Capítulo 39

O Programa de *Compliance* como Medida de Prevenção e Mitigação de Riscos Emanados por Inteligências Artificiais no Tratamento de Dados Pessoais

The Compliance Program as a Measure for the Prevention and Mitigation of Risks Arising from Artificial Intelligence in the Processing of Personal Data

Victor Antonio Cecyn

Mestre em Ciência Jurídica pela Universidade do Vale do Itajaí. Professor na Associação Catarinense de Ensino. Advogado.

Resumo: O presente estudo busca analisar a implementação de programas de compliance como uma medida disposta à prevenção e mitigação dos riscos associados ao uso de inteligências artificiais no tratamento de dados. Ao longo da história, destacam-se quatro revoluções industriais que moldaram a sociedade e a economia, sendo que a Quarta Revolução Industrial, marcada por avanços tecnológicos, desafia as estruturas governamentais e institucionais, incluindo o sistema judiciário. A globalização acelerada, impulsionada pelas tecnologias de informação e comunicação, trouxe novas ferramentas para a automação e digitalização de processos industriais, como a inteligência artificial. No entanto, essa rápida evolução tecnológica também trouxe desafios significativos, como a falta de uma regulamentação eficaz. Além disso, o presente estudo destaca a importância das leis de proteção de dados na União Europeia, que surgiram após a Segunda Guerra Mundial, e sua influência na legislação brasileira, incluindo a Lei Geral de Proteção de Dados, bem como discute os conceitos de inteligência artificial e os dilemas éticos e jurídicos que surgem com seu uso. Diante desses desafios, sugere-se que os programas de compliance digital desempenham um papel fundamental na prevenção e mitigação de riscos associados à inteligência artificial, de forma que os programas não apenas ajudam as organizações a cumprir as regulamentações, mas também promovem a transparência e a responsabilidade na era da economia de dados.

Palavras-chave: judiciário; globalização; inteligência artificial.

Abstract: This study aims to analyze the implementation of compliance programs as a measure for the prevention and mitigation of risks associated with the use of artificial intelligence in data processing. Throughout history, four industrial revolutions have significantly shaped society and the economy. The Fourth Industrial Revolution, characterized by technological advancements, challenges governmental and institutional structures, including the judicial system. Accelerated globalization, driven by information and communication technologies, has introduced new tools for the automation and digitalization of industrial processes, such as artificial intelligence. However, this rapid technological evolution has also brought significant challenges, notably the lack of effective regulation. Furthermore, this study highlights the importance of data protection laws in the European Union, which emerged after World War II, and their influence on Brazilian legislation, including the General Data Protection Law (LGPD). It also discusses the concepts of artificial intelligence and the ethical and legal dilemmas arising from its use. In light of these challenges, it is suggested that digital compliance programs play

DOI: 10.47573/aya.5379.3.1.39

a fundamental role in preventing and mitigating risks associated with artificial intelligence. These programs not only assist organizations in complying with regulations but also promote transparency and accountability in the data-driven economy.

Keywords: judiciary; globalization; artificial intelligence.

INTRODUÇÃO

Sociedade da Informação, Economia de Dados e Revoluções Industriais

Com o passar do tempo, ocorreram grandes quebras na organização estrutural da sociedade, de modo que em cada período, um elemento restou determinante para que ocorra a mudança de paradigma e, devido a essa estruturação, tais os elementos tornaram-se marcos históricos (Silva, 2009).

O primeiro marco na linha histórica estudada resume-se na chamada Primeira Revolução Industrial, a qual teve início na região britânica por volta do século XVIII, por meio da desestruturação massiva da economia agrícola e da dependência de métodos mecânicos de produção neste novo período, destacando-se a construção de ferrovias e máquinas movidas a vapor. O período seguinte foi marcado por alterações ainda mais disruptivas, incluindo o desenvolvimento do motor de combustão interna, o uso do petróleo como fonte de combustível, a chegada da eletricidade e da linha de produção contínua e a produção em massa em escala industrial, marcando assim a segunda revolução industrial no final do século XIX. A chegada da microeletrônica e da tecnologia da informação nos processos industriais marcou o início de um longo período da sociedade globalizada, marcada pela produção otimizada e automatizada no final da década de 1960, fato que abrange a terceira revolução industrial (Drath; Horch, 2014).

Na visão de Klaus Schwab, entender as novas revoluções tecnológicas que surgiram e se inverteram na Quarta Revolução Industrial tornou-se o maior desafio da sociedade, pois as mudanças trazidas por esses movimentos vão além do entendimento atual de como as atividades de trabalho são realizadas e como os indivíduos se comunicam com o padrão de referência, mas também abrange a reestruturação governamental e institucional, fator que acaba afetando o Judiciário e o estabelece como referencial teórico deste estudo (Schwab, 2016).

