador, 2020. e-Book, p. 102-103).

[262] Aqui importante destacar a necessidade que seja em um local não vigilado por câmeras a fim de que o trabalhador não se sinta coibido em realizar a denúncia (como caixas deixadas no banheiro por exemplo).

[263] PASSOS, Matheus. LGPD, **Governança de Dados e Gestão de Metadados**. Curso online. Data Science Academy. 2020. Realizado pelo link: https://www.datascienceacademy.com.br/course/lgpd-governanca-de-dados-e-gestao-de-metadados.

terá a decisão de mitigar o risco, descartá-lo e/ou aplicar sanções inerentes ao caso em concreto[264].

Um programa de *compliance* não é robusto se não houver a efetiva concretização de todos os pilares. Uma empresa que define suas políticas e procedimentos deve poder provar, que as medidas estão sendo concretizadas, em vigilância aos princípios da responsabilização e prestação de contas. Não se justifica a criação de estratégias na sua política, definir os procedimentos específicos, repassar esses procedimentos os colaboradores em treinamentos, mas não serem consolidados de forma efetiva[265].

À luz deste entendimento, verifica-se a necessidade de implementação na prática da verificação se os procedimentos estão efetivamente sendo concretizadas, a qual se dará por meio das investigações internas.

Com o propósito estabelecido, os mecanismos de *compliance* de dados deverão ser devidamente gerenciados, verificando na prática se cada responsável por determinada atitude está engajado e comprometidos com a proteção de dados. Caso seja identificada a falta de comprometimento por alguns dos colaboradores, por exemplo, indica-se como solução reforçar os treinamentos, melhorar e estruturar as etapas de resposta, caso identificado falha no documento de políticas, ou se for o caso, aplicar as sanções ali descritas [266].

É de grande necessidade esta verificação, a fim de checar se houve algum problema e, em caso positivo, se foi devidamente resolvido e apurar a possível melhoria dos processos internos com o fito de evitar que este problema se repita em momento futuro. Assim como a importância da comprovação em todos os outros pilares, implica-se, após a investigação emitir relatórios para indicar como se encontra a situação atual da empresa, a fim de manter um plano de resposta à violações de dados que possa a vir incorrer [267].

---

[264] GONSALES, Alessandra; SIBILLE, Daniel. Investigações Internas e medidas disciplinares. In: CUNHA, Matheus Lourenço Rodrigues; EL KALAY, Mário. **Manual de *compliance: compliance mastermind***. São Paulo: LEC, 2019. p. 220.

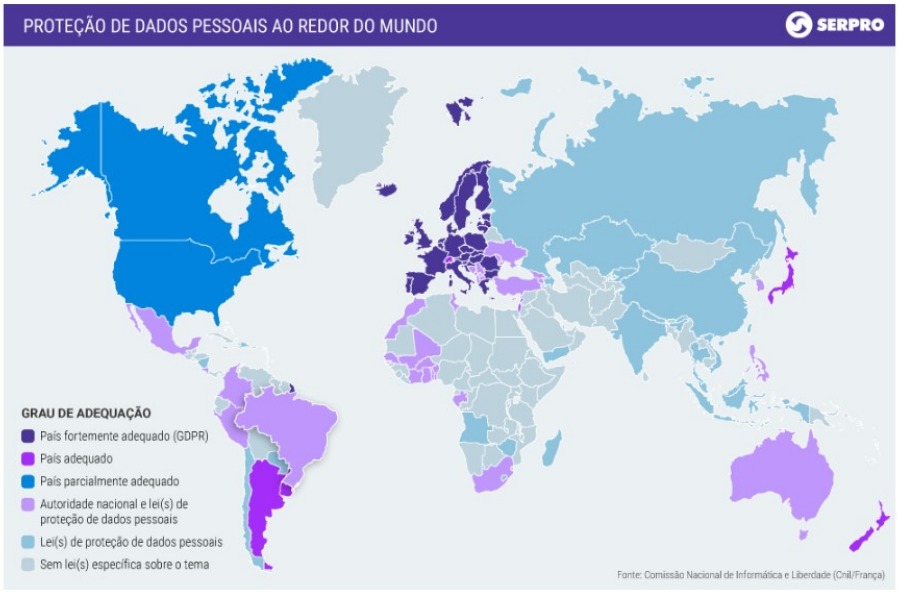
[265] PASSOS, Matheus. LGPD, **Governança de Dados e Gestão de Metadados**. Curso online. Data Science Academy. 2020. Realizado pelo link: https://www.datascienceacademy.com.br/course/lgpd-governanca-de-dados-e-gestao-de-metadados.

[266] FARIA, Felipe. Comunicação e treinamento de compliance: difundindo a cultura da integridade. In: CUNHA, Matheus Lourenço Rodrigues; EL KALAY, Mário. **Manual de *compliance: compliance mastermind***. São Paulo: LEC, 2019. p. 222.

[267] PASSOS, Matheus. LGPD, **Governança de Dados e Gestão de Metadados**. Curso online. Data Science Academy. 2020. Realizado pelo link: https://www.datascienceacademy.com.br/course/lgpd-governanca-de-dados-e-gestao-de-metadados.

Antes de adentrar nos aspectos práticos da *due diligence*, cumpre salientar que a proteção de dados é de extrema importância em todo o mundo. Conforme se infere do mapa abaixo, que trata das legislações de proteção de dados (especificamente dos dados pessoais) no mundo como um todo, verifica-se a relevância e necessidade de conhecer a respeito da legislação da proteção de dados de uma maneira geral[268].

Figura 5 - Proteção de dados ao redor do mundo



Fonte SERPRO [269]

O mapa acima apresentado aponta a dimensão da expansão quanto às exigências do cumprimento das normas de proteção de dados.

Retomando aos pilares, de maneira prática, proporcionando contornos mais completos à *due diligence*, esta pode ser efetivada através de um *background check*[270], sendo entendida como verificação de antecedentes. Normalmente envolve

---

[268] CUNHA. Matheus Lourenço Rodrigues da. Due diligence de integridade: uma estratégia para a gestão de riscos de terceiro. *In:* CUNHA, Matheus Lourenço Rodrigues; EL KALAY, Mário. **Manual de compliance***:* compliance mastermind. São Paulo: LEC, 2019. p. 264.

[269] Comparativo da proteção de dados ao redor do mundo disponível no sítio eletrônico. (EM QUE "ESTÁGIO" estamos? Confira o mapa da proteção de dados pessoais no mundo. Disponível em: https://www.serpro.gov.br/lgpd/menu/a-lgpd/mapa-da-protecao-de-dados-pessoais. Acesso em: 2022).

[270] Nas palavras de Tatiana Camarão é “a avaliação detida do comportamento passado”. (CAMARÃO, Tatiana. A gestão por competência na nova lei de licitações e contratos. **Consultor Jurído**, 2021. Disponível em: https://repositorio.ufsc.br/bitstream/handle/123456789/229560/ConJur%20-%20Tatiana%20Camar%C3%A3o_%20Gest%C3%A3o%20por%20compet%C3%AAncia%20na%20nova%20Lei%20de%20Licita%C3%A7%C3%B5es.pdf?sequence=1. Acesso em: 26 out. 2022).

pesquisas em fontes públicas e privadas[271], pesquisas de campo, incluindo a busca por certidões de distribuição de processos judiciais, investigações relevantes (especialmente criminais), relacionamentos com pessoas praticamente expostas, notícias de mídia, registros em listas de sanções, dentre outros. Porém, uma ferramenta bastante rica são os questionários da *due diligence*[272], pelo fato de que é a oportunidade que o terceiro tem em apresentar as informações de importância que a diligência não tenha efetivamente encontrado (como os casos dos processos de segredo de justiça, por exemplo) [273].

A título exemplificativo, a pesquisa em questão importa em verificar as vulnerabilidades que a empresa, ao realizar o negócio com outra estará suscetível, revisar as políticas empregadas na organização terceira a fim de diminuir a assimetria de informações[274], identificar as políticas de proteção de dados e de

---

[271] Cumpre destacar algumas fontes de pesquisas de dados públicos: CEIS- Cadastro Nacional de Empresa Idôneas e Suspensas: pessoas físicas e jurídicas que sofreram sanções e estão restritas de participar de licitações ou celebrar contratos com a administração pública; CNEP- Cadastro Nacional de Empresas Punidas: pessoas jurídicas que sofreram punições previstas na Lei Anticorrupção (Lei 12.846/2013); CEPIM- Cadastro de Entidades Privadas Impedidas sem Fins Lucrativos: pessoas jurídicas que estão impedidas de realizar contratações com a administração pública federal; CADE- Conselho Administrativo de Defesa Econômica: Entidade vinculada ao Ministério da Justiça que tem como finalidade a prevenção e a repressão às infrações contra a ordem econômica; COAF- Conselho de Controle de Atividades Financeiras: pessoas jurídicas que estão impedidas de realizar contratações com a administração pública federal, tendo em vista o repasse de recursos; CVM- Comissão de Valores Mobiliários: Fiscalização das atividades de mercado imobiliário e de capitais; CNCIAI/CNJ (Cadastro Nacional de Condenações Cíveis por Ato de Improbidade Administrativa e Inelegibilidade. No que se refere às fontes de dados privados, destaca-se: UpMiner: Sistema que utiliza os dados disponíveis na internet como fonte de coleta de informações através de buscas automotizadas tanto de pessoas físicas quanto jurídicas; LexisNexis: Semelhante ao anterior; Factiva (Dow Jones): Fonte mundial de dados, fornece alertas e capacidade de investigação, com acesso a fontes de mais de 22 (vinte e dois) milhões de empresas públicas e privadas; Risk & Compliance (Dow Jones): Fonte de dados para monitorar riscos associados a terceiros, auxiliando empresas a cumprirem os requisitos regulamentares sobre lavagem de dinheiro, anticorrupção e antisuborno.

[272] Tendo em vista que o questionário de *due diligence* deve ser elaborado consoante a realidade de cada empresa, segue alguns modelos que podem ser utilizados para guiar a organização na elaboração do questionário adequado para sua realidade:

1) <https://webcache.googleusercontent.com/search?q=cache:-FQKUL03mh8J:https://www.anbima.com.br/data/files/4A/F6/CC/F6/EDB5D5100A6685D599A80AC2/Questionario-Due-Diligence-Secao-I.doc.doc&cd=1&hl=pt-BR&ct=clnk&gl=br; https://webcache.googleusercontent.com/search?q=cache:VHS8a1B_RtoJ:https://www.cob.org.br/pt/documentos/download/3ed43f5c7271c/&cd=17&hl=pt-BR&ct=clnk&gl=br>

2)<https://webcache.googleusercontent.com/search?q=cache:IM3IsJ5sxAIJ:https://docplayer.com.br/62787801-Questionario-de-due-diligence.html&cd=11&hl=pt-BR&ct=clnk&gl=br> e

3) <https://www.neoenergiaelektro.com.br/Media/Default/Chamada-Publica-2022/Anexo10-Questionario-Due-Diligence-CPP2022.pdf> .

[273] CUNHA. Matheus Lourenço Rodrigues da. Due diligence de integridade: uma estratégia para a gestão de riscos de terceiro. *In:* CUNHA, Matheus Lourenço Rodrigues; EL KALAY, Mário. **Manual de compliance***:* compliance mastermind. São Paulo: LEC, 2019.

[274] A assimetria informacional consubstancia em “uma das partes naturalmente tem um conhecimento mais aperfeiçoado sobre o objeto da transação”, o que gera consequência a alteração do comportamento racional dos indivíduos, bem como da estrutura de preços no mercado, o que abre

segurança de informação que a empresa utiliza, bem como buscar históricos e reputação dos terceiros prestadores de serviços.

Destaca-se que essa etapa envolve descrever os riscos que forem passíveis de verificar na análise, destacando as causas e consequências mais abrangentes da infração, caso venha a ocorrer. Isso porque, somente com a correta identificação dos riscos os outros pilares do *compliance* poderão ser executados de maneira eficaz[275].

Após serem identificados, deve-se proceder a avaliação dos riscos da *due diligence*, compreendidos através de escalas de probabilidade de ocorrência de acordo com o nível e natureza do risco, que poderá ser classificada, em categorias crescentes de menor ao maior grau de probabilidade de incidência (a título de exemplo como destacado anteriormente- baixo, médio ou alto), avaliados a partir das informações levantadas na realização das práticas de *due diligence* [276].

Assim, após identificado o nível de probabilidade de ocorrência do risco ao se contratar a empresa terceira, deverá ser identificada a escala de impacto (conforme explanado no tópico da análise do risco- probabilidade x impacto) caso ocorra a materialização do risco. Finalmente, após a identificação das causas, das possíveis consequências e caso ocorra a materialização do risco, se elegerão as melhores estratégias para tratamento de cada nível de risco, seja concluindo para realizar o planejamento de ações que buscam modificar, ou até mesmo evitar a parceria/contratação [277].

---

margem para atitudes desonestas, com o consequente aumento dos custos de transação, tendo em vista a ineficiência do Estado em proibir tais condutas (RIBEIRO; KLEIN, 2016, p. 89-95)- RIBEIRO, Marcia Carla Pereira; KLEIN, Vinicius. **O que é análise econômica do direito: uma introdução** / Marcia Carla Pereira Ribeiro; Vinicius Klein (Coord.). 2. ed. Belo Horizonte: Fórum, 2016. Contudo, o compliance visa reduzir esse custo, sendo um dos mecanismos criados com o fito de reduzir a assimetria de informação.

[275] CUNHA, Matheus Lourenço Rodrigues da; CASTRO, Rodrigo Pironti Aguirre de. Compliance risk assessment: análise de caso de participação em licitações e contratos públicos. In: CUNHA, Matheus Lourenço Rodrigues; EL KALAY, Mário. **Manual de *compliance: compliance mastermind*.** São Paulo: LEC, 2019, p. 274.

[276] CUNHA. Matheus Lourenço Rodrigues da. *Due diligence* de integridade: uma estratégia para a gestão de riscos de terceiro. *In:* CUNHA, Matheus Lourenço Rodrigues; EL KALAY, Mário. **Manual de *compliance*: *compliance mastermind***. São Paulo: LEC, 2019, p. 265.

[277] CUNHA, Matheus Lourenço Rodrigues da; CASTRO, Rodrigo Pironti Aguirre de. *Compliance risk assessmen*t: análise de caso de participação em licitações e contratos públicos. In: CUNHA, Matheus Lourenço Rodrigues; EL KALAY, Mário. Manual de compliance: compliance mastermind. São Paulo: LEC, 2019, p. 159.