Por outro lado, deve-se ressaltar que a globalização acelerada é essencial para a transformação do cenário de mercado, proporcionada pelas tecnologias de informação e comunicação e, assim, o surgimento de novas ferramentas aplicáveis aos processos industriais, como automação e digitalização de processos e serviços, análise de big data, software embarcado, sistemas de comunicação e rede (cloud systems), sistemas embarcados integrados, robôs autônomos, inteligência artificial, etc., gerando a concepção do termo “Indústria 4.0”, proposta principalmente por parte do governo alemão na Feira de Hannover (2011), revertida no marco da Quarta Revolução Industrial (Salkin *et al.,* 2018).

Embora a tecnologia já tenha aparecido na terceira revolução industrial, a maior diferença em relação ao salto da quarta revolução é que a tecnologia tem a capacidade de rápida evolução e óbvio crescimento acelerado. Eric Brynjolfsson e Andrew McAffe a chamaram de "a segunda era da máquina", as novas máquinas elevam a sociedade humana a outro patamar, de forma que atualmente estão afetando o pensamento humano e sua compreensão, não se limitando a alterar os padrões de produção econômica e a arrombar novos domínios de interação pessoal (Brynjolfsson; Mcaffe, 2014).

Os modelos atuais de organização social giram em torno da "informação" como elemento essencial do desenvolvimento econômico, questão que substitui as antigas rendas que constituíram a revolução industrial, seja ela agrícola, industrial ou pós-industrial (Bioni, 2019).

Na visão de Schwab, as relações sociais estando se afogando no fluxo informacional de dados processados em velocidade sem precedentes, considerando que neste momento não existem barreiras físicas por distância ou escalabilidade, esse fato também muda a compreensão pessoal dos conceitos de tempo e espaço (Bioni, 2019).

Novos e inimagináveis parâmetros computacionais para processamento de dados levaram, assim, a uma evolução rápida nos métodos de coleta, armazenamento e processamento de dados, um ciclo histórico marcado por termos como big data, Internet das Coisas e inteligência artificial, resumidos pelo uso da tecnologia na automatização de operações de processamento de dados, os quais suportam a nomenclatura de "economia de dados" (Vainzof, 2020).

Nesse sentido, Schwab destaca os três pilares que compõem a insurgência da nova revolução industrial, a saber, a velocidade com que as revoluções permeiam, a amplitude e profundidade da mudança acelerada pela integração de tecnologias em um ambiente globalizado e amplamente interconectado, horizontes nunca experimentados , envolvendo sociedades, economias e agora os próprios humanos e, finalmente, tendo efeitos sistêmicos no nível de Estados soberanos e suas estruturas internas, como instituições governamentais e a sociedade como um todo (Schwab, 2016).

Ascensão Histórica Acerca da Positivação da Tutela Jurisdicional Sob o Viés da Proteção e Privacidade de Dados no Contexto Europeu e Brasileiro

Com base no viés de globalização apresentado, é preciso descortinar os procedimentos históricos cometidos para que o ordenamento jurídico brasileiro finalmente reconheça o direito à proteção de dados e à privacidade, fatores fundamentais que justificam a importância das medidas técnicas e administrativas no âmbito da governança digital.

Primeiramente, é importante ressaltar que este ensaio visa evidenciar o contexto histórico em que surgiram os diplomas legais ao direito à privacidade, tema

que se contrapõe ao arcabouço teórico apresentado por Brandeis e Louis em seu ensaio "*The Right to Privacy*", publicado na Harvard Magazine em 1930 (Doneda, 2020).

Nesse sentido, referencia-se a convenção Europeia dos direitos do homem (CEDH), publicada pelo Conselho da Europa em 1950, que ascende após a Segunda Guerra Mundial por iniciativa dos Estados soberanos localizados no continente europeu, a fim de permitir o Estado de direito, a democracia, os direitos humanos e o desenvolvimento humano e social (Europa, 2014).

Sob este aspecto, o Conselho da Europa assumiu no respectivo ordenamento jurídico interno de cada membro as obrigações dispostas na CEDH, incluindo-se a jurisdição ativa do Tribunal Europeu dos Direitos do Homem (TEDH), criado em 1959 na cidade de Estrasburgo, França (Europa, 2014).

O cenário pós-guerra instaura a disposição expressa acerca do direito à privacidade sob a inteligência do artigo 8º da Convenção Europeia dos Direitos do Homem:

> Artigo 8° Direito ao respeito pela vida privada e familiar 1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência. 2. Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar económico do país, a defesa da ordem e a prevenção das infracções penais, a protecção da saúde ou da moral, ou a protecção dos direitos e das liberdades de terceiros (CEDH, 1950).

Compulsando o estudo destacado, evidencia-se o marco legal da privacidade, sendo que sua tutela restou assegurada de forma extensiva aos dados dos indivíduos por meio da jurisprudência advinda do TEDH, a partir de julgamentos que versaram sobre a ilegalidade da prática de interceptação comunicacional, diversas formas de vigilância e espionagem, incorrendo no marco internacional da proteção e privacidade de informações (Europa, 2014).

Nesse sentido, o TEDH fundamentou suas ações nas obrigações advindas do artigo 8º da CEDH, não se restringindo à vedação da prática de atos ilegais e atentatórios à privacidade por parte dos Estados, porém insurgiu sob o aspecto de uma obrigação positiva, no intento de garantir ativamente a tutela da vida privada e familiar (Europa, 2014).

Não obstante o surgimento do direito à proteção e privacidade de informações, as inovações tecnológicas advindas durante a década de 1960 impuseram aos Estados a criação de diplomas legais mais complexos sobre a temática, motivo pelo qual na década seguinte os Estados-membro da União Europeia criaram diversos regulamentos, instruções complementares e soluções sobre a proteção de dados advindas do Comitê de Ministros do Conselho da Europa (Doneda, 2020).

Sob este viés, os autores Manual da Legislação Europeia sobre a Proteção de Dados abordam que a Convenção nº 108, diploma legal que versa sobre a proteção das pessoas e o tratamento automatizado de dados de caráter pessoal, reverteu-se à época de seu estabelecimento no "único instrumento internacional juridicamente vinculativo no campo da proteção de dados" (Europa, 2014). Sua relevância respalda-se, sobretudo, na amplitude da regulação das atividades de tratamento realizadas pelos setores públicos e privados e na instituição de princípios para o legítimo tratamento de dados pessoais (Europa, 2014).

Neste sentido, ao obter uma análise das normas referentes à proteção de dados que surgiram na década de 80 neste contexto europeu, verificou-se a necessidade de consolidar um regramento harmônico entre os Estados-membro da União Europeia, haja vista que diversos entes iniciaram a promulgação de diplomas esparsos, ocasião que gerou a vinda da Diretiva 95/46/CE, estabelecida através do Parlamento Europeu e do Conselho Europeu em 24/10/1985 (Europa, 1985).

Em sequência, proclamou-se a Carta dos Direitos Fundamentais da União Europeia (2000), com o objetivo de estabelecer e consolidar costumes e obrigações internacionais acordadas entre os Estados participantes da União Europeia, lidando com direitos de natureza cível, política, econômica e social de todos os indivíduos e, inclusive, abarcando o respeito pela vida privada e familiar a partir da previsão contida no artigo 7º, assim como do direito à proteção de dados no artigo seguinte (8º), momento em que destaca a proteção de dados como direito fundamental protegido pela União Europeia (Europa, 2000).

Por fim, o contexto histórico-legislativo da proteção e privacidade de dados na União Europeia é marcado pelo advento de um projeto normativo trazido à tona em razão do desenvolvimento desenfreado de novas tecnologias, causando a necessidade de reformular o contexto normativo, motivo pelo qual, o cenário global relacionado à proteção e privacidade de dados restou marcado pelo advento do General Data Protection Regulation (EU 2016/679), diploma de relevância internacional, o qual gerou grande influência no próprio ordenamento jurídico brasileiro no que tange à Lei Geral de Proteção de Dados.

No que diz respeito ao caso do Brasil, apesar de que a Lei Geral de Proteção de Dados vem à tona apenas no ano de 2018, houve igualmente uma escadaria legislativa permeada para que se alcançasse este patamar. A Constituição Cidadã (1988) foi o primeiro documento jurídico relevante ao ordenamento jurídico brasileiro, o qual evidenciou de forma explícita o direito à vida privada e à intimidade (art. 5º, inciso X, CF/1988), assim como elegeu a privacidade ao patamar de direito fundamental, causando um grande marco legislativo para a tutela da privacidade na legislação brasileira.

Apesar do mencionado marco legislativo, importante ressaltar que a privacidade já era tutelada de forma implícita, isto porque o direito à privacidade remete diversos outros direitos fundamentais (igualdade, da liberdade de escolha, não discriminação, entre outros), logo estava implícito dentro de legislações e matérias esparsas no ordenamento jurídico brasileiro, exemplo disso é a proteção à propriedade dos indivíduos, tema que não deixam de abarcar a privacidade dos mesmos em um segundo plano, distante do texto explícito (Doneda, 2020).

Tal como ocorreu na União Europeia, a sociedade tecnológica formada no início do século 21 foi fundamental para os desdobramentos jurídicos que tornaram possíveis a elaboração de legislações específicas sobre a privacidade e proteção de dados no ordenamento jurídico brasileiro, uma vez que a legislação admite a necessidade de eleger a regulação de espaços e situações específicas diante de um desenvolvimento legislativo ao mesmo tempo em que tenta alcançar os avanços da tecnologia, exemplo disso é o advento do Marco Civil da Internet (Lei 12.965/2014), Lei da qual estampa e exclama em seu preâmbulo que adveio para "estabelecer princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

Nessa toada, o Senado Federal protocolou a Proposta de Emenda à Constituição n. 17/2019, devidamente aprovada e revertida na Emenda Constitucional 115/2022, a qual finalmente tutelou o direito à proteção de dados pessoais a título de direito fundamental.

O Surgimento da "Inteligência Artificial", Riscos em um Desenvolvimento Desenfreado

Em que pese o surgimento de novas tecnologias dotadas de inteligência artificial ser um tema aclamado pela atual doutrina internacional e nacional, haja vista o desenvolvimento desenfreado de tecnologias e a iminente ameaça à perseverança de preceitos fundamentais frente a uma economia de dados (Bioni, 2020), Turing já questionara a capacidade de auto desenvolvimento das máquinas em 1950 (Turing, 1950).