Após finalizar todos os levantamentos de dados, que em regra é feito por escrito como uma espécie de parecer[278], com descrição dos fatos relevantes indicação da conclusão mais prudente ser tomada, deverá ser entregue aos gestores para dar suporte à tomada de decisão. No corpo do conteúdo deverão constar os pontos de destaque encontrados na pesquisa que possam representar riscos para o negócio/operação que a organização deseja realizar. Na conclusão, ao final, deve-se recomendar a ação a ser tomada pela alta gestão com base nas informações encontradas[279].

Como bem destaca Rodrigo Pironti Aguirre de Castro:

> Tomadas as devidas providências, o gestor poderá, em eventual processo de responsabilização, seja ele administrativo ou judicial, apresentar tais elementos e comprovar que dentro da sua alçada e atribuições não se omitiu ou "agiu com cegueira deliberada" e que tomou as providências necessárias que lhe eram possíveis no caso concreto [280].

A *due diligence* também se aplica na contratação de colaboradores, área esta de extrema relevância e que precisa ser tratada com muita atenção, especialmente por saber da existência de sistemas de recrutamento automatizados em que o titular simplesmente insere os seus dados pessoais em um determinado sistema e este, por sua vez, gerará o resultado. No caso, além da proteção de dados que deve haver vigilância quanto do recolhimento para análise de recrutamento de colaboradores, deve-se realizar todo o procedimento de verificação aqui tratado[281].

Cumpre aqui ressaltar, possível antinomia entre a lei geral de proteção de dados e a *due diligence.* Isso porque, durante este processo de análise são

---

[278] Segue exemplos de relatório de *due diligence*: que podem ser acessados nos seguintes sítios eletrônicos <http://webcache.googleusercontent.com/search?q=cache:up7KBKzIlBMJ:resind.com.br/wp-content/uploads/2021/05/Relatorio-de-Due-Diligence-Resind-Industria-e-Comercio-2020-Portugues-01.05.pdf&cd=16&hl=pt-BR&ct=clnk&gl=br> e <https://www.csn.com.br/wp-content/uploads/sites/452/2021/03/Relatorio-de-Due-Diligence-2020.pdf>

[279] PASSOS, Matheus. LGPD, **Governança de Dados e Gestão de Metadados**. Curso online. Data Science Academy. 2020. Realizado pelo link: https://www.datascienceacademy.com.br/course/lgpd-governanca-de-dados-e-gestao-de-metadados.

[280] CASTRO, Rodrigo Pironti Aguirre de. **A due diligence**: instrumento de compliance à serviço da governança e da segurança jurídica nas relações empresariais em PPP´s. Disponível em: https://www.cafecompliance.com.br/?area=artigo&c=819280cbb9e37d853ccaa9f3632cf1b8. Acesso em: 19 ago. 2022.

[281] CUNHA. Matheus Lourenço Rodrigues da. *Due diligence* de integridade: uma estratégia para a gestão de riscos de terceiro. *In:* CUNHA, Matheus Lourenço Rodrigues; EL KALAY, Mário. **Manual de *compliance: compliance mastermind***. São Paulo: LEC, 2019, p. 266.

verificadas informações fornecidas pela própria pessoa interessada, seja ela jurídica ou física, bem como realiza-se a coleta por meio de variadas bases de dados de informações para auxílio na tomada de decisões (bases públicas e privadas). Ainda, são analisados aspectos financeiros, reputacionais, regulatórios, jurídicos e as variáveis vertentes a depender do nível de abrangência definido pela empresa [282].

Esse fato culmina na indagação de como proceder a coleta de informações para o levantamento de dados sobre terceiros com quem a organização pretende firmar relações negociais, respeitando a legislação da proteção aos dados pessoais. Nesse sentido, verifica-se que a aplicação do programa de *compliance* (pelas regras de anticorrupção) bem como a Lei Geral de Proteção de Dados, refletem em conjuntos normativos que integram um mosaico protetivo de direitos fundamentais que, se relativizados, podem sujeitá-los a graves lesões. Assim sendo, não se pode desconsiderar ou sobressair um em relação ao outro, mas, como saída, buscar uma aplicação dialógica [283].

Por essa razão, recomenda-se que, a *due diligence* seja realizada, inicialmente, encaminhando um relatório para que o terceiro mesmo realize o preenchimento e, na mesma oportunidade, haja a informação e solicitação de autorização para o colhimento de dados do titular, especificando quais serão utilizados para proceder a pesquisa, apresentando a fundamentação para utilização e, após, comprovando o descarte/apagamento desses dados [284].

Nesse caso, significa dizer que a empresa precisará fazer a atividade de tratamento aplicando todos os itens da Lei Geral de Proteção de Dados, terá que dispor dos princípios, utilizar uma base legal e precisará garantir os mecanismos de segurança da informação que dependendo do contexto necessitarão realizar uma transferência Internacional, condição esta que exigirá a escolha do melhor modelo para transferência [285].

---

[282] CUNHA. Matheus Lourenço Rodrigues da. *Due diligence* de integridade: uma estratégia para a gestão de riscos de terceiro. *In:* CUNHA, Matheus Lourenço Rodrigues; EL KALAY, Mário. **Manual de *compliance*: *compliance mastermind***. São Paulo: LEC, 2019, p. 267.

[283] DONEDA, Danilo. O direito fundamental à proteção de dados pessoais. In: MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti (Coords.). **Direito digital: direito privado e Internet**. 3. ed. Indaiatuba: Foco, 2020, p. 48.

[284] PASSOS, Matheus. LGPD, **Governança de Dados e Gestão de Metadados**. Curso online. Data Science Academy. 2020. Realizado pelo link: https://www.datascienceacademy.com.br/course/lgpd-governanca-de-dados-e-gestao-de-metadados.

[285] FERNANDES, Alessandro; ZANI, João. Compartilhamento de dados de pessoas politicamente expostas pelas instituições financeiras: uma proposta de modelo de gestão e mitigação de

Por isso, importante sempre levar em consideração o limite da pesquisa e destacar as informações estritamente ligadas às necessidades profissionais da empresa, ou seja, é aplicar o princípio da finalidade[286] e o princípio da necessidade[287] (chamado no regulamento europeu de princípio da minimização de dados), haja vista que a coleta se restringirá apenas ao mínimo possível.

Outro fato de grande relevância é tentar manter relações com empresas que possuem certificações da ISO. Caso a empresa não possua certificação e a relação seja a longo prazo, pode-se solicitar e abrir um prazo para que esta outra organização venha a se certificar. Se a instituição já possuir esta declaração lhe proporciona um diferencial competitivo, imagine-se se o relacionamento daquela organização se der somente com empresas que procuram o mesmo caminho e ser certificado [288].

Ao adentrar-se na fase de avaliação e melhoria cumpre destacar que será o momento em que a empresa/organização irá realizar levantamentos a fim de averiguar se o que foi proposto no programa está sendo efetivamente cumprido, bem como se está sendo realizada as vigilâncias às normas. A auditoria vai além da verificação, sendo importante destacar que o programa se trata de um ciclo e que, nesta etapa, a função é detectar se as atividades de tratamento estão sendo corretamente realizadas, bem como sempre buscar melhorias[289].

---

risco. **Brazilian Journal of Business**, v. 4, n. 3, p. 1376-1390, 2022. Disponível em < https://ojs.brazilianjournals.com.br/ojs/index.php/BJB/article/view/52194>. Acesso em 19 dez. 2022.

[286] Por propósitos legítimos, quer se referir a uma finalidade movida pelo bom senso, razão, legalidade, bons costumes e boa fé, distanciando-se, portanto, da iniciativa subalterna, emulativa, emocional, ilícita e de má fé. (PESTANA, Mácio. **Os princípios no tratamento de dados na LGPD (Lei Geral da Proteção de Dados Pessoais)**. Disponível em: https://www.conjur.com.br/dl/artigo-marcio-pestana-lgpd.pdf. Acesso em: 2022, p. 2).

[287] O princípio da necessidade consubstancia-se na limitação da realização do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados. A regra geral, portanto, trazida pela LGPD, é não se realizar o tratamento; a exceção, ao reverso, é a de realiza-la, se e quando o atingimento de determinada finalidade se mostrar relevante para que o tratamento seja realizado. No caso, somente deverão ser tratados os dados pertinentes, ou seja, aqueles que se mostrem imprescindíveis para que o objetivo previamente tracejado seja atingido. Nem poderia ser diferente, pois seria de todo impróprio serem tratados dados que não se mostrassem pertinentes e relevantes para o tratamento em questão. (PESTANA, Mácio. **Os princípios no tratamento de dados na LGPD (Lei Geral da Proteção de Dados Pessoais)**. Disponível em: https://www.conjur.com.br/dl/artigo-marcio-pestana-lgpd.pdf. Acesso em: 12 de agosto de 2022.

[288] AZEVEDO, Mateus Miranda de Azevedo; CARDOSO, Antônio Almeida; DARTE, Jairo Gonçalves; FEREICO, Bianca Ellen; LIMA, Marco Antônio Ferreira. O *compliance* e a gestão de riscos nos processos organizacionais. Disponível em < http://www.fics.edu.br/index.php/rpgm/article/view/507/555>. Acesso em 30 dez. 2022.

[289] LEME, Daniela. Monitoramento e auditoria de *compliance:* melhoria contínua e sustentação do programa de integridade. *In:* CUNHA, Matheus Lourenço Rodrigues; EL KALAY, Mário. **Manual de *compliance: compliance mastermind***. São Paulo: LEC, 2019, p. 301.

Concluindo, nesta etapa, será realizado a auditoria, com a consequente monitoria e verificações frequentes e, ato seguinte, com base nesses resultados, haverá a tomada de decisões para melhoria das próprias atividades de tratamento. Quando a conclusão se sucede para a realização de melhorias, retorna-se ao projeto daquela proteção de dados inicialmente realizado, planejam-se as melhorias, as ideias para transformar, entrando, assim, em um círculo virtuoso, em que a organização estará continuamente buscando por melhorias dentro da sua própria estrutura organizacional [290].

Exemplificando passo a passo, ao se verificar, na fase de avaliação e melhoria (aqui intitulada como auditoria) que uma determinada atividade (coleta de e-mails no site, alteração de fornecedor, alteração dos termos de uso, etc.) de tratamento está ocorrendo de uma maneira, contudo se fosse realizada de outra forma seria mais benéfica, o controlador retorna ao projeto inicial, planeja a melhoria pretendida. Estabelecendo assim o projeto, remete, posteriormente, para a alta direção, que após declarar aceite, passa-se a fase do desenvolvimento e implementação, cujo projeto, voltará para a presente fase de avaliação e melhoria a fim de averiguar se essas mudanças foram efetivas [291].

A presente etapa deve sempre estar em atividade, haja vista a constante evolução do avanço da tecnologia e alterações normativas, razão pela qual o pilar da auditoria é de grande valia para a implementação do *compliance* de dados [292].

Destaca-se, ainda, nessa fase, a necessidade de monitoramento de leis e regulamentações de proteção de dados (basicamente o que no programa de *compliance* já é entendido), averiguando sempre as orientações dos órgãos de proteção de dados ou eventuais normativas que surjam. Para essa exigência, deve existir um planejamento/procedimento realizado com frequência, como título de sugestão, a ser realizado no mínimo uma vez por semana, tendo em vista que pode

---

[290] LEME, Daniela. Monitoramento e auditoria de *compliance:* melhoria contínua e sustentação do programa de integridade. *In:* CUNHA, Matheus Lourenço Rodrigues; EL KALAY, Mário. **Manual de *compliance*: *compliance mastermind***. São Paulo: LEC, 2019, p. 311.

[291] PASSOS, Matheus. LGPD, Governança de Dados e Gestão de Metadados. Curso online. Data Science Academy. 2020. Realizado pelo link: https://www.datascienceacademy.com.br/course/lgpd-governanca-de-dados-e-gestao-de-metadados.

[292] LEME, Daniela. Monitoramento e auditoria de *compliance:* melhoria contínua e sustentação do programa de integridade. *In:* CUNHA, Matheus Lourenço Rodrigues; EL KALAY, Mário. **Manual de *compliance*: *compliance mastermind***. São Paulo: LEC, 2019, p. 299.

surgir alguma coisa distinta em termos legais que obriga a organização a alterar as suas políticas e seus procedimentos internos [293].

No caso, se trata de uma espécie de auto avaliação, que remete a ideia realizada no *benchmarking*. Conforme conceitua a *Internacional Benchmarking Clearinghouse* (IBC)[294], *benchmarking* é um procedimento sistemático, "trata-se de um processo para medir e comparar continuamente os processos empresariais de uma organização em relação aos líderes mundiais". Em suma, se trata de um procedimento que visa ajudar a empresa a agir para melhorar seu desempenho.

Em outras palavras, um *benchmarking* é uma situação em que a organização realiza uma auto-avaliação, por exemplo, uma avaliação no mês de janeiro, depois realiza exatamente a mesma avaliação, com os mesmos critérios, com as mesmas variáveis, com a mesma tecnologia, após três meses, depois novamente após o lapso igual de tempo. Essas avaliações contínuas e sistemáticas, levam ao benchmarking, gerando a possibilidade de comparar resultados de avaliações diferentes em relação aos anteriores, com o fito de identificar as melhorias ou áreas que possam ter deteriorado, ou ainda medir a performance de privacidade da organização em relação a outras entidades semelhantes. Essa comparação com outras empresas possui como objetivo avaliar a sua posição com relação à concorrência no mercado [295].

Ainda, no contexto das avaliações e *benchmarking*, pode-se realizar consoante o tema específico (análise de proteção de dados pessoais, análise de dados do negócio etc.) ou pode ser realizado por áreas (suporte ao cliente, setor de vendas e marketing, departamento de TI, entre outros). No caso da segunda possibilidade, se tratará de uma auto-avaliação gerida pelo membro do comitê de privacidade daquela área. Contudo, se a referida implementação for direcionada para pequena empresa que não possui subdivisão em setores na empresa, nesses

---

[293] PASSOS, Matheus. LGPD, **Governança de Dados e Gestão de Metadados**. Curso online. Data Science Academy. 2020. Realizado pelo link: https://www.datascienceacademy.com.br/course/lgpd-governanca-de-dados-e-gestao-de-metadados.