Apesar das prévias discussões suscitadas por Turing, o advento do termo "Inteligência Artificial" ocorre tão somente em 1956, a partir do "Projeto de Pesquisa de verão de Dartmouth em Inteligência Artificial (Mccarthy; Minsky; Rochester; Shannon, 1955).

Para uma compreensão aprofundada, torna-se imperioso trazer a conceituação de Inteligência Artificial, tema que por si só abarca uma alongada polêmica somada às constantes mudanças implicadas nas tecnologias, motivo pelo qual surge esta complexidade e árdua missão de abarcar diversas aplicações a um único termo.

Em 1985, Charniak e Mcdermott definiram que a "Inteligência Artificial é o estudo das faculdades mentais através do uso de modelos computacionais" (Charniak; Mcdermott, p. 6, 1985), expondo ainda que o cerne fundamental da Inteligência Artificial é que a cognição cerebral humana pode ser realizada, sob determinada proporção, como um tipo de computação (Charniak, Mcdermott, 1985).

A abordagem é reafirmada por Haugeland neste movimento para que a Inteligência Artificial oportunize que a racionalização das máquinas, que estas pensem como mentes em sua fiel expressividade (Haugeland, 1985).

Em um tom progressista e abrangente, Kurzweil abordou que a Inteligência Artificial concretiza-se pelo campo de estudo cujo objetivo resume-se na tentativa de reproduzir a inteligência humana em uma máquina, envolvida ainda pelo aprendizado automático e autorreprodução (Kurzweil, 1990).

Sob o viés legislativo, a União Europeia propôs um Regulamento de Inteligência Artificial 2021/0105 (COD) (Europa, 2021) que eventualmente poderá reverter-se no marco global legislativo para a regulação da matéria, de forma que conceituou Inteligência Artificial como um software desenvolvido sob determinadas técnicas do qual possibilite a criação de resultados, previsões, decisões automatizadas sob os ambientes em que relaciona-se, todavia, o item "6" da mencionado diploma impera a necessidade complementar a definição de Inteligência Artificial em conjunto com uma lista de técnicas utilizadas para a criação desta, a qual deverá ser atualizada no intuito de acompanhar o desenvolvimento tecnológico presente no mercado, no intuito de garantir a segurança jurídica (Europa, 2021).

Na mesma toada, a Organização para a Cooperação e Desenvolvimento Econômico (OCDE) emitiu, em 2019, recomendação para o desenvolvimento de "Sistemas de Inteligência Artificial", adotada inclusive pelo Brasil, a qual conceitua Sistema de Inteligência Artificial como um:

> "sistema baseado em máquina que pode, para um determinado conjunto de objetivos definidos pelo homem, fazer previsões, recomendações ou decisões que influenciam ambientes reais ou virtuais. Os sistemas de IA são projetados para operar com vários níveis de autonomia" (OCDE, 2019, p.7).

Em uma célere movimentação, o ordenamento brasileiro já conta com três Projetos de Lei (PL 5.051/2019, PL21/2020 e PL 872/2021) que buscam reverter-se no diploma legal destinado ao estabelecimento de princípios, regras, diretrizes e fundamentos à devida regulação do desenvolvimento e utilização da Inteligência Artificial no Brasil (Senado, 2022).

Surpreendentemente, tão somente o Projeto de Lei nº 21/2020 atentou-se ao estabelecimento do significado de "Sistema de Inteligência Artificial", adotando-se o conceito exposto no inciso 1º, art. 2º, PL21/2020 como um:

> "I - sistema de inteligência artificial: o sistema baseado em processo computacional que pode, para um determinado conjunto de objetivos definidos pelo homem, fazer previsões e recomendações ou tomar decisões que influenciam ambientes reais ou virtuais;" (Senado, 2020, p.1).

A partir de uma breve análise, verifica-se que o PL21/2020 possui grande influência advinda das recomendações emitidas pelo Conselho de Inteligência Artificial da OCDE, haja vista a homogênea expressão textual contida em ambos os documentos.

Neste aspecto, a Inteligência Artificial pode ser programada a partir de regras pré-estabelecidas (IA simbólica) ou no conhecimento gerado a partir da inexistência de regras e aprendizado por decisões automatizadas e estatísticas (machine learning), nesta última, o sistema racionaliza suas decisões apenas sob os problemas e dados inseridos (Vainzof, 2022).

Apesar de que a Inteligência Artificial pode desenvolver-se conforme experiência obtida, uma grande polêmica emerge acerca da possibilidade de auditar

o meio com que o sistema chegou aos resultados, ou seja levanta-se um cenário marcado por insegurança e dúvida sobre a tomada de decisões discriminatórias e violações aos direitos fundamentais de proteção e privacidade de dados (Vainzof, 2022).

Não bastasse isso, Agrawal, Gans e Goldfarb explanam diversos cenários de insegurança gerados a partir da utilização de Inteligências Artificiais, tais como I. a ineficácia da tecnologia nos contextos de escassez de dados, de forma que a previsão fornecida como assertiva, todavia, é falsa; II. dados inseridos incorretamente também geram decisões equívocas em máquinas preditivas, sem contar a insegurança dos indivíduos envolvidos frente à ataques cibernéticos; III. a diversidade contida nos dados imputados também pode gerar riscos de enganos em uma análise em massa, considerando ainda a catalogação e mapeamento de perfis; IV, a atividade do sistema pode ser espionada, causando o risco de furto do algoritmo criado por parte de agentes externos maliciosos e; V. o retorno final pode ser alterado para que o sistema aprenda a tomar decisões dotadas de comportamentos discriminatórios e destrutivos (Agrawal, Gans e Goldfarb, 2019).

A seara de dilemas éticos permeados pela utilização de Inteligências Artificiais tampouco carece de riscos expoentes, conforme questionado por Renda, como serão realizadas as decisões tomadas por Inteligências Artificiais envolvendo alto risco e vidas humanas? será aplicado um método qualitativo ou quantitativo mediante o sacrifício e o resguardo dos indivíduos? Caso haja o comprometimento de patrimônio vultoso em relação ao resguardo de vidas humanas, deverão ser atingidos bens públicos ou privados? (Renda, 2018).

Danaher traz dilemas polêmicos e pertinentes ao debate, com o atual desenvolvimento tecnológico, surge a capacidade de criação de robôs sexuais dotados de inteligência artificial. Desta feita, o autor abrange a aplicação penal para comportamentos reprováveis, tal como caso da pedofilia e estupro. Eventualmente o fabricante poderia criar robôs que buscassem reproduzir a imagem de crianças ou elaborar interações para a reprodução de situações de estupro? (Danaher, 2017).

São incessantes as naturezas de direito que podem ser afetadas, Martins condena as práticas de *geopricing e geoblocking* destinadas à discriminação de consumidores, de forma que empresas tomam vantagem a partir da seleção dos perfis, comportamentos e atividades mapeadas de indivíduos para aplicação de preços, agravado ainda pela ignorância do consumidor acerca do algoritmo utilizado e dados indevidamente coletados (Martins, 2019).

Conforme denota-se do cenário de insegurança amplamente debatido pela doutrina nacional e internacional, a utilização de Sistemas de Inteligência Artificial promete uma evolução inimaginável e desenfreada frente à falta de regulação normativa a nível global. Nesse sentido, o próximo tópico abordará a utilização de um programa de *compliance* digital como medidas de prevenção e mitigação de riscos decorrentes de Sistemas de Inteligência Artificial.

O Programa de *Compliance* e sua Aplicabilidade na Mitigação e Prevenção de Riscos

Frente a este polêmico cenário marcado pelo desenvolvimento descontrolado de Inteligências Artificiais e uma insegurança inquietante em virtude de um processo regulatório que anda a passos lentos, aborda-se a possibilidade de utilização dos programas de *compliance* digital para o desenvolvimento controlado de tais tecnologias.

Os programas de *compliance* de dados[1] aplicados em organizações ganham relevância junto ao advento das legislações que tutelam a proteção e privacidade de dados, relevam-se diversos fatores que trazem enfoque ao tema, tais como a incidência em todas as relações permeadas, incluindo-se clientes, colaboradores, fornecedores e todos os stakeholders envolvidos na atividade, o processamento de dados em alta escala (big data) e a própria obrigação regulatória advinda dos diplomas legais, trazido de forma pioneira pelo ordenamento da União Europeia (Frazão; Oliva; Abílio, 2019).

Para além de simplesmente cumprir legislações, as ações de um programa de *compliance* estão envoltas do discernimento entre certo e errado dos indivíduos, não se limitando somente às imposições do Estado, ou seja, alcançando as medidas implementadas em organizações públicas e privadas (Lamy, Lamy, 2022).

Acerca deste viés que norteia o conceito de agir corretamente, o programa de *compliance* conta com o essencial elemento da "governança", conceito que acaba por abranger uma ampla gama de elementos que afetam a gestão empresarial, incluindo a distribuição de poder, a configuração da organização, o processo de tomada de decisões e seu impacto na esfera econômica e social (Saad, 2021).

Para Rosenau, a Governança engloba não apenas as instituições governamentais, mas também incorporando mecanismos informais e não governamentais que orientam as pessoas e organizações em sua esfera de influência para adotarem comportamentos específicos, assim como suas necessidades e solicitações (Rosenau, 2000).

Em que pese seja um termo complexo por abarcar diversos, entende-se, objetivamente, que a governança nada mais é do que um "meio e processo capaz de produzir resultados eficazes, sem necessariamente a utilização expressa da coerção" (Gonçalves, 2005, p.8).

Em vista disso, a governança não reverte-se unicamente em um elemento essencial ao programa de *compliance*, mas também mostra-se um fator indeclinável ao caso em questão, em razão da necessidade de garantir a proteção de direitos fundamentais e panoramas de segurança nacional (Buz, 2020).