[294] Andersen menciona que menciona que a instituição internacionalmente conhecida como a que concebeu o Código de Ética do Benchmarking é a American Productivity and Quality Center – (APQC), sendo esta detentora da marca International Benchmarking Clearinghouse (IBC), contendo mais de 500 empresas registradas. ANDERSEN, A. The American productivity and quality center. The knowledge management assessment tool: External benchmarking version.

[295] PASSOS, Matheus. LGPD, **Governança de Dados e Gestão de Metadados**. Curso online. Data Science Academy. 2020. Realizado pelo link: https://www.datascienceacademy.com.br/course/lgpd-governanca-de-dados-e-gestao-de-metadados.

casos, há um posicionamento diferenciado, tendo em vista que poderá eventualmente ser o próprio empregador que vai realizar esse tipo de avaliação [296].

Nesse contexto, também uma vez ciente de uma nova proposta de padrão, leis, regulamentações ou códigos de eventuais emendas, deve-se reportar às partes interessadas apropriadas sobre o impacto do desenvolvimento que a organização terá em seu programa de privacidade ou nas atividades de negócio que possuem riscos à privacidade. A ideia aqui é efetivamente seguir o desenvolvimento dessas alterações legislativas, compreender o que nelas está sendo feito, analisar os eventuais impactos dessas alterações na própria empresa e estar preparado para o resultado [297].

Toda auditoria, gerará resultados que devem informar e guiar as decisões dos responsáveis pela proteção de dados, no sentido de criar ou atualizar políticas, projetar ou adaptar procedimentos, conduzir treinamento ou se empenhar em outras atividades para minimizar o risco na área de proteção de dados, para cumprir com os requerimentos de proteção de dados internos e externos. A auditoria não possui como finalidade apontar os erros dos indivíduos, mas sim em concretizar o ciclo e buscar a melhoria contínua[298].

Partindo-se, de outro viés, como se sabe, por ser amplamente difundido, a inteligência artificial para seu bom funcionamento precisa de dados, em seu maior número possível, em termos de quantidade, podendo abranger os dados pessoais. Inicialmente, antes de adentrar neste tópico, insurge-se que as legislações de proteção de dados não buscam impedir em absoluto o uso de dados pessoais, mas o que almejam é fazer com que empresas, controladores e operadores, usem os dados pessoais dos titulares de maneira clara, transparente e responsável.

Relembrando Stefano Rodotà, cumpre anotar que a “tecnologia, portanto, não pode se referir a fins medidos apenas em suas necessidades. Por razões de princípio ele deve medir-se com os valores constitucionais” [299].

---

[296] PASSOS, Matheus. LGPD, **Governança de Dados e Gestão de Metadados**. Curso online. Data Science Academy. 2020. Realizado pelo link: https://www.datascienceacademy.com.br/course/lgpd-governanca-de-dados-e-gestao-de-metadados.

[297] PASSOS, Matheus. LGPD, **Governança de Dados e Gestão de Metadados**. Curso online. Data Science Academy. 2020. Realizado pelo link: https://www.datascienceacademy.com.br/course/lgpd-governanca-de-dados-e-gestao-de-metadados.

[298] PASSOS, Matheus. LGPD, Governança de Dados e Gestão de Metadados. Curso online. Data Science Academy. 2020. Realizado pelo link: https://www.datascienceacademy.com.br/course/lgpd-governanca-de-dados-e-gestao-de-metadados.

[299] RODOTÀ, Stefano. Laicizzare il rapporto fra innovazione e società. *In:* RASI, Gaetano (Ed.). **Innovazioni tecnologiche e privacy**: sviluppo economico e progresso civile. Roma: Garante

Tecnologia e inovação são empolgantes e fazem crer que suas vantagens se sobrepõem às eventuais desvantagens. Contudo, há um lado nefasto da amplitude comunicacional que, embora não possa ser atribuído aos sistemas e plataformas, mas, sim, à imprudência e à falta de controles e filtros de quem deles se utiliza, causa inegáveis danos [300].

Existem inúmeras pesquisas que demonstram a existência de tecnologias que possibilitam a utilização em empresas quando se trata dos direitos dos titulares dos dados, porém a questão a ser enfrentada é como se procederá para que essas tecnologias possam ser utilizadas de maneira adequada, já que a celeuma dos riscos enfrentados, gira em torno da falta de controles, da imprudência e de filtros de quem deles se utiliza, que como consequência podem gerar danos irreparáveis. O Webinar nomeado *Beyound the exit strategy: ethical uses of data-driven technology in the fight against COVID-19* destaca que não há proteção contra o uso de tecnologias irresponsáveis, devido ao fato de que as leis de proteção de dados não abrangem as liberdades e os direitos do grupo, mas se destinam exclusivamente à proteção de dados pessoais [301].

Sobre esse ponto, entende-se por nefastos danos irreparáveis, a possibilidade de acesso de informações de colaboradores à base dos dados de negócio, dados pessoais dos consumidores, que se divulgados à terceiros poderá gerar danos de grande proporção à empresa, sejam eles financeiros ou reputacionais [302].

Em linhas conclusivas, o presente capítulo apresentou proposta de estruturação, implementação e execução de um programa de *compliance* de dados detalhado, apresentando *insights* para sua implementação, haja vista que *compliance* deve ser adaptado a cada realidade empresarial.

Privacy, 2005, p. 18, tradução livre. No original: "*La tecnologia, dunque, non può far riferimento a fini misurati soltanto sulle sue esigenze. Per ragioni di principio deve misurarsi con i valori costituzionali* […]."

[300] PASSOS, Matheus. LGPD, **Governança de Dados e Gestão de Metadados**. Curso online. Data Science Academy. 2020. Realizado pelo link: https://www.datascienceacademy.com.br/course/lgpd-governanca-de-dados-e-gestao-de-metadados.

[301] NUFFIELD COUNCIL ON BIOETHICS. **Joint webinar - Beyound the exit strategy**: ethical uses of data-driven technology in the fight against COVID-19. 2020. Disponível em: https://www.nuffieldbioethics.org/publications/covid-19/webinar-beyond-the-exit-strategy-ethical-uses-of-data-driven-technology-in-the-fight-against-covid-19. Acesso em: 20 set. 2022.

[302] PASSOS, Matheus. LGPD, **Governança de Dados e Gestão de Metadados**. Curso online. Data Science Academy. 2020. Realizado pelo link: https://www.datascienceacademy.com.br/course/lgpd-governanca-de-dados-e-gestao-de-metadados.

4.2 Mecanismos para implementação e execução do *compliance* de dados com elementos essencialmente práticos: utilização da *blockchain*

É notório que a adoção de ferramentas digitais, como inteligência artificial (em que pese seus lados nefastos), internet das coisas, a utilização da *blockchain* e plataformas, são colocados no centro da transformação digital que se está vivenciando.

Por esse fato, é de relevante saber lidar com os lados negativos, porém a empresa precisa sempre buscar evoluir em suas tecnologias, ser sempre transparente e ética, eis que suas atitudes levarão a instituição a ter um diferencial competitivo com as demais organizações e, consequentemente, garantir uma evolução exponencial.

No estudo realizado, percebeu que a utilização da tecnologia *blockchain* é um grande aliado do empresário, seja ele de pequeno, médio ou grande porte, já que demonstra, com efetividade, a segurança dos dados.

A proposta de rastreabilidade utilizando como meio a tecnologia *blockchain*, Danielle Mendes Thame Denny, Roberto Ferreira Paulo e Douglas de Castro[303] explicam que:

> as transações usando essa tecnologia são verificáveis por meio de um uso de criptografia de chave pública. Cada usuário possui duas “chaves”, uma privada, secreta, como uma senha pessoal e intransferível, e outra pública, que pode ser compartilhada com todos e identifica as transações realizadas por esse determinado usuário. Além disso, nas chaves públicas, qualquer um pode verificar que a transação foi de fato assinada com uma chave privada, sendo, portanto, uma troca autêntica que passa a ser registrada de forma perene, identificada com data e hora e divulgada no banco de dados que arquiva todos os registros de transações feitas, como se fosse um grande um livro-razão, chamado de *blockchain*.

Consoante destaca Eduardo H. Diniz[304], cada transação nova elabora um bloco de transações que reúne as informações das operações anteriores, criando um novo bloco de negócios e um novo carimbo, registrando esta nova transação e

---

[303] DENNY, Danielle Mendes Thame; PAULO, Roberto Ferreira; CASTRO, Douglas de. Blockchain e Agenda 2030. **Revista Brasileira de Políticas Públicas**, Brasília, v. 7, n. 3, 2017. Disponível em: https://www.publicacoes.uniceub.br/RBPP/article/view/4938/0. Acesso em: 18 jul. 2022, p. 132.

[304] DINIZ, Eduardo H. Emerge uma nova tecnologia disruptiva. **GV Executivo**, São Paulo, p. 5, 2017. Disponível em: https://bibliotecadigital.fgv.br/ojs/index.php/gvexecutivo/article/view/68676 . Acesso em: 15 ago. 2022.

as anteriormente realizadas. Importa destacar que a principal característica de um *blockchain* é ser um modelo *append-only*, o que remete à informação de que cada novo dado é registrado no banco como um novo registro e, nenhuma atualização sobressai outra já existente com o novo valor[305]. A própria *blockchain* é conceituada por essa cadeia de blocos em que cada um, em sua singularidade, realiza uma gravação de alguma informação, e esses blocos vão sendo literalmente adicionados, um após ao outro.

Mike Orcutt[306] esclarece que o que torna essa cadeia inviolável é a impressão digital única que cada um desses blocos possui, denominada *hash*[307], cada novo bloco inclui o *hash* exclusivo do bloco anterior, servindo como link no *blockchain.*

A credibilidade da *blockchain* se dá justamente por esse fundamento, haja vista que com a impossibilidade de mudanças de dados lançados na cadeia de informações, não há a probabilidade de alterar algum dado já difundido, havendo a transparência, em caso de ocorrência de riscos, de quem foi o real responsável pela fraude, erro ou qualquer ação que diminua a reputação da empresa.

A tecnologia *blockchain*, como uma tecnologia de registro de forma distribuída, tem tornado bastante relevante e é inegável há o contato entre essa com a proteção de dados. Tanto é que a *EU Blockchain Observatpry and Forum*[308] já estuda a aplicação da *blockchain* na Europa e um dos pontos que esse grupo de

---

[305] CROOK, P. **Append-only Data Store - FAIMS Mobile Platform User Guide - FAIMS Wiki**. Disponível em: https://webcache.googleusercontent.com/search?q=cache:fLcMk4s7JCkJ:https://osf.io/ahf8q/download/%3Fformat%3Dpdf&cd=1&hl=pt-BR&ct=clnk&gl=br. Acesso em: 23 set. 2022.

[306] ORCUTT,Mike. How secure is blockchain really. **MIT Technology Review**, apr. 2018. Disponível em: https://www.technologyreview.com/s/610836/how-secure-is-blockchain-really/. Acesso em: 29 ago. 2022.

[307] A função *hash* é conceituada basicamente como um algoritmo que mapeia os dados de comprimento variável para dados de comprimento fixo e, os valores retornados por uma função *hash* são reputados como valores *hash*, códigos *hash*, somas *hash*, ou simplesmente *hashes* (ROBSHAW, M.J.B. On Recent Results for MD2, MD4 and MD5. **RSA Laboratories Bulletin**, 4, nov. 1996. Disponível em: https://networkdls.com/Articles/bulletn4.pdf . Acesso em: 10 nov. 2022). Em outras palavras, h*ash* é basicamente é uma função algorítmica em que você coloca qualquer coisa, digamos assim, como entrada e a saída sempre vai ser igual, no que diz respeito à sua extensão. Portanto destaco as calculadores de *hashs* que existem na internet, em que o indivíduo coloca ali qualquer tipo de informação (seja seu nome, seja um número, seja um livro), ao inserir como entrada, o resultado sempre é o mesmo. (CALCULADORA Hash. Disponível em: https://pt.infobyip.com/hashcalculator.php. Acesso em: 2022).

[308] “The EU Blockchain Observatory and Forum is a European Parliament Pilot Project with the financial support of the European Union. The content of this website reflects only the authors' views. The European Commission is not responsible for any use that may be made of the information it contains”. (ON BLOCKCHAINS and the General Data Protection Regulation (GDPR). Disponpivel em: https://www.eublockchainforum.eu/research-paper/blockchains-and-general-data-protection-regulation-gdpr. Acesso em: 2022).

estudo levou em consideração foi justamente a relação entre essa tecnologia e a proteção de dados [309].

Vislumbra-se que a *blockchain* é uma importante tecnologia da Internet e possui apelo global, a qual proporciona uma vantagem competitiva para quem a ela se adere. A indústria, como por exemplo, por meio da inovação, o governo ao implementar política calculada de supervisão, pelo fato de ser promotor de padrões comuns a serem seguidos, têm a responsabilidade de investir nesta tecnologia potencialmente revolucionária para gestão de confiança na economia digital.[310]

A *blockchain* foi criada como tecnologia objetivando, em princípio, o não apagamento de dados, não importando de qual espécie seja. A ideia é justamente ser uma tecnologia que permita o registro de informações, sendo que este impede o seu apagamento, evitando, consequentemente, o repúdio de autoria de informações por parte de alguém que participou daquela cadeia [311].

Utilizando como exemplo a utilização da tecnologia em uma empresa que atua em segmento de suprimento, registra-se que a *blockchain* permite que todos os participantes da cadeia, desde o primeiro até o último estágio, possam inserir informações na rede de maneira identificada e auditável, o que acrescenta confiança adicional ao processo da cadeia e a empresa responsável. O processo de um negócio se torna transparente e ainda rastreável ao colocar uma cadeia de suprimentos na *blockchain*, pois cada nó nesse sistema pode representar uma pessoa/empresa que participou do processo desde os insumos até a loja, tornando, ainda, em caso de ocorrência de um empresa vender um suprimento infectado para um local certo, desvendar com maior precisão a ocorrência, de uma forma rápida e descomplicada que pode fazer com que produtos alterados sejam tirados das prateleiras antes mesmo de serem comprados [312].

---

[309] IBÁÑEZ, Luis-Daniel; O'HARA, Kieron; SIMPERL, Elena. On blockchains and the General Data Protection Regulation. Disponível em: https://www.eublockchainforum.eu/sites/default/files/research-paper/blockchains-general-data_4.pdf. Acesso em: 2022.

[310] SHYAMASUNDAR, R. K; PATIL, V. T. Blockchain: the revolution in trust management. **Proc Indian Natn Sci Acad**, v. 84, n. 2, p. 385-407, jun. 2018. DOI: 10.16943/ptinsa/2018/49340. Disponível em: http://insajournal.in/insaojs/index.php/proceedings/article/view/551. Acesso em: 03 set. 2022.