1 Em uma visão simplificada, entende-se por programa de compliance de dados como o conjunto de ações e controles a serem implementados no ambiente corporativo, no intuito de reforçar o cumprimento às normas internas e legislação vigente, bem como de prevenir a ocorrência de infrações sob o âmbito da garantia de direitos fundamentais dos titulares de dados (Frazão, 2022). Todavia, destaca-se que a noção de compliance se destaca muito além disso.

De acordo com as dificuldades já anunciadas, diversos doutrinadores destacam a importância do programa de *compliance* para efetivação da LGPD, muito embora haja uma expressa disposição obrigacional, a lei insere muita esperança na disposição voluntária dos agentes de tratamento em seguir suas diretrizes, logo compreende-se que há um direto interesse em estimular a implementação de soluções ajustáveis a cada modelo de negócio (Frazão, 2022).

Não bastasse isso, o programa de *compliance* assume papéis evitar, antecipar, implementar e suplementar a legislação (Bennet, Raab, 2006), fator essencial para acompanhar as regulações de tratamento de dados e desenvolvimento de novas tecnologias.

Rowland, Kohl e Charlesworth (2016) destacam que o risco de novas tecnologias respalda-se característica de que um código não necessita de visibilidade para ser efetivo, pode-se facilmente influenciar o comportamento sem sua devida atenção, prejudicando desta forma a transparência e *accountability* (Rowland, Kohl, Charlesworth, 2016). Todavia, o Ministro Cueva explora na mesma medida que os programas de *compliance* de dados são fundamentados nos princípios de transparência e *accountability* (Cueva, 2020).

Nesta senda, o conjunto de medidas e procedimentos dos quais compõem a estratégia de um programa de *compliance* não se coadunam apenas com o cumprimento das presentes regulações, mas alinham-se às atuais preocupações acerca da prevenção e mitigação de riscos em meio à utilização de novas tecnologias que realizam tratamento de dados de forma desenfreada (Pinheiro, Lorca, Araújo, 2021).

Em que pese as estratégias não possuam uma linearidade obrigatória, Giovanini sugere a estratégia do programa de *compliance* siga pela "Identificação dos Riscos -> Definição dos Requisitos -> Estruturação de um Projeto -> Desenho dos Processos e Controles -> Implementação dos Processos e Controles -> Geração das Evidências -> Auditoria -> Ajustes -> Reteste" (Giovanini, 2019, p. 61), ainda mais valioso que as fases do programa, ressalta-se a necessidade de implementação de controles, sendo os principais: I) análise de maturidade, II) due diligence, III) relatório e matriz de riscos, IV) indicadores, V) compromisso da alta administração, VI) código de ética e políticas, (VII) treinamentos e comunicação, (VIII) canal de denúncias, (IX) comitê de ética e entre outros (Lamy, Lamy, 2020).

É nesta senda que Bennet e Raab advertem a necessidade de tomada de tais políticas e estratégia frente à construção de uma cultura de proteção da privacidade, a fim de evitar-se o determinismo tecnológico (Bennet, Raab, 2006).

Da mesma forma em que o estabelecimento de normas anticorrupção não sanaram por completo a prática de atos ilícitos, há também um papel complementar entre o direito, a tecnologia e os programas de *compliance* de dados na construção deste regime de proteção da privacidade, visto que frente ao atual mundo digital, globalizado e conectado, não se verifica a possibilidade de que o conjunto de normas positivadas pelo ordenamento jurídico supram a atual necessidade (Cohen, 2000).

CONSIDERAÇÕES FINAIS

À vista do exposto, a implementação de um programa de *compliance* se mostra fundamental como medida de prevenção e mitigação de riscos relacionados à utilização de inteligência artificial no tratamento de dados. A evolução tecnológica, especialmente na área da inteligência artificial, trouxe consigo uma série de desafios e dilemas éticos que exigem uma abordagem regulatória adequada.

Historicamente, as revoluções industriais alteraram profundamente a sociedade, redefinindo a economia e a organização social, sendo que atualmente vivencia-se a Quarta Revolução Industrial, marcada pelo rápido desenvolvimento da inteligência artificial e da automação. Essa revolução tecnológica está transformando não apenas a maneira como trabalhamos e nos comunicamos, mas também as estruturas governamentais e institucionais.

A inteligência artificial, com sua capacidade de evoluir rapidamente, traz consigo desafios significativos, tais como a possibilidade de discriminação algorítmica, violações de privacidade e decisões automatizadas questionáveis. Além disso, a falta de regulamentação adequada nessa área cria incertezas e riscos.

No contexto europeu, a proteção da privacidade de dados ganhou destaque com a Convenção Europeia dos Direitos do Homem e o surgimento de regulamentos abrangentes, como o Regulamento Geral de Proteção de Dados (GDPR). No Brasil, a Constituição de 1988 já estabelecia a proteção da privacidade como um direito fundamental.

No entanto, as tecnologias de inteligência artificial continuam a avançar, apresentando desafios significativos em relação à transparência, responsabilidade e governança. Os sistemas de inteligência artificial podem tomar decisões baseadas em algoritmos complexos, tornando difícil a auditoria e o entendimento de como essas decisões são tomadas.

Nesse contexto, a implementação de programas de *compliance* digital se torna crucial. Esses programas não apenas ajudam as organizações a cumprir regulamentações existentes, como a LGPD, mas também permitem que elas adotem uma abordagem proativa na identificação e mitigação de riscos relacionados à inteligência artificial.

É importante ressaltar que os programas de *compliance* não são apenas uma resposta às regulamentações existentes, mas também uma forma de garantir que as organizações estejam preparadas para os desafios futuros que a inteligência artificial pode apresentar. Eles podem ajudar a evitar a discriminação algorítmica, a proteger a privacidade dos dados e a garantir que as decisões automatizadas sejam tomadas de maneira ética e responsável.

Em conclusão, a implementação de programas de *compliance* digital desempenha um papel fundamental na prevenção e mitigação de riscos relacionados à inteligência artificial no tratamento de dados. À medida que a tecnologia continua a avançar, esses programas se tornam ainda mais importantes para garantir que as organizações operem de maneira ética e responsável no ambiente digital em constante evolução.

REFERÊNCIAS

AGRAWAL, Ajay; GANS, J.; GOLDFARB, A. **"Economic Policy for Artificial Intelligence".** Working Paper n. 24.690, National Bureau of Economic Research (NBER), jun. 2018.

BENNETT, Colin J.; RAAB, Charles D. **The governance of privacy.** Policy instruments in global perspective. Cambridge: The MIT Press, 2006, pp. 151-152.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019. 423 p.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil: promulgada em 5 de outubro de 1988.** 4. ed. São Paulo: Saraiva, 1990.

BRASIL. **Lei n. 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 05 Set. 2023.

BRASIL. **Projeto de Lei do Senado Federal nº 5051, de 2019**. Disponível em:<https://legis.senado.leg.br/sdleg-getter/documento?dm=8009064&ts=1570126400907&disposition=inline>. Acesso em: 1º Set. 2023

BRASIL. Marco Civil da Internet. **Lei 12.964/14**. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm >. Acesso em: 06 Set. 2023.

BRYNJOLFSSON, Erik; MCAFFE, Andrew. **The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies.** W Norton & Company. 2014.

BUZ, Marcelo. **A importância da identificação digital segura: confiança.** In: BLUM, Renato Opice; WAJSBROT, Shirly (org.). Cyber Risk Estratégias: estratégias nacionais e corporativas sobre riscos e segurança cibernética. São Paulo: Thompson Reuters Brasil, 2020. Cap. 3.

CATELLI, Maria Augusta Peres; IDIE; Renata Yumi. **Prevenir para Mitigar: a importância do desenvolvimento de cultura de segurança cibernética nas organizações**. In: BLUM, Renato Opice; WAJSBROT, Shirly (org.). Cyber Risk Estratégias: estratégias nacionais e corporativas sobre riscos e segurança cibernética. São Paulo: Thompson Reuters Brasil, 2020. Cap. 1.

CHARNIAK, Eugene; MCDERMOTT, Drew. **A Bayesian Model of Plan Recognition.** Massachusetts: Addison-Wesley, 1985.

COHEN, Julie E. **Examined lives: informational privacy and the subject as object.** Stanford Law Review, v. 52, 2000, pp. 1373-1438, p. 1377.

CONSELHO DA EUROPA. **Manual da Legislação Europeia de Proteção de Dados.** 2014, ISBN 978-92-871-9939-3. Disponível em: <http://www.echr.coe.int/Documents/Handbook_data_protection_POR.pdf>

CONSELHO NACIONAL DE JUSTIÇA. **Inteligência Artificial no Poder Judiciário Brasileiro.** Brasília: Conselho Nacional de Justiça, p. 29. Disponível em: https://www.cnj.jus.br/wp-content/ uploads/2020/05/Inteligencia_artificial_no_ poder_judiciario_brasileiro_2019-11-22. pdf, acesso em 1º de agosto de 2023. TH, Rainer; HORCH, Alexander. Industrie 4.0: Hit or Hype? [Industry Forum]. IEEE Industrial Electronics Magazine, [S. l.], v. 8, n. 2, p. 56-58, 2014. DOI: 10.1109/ MIE.2014.2312079. Disponível em: http://ieeexplore.ieee.org/document/6839101/. Acesso em: 09 Set. 2023.

DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais**. 2. ed. SãoPaulo: Thompson Reuters, 2020. 364 p.

GIOVANINI, Wagner. **COMPLIANCE: A excelência na prática**. 2ª ed. São Paulo, 2019.

GONÇALVES, Alcindo. **O Conceito de Governança.** XIV Congresso Nacional do Conpedi – Conselho Nacional de Pesquisa e Pós-Graduação em Direito – Fortaleza, 2005.

HAUGELAND, John. **Artificial Intelligence: The Very Idea**. Massachusetts: The MIT Press, 1985.

JAMBEIRO FILHO, Jorge Eduardo de Schoucair. **Inteligência Artificial no Sistema de Seleção Aduaneira por Aprendizado de Máquina.** Secretaria da Receita Federal do Brasil – 14º Prêmio RFB – 2015. Disponível em: https:// repositorio.enap.gov.br/bitstream/1/4622/1/1%C2%BA%20lugar%20do%20 14%C2%BA%20Premio%20RFB.pdf. Acesso em: 28 julho 2023.