[311] PARIPASSU, Lívia Lima. **A tecnologia blockchain aplicada à rastreabilidade de alimentos**. Dispoível em: https://www.paripassu.com.br/blog/blockchain-rastreabilidade-de-alimentos/. Acesso em: 25 ago. 2022.

[312] MILLER, Ron. **Walmart aposta no blockchain para melhorar a segurança alimentar**. Disponível em: https://techcrunch.com/2018/09/24/walmart-is-betting-on-the-blockchain-to-improve-food-safety/. Acesso em: 06 set. 2022.

Ressalta-se, ainda, que a *blockchain* aplicada à rastreabilidade é magnificente para todos os elos e envolvidos da cadeia produtiva, cujo objetivo é enfatizar para o consumidor, que é quem está mais frequente na busca de informações sobre a origem e processamento dos alimentos que consome [313].

Para melhor ilustração, serão apresentado a seguir exemplos de empresas que implementaram a tecnologia *blockchain* em seu segmento e os fatores positivos que sucederam. Neste primeiro momento, são destacados alguns casos de empresas que se importam com a segurança dos alimentos (que se difere de segurança alimentar), as quais aderiram à utilização do sistema de *blockchain* demonstrando o caminho perscrutado pelo alimento, passando por todas as cadeias, até chegar ao consumidor final. Inobstante, o ditado difundido “prevenir é melhor do que remediar” se enquadra nessa perquirição, já que, na maioria dos casos, despende-se mais tempo e investimentos na tentativa de reparar os problemas já ocorridos do que investir em sua prevenção, visto que, de modo geral, as empresas e, especialmente no exemplo aqui a ser apresentado, no caso dos produtores, é de praxe, buscar a solução para os problemas já instaurados [314].

Uma das empresas que utiliza a tecnologia com o fito de avaliar desde a origem da matéria-prima até a entrega dos produtos finais é a Bunge. Em seu relatório anual de sustentabilidade, a Bunge[315] exprime que:

> Por meio da metodologia NPS (Net Promoter Score) é feita uma classificação entre Promotores (que recomendariam a outros os produtos e serviços da Bunge) ou Detratores (aqueles que não estão satisfeitos e não recomendariam), sendo que os resultados são utilizados para orientar mudanças e aumentar o grau de satisfação dos clientes. Com uma estrutura específica de gestão da Qualidade, nossas operações de Alimentos & Ingredientes também são guiadas por processos que possibilitam o atendimento aos mais exigentes padrões.

---

[313] PARIPASSU, Lívia Lima. **A tecnologia blockchain aplicada à rastreabilidade de alimentos**. Dispoível em: https://www.paripassu.com.br/blog/blockchain-rastreabilidade-de-alimentos/. Acesso em: 25 ago. 2022.

[314] PASSOS, Matheus. LGPD, **Governança de Dados e Gestão de Metadados**. Curso online. Data Science Academy. 2020. Realizado pelo link: https://www.datascienceacademy.com.br/course/lgpd-governanca-de-dados-e-gestao-de-metadados.

[315] BUNGUE BRASIL. **Relatório anual de sustentabilidade**: 2017. Disponível em http://www.bunge.com.br/sustentabilidade/2018/port/downloads/Bunge_RS18.pdf. Acesso em: 16 ago. 2022

São exemplos de empresas que seguem esse protótipo a Brasil Foods (BRF), um dos maiores empreendimentos atuantes no segmento alimentício, em que a sua gestão da qualidade se baseia em dois grandes princípios: *food safety e food transparency* que em conjunto com a rede varejista Carrefour elas se uniram à IBM Brasil [316] para desenvolver o projeto "*Food Tracking*", com o fito de rastrear os produtos por meio da utilização da *blockchain*. O intuito da implementação do mecanismo foi no sentido de informar de maneira objetiva e simples ao consumidor, a procedência dos alimentos, desde a parte produtiva até a logística.[317]

Similarmente, há casos de utilização em um viés distinto do alimentício, que é o da empresa Leroy Merlin, que expressou a intenção em utilizar a *blockchain* para ajudar na integração de toda a cadeia de madeira, propensa a rastrear e certificar os produtos, desde o processamento do corte da madeira, posteriormente quando na preparação na indústria, dos processos artesanais da fabricação, até a entrega efetiva ao cliente [318].

As grandes corporações que trabalham com carne pararam de comprar dos produtores que operavam na região amazônica, pelo fato de que os animais adquiridos que foram ali criados eram vistos como atrelados ao desmatamento, mesmo sem ter certeza de que havia mesmo relação entre as duas atividades. E como solução para esse imbróglio se deu a observação remota e digital do território de criação do animal para certificar que não houve práticas negativas socioambientais, como desmatamento ou trabalho escravo [319].

Além desses benefícios cumpre ainda destacar, como exemplo, que antes da Walmart implementar o processo para a *blockchain*, normalmente demorava cerca de sete dias para rastrear a origem do alimento que deveria ser retirado do mercado por algum erro/problema encontrado no processamento. Com a *blockchain*, foi reduzido para dois vírgula dois segundos. Isso reduz substancialmente a

---

[316] IBM – Indústria, Máquinas e Serviços LTDA.

[317] IBM. **BRF e Carrefour se unem á IBM para reforçar a rastreabilidade dos alimentos**. 9 nov 2017. Disponível em: https://www.ibm.com/blogs/ibm-comunica/rastreabilidade-de-alimentos/#:~:text=BRF%20e%20Carrefour%20se%20unem%20%C3%A0%20IBM%20para%20refor%C3%A7ar%20a%20rastreabilidade%20de%20alimentos,-9%20de%20novembro&text=A%20BRF%2C%20uma%20das%20maiores,meio%20da%20tecnologia%20de%20blockchain. Acesso em: 30 ago. 2022.

[318] ASSOCIAÇÃO BRASILEIRA DE LOGÍSTICA. **Cultura da inovação essencial para a logística**. 16 out. 2018. Disponível em: https://www.abralog.com.br/noticias/cultura-da-inovacao-essencial-para-a-logistica/. Acesso em: 31 ago. 2022.

[319] MARCOLIN, Neldson; VASCONCELOS, Yuri. Agricultura digital. **Revista Fapesp**, n. 268, jul. 2018. Disponível em: https://revistapesquisa.fapesp.br/2018/07/19/folheie-a-edicao-269/. Acesso em: 03 set. 2021.

probabilidade de que alimentos infectados cheguem ao consumidor e que a empresa seja reputada negativamente por esse imbróglio [320].

A princípio, as certificações da segurança do alimento realizadas via *blockchain,* parecem ao consumidor se tratar de uma boa forma de garantir que os produtos que ele está obtendo perscrutaram por processos produtivos que tiveram menor impacto ambiental, podendo ser considerado sustentáveis, apresentando ser empresas que respeitaram a lei. Porém, os benefícios vão além, pois os produtos certificados possuem maior valor agregado, disparidade no mercado e a certificação passa a ser crucial para o acesso a mercados exigentes (como a necessidade de comprovação de um programa de *compliance*), na lona do que ocorre na Comunidade Europeia [321].

Sobre esse aspecto fundamental, a imutabilidade dos dados gravados em um *blockchain,* em princípio, são imutáveis. Porém, como em uso de toda tecnologia, cumpre trazer à baila que essa inserção de informações que não possibilita o apagamento, gera um reflexo negativo no âmbito da proteção de dados na utilização da *blockchain*, pois como realizar a exclusão de dados de um banco que foi criado para o não apagamento. Trata-se de contradições já que são questões que podem ter solução, mas que necessitam de atenção, caso a empresa decida utilizar a tecnologia *blockchain* nos seus projetos que envolvam dados pessoais [322].

A informação em uma *blockchain* não flui linearmente dos usuários para os provedores de serviço (ou vice-versa) mas sim de maneira distribuída, pelo fato de que os dados não estão mais armazenados em uma única empresa, não há apenas um único controlador, podendo, no caso, existir vários destes, como nos exemplos acima demonstrados, que serão aqueles que estão conectados à rede, razão que faz com que a tecnologia seja virtualmente à prova de falhas [323].

---

[320] MILLER, Ron. **Walmart aposta no blockchain para melhorar a segurança alimentar**. 2018. Disponível em: https://techcrunch.com/2018/09/24/walmart-is-betting-on-the-blockchain-to-improve-food-safety/. Acesso em: 06 set. 2022.

[321] COSTA, Juliana. *Blockchain x Compliance*: facilidades e limitações impostas pela LGPD. Disponível em <https://www.serpro.gov.br/lgpd/noticias/2020/compliance-blockchain-lgpd-dados-pessoais-empresas>. Acesso em 28 dez. 2022

[322] PARIPASSU, Lívia Lima. **A tecnologia blockchain aplicada à rastreabilidade de alimentos**. Dispoível em: https://www.paripassu.com.br/blog/blockchain-rastreabilidade-de-alimentos/. Acesso em: 25 ago. 2022.

[323] PASSOS, Matheus. LGPD, **Governança de Dados e Gestão de Metadados**. Curso online. Data Science Academy. 2020. Realizado pelo link: https://www.datascienceacademy.com.br/course/lgpd-governanca-de-dados-e-gestao-de-metadados.

Analisando dessa maneira, sob o ponto de vista do titular dos dados, quando quiser exercer o direito acerca do acesso, retificação, apagamento de dados quando da utilização do direito da oposição e o direito de questionar decisões automatizadas, necessário se faz que a empresa tenha transparência e detalhamento em como o usuário pode buscar o meio para efetivar seus direitos [324].

Nesse sentido, verifica-se a importância da empresa evitar armazenar dados pessoais em uma *blockchain* e fazer uso completo das técnicas de ofuscação, anonimização e pseudonimização. Isso porque, se os dados lançados na plataforma forem anonimizados, se encontram fora do escopo da legislação de proteção de dados, mas se forem apenas pseudonimizados, o controlador tem responsabilidade acerca desses dados [325].

Em que pese saltar ao assunto específico, necessário se faz conceituar pseudonimização e a anonimização. Ambos tratam de métodos de tratamento que utilizam de atributos de identificação, induzindo na possibilidade de identificação de um indivíduo a partir de seus dados pessoais. Assim sendo, somente a partir da análise do caso concreto, a depender do nível de dificuldade, custos, tempo gasto e atividades essenciais para identificar uma pessoa, é que poderá ser observado se o contexto envolve pseudonimização ou da anonimização, bem como se as informações tratadas/em tratamento são ou não de dados pessoais[326].

A pseudonimização se trata de um meio utilizado para complexificar a identificação das pessoas no tratamento de dados pessoais[327]. A sua efetivação se dá pela criação de pseudônimos, ou seja, pela substituição de um atributo de um

---

[324] PASSOS, Matheus. LGPD, **Governança de Dados e Gestão de Metadados**. Curso online. Data Science Academy. 2020. Realizado pelo link: https://www.datascienceacademy.com.br/course/lgpd-governanca-de-dados-e-gestao-de-metadados.

[325] PASSOS, Matheus. LGPD, **Governança de Dados e Gestão de Metadados**. Curso online. Data Science Academy. 2020. Realizado pelo link: https://www.datascienceacademy.com.br/course/lgpd-governanca-de-dados-e-gestao-de-metadados.

[326] RIBEIRO, Florbela da Graça Jorge da Silva. **O tratamento de dados pessoais de clientes para marketing**. 2017. Dissertação (Mestrado em Direito) – Departamento de Direito, Universidade Autónoma de Lisboa, Lisboa, 2017. Disponível em: https://repositorio.ual.pt/bitstream/11144/3048/3/DISSERTA%c3%87%c3%83O_Tratamento_dados_pessoais_clientes_marketing.pdf. Acesso em: 2022, p. 55-56.

[327] RIBEIRO, Florbela da Graça Jorge da Silva. **O tratamento de dados pessoais de clientes para marketing**. 2017. Dissertação (Mestrado em Direito) – Departamento de Direito, Universidade Autónoma de Lisboa, Lisboa, 2017. Disponível em: https://repositorio.ual.pt/bitstream/11144/3048/3/DISSERTA%c3%87%c3%83O_Tratamento_dados_pessoais_clientes_marketing.pdf. Acesso em: 2022, p. 59-60.

registro por outro diferente[328]. Para essa alteração, pode-se utilizar a encriptação, ou seja, a dados encriptados, por meio de uma chave criptográfica, que se trata de uma cifra, conhecida apenas por quem está realizando o tratamento dos dados ou a quem permitido for[329].

Em outras palavras, a pseudonimização refere-se a um tratamento de dados pessoais de forma que deixem de poder ser atribuídos a um titular de dados específico, sem recorrer a informações suplementares, as quais devem ser mantidas separadamente. Trata-se daquela situação em que o colaborador tem que identificador e com base nesse identificador, consegue saber a quem aqueles dados se relacionam. A título de exemplo, ser citado o colaborador nº 1715, que labora em uma empresa em certa área específica, sendo que o administrador da empresa sabe de quem se trata, mas quem apenas tem contato com o número não. A pseudonimização não tira o dado pessoal do escopo da legislação de dados, ou seja, neste caso, o número do colaborador é um dado pessoal, porém pseudonimizado. São dados pessoais e devem seguir toda a legislação de proteção de dados [330].

Cumpre ainda destacar que a pseudonimização é uma medida de segurança. Isso porque, supondo que os dados são pseudonimizados para o operador, mas o colaborador sabe os dados de referência e realmente de quem se trata, caso ocorra uma falha no sistema do operador ocorrerá apenas um incidente de segurança, porém sem violações dos dados pessoais, já que estão pseudonimizados. Diferentemente, se ocorrer na base do controlador, haverá um vazamento de dados pessoais, diante da possibilidade de identificar os dados em questão [331].

Por outro giro, no que se refere à anonimização, esta consiste na remoção ou na ofuscação de toda a informação pessoal de uma base de dados, com a finalidade

---

[328] GRUPO DE TRABALHO DE PROTEÇÃO DE DADOS DO ARTIGO 29º. **Parecer 05/2014 sobre as técnicas de anonimização**. 2014. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_pt.pdf. Acesso em: 2022, p. 22.