KURZWEIL, Ray. **The Age of Spiritual Machines.** Massachusetts: The MIT Press, 1990.

KUHN, T. S. A **Estrutura das Revoluções científicas.** 11ª Edição, São Paulo: Editora Perspectiva, 2011.

LAMY, Ana Carolina Faraco; LAMY, Eduardo de Avelar. **Compliance Empresarial.** 1º Edição, Rio de Janeiro: Forense, 2022.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (org.). **LGPD: Lei Geral de Proteção de Dados comentada.** 2. ed. São Paulo: Thompson Reuters, 2020. 474 p.

MARTINS, Roberta Zumblick Martins da. **Inteligência artificial e direito.** Curitiba: Alteridade, 2020.

MCCARTHY, J; MINSKY, M; ROCHESTER, N; SHANNON, C. **A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence.** 1955. <http://www-formal.stanford.edu/jmc/history/dartmouth/dartmouth.html>. Consultado: 18 de JUL de 2023.

PARLAMENTO EUROPEU E CONSELHO. **Proposta de regulamento do Parlamento Europeu e do Conselho que estabelece regras harmonizadas em**

matéria de inteligência artificial (Regulamento inteligência artificial) e altera determinados atos legislativos da união. 21/04/2021, COM/2021/206 final, https://eurlex.europa.eu/legal-content/PT/TXT/?uri=CELEX:52021PC0206.

PINHEIRO, Thiago Jabor; LORCA, Paola Piva; ARAÚJO, Victor Henrique Aversa. **Due Diligence: Anticorrupção de terceiros e em fusões e aquisições**. in: Manual de Compliance. 3ªed. Forense, 2021.

ROSENAU, James N. **"Governança, Ordem e Transformação na Política Mundial".** In: Rosenau, James N. e Czempiel, Ernst-Otto. Governança sem governo: ordem e transformação na política mundial. Brasília: Ed. Unb e São Paulo: Imprensa Oficial do Estado, 2000. pp. 11-46

ROWLAND, Diane; KOHL, Uta; CHARLESWORTH, Andrew. **Information Technology Law.** New York: Routledge, Op. cit., p. 14. 2016.

SAAD, Eduardo Diniz. **Ética Negocial e Compliance**. 1ed. Thompson Reuters Brasil, 2019.

SALKIN, Ceren; ONER, Mahir; USTUNDAG, Alp; CEVIKCAN, Emre. **A Conceptual Framework for Industry 4.0.** In: USTUNDAG, Alp; CEVIKCA, Emre (org.). Industry 4.0: Managing The Digital Transformation. Cham: Springer International Publishing, 2018. DOI: 10.1007/9783319578705_1. Disponível em: http://link.springer.com/10.1007/9783319578705_1.

SCHWAB, Klaus. **A Quarta Revolução Industrial.** 1a ed. São Paulo: Edipro, 2016.

SILVA, Daniel Pereira Militão. **Desafios do ensino jurídico na pós-modernidade: da sociedade agrícola e industrial para a sociedade da informação**. Dissertação (Mestrado) – Faculdade de Direito da Pontifícia Universidade Católica de São Paulo. São Paulo, 2009.

TURING, A. C**omputing Machinery and Intelligence.** Computer Media and Communication: A Reader, p. 37-58. Oxford: Oxford University Press, 1999

UNIÃO EUROPEIA. **CEDH de 04 de novembro de 1950**. Convenção Europeia dos Direitos do Homem. Roma.

UNIÃO EUROPEIA. **Carta dos Direitos Sociais Fundamentais da União Europeia**. Disponível em: <http://ue.eu.int/df/default.asp?land=pt>. Acesso em: 26 Set 2023.

UNIÃO EUROPEIA .**Convenção Europeia dos Direitos do Homem, 1950**. Disponível em: <https://www.echr.coe.int/Documents/Convention_POR.pdf>. Acesso em: 26 Set 2023.

UNIÃO EUROPEIA. **Diretiva 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 (Regulamento Geral sobre a Proteção de Dados).** Jornal Oficial da União Europeia, Estrasburgo, 24/10/1995. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=celex:31995L0046>. Acesso em: 26 Set 2023.

UNIÃO EUROPEIA. **Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho, de 23 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)**. Jornal Oficial da União Europeia, Estrasburgo, 04/05/2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=PT>. Acesso em: 26 Set 2023.

VAINZOF, Rony. **Relatório de impacto à proteção de dados pessoais**. In: Renato Opice Blum. (Org.). Proteção de Dados - Desafios e Soluções na Adequação à Lei. 1ed.Rio de Janeiro: Forense, 2020, v. 1, p. 141-168.

VAINZOF, Rony. **Comentários ao artigo 3º da LGPD.** In: MALDONADO; Viviane Nóbrega; OPICE BLUM, Renato (coords.). Lei Geral de Proteção de Dados Pessoais comentada [livro eletrônico]. 3. ed. São Paulo: Thomson Reuters Brasil, 2021.