[329] RIBEIRO, Florbela da Graça Jorge da Silva. **O tratamento de dados pessoais de clientes para marketing**. 2017. Dissertação (Mestrado em Direito) – Departamento de Direito, Universidade Autónoma de Lisboa, Lisboa, 2017. Disponível em: https://repositorio.ual.pt/bitstream/11144/3048/3/DISSERTA%c3%87%c3%83O_Tratamento_dados_pessoais_clientes_marketing.pdf. Acesso em: 2022, p. 59-60.

[330] PASSOS, Matheus. LGPD, **Governança de Dados e Gestão de Metadados**. Curso online. Data Science Academy. 2020. Realizado pelo link: https://www.datascienceacademy.com.br/course/lgpd-governanca-de-dados-e-gestao-de-metadados.

[331] PASSOS, Matheus. LGPD, **Governança de Dados e Gestão de Metadados**. Curso online. Data Science Academy. 2020. Realizado pelo link: https://www.datascienceacademy.com.br/course/lgpd-governanca-de-dados-e-gestao-de-metadados.

de impedir a identificação dos indivíduos, onde é utilizado técnicas que pretendem tornar impraticável ou quase impossível, a reidentificação do dado, inclusive pelo próprio técnico que realizou a operação originária[332].

Em outros termos a anonimização utiliza de meios técnicos razoáveis e disponíveis no momento do tratamento por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo. Não se tem uma pessoa identificada ou identificável, diferente da pseudonimização. Pode-se citar, como a título de exemplo, pesquisas realizadas na rua sem solicitar a identificação da pessoa, realizado de forma anônima [333].

Retornando à utilização da tecnologia *blockchain*, se não for mesmo possível retirar a utilização dos dados pessoais, a medida que se impõe é recorrer à *off-chain*, que se trata da medida imposta com a finalidade de promover o armazenamento de dados em serviços descentralizados de armazenamento, onde somente suas referências ficarão nos blocos da *blockchain*[334]. Pensando em uma maneira mais simplificada, o armazenamento de dados pode se dar em uma planilha de excel, por exemplo, armazenando, na própria *blockhchain*, apenas o *hash* daquela tabela, haja vista que realizando este procedimento é possível comprovar o horário e autoria da criação daquele conteúdo.

Há ainda na *blockchain* outra solução para a contradição apresentada entre a proteção de dados pessoais ou dados de negócio com a utilização da *blockchain* que é a utilização de *sidechains*. Iago S. Ochoa, Bruno A. Silva e Valderi R. Q. Leithardt[335] conceituam o termo *sidechain*:

> Uma *sidechain* consiste em uma *blockchain* conectada a outra *blockchain* realizando a troca de informações, essa técnica permite que o mercado existente não se fragmente com o desenvolvimento de novas aplicações. A técnica de mineração unida utiliza um mesmo algoritmo para a mineração

---

[332] PINHO, Frederico A. S. O. **Anonimização de bases de dados empresariais de acordo com a nova Regulamentação Europeia de Proteção de Dados**. 2017. Dissertação (Mestrado em Segurança Informática) –Faculdade de Ciências, Universidade do Porto, Porto, 2017. Disponível em: https://core.ac.uk/download/pdf/302939053.pdf. Acesso em: 2022, p. 29.

[333] PASSOS, Matheus. LGPD, **Governança de Dados e Gestão de Metadados**. Curso online. Data Science Academy. 2020. Realizado pelo link: https://www.datascienceacademy.com.br/course/lgpd-governanca-de-dados-e-gestao-de-metadados.

[334] ROCHA, F. H *et al.* Uma avaliação de desempenho de soluções *off-chainbaseadas* em sistemas de armazenamento distribuído. **iSys: Revista Brasileira de Sistemas de Informação**, v. 14, n. 1, p. 4-23, 2021. DOI: 10.5753/isys.2021.808. p. 6. Disponível em: https://sol.sbc.org.br/journals/index.php/isys/article/view/808/1752. Acesso em: 14 set. 2022.

[335] OCHOA, Iago S.; SILVA, Bruno A. da; LEITHARDT, Valderi R. Q. **Proposta de arquitetura para o uso de blockchain em redessmart grid**. Disponível em: https://sol.sbc.org.br/index.php/eradrs/article/view/7083/6972. Acesso em: 17 set. 2022.

> em duas ou mais *blockchains* diferentes, permitindo ao usuário obter diferentes criptomoedas utilizando um mesmo algoritmo de mineração.

Usando uma *sidechain*, o responsável pela proteção de dados consegue contornar o problema central da *blockchain* referente ao seu não apagamento ou não alteração dos dados ali gravados. Conclui-se, portanto que, em caso de utilização da *blockchain*, ao se coletar os dados pessoais e os estratégicos, devem ser guardados em *blockchains* privadas, já que esta é mais fácil de ser administrada pelo fato de existir inúmeros recursos[336].

Por fim, além da importância de sempre buscar a inovação, cumprir com o dever de informação e transparência, e sempre expor, de maneira ampla, os usuários do negócio, que os serviços prestados pela empresa utilizam a tecnologia *blockchain*, a qual possui essa característica de não apagamento, deve, portanto, o usuário/consumidor estar ciente e manifestar seu aceite[337].

Nessa seara, não há dúvidas de que a tecnologia *blockchain* possui potencial para ser aplicada nos mais variados campos da sociedade empresarial, razão pela qual, conclui-se a possibilidade da aplicação da *blockchain* na efetivação do programa de *compliance* de dados, necessitando, no entanto, a observação das soluções indicadas para os empecilhos que aparecerem nos riscos não mitigados.

---

[336] ALVES, Paulo Henrique, LAIGNER, Rodrigo; NASSER, Rafael Nasser; ROBICHEZ, Gustavo; LOPES, Hélio; KALINOWSKI, Marcos. Desmistificando Blockchain: Conceitos e Aplicações. Disponível em <https://www-di.inf.puc-rio.br/~kalinowski/publications/AlvesLNRLK20.pdf>. Acesso em 20 nov. 2022.

[337] PASSOS, Matheus. LGPD, **Governança de Dados e Gestão de Metadados**. Curso online. Data Science Academy. 2020. Realizado pelo link: https://www.datascienceacademy.com.br/course/lgpd-governanca-de-dados-e-gestao-de-metadados.

5 CONSIDERAÇÕES FINAIS

A aplicação do *compliance* de dados nas empresas está tomando mais evidência após a criação da LGPD, que por força de lei agora determina a aplicação à proteção aos dados. A primeira observação que se pode extrair desse contexto é a de que o conceito de privacidade sofreu interferências pelo avanço tecnológico, sendo analisado, atualmente, sob ângulos contextuais. A garantia de um direito fundamental à proteção dos dados pessoais se revelou imprescindível para a conciliação das dimensões que compõem a privacidade. Porém, deixou-se de lado a necessidade de proteção de dados como um todo (dados de segredo do negócio, dados empresariais etc), sendo que todos integram um banco de valor para a empresa.

Se os agentes de tratamento de dados quiserem mitigar os riscos desta atividade – essencial na era da sociedade da informação – devem seguir à risca as melhores práticas do programa de integridade, expostas neste trabalho através dos pilares.

Como se pode denotar do conteúdo demonstrado no presente trabalho, a implementação de um efetivo programa de *compliance*, saindo do âmbito empresarial para a matéria de proteção de dados se trata de uma tarefa complexa. Isso porque demanda a colaboração de inúmeros setores da empresa, desde o topo da alta administração até o funcionário do mais baixo nível, bem como dos colaboradores que com ela se relacionam, a fim de atender os padrões estabelecidos pela LGPD e as demais leis que a empresa deve vigilância, se aplicando assim, conformidade com a norma e um caminho para evolução da aplicação do direito de dados.

Nesse diapasão, o presente estudo pretendeu demonstrar como garantir a proteção de dados com a aplicação do programa de *compliance* sob a ótica dos seus pilares, bem como qual a importância para sua implementação e consequências diante da ausência em uma empresa. Não há dúvidas de que se tornará cada vez mais essencial a aplicação do programa de *compliance* em uma organização, a fim de mitigar riscos e gerar uma boa reputação da imagem com o público externo.

Demonstrou-se, ainda, que uma das soluções para minimizar riscos seria a implementação de um programa de *compliance* de dados e sua efetiva prestação,

bem como utilizar da tecnologia *blockchain* para segurança (tanto do colaborador quanto do empresário), no que tange às informações que estão sendo disponibilizadas e a qual integrante da cadeia está sendo repassado, devendo-se observar as soluções indicadas para os obstáculos que surgirem nas ações de tratamento de dados.

O programa de *compliance* não se resume ao estabelecimento e publicação de códigos de ética ou de conduta, ou ainda, produtos de prateleira já prontos e soluções como utilização de softwares específicos, bem como de sistemas de gestão de informação para integridade que não guardam a mínima relação com a atividade desenvolvida pela empresa, eis que receitas genéricas não combinam com *compliance*.

A necessidade de implementação de um programa de *compliance* de dados reside o maior desafio: além do fato da elevação do grau de digitalização das empresas e da sociedade, propulsar o acesso indevido a dados empresarias, há ainda a conversão de benefícios intangíveis em benefícios monetizados. Necessita-se ter em mente que todo o gasto a ser despendido deve ser vislumbrado como investimento, convertendo os dados em benefícios financeiros tangíveis e mensuráveis.

Sob essa ótica, a incursão dos capítulos, constituiu em apresentar um diagnóstico da alocação dos dados como um ativo de valor, o surgimento do *compliance* apresentando seus pilares e consequentemente a sua aplicação no *compliance* de dados.

Por essa razão, diante da necessidade atual das empresas, o presente estudo apresentou *insights* e colaboração para que os interessados em implementar o programa de *compliance* de dados em sua empresa, busquem adaptá-lo à sua realidade, já que em cada setor há uma vigilância de fiscalização das normas da Lei Geral de Proteção de Dados, harmonizada com outras normas, bem como com outras regulações setoriais, a exemplo das áreas da saúde, educação e bancária, que possuem diversas regulações que tratam sobre o sigilo de informações, governança e segurança cibernética.

Apresentou-se ideias para implementação de um programa efetivo, indicando ideias para noção inicial e aprimoramento da ideia de sua efetivação na empresa, indicando como ideia final a aplicação da *blockchain* para garantia da efetivação do

tratamento de dados, apresentando exemplos práticos de aplicação sucedidas positivamente.

REFERÊNCIAS

ACADEMIA BRASILEIRA DE LETRAS. **Dicionário escolar da língua portuguesa**. [*S.l.*]: Companhia Nacional, 2008.

AGRO + integridade selo agro: integridade empresas do agronegócio. KPMG Consultoria, 2017. Disponível em: https://www.legiscompliance.com.br/images/pdf/br_selo_agro_integridade.pdf. Acesso em: 20 de out de 2022.

ALBUQUERQUE, Ricardo. **Segurança no desenvolvimento de software: como garantir a segurança do sistema para seu cliente usando a ISSO/IEC**. Ricardo Albuquerque, Bruno Ribeiro Imprenta. Rio de Janeiro: Campus, 2002.

ALMEIDA, Gláucio de Oliveira. NASCIMENTO, Pedro Carvalho; SEIXAS, Flávio Luiz**. Pesquisa qualitativa das práticas de segurança nas empresas do setor do TI**. Disponível em < https://app.uff.br/riuff/bitstream/handle/1/26255/04__VERSAO_FINAL_ARTIGO.pdf?sequence=1&isAllowed=y >. Acesso em 18 dez. 2022.

ALVES, Paulo Henrique, LAIGNER, Rodrigo; NASSER, Rafael Nasser; ROBICHEZ, Gustavo; LOPES, Hélio; KALINOWSKI, Marcos. **Desmistificando *Blockchain*: Conceitos e Aplicações**. Disponível em <https://www-di.inf.puc-rio.br/~kalinowski/publications/AlvesLNRLK20.pdf>. Acesso em 20 nov. 2022.

ANDRADE, Adriana; ROSSETTI, José Paschoal. **Governança corporativa**: fundamentos, desenvolvimento e tendências. 4. ed. São Paulo: Atlas, 2009.

AMARAL, Fernando. **Introdução à ciência de dados**. Rio de Janeiro: Alta Books, 2016. p.17

ARMELIN, Ruth Maria Guerreiro da Fonseca; TEIXEIRA, Tarcisio. **Lei geral de proteção de dados pessoais comentada artigo por artigo**. Salvador: Juspodim, 2019.

ASSOCIAÇÃO BRASILEIRA DE LOGÍSTICA. **Cultura da inovação essencial para a logística**. 16 out. 2018. Disponível em: https://www.abralog.com.br/noticias/cultura-da-inovacao-essencial-para-a-logistica/. Acesso em: 31 ago. 2022.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT/CEE-063**: Projeto de revisão ABNT NBR ISO 31000: 2018. Disponível em: https://drive.google.com/file/d/1fdNcTyTZ3Qs7LpGYf_g4-a054fVtiC6b/view. Acesso em: 2022.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - **ABNT. NBR ISO/IEC 27002** – Tecnologia da Informação - Código de Prática para a Gestão de Segurança da Informação – 2013. Disponível em

<https://profjefer.files.wordpress.com/2013/10/nbr_iso_27002-para-impressc3a3o.pdf>. Acesso 18 dez. 2022.

AZEVEDO, Mateus Miranda de Azevedo; CARDOSO, Antônio Almeida; DARTE, Jairo Gonçalves; FEREICO, Bianca Ellen; LIMA, Marco Antônio Ferreira. **O *compliance* e a gestão de riscos nos processos organizacionais**. Disponível em < http://www.fics.edu.br/index.php/rpgm/article/view/507/555>. Acesso em 30 dez. 2022.

BASRI, Carole. **Corporate compliance**. [*S.l.*]: Carolina Academic Press, 2017. Edição do Kindle.
BATISTA, Lucas Oliveira, SILVA, Gabriel Adriano de; ARAÚJO, Vanessa Souza; ARAÚJO, Viníciu Jonathan Silva; REZENDE, Thiago Silva, GUIMARÃES, Augusto Junio; SOUZA, Paulo Vitor de Campos. **Utilização de Redes Neurais Nebulosas para criação de um Sistema Especialista em Invasões Cibernéticas**. Icofcs, 2018, p. 1. Disponível em <http://icofcs.org/2018/ICoFCS-2018-002.pdf>. Acesso em 18 dez. 2022.

BATISTI, Beatriz Miranda; KEMPFER, Marlene. Parâmetros de compliance por meio da metodologia de análise de risco para a mitigação da responsabilidade objetiva diante da lei anticorrupção (12.846/2013) em face de negócios públicos. **Revista Brasileira de Direito Empresarial**, v. 2, n. 1, p. 184-200, 2016. Disponível em: https://www.indexlw.org/index.php/direitoempresarial/article/view/1019. Acesso em: 05 fev. 2022.

BHARATH, B. S. **The nudge theory**: a stellar strategy for a better outcome. Disponível em: https://uxdesign.cc/nudge-theory-a-stellar-strategy-for-a-better-outcome-8504d5f7af74. Acesso em: 05 out. 2022.

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

BIONI, Bruno Ricardo. Xeque-mate: o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil. **Privacidade e Vigilância**, São Paulo, 2015.

BISSO, Rodrigo *et al.* Vazamentos de dados: histórico, impacto socioeconômico e as novas leis de proteção de dados. **Revista Eletrônica Argentina-Brasil de Tecnologias da Informação e da Comunicação**, v. 3, n. 1, mar. 2020.

BLOCK, Marcella. **Compliance e governança corporativa**: atualizado de acordo com a Lei Anticorrupção Brasileira (Lei 12.846) e Decreto-Lei 8.421/2015. Rio de Janeiro: Freitas Bastos, 2017.

BLOK, Marcella. **Compliance e governança corporativa**. 3. ed. Rio de Janeiro: Freitas Bastos, 2020.

BLUM, Renato Opice. MALDONADO, Viviane. **Comentários ao GDPR: Regulamento Geral de Proteção de Dados da União Européia**. São Paulo. Thomson Reuters Brasil. 2018.

BLUM, Renato; VAINZOF, Rony; MORAES, Henrique. **Data Protection Officer*:*** teoria e prática de acordo com a LGPD e GDPR. São Paulo: Thomson Reuters Brasil, 2020.

BOBBIO, Norberto. **Teoria do ordenamento jurídico**. São Paulo/Brasília: Pollis/Universidade de Brasília, 1990.

BRASIL. **Lei nº 12.846, de 1º de agosto de 2013**. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2013/Lei/L12846.htm. Acesso em: 21 jan. 2021.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). 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: 18 set. 2022.

BRASIL. **Lei nº 14.063 de 23 de setembro de 2020.** Dispõe sobre o uso de assinaturas eletrônicas em interações com entes públicos, em atos de pessoas jurídicas e em questões de saúde e sobre as licenças de softwares desenvolvidos por entes públicos; e altera a Lei nº 9.096, de 19 de setembro de 1995, a Lei nº 5.991, de 17 de dezembro de 1973, e a Medida Provisória nº 2.200-2, de 24 de agosto de 2001. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/L14063.htm. Acesso em: 25 jul. 2022.

BRASIL. **Medida Provisória nº 2.200-2 de 24 de agosto de 2001.** Disponível em: http://www.planalto.gov.br/ccivil_03/MPV/Antigas_2001/2200-2.htm. Acesso em: 25 set. 2022.

BRASIL. Ministério da Economia. **MP simplifica assinatura eletrônica de documentos públicos e substitui o papel**. Disponível em: https://www.gov.br/economia/pt-br/assuntos/noticias/2020/junho/mp-simplifica-assinatura-eletronica-de-documentos-publicos-e-substitui-o-papel. Acesso em: 18 set 2022.

BRASIL. Senado Federal. **Emenda à Constituição nº 115 de 10 de fevereiro de 2022**. Disponível em: https://legis.senado.leg.br/norma/35485358. Acesso em: 10 nov. 2022.

BRASIL. Senado Federal. **Projeto de Lei nº 4 de 2022**. Disponível em: https://www.congressonacional.leg.br/materias/materias-bicamerais/-/ver/pl-4-2022. Acesso em: 20 de novembro de 2022.

BRASIL. Senado Federal. **Proposta de Emenda à Constituição nº 17, de 2019.** 2019. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/135594Acesso em: 20 dez. 2020.

BRASIL. Supremo Tribunal Federal. **STF suspende compartilhamento de dados de usuários de telefônicas com IBGE**. 2020. Disponível em:

http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=442902. Acesso em: 03 jan. 2020.

BROTTO, Natália; CAMARGO, Pedro Henrique Dalgallo. Autoridade Nacional de Proteção de Dados, aspectos pendentes de regulação e cultura de proteção de dados. In: **Lei Geral de Proteção de Dados: estudos sobre um novo cenário de Governança Corporativa**/ coordenado por Rodrigo Pironti. Belo Horizonte: Fórum, 2020.

CALCULADORA Hash. Disponível em: https://pt.infobyip.com/hashcalculator.php. Acesso em: 2022.

CAMARÃO, Tatiana. A gestão por competência na nova lei de licitações e contratos. **Consultor Jurído**, 2021. Disponível em: https://repositorio.ufsc.br/bitstream/handle/123456789/229560/ConJur%20-%20Tatiana%20Camar%C3%A3o_%20Gest%C3%A3o%20por%20compet%C3%ACncia%20na%20nova%20Lei%20de%20Licita%C3%A7%C3%B5es.pdf?sequence=1. Acesso em: 26 out. 2022.

CAPANEMA, Walter Aranha**.** A responsabilidade civil na Lei Geral de Proteção de Dados. **Cadernos Jurídicos**, São Paulo, v. 21, n. 53, p. 163-170, 2020.

CARVALHO, André Castro *et al.* (Coord.). **Manual de compliance.** 2. ed. Rio de Janeiro: Forense, 2020.

CARNEIRO, Claúdio. **Compliance em tempos de pós-covid-19**. 08 jun. 2020. Disponível em: https://www.editorajc.com.br/18814-2/. Acesso em: 22 ago. 2022.

CARVALHO, Itamar; ABREU, Bruno Cesar Almeida. Programas de compliance: o programa de integridade. *In:* CARVALHO, André Castro *et al.* **Manual de compliance**. 2. ed. Rio de Janeiro: Forense, 2020.

CASTELLS, Manuel. **The Internet galaxy**: reflections on the Internet, business, adn society. Oxford: Oxford University Press, 2001.

CASTELLS, Manuel. **Sociedade em rede**. Tradução de Roneide Venâncio Majer. 6. ed. São Paulo: Paz e Terra, 1999.

CASTRO, Leonardo Bellini de. **Lei anticorrupção:** impactos sistêmicos e transversais. Leme, SP: JH Mizuno, 2019.

CASTRO, Rita de C. C. de; SOUSA, Verônica L. Pimental de. **Segurança em cloud computing**: governança e gerenciamento de riscos de segurança. Disponível em: https://www.academia.edu/7520311/Seguran%C3%A7a_em_Cloud_Computing_Governan%C3%A7a_e_Gerenciamento_de_Riscos_de_Seguran%C3%A7a. Acesso em: 25 out. 2022.

CASTRO, Rodrigo Pironti Aguirre de. **Compliance**: repensando o óbvio, para não cair no senso comum. Disponível em: https://www.cafecompliance.com.br/?area=autores&a=10. Acesso em: 28 out. 2022.

CASTRO, Rodrigo Pironti Aguirre de. **A due diligence**: instrumento de compliance à serviço da governança e da segurança jurídica nas relações empresariais em PPP´s. Disponível em: https://www.cafecompliance.com.br/?area=artigo&c=819280cbb9e37d853ccaa9f3632cf1b8. Acesso em: 19 ago. 2022.

CITADIN, Daniara Regina. **Redesign de interface de landing page**: um estudo de caso do site sienge. 2017. Trabalho de Conclusão de Curso (Graduação em Design) – Universidade do Sul de Santa Catarina, Florianópolis, 2017. Disponível em: https://repositorio.animaeducacao.com.br/bitstream/ANIMA/7791/1/TCC%203%20-%20Daniara%20Citadin.pdf. Acesso em: 5 mar. 2022.

COELHO, Cláudio Carneiro Bezerra Pinto. **Compliance na Administração Pública**: uma necessidade para o Brasil. 2016. Disponível em:<https://www.researchgate.net/publication/323352076_O_COMPLIANCE_NA_ADMINISTRACAO_PUBLICA_E_A_LEI_1330316>. Acesso em: 06 fev. 2022.

COIMBRA, Marcelo de Aguiar; MANZI, Vanessa Alessi (Org.). **Manual de compliance**: preservando a boa governança e a integridade das organizações. São Paulo: Atlas, 2010.

COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION. **[Site]**. Disponnível em: https://www.coso.org/SitePages/Home.aspx. Acesso em: 2022.

COMPLIANCE: repensando o óbvio para não cair no senso comum. 12 mar. 2019. Disponível em: https://cafe.jmlgrupo.com.br/compliance-repensando-o-obvio-para-nao-cair-no-senso-comum/. Acesso em: 2022.

CONTROLADORIA GERAL DA UNIÃO. **Programa de integridade:** diretrizes para empresas privadas. set. 2015. Disponível em: https://www.legiscompliance.com.br/images/pdf/programa_integridade_diretrizes_para_empresas_privadas_cgu.pdf. Acesso em: 21 jan. 2022.

COSTA, Juliana. ***Blockchain x Compliance*: facilidades e limitações impostas pela LGPD**. Disponível em <https://www.serpro.gov.br/lgpd/noticias/2020/compliance-blockchain-lgpd-dados-pessoais-empresas>. Acesso em 28 dez. 2022

COSTA, Marta Maia Campos. **O sistema de vigilância na União Europeia**: a conservação de dados pessoais gerados no contexto das comunicações eletrónicas e a violação da carta dos direitos fundamentais da União Europeia. 2016. Dissertação (Mestrado em Direito Público, Internacional e Europeu) – Escola de Direito, Universidade Portuguesa, Porto, 2016. Disponível em: https://repositorio.ucp.pt/bitstream/10400.14/21981/1/Disserta%C3%A7%C3%A3o%20Marta%20Campos%20Costa%20-%202016%20.pdf. Acesso em: 25 nov. 2022.

COSTA JÚNIOR, Paulo José da. **O direito de estar só**: tutela penal da intimidade. São Paulo: Revista dos Tribunais, 1995.

COUNCIL OF EUROPE. **Convention for the protection of individuals with regard to automatic processing of personal data**. Strasbourg, 1981. Disponível em: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108. Acesso em: 20 abr. 2021.

COUTINHO, Doris Terezinha Pinto Cordeiro de Miranda. **Finanças públicas**: travessia entre o passado e o futuro. São Paulo: Blucher, 2018. Disponível em: https://www.editoraforum.com.br/wp-content/uploads/2015/08/lei-anticorrupcao-compliance.pdf. Acesso em: 16 fev. 2022.

CROOK, P. **Append-only Data Store - FAIMS Mobile Platform User Guide - FAIMS Wiki**. Disponível em: https://webcache.googleusercontent.com/search?q=cache:fLcMk4s7JCkJ:https://osf.io/ahf8q/download/%3Fformat%3Dpdf&cd=1&hl=pt-BR&ct=clnk&gl=br. Acesso em: 23 set. 2022.

CUEVA, Pablo. *Informática y Protección de Datos Personales*. ***Revista Chilena de Derecho Informático***. 2011. Disponível em <https://www.researchgate.net/publication/314947621_Informatica_y_Proteccion_de_Datos_Personales>. Acesso em: 20 dez. 2022.

CUEVA, Ricardo Villas Bôas. Funções e Finalidades dos Programas de *Compliance.* In: LAMACHIA, Claudio; PETRARCA, Carolina (org.). ***Compliance*: essência e efetividade**. Brasília: OAB, Conselho Federal, 2018. p. 215-224.

CUNHA, Matheus Lourenço Rodrigues da. Due diligence de integridade: uma estratégia para a gestão de riscos de terceiro. *In:* CUNHA, Matheus Lourenço Rodrigues; EL KALAY, Mário. **Manual de compliance***:* compliance mastermind. São Paulo: LEC, 2019.

CUNHA, Matheus Lourenço Rodrigues da; CASTRO, Rodrigo Pironti Aguirre de. *Compliance risk assessment*: análise de caso de participação em licitações e contratos públicos. In: CUNHA, Matheus Lourenço Rodrigues; EL KALAY, Mário. **Manual de *compliance: compliance mastermind***. São Paulo: LEC, 2019.

CUNHA, Matheus Lourenço Rodrigues; EL KALAY, Mário. **Manual de compliance***:* compliance mastermind. São Paulo: LEC, 2019.

DA PRIVACIDADE ao lucro: como obter retornos positivos sobre investimentos em privacidade. Estudo comparativo de privacidade de dados. Cisco 2020. Disponível em: https://www.cisco.com/c/dam/global/pt_br/solutions/pdfs/2020-data-privacy-report-ptbr.pdf. Acesso em: 15 nov. 2022.

DASSAN, Pedro Augusto Amaral. **A posição de garante no contexto empresarial**: contributo ao estudo da responsabilidade do Compliance Officer. 2017. Dissertação (Mestrado) – Faculdade de Direito, Universidade de Coimbra. Disponível em: https://estudogeral.sib.uc.pt/bitstream/10316/84041/1/Texto_final.pdf. Acesso em: 2022.

DAVENPORT, Thomas H.; PRUSAK, Laurence. **Working knowledge**: how organizations manage what they know. [*S.l.*]: Harvard Business Press, 1998.

DENNY, Danielle Mendes Thame; PAULO, Roberto Ferreira; CASTRO, Douglas de. Blockchain e Agenda 2030. **Revista Brasileira de Políticas Públicas**, Brasília, v. 7, n. 3, 2017. Disponível em: https://www.publicacoes.uniceub.br/RBPP/article/view/4938/0. Acesso em: 18 jul. 2022.

DIAS, Jean Miguel; RODRIGUES, Rita de Cássia M. C.; PIRES, Daniel Facciolo. A segurança de dados na computação em nuvens nas pequenas e médias empresas. **Revista Eletrônica de Sistemas de Informação e Gestão Tecnológica**, v. 2, n. 1, 2012. Disponível em: http://periodicos.unifacef.com.br/index.php/resiget/article/view/287/278. Acesso em: 18 jul. 2022.

DIJK, Jan Van. **The network society**. 2. ed. Londres: Sage, 2006. E-book.

DINIZ, Eduardo H. Emerge uma nova tecnologia disruptiva. **GV Executivo**, São Paulo, p. 5, 2017. Disponível em: https://bibliotecadigital.fgv.br/ojs/index.php/gvexecutivo/article/view/68676 . Acesso em: 15 ago. 2022.

DIRECTIVA 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046. Acesso em: 2022.

DONDA, Daniel. **Guia prático da implementação da LGPD**: tudo o que sua empresa precisa saber para estar em conformidade. São Paulo: Labrador, 2020. e-Book.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico**, Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais [livro eletrônico]: **elementos da formação da lei geral de proteção de dados.** 1. Ed. São Paulo: Thomson Reuters Brasil, 2019. P. RB-2.1.

DONEDA. Danilo. Princípios da proteção de dados pessoais. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira Pereira de (Coord.). ***Direito e Internet III*. Marco Civil da Internet. Lei nº 12.965/2014**. Tomo I. São Paulo: Quartier Latin, 2015.

DONEDA, Danilo. O direito fundamental à proteção de dados pessoais. In: MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti (Coords.). **Direito digital: direito privado e Internet**. 3. ed. Indaiatuba: Foco, 2020.

ELETROBRAS. **Política Anticorrupção das Empresas**. Rio de Janeiro, 2018. Disponível em < https://www.eletronuclear.gov.br/Canais-de-

Negocios/Documents/Etica%20e%20Compliance/Pol%C3%ADtica%20Anticorrup%C3%A7%C3%A3o%20das%20Empresas%20Eletrobras.pdf>. Acesso 19 dez 2022.

EM QUE "ESTÁGIO" estamos? Confira o mapa da proteção de dados pessoais no mundo. Disponível em: https://www.serpro.gov.br/lgpd/menu/a-lgpd/mapa-da-protecao-de-dados-pessoais. Acesso em: 2022.

FALEIROS JÚNIOR, José Luiz de Moura. **Administração pública digital**: proposições para o aperfeiçoamento do regime jurídico administrativo na sociedade da informação. São Paulo: Foco, 2020.

FARIA, Felipe. Comunicação e treinamento de *compliance:* difundindo a cultura da integridade. *In*: CUNHA, Matheus Lourenço Rodrigues; EL KALAY, Mário. **Manual de compliance***: compliance mastermind*. São Paulo: LEC, 2019.

FERNANDES, Alessandro; ZANI, João. Compartilhamento de dados de pessoas politicamente expostas pelas instituições financeiras: uma proposta de modelo de gestão e mitigação de risco. ***Brazilian Journal of Business***, v. 4, n. 3, p. 1376-1390, 2022. Disponível em < https://ojs.brazilianjournals.com.br/ojs/index.php/BJB/article/view/52194>. Acesso em 19 dez. 2022.

FERNANDES, Milton. **Proteção civil da intimidade**. São Paulo: Saraiva, 1977.

FERNANDES, Nelson Ricardo. **Análise de risco parametrizada**: manual prático do planejamento e gestão de riscos. [*S.l.*]: Editora Clube do Autor, 2015.

FERREIRA. Luciene Braz; RAMOS, Anatália Saraiva Martins. Tecnologia da informação: commodity ou ferramenta estratégica? **Revista de Gestão da Tecnologia e Sistemas de Informação *Journal of Information Systems and Technology Management***. Vol. 2, nº 1- 2005, pp. 69-79, P.76. Disponível em <>. Acesso em 19 dez. 2022.

FIGUEIRAS, Fernando; SILVA, Bárbara. Desenhando políticas e governança de dados para cidades inteligentes: ensaio teórico com o uso da IAD Framework para analisar políticas orientadas por dados. **Revista de Administração Pública**, 2022. Disponível em: https://www.scielo.br/j/rap/a/fNVvVDxzNdD6bvczcjWdvLB/?lang=pt&format=pdf. Acesso em: 29 nov. 2022.

FLENDER, Samuel. **Data is not the new oil.** 10 fev. 2019. Disponível em https://towardsdatascience.com/data-is-not-the-new-oil-bdb31f61bc2d. Acesso em: 05 maio 2022.

FONTES, Edson; **Políticas e normas para a segurança da informação**. Editora Brasport, 1ª Edição, 2021.

FRAMEWORK. *In*: CAMBRIDGE dictionary. Disponível em: https://dictionary.cambridge.org/us/. Acesso em: 2022.

FREEDOM OF INFORMATION ACT. **[Site]**. Disponível em: https://www.foia.gov/. Acesso em: 04 out. 2022.

FUNDAÇÃO ESCOLA NACIONAL DE ADMINISTRAÇÃO PÚBLICA. **Governança de dados- módulo 1:** contexto da governança de dados na administração pública. Brasília, 2019. Disponível em https://repositorio.enap.gov.br/bitstream/1/5008/1/M%C3%B3dulo%201%20-%20Contexto%20da%20Governan%C3%A7a%20de%20Dados%20na%20Administra%C3%A7%C3%A3o%20P%C3%BAblica.pdf. Acesso em: 25 nov. 2022.

FUNDAÇÃO ESCOLA NACIONAL DE ADMINISTRAÇÃO PÚBLICA. **Governança de dados- módulo 2**: princípios, importância e desafios do gerenciamento de dados. Brasília, 2019. Disponível em: https://repositorio.enap.gov.br/bitstream/1/7092/2/M%C3%B3dulo%202%20-%20Princ%C3%ADpios%2C%20Import%C3%A2ncia%20e%20Desafios%20do%20Gerenciamento%20de%20Dados%2003-2021.pdf. Acesso em: 25 nov. 2022.

FUNDAÇÃO ESCOLA NACIONAL DE ADMINISTRAÇÃO PÚBLICA. **Governança de dados**- módulo 4: gerenciamento de metadados e da qualidade de dados. Brasília, 2019. Disponível em: https://repositorio.enap.gov.br/bitstream/1/5008/4/M%C3%B3dulo%204%20-%20Gerenciamento%20de%20Metadados%20e%20da%20qualidade%20de%20Dados.pdf. Acesso em: 25 nov. 2022.

GABARDO, Emerson; CASTELLA, Gabriel Morettini e. A nova lei anticorrupção e a importância do compliance para as empresas que se relacionam com a Administração Pública. **Revista de Direiro Administrativo e Constitucional**, Belo Horizonte, v. 15, n. 60, p. 129-147, abr./jun. 2015. Disponível em: https://www.editoraforum.com.br/wp-content/uploads/2015/08/lei-anticorrupcao-compliance.pdf. Acesso em: 18 fev. 2020.

GARCEL, Adriane; MORO, Sergio Fernando; SOUZA NETTO, José Laurindo de; HIPPERTT, Karen Paiva. Lei geral de proteção de dados: diretrizes e implicações para uma sociedade pandêmica. **Coletâneas de artigos jurídicos: em homenagem ao Professor José Laurindo de Souza Netto**. Viviane C. de S. K., Adriane G., José L. de S. N. 1.ed., Curitiba: Clássica Editora, 2020. ISBN 978-65-87965-03-1. Disponível em <https://www.tjpr.jus.br/documents/18319/47149551/42.+Artigo+Lei+Geral+de+Prote%C3%A7%C3%A3o+de+Dados.pdf/f4e4281e-2318-9799-39a8-f394a68230b3>. Acesso em 20 dez. 2022.

GAZONI, Carolina. Pilar 1- Tone from the top- comprometimento e suporte da Alta Administração *In:* CUNHA, Matheus Lourenço Rodrigues; EL KALAY, Mário. **Manual de compliance***:* compliance mastermind. São Paulo: LEC, 2019. v. 1.

GEDIEL, José Antônio Peres; CORRÊA, Adriana Espíndola, p.146. Proteção jurídica de dados pessoais: a intimidade sitiada entre o Estado e o mercado. **Revista da Faculdade de Direito UFPR**, v. 47, 2008.

GONSALES, Alessandra; SIBILLE, Daniel. Investigações Internas e medidas disciplinares. In: CUNHA, Matheus Lourenço Rodrigues; EL KALAY, Mário. **Manual de *compliance: compliance mastermind***. São Paulo: LEC, 2019. p. 220.

GONZÁLEZ, Elena Gil. **Big data**: privacidade y protección de dados. Madrid: Agencia Española de Protección de Datos, 2016. Disponível em: https://www.researchgate.net/publication/324831404_Big_data_privacidad_y_proteccion_de_datos. Acesso em: 27 set. 2021.

GRUBBA, Leilane. Os limites do idealismo na Declaração Universal dos Direitos Humanos: uma análise epistemológica. *Legis Augustus*, n. 1-3, p. 2, 2012.

GRUPO DE TRABALHO DE PROTEÇÃO DE DADOS DO ARTIGO 29º. **Parecer 05/2014 sobre as técnicas de anonimização**. 2014. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_pt.pdf. Acesso em: 2022.

HARARI, Yuvah Noah. **In the battle against coronavirus**: humanity lacks leadership. 2020. Disponível em: https://time.com/5803225/yuval-noah-hararicoronavirus-humanity-leadership/. Acesso em: 17 set. 2021.

HARARI, Yuval Noah. **21 lições para o século 21**. Tradução de Paulo Geiger. São Paulo: Companhia das Letras, 2018.

IBÁÑEZ, Luis-Daniel; O'HARA, Kieron; SIMPERL, Elena. On blockchains and the General Data Protection Regulation. Disponível em: https://www.eublockchainforum.eu/sites/default/files/research-paper/blockchains-general-data_4.pdf. Acesso em: 2022.

IBM. **BRF e Carrefour se unem á IBM para reforçar a rastreabilidade dos alimentos**. 9 nov 2017. Disponível em: https://www.ibm.com/blogs/ibm-comunica/rastreabilidade-de-alimentos/#:~:text=BRF%20e%20Carrefour%20se%20unem%20%C3%A0%20IBM%20para%20refor%C3%A7ar%20a%20rastreabilidade%20de%20alimento,-9%20de%20novembro&text=A%20BRF%2C%20uma%20das%20maiores,meio%20da%20tecnologia%20de%20blockchain. Acesso em: 30 ago. 2022.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. **Governança corporativa.** Disponível em: https://www.ibgc.org.br/conhecimento/governanca-corporativa. Acesso em: 2022.

INSTITUTO ETHOS. **Empresa pro-ética.** 2016. Disponível em: https://www.ethos.org.br/conteudo/projetos/integridade/empresa_pro_etica/#.WSnRImjyvIU. Acesso em: 27 maio 2022.

INSTITUTO ETHOS. **Sobre o Instituto**. Disponível em: https://www3.ethos.org.br/conteudo/sobre-o-instituto/#.WSm7B2jyvIV . Acesso em: 27 maio 2022.

JÚNIOR, Filipa Marques; MEDEIROS, João. A elaboração de programas de compliance. *In*: SOUSA MENDES, Paulo de; PALMA, Maria Fernanda; SILVA DIAS, Augusto. **Estudos sobre law** enforcement, compliance e direito penal. Lisboa: Almedina, 2018.

KESSLER, Felix. **Empurrõezinhos e nossos processos cerebrais**. Disponível em: http://www.economiacomportamental.org/nacionais/empurroezinhos-e-nossos-processos-cerebrais/. Acesso em: 25 ago. 2022.

KLINCZAK. Marjori. Uso da inteligência na detecção de ameaças cibernéticas. ***The eleventh International Conference on forensic computer Science na cyber law***. São Paulo, Brasil. Novembro, 2019. Disponível em <http://icofcs.org/2019/ICoFCS2019-002.pdf>. Acesso em 19 dez. 2022.

KLEE, Antonia Espíndola Longoni; PEREIRA NETO, Alexandre Nogueira. A Lei Geral de Proteção de Dados (LGPD): uma visão panorâmica. *In:* THEMOTEO, Reinaldo J. (Coord.). **Proteção de dados pessoais**: privacidade versus avanço tecnológico. Rio de Janeiro: Fundação Konrad Adenauer, 2019.

LANZINI, Luiz Eduardo. **Governança corporativa e compliance**: global trading Curitiba: Contentus, 2020.

LE COADIC, Yves-François. **A ciência da informação**. Brasília: Briquet de Lemos, 1996.

LIMA, Cíntia Rosa Pereira de; PEROLI, Kelvin. **Direito digital**: compliance, regulação e governança. São Paulo: Quartier Latin, 2019.

LOOSLI, Marilia Zulini da Costa; IKO, Massamitsu Alberto. Código de ética e de conduta, políticas e procedimentos: os documentos normativos relacionados ao programa de integridade da empresa. In: CUNHA, Matheus Lourenço Rodrigues; EL KALAY, Mário. **Manual de compliance: compliance mastermind**. São Paulo: LEC, 2019, p. 162.

LOOSLI, Marilia Zulini da Costa; IKO, Massamitsu Alberto; CUNHA, Matheus Lourenço Rodrigues da. Canais de comunicação com o programa de *compliance*. *In*: CUNHA, Matheus Lourenço Rodrigues; EL KALAY, Mário. **Manual de compliance***:* compliance mastermind. São Paulo: LEC, 2019, p. 233.

LÓSSIO, Claudio Joel Brito. Proteção de Dados e Compliance Digital. São Paulo: Almedina, 2021, p. 20.

LUCENA, Gustavo. Pilar 2- Risk Assessment: metodologia de análise de riscos para conformidade legal *In*: CUNHA, Matheus Lourenço Rodrigues; EL KALAY, Mário. **Manual de compliance***:* compliance mastermind. São Paulo: LEC, 2019.

MACHADO, Diego; DONEDA, Danilo. Proteção de dados pessoais e criptografia: tecnologias criptográficas entre anonimização e pseudonimização de dados. **Revista dos Tribunais**, São Paulo, v. 998, p. 99-128, 2018. Caderno Especial.

MACHADO, Felipe Nery Rodrigues; ABREU, Maurício Pereira de. **Projeto de banco de dados: uma visão prática**. 17ª edição. Saraiva.

MACHADO, Luciana Cristina Pinto; MARCONI, Licia Pimentel. **Estudos preliminares sobre os princípios aplicados ao tratamento de dados pessoais na Lei nº 13.709/2018- LGPD**.Enepe- Encontro Nacional de Ensino, Pesquisa e Extensão- Inteligência emocional e autodesenvolvimento. Unoeste, 2020. Disponível em < https://www.unoeste.br/Areas/Eventos/Content/documentos/EventosAnais/564/anais/Sociais%20Aplicadas/Direito.pdf#page=190>. Acesso em 30 dez. 2022.

MAIA, Maurilo Casas. Telemedicina, prontuário eletrônico e atualização do código de defesa do consumidor- a tutela da hipervulnerabilidade eletrônica do paciente e de sua personalidade virtual. **Revista de Direito do Consumidor**, v. 89, p. 303-319, set./out. 2013.

MANZI, Vanessa Alessi. **Compliance no Brasil**: consolidação e perspectivas. São Paulo: Saint Paul, 2008.

MARCOLIN, Neldson; VASCONCELOS, Yuri. Agricultura digital. **Revista Fapesp**, n. 268, jul. 2018. Disponível em: https://revistapesquisa.fapesp.br/2018/07/19/folheie-a-edicao-269/. Acesso em: 03 set. 2021.

MARTÍNEZ, Ricard. ***El derecho fundamental a la protección de datos: perspectivas***. Revista Internet, Derecho y Política, nº 5, 2007. Disponível em <https://www.researchgate.net/publication/28178556_El_derecho_fundamental_a_la_proteccion_de_datos_perspectivas>. Acesso em: 20 dez. 2022.

MARKOWSKI, A.; MANNAN, S. Fuzzy risk matrix. **Journal of Hazardous Materials**, v. 159, n. 1, p. 152-157, 2008.

MARQUES, Claudia Lima. Superação das antinomias pelo diálogo das fontes. **Revista de Direito do Consumidor**, São Paulo, v. 51, p. 34-67, jul./set. 2004.

MARZZOCO, Diogo Silva. A figura do encarregado pela proteção de dados pessoais. In: **Lei Geral de Proteção de Dados: estudos sobre um novo cenário de Governança Corporativa/** coordenado por Rodrigo Pironti. Belo Horizonte: Fórum, 2020.

MAXIMIANO, Antonio Cesar Amaru; NOHARA, Irene Patrícia. **Gestão Pública**: abordagem integrada da administração e do direito administrativo. São Paulo: Atlas, 2017.

MENDES, Francisco Schertel; CARVALHO, Vinicius Marques de. **Compliance:** concorrência e combate à corrupção. São Paulo: Trevisan, 2017. 15 Mb; ePUB.

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

MENDES, Pedro Alexandre Brandão. **Análise de Risco no GDPR**. 2018. Disponível em < https://repositorio.ul.pt/bitstream/10451/35494/1/ulfc124806_tm_Pedro_Mendes.pdf> . Acesso em 20 dez. 2022.

MILLER, Ron. **Walmart aposta no blockchain para melhorar a segurança alimentar**. Disponível em: https://techcrunch.com/2018/09/24/walmart-is-betting-on-the-blockchain-to-improve-food-safety/. Acesso em: 06 set. 2022.

MOONEY, S. J.; PEJAVER V. Big data in public health: terminology, machine learning, and privacy. **Annu Rev. Public Health**, n. 39, p. 95-112, 2018.

MORGADO, L. F. O cenário internacional de proteção de dados pessoais. Necessitamos de um Código Brasileiro?. **Âmbito Jurídico**, Rio Grande, v. 12, n. 65, jun. 2009. Disponível em: http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=6336. Acesso em: 19 nov. 2021.

MOSHELL, Ryan. And there was one: the outlook for a self-regulatory United States amidst a global trend toward comprehensive data protection. **Texas Tech Law Review**, v. 37, p. 366-367, 2005.

NERY, P. F. **Errar é humano**: economia comportamental aplicada à aposentadoria. Brasília: Núcleo de Estudos e Pesquisas/CONLEG/ Senado, 2016. Texto para Discussão n. 188. Disponível em: www.senado.leg.br/estudos. Acesso em: 15 fev. 2022.

NEVES, Edmo Colnaghi. **Compliance empresarial**: o tom da liderança: estrutura e benefícios do programa. São Paulo: Trevisan, 2018. 500 Mb; ePUB.

NUFFIELD COUNCIL ON BIOETHICS. **Joint webinar - Beyound the exit strategy**: ethical uses of data-driven technology in the fight against COVID-19. 2020. Disponível em: https://www.nuffieldbioethics.org/publications/covid-19/webinar-beyond-the-exit-strategy-ethical-uses-of-data-driven-technology-in-the-fight-against-covid-19. Acesso em: 20 set. 2022.

OCHOA, Iago S.; SILVA, Bruno A. da; LEITHARDT, Valderi R. Q. Proposta de arquitetura para o uso de blockchain em redessmart grid. Disponível em: https://sol.sbc.org.br/index.php/eradrs/article/view/7083/6972. Acesso em: 17 set. 2022.

OLIVEIRA, Paulo Henrique de Souza; MACHADO, Alencar. **Uso de boas práticas de segurança no tratamento das principais vulnerabilidades de software no desenvolvimento para web**. Disponível em < https://publicacoeseventos.unijui.edu.br/index.php/salaoconhecimento/article/view/16694/15376>. Acesso em 25 dez. 2022.

ON BLOCKCHAINS and the General Data Protection Regulation (GDPR). Disponpivel em: https://www.eublockchainforum.eu/research-paper/blockchains-and-general-data-protection-regulation-gdpr. Acesso em: 2022.

ORCUTT,Mike. How secure is blockchain really. **MIT Technology Review**, apr. 2018. Disponível em: https://www.technologyreview.com/s/610836/how-secure-is-blockchain-really/. Acesso em: 29 ago. 2022.

OS 10 PILARES de um programa de compliance. Disponível em: https://lec.com.br/os-10-pilares-de-um-programa-de-compliance/. Acesso em: 2022.

PASSOS, Matheus. LGPD, **Governança de Dados e Gestão de Metadados**. Curso online. Data Science Academy. 2020. Realizado pelo link: https://www.datascienceacademy.com.br/course/lgpd-governanca-de-dados-e-gestao-de-metadados

PEREZ FILHO, Augusto Martinez. **O compliance na administração pública**: combate à corrupção e efetivação do direito à boa administração. São Paulo: JH Mizuno, 2019.

PÉREZ LUÑO, Antonio Enrique. ***Manual de informática y derecho***. Barcelona: Ariel, 1996.

PESTANA, Mácio. **Os princípios no tratamento de dados na LGPD (Lei Geral da Proteção de Dados Pessoais)**. Disponível em: https://www.conjur.com.br/dl/artigo-marcio-pestana-lgpd.pdf. Acesso em: 2022.

PINHO, Frederico A. S. O. **Anonimização de bases de dados empresariais de acordo com a nova Regulamentação Europeia de Proteção de Dados**. 2017. Dissertação (Mestrado em Segurança Informática) –Faculdade de Ciências, Universidade do Porto, Porto, 2017. Disponível em: https://core.ac.uk/download/pdf/302939053.pdf. Acesso em: 2022.

PORTO, Ederson Garin. **Compliance e governança corporativa, uma abordagem pratica e objetiva**. Kindle Edition 107, 297. Lawboratory Press: 2021.

RÊGO, Bergson Lopes. **Gestão e governança de dados**: promovendo os dados como ativo de valor nas empresas. Rio de Janeiro: Brasport, 2013.

REIS, Luciano Elias; LIPPMANN, Rafael Knorr. A administração pública na lei geral de proteção de dados. In: **Lei Geral de Proteção de Dados: estudos sobre um novo cenário de Governança Corporativa**/ coordenado por Rodrigo Pironti. Belo Horizonte: Fórum, 2020.

REZENDE, Denis Alcides; DE ABREU, Aline França. Planejamento estratégico da tecnologia de informação alinhado ao planejamento estratégico de empresas. **Revista de Administração Mackenzie**, v. 3, n. 2, 2008.

RIBEIRO, Florbela da Graça Jorge da Silva. **O tratamento de dados pessoais de clientes para marketing**. 2017. Dissertação (Mestrado em Direito) – Departamento de Direito, Universidade Autónoma de Lisboa, Lisboa, 2017. Disponível em: https://repositorio.ual.pt/bitstream/11144/3048/3/DISSERTA%c3%87%c3%83O_Tratamento_dados_pessoais_clientes_marketing.pdf. Acesso em: 2022.

RIBEIRO, Marcia Carla Pereira; KLEIN, Vinicius. **O que é análise econômica do direito: uma introdução** / Marcia Carla Pereira Ribeiro; Vinicius Klein (Coord.). 2. ed. Belo Horizonte: Fórum, 2016.

ROBSHAW, M.J.B. On Recent Results for MD2, MD4 and MD5. **RSA Laboratories Bulletin**, 4, nov. 1996. Disponível em: https://networkdls.com/Articles/bulletn4.pdf . Acesso em: 10 nov. 2022.

ROCHA, F. H *et al.* Uma avaliação de desempenho de soluções *off-chainbaseadas* em sistemas de armazenamento distribuído. **iSys: Revista Brasileira de Sistemas de Informação**, v. 14, n. 1, p. 4-23, 2021. DOI: 10.5753/isys.2021.808. p. 6. Disponível em: https://sol.sbc.org.br/journals/index.php/isys/article/view/808/1752. Acesso em: 14 set. 2022.

RODRIGUES, Luís Augusto Antunes. A importância do compliance como instrumento de combate aos crimes cibernéticos. **Revista Pan-americana de direito**. Disponível em < https://periodicosfapad.emnuvens.com.br/rtpj/article/view/60/56>. Acesso em 17 dez. 2022.

RODOTÀ, Stefano. Laicizzare il rapporto fra innovazione e società. *In:* RASI, Gaetano (Ed.). **Innovazioni tecnologiche e privacy**: sviluppo economico e progresso civile. Roma: Garante Privacy, 2005.

SANTOS JÚNIOR, Belisário dos, SANTOS, Juliana Vieira dos. Autodeterminação informativa: surge um novo direito fundamental. **Aspectos relevantes da lei geral de proteção de dados/** (organizadores) Gustavo Marinho (et al.). 1 ed. São Paulo: Editora Contracorrente, 2021.

SARAIVA, Renata Machado. **Criminal compliance como instrumento de tutela ambiental**: a propósito da responsabilidade penal das empresas. São Paulo: LiberArs, 2018.

SARLET, Ingo Wolfgang. **Proteção de dados pessoais como direito fundamental na Constituição Federal de 19881: contributo para a construção de uma dogmática constitucionalmente adequada**. Direitos e Fundamentos & Justiça, Belo Horizonte, ano 14, n. 42.

SCATOLIN, Carolina Lanzini. Uso da Tecnologia blockchain no compliance de dados: uma análise da possibilidade e entraves a serem resolvidos. **Revista de Economia, Empresas e Empreendedores na CPLP**. Volume 08, número 01| 10.29073/e3.v8i1.611. Disponível em <https://revistas.ponteditora.org/index.php/e3/article/view/611/418>. Acesso em 19 dez. 2022.

SCHEIN, Edgar H. **Cultura organizacional e liderança**. SãoPaulo: Atlas, 2009.

SCHWAB, Klaus; VANHAM, Peter. ***Stakeholder Capitalism: A Global Economy that Works for Progress, People and Planet***. John Wiley & Sons: New Jersey, 2021.

SHYAMASUNDAR, R. K; PATIL, V. T. Blockchain: the revolution in trust management. **Proc Indian Natn Sci Acad**, v. 84, n. 2, p. 385-407, jun. 2018. DOI: 10.16943/ptinsa/2018/49340. Disponível em: http://insajournal.in/insaojs/index.php/proceedings/article/view/551. Acesso em: 03 set. 2022.

SILVA, Daniel Calvacante; COVAC, José Roberto. **Compliance como boa prática de gestão de ensino superior privado.** São Paulo: Saraiva, 2015.

SILVA, Daniela Juliano. Govtech à Brasileira: o plano nacional de internet das coisas e o cadastro base do cidadão. *In:* LEAL, Fernando; MENDOÇA, José Vicente Santos de (Org.). **Transformações do direito administrativo:** liberdades econômicas e regulação. Rio de Janeiro: FGV Direito Rio, 2019.

SILVA, Michael César; SANTOS, Wellington Fonseca. **O direito do consumidor nas relações de consumo virtuais**. Revista da Faculdade Mineira de Direito, v.15, n. 30, jul./dez. 2012 – ISSN 1808-9429. Disponível em < http://periodicos.pucminas.br/index.php/Direito/article/view/P.2318-7999.2012v15n30p119>. Acesso em 17 dez. 2022.

SILVA, Miguel Moura e. **Inovação transferência de tecnologia e concorrência**: estudo comparado do direito da concorrência dos Estados Unidos e da União Européia. Coimbra: Almedina, 2003.

SOBRE a Cisco. Disponível em: https://www.cisco.com/c/pt_br/about.html. Acesso: 2022.

STAPLES, William G. **Encyclopedia of privacy**. Westport: Greenwood, 2007.

STATISTICS: fines imposed over time. Disponível em: https://www.enforcementtracker.com/?insights. Acesso em: 2022.

TERADA, Routo. **Segurança de dados:** criptografia em redes de computador. São Paulo: Blucher, 2008.

THALER, Richard H; SUSTEIN, Cass R. **Nudge**: improving decisions about health, wealth and happiness. London: Penguin, 2009.

THE GLOBAL COMPACT. **Guia de avaliação de risco de corrupção**. 2013. Disponível em: https://www.gov.br/dnit/pt-br/assuntos/integridade/coordenacao-geral-de-integridade/legislacao-basica/guia-de-avaliacao-de-risco-de-corrupcao.pdf. Acesso em: 25 jun. 2022.

THE GLOBAL COMPACT**. Guia de avaliação de risco de corrupção**. Disponível em: https://www.gov.br/dnit/pt-br/assuntos/integridade/coordenacao-geral-de-integridade/legislacao-basica/guia-de-avaliacao-de-risco-de-corrupcao.pdf. Acesso em: 25 jun. 2022.

THE INSTITUTE OS INTERNAL AUDITORS. **Definition of internal auditing***,* 2019. Disponível em https://www.theiia.org/en/standards/what-are-the-standards/definition-of-internal-audit/. Acesso em 28 out. 2022.

WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. **Harvard Law Review**, v. 4, n. 5, p. 193-220, dez. 1890. Disponível em: http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html. Acesso em 25 out. 2022.

VIANA, César Pereira. **O Princípio Constitucional Da Transparência e a sua relação com o modelo de excelência em Gestão Pública**. IV Congresso Consad. Disponível em <https://www.administracao.go.gov.br/noticias/311-gest%C3%A3o/modernizacao/banco-de-boas-praticas-de-gestao/gestao-e-planejamento/15522-o-principio-constitucional-da-transparencia-e-a-sua-relacao-com-o-modelo-de-excelencia-em-gestao-publica.html>. Acesso em: 15 dez. 2022. p.7

VIDOR, Daniel Martins. **Os princípios da Lei Geral de Proteção de Dados e aplicabilidade**. Blog Mercury. 27 de março de 2019. Disponível em <https://pt.linkedin.com/pulse/os-princ%C3%ADpios-da-lei-geral-de-prote%C3%A7%C3%A3o-dados-e-daniel-martins-vidor>. Acesso em 12 de dez. de 2022.