


A PROTEÇÃO DE DADOS E O COMPLIANCE APLICADO NA RELAÇÃO LABORAL DAS EMPRESAS PRIVADAS: UMA ANÁLISE DA POLÍTICA DE PRIVACIDADE DA C&A

 <https://doi.org/10.22533/at.ed.926112430096>

Data de aceite: 16/10/2024

Roberta Lísie D’Almeida Barcelos

Advogada. Mestranda em Direito Privado Acadêmico pela Universidade 7 de Setembro (UNI7). Pós-graduada em Direito Constitucional pela Universidade Única de Ipatinga. Pós-graduada em Direito Público pelo Instituto de Ensino Superior de Fortaleza

Resumo: O presente artigo trata sobre três temas relevantes da atualidade: a Lei n.º 13.709/2018 que regulamenta a Lei Geral de Proteção de Dados Pessoais, conhecida como LGPD, o *compliance* e sua aplicação no ambiente laboral. A LGPD aborda em um de seus artigos sobre a criação de programas que se moldem aos procedimentos de tratamento de dados pessoais que eventualmente possam causar riscos à liberdade civil e aos direitos fundamentais dos indivíduos; possuindo alternativas de prevenção contra a ocorrência de danos. Na LGPD há orientações acerca da efetivação da tutela da privacidade de dados, prevendo sobre o correto manuseio dos dados pessoais por parte das pessoas jurídicas, indicando o modo em que deve ocorrer o exame do conteúdo dessas informações. Este artigo tem como objetivo, ainda, investigar como

a utilização de algumas tecnologias de inteligência artificial por parte das empresas privadas podem gerar violações de direitos à imagem, à honra, aos direitos sociais do trabalho e à proteção de dados do trabalhador dentro do ambiente de trabalho. Deste modo, percebe-se a necessidade de haver o desenvolvimento de tecnologias, em harmonia com as políticas de governança de privacidade e normas gerais de proteção de dados.

Palavras-chave: Lei Geral de Proteção de Dados; *Compliance*; Dados Pessoais; Privacidade; Relação Laboral.

DATA PROTECTION AND COMPLIANCE APPLIED IN THE LABOR RELATIONSHIP OF PRIVATE COMPANIES: AN ANALYSIS OF C&A'S PRIVACY POLICY

Abstract: This article deals with three relevant current topics: Law No. 13,709/2018, which regulates the General Personal Data Protection Law, known as LGPD, compliance and its application in the workplace. The LGPD addresses in one of its articles the creation of programs that adapt to personal data processing procedures that may eventually cause risks to civil liberty and

the fundamental rights of individuals; having alternatives to prevent damage from occurring. In the LGPD there are guidelines on the implementation of data privacy protection, providing for the correct handling of personal data by legal entities, indicating the way in which the content of this information should be examined. This article also aims to investigate how the use of some artificial intelligence technologies by private companies can generate violations of rights to image, honor, social labor rights and worker data protection within the work environment. Therefore, there is a need to develop technologies in harmony with privacy governance policies and general data protection standards.

Keywords: General Data Protection Law; Compliance; Personal Data; Privacy; Labor Relationship.

INTRODUÇÃO

Tendo em vista o desenvolvimento da *internet* e das tecnologias de comunicação, que teve uma maior adesão do final dos anos 90 para cá, houve o surgimento de potenciais riscos de violações a direitos referentes ao uso indevido de dados pessoais.

Hoje o ambiente virtual é algo inerente à nossa vida social, estando inserido nas relações de consumo, de trabalho, nas atividades desempenhadas pelas instituições públicas e empresas privadas. Com isso, requer-se a observância da proteção dos direitos fundamentais das pessoas naturais por serem estas a parte mais sensível e vulnerável da relação jurídica.

Vindo para o nosso tema, nas relações de trabalho, há também, essa necessidade de tutelar não somente os dados pessoais, mas também, os dados sensíveis do empregado, pois este, fornece ao empregador e à empresa informações não somente ligadas às suas aptidões profissionais, mas também, referente ao seu histórico de saúde, intimidade e privacidade.

Como em toda atividade econômica aqueles que possuem o privilégio de possuírem a detenção dos dados e informações passaram a ter uma “superioridade em relação aos demais cidadãos e órgãos” (Bioni; Luciano, 2019, p. 216).

Tendo em vista a dinâmica do nosso atual mundo digital houve a necessidade da elaboração de uma norma jurídica que regulamentasse sobre o tema de proteção de dados. Assim, foi promulgada a Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018, sendo esta uma lei geral que trata expressamente acerca da tutela e política de privacidade dos dados pessoais da pessoa natural ou da pessoa jurídica de direito público ou privado, conforme aduz o art. 1º, *caput*, da Lei nº 13.709/2018¹.

O objetivo pretendido pela referida legislação é regular o tratamento de dados, proteger os direitos constitucionais e fundamentais da liberdade, privacidade e intimidade (art. 1º e art. 17 da Lei nº 13.709/2018)², visando também, resguardar o sujeito a quem se refere os dados pessoais objeto de proteção legal (art. 5º, V, da referida lei).

1. Art. 1º da Lei nº 13.709/2018 : Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

2. Art. 17º da Lei nº 13.709/2018: Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei.

Art. 5º da Lei nº 13.709/2018: Para os fins desta Lei, considera-se: V- titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

Os riscos que cercam a vigilância sobre os dados surgem não apenas das atividades dos órgãos de segurança pública, mas também, da coleta de informações feita por parte das empresas privadas (Rodotà, 2013).

Diante da relevância do tema, a Organização Internacional do Trabalho (OIT), no ano de 1997, dispõe: “Os empregadores, os trabalhadores e seus representantes devem cooperar na proteção de dados pessoais e na elaboração de uma política de empresa que respeite a vida privada dos trabalhadores”.

Uma das condutas sugeridas pela OIT para a garantia da proteção dos dados pessoais e sensíveis dos empregados consiste no uso de programas de *compliance*, de acordo com a legislação do Estado e normas de conduta (ANDRADE, 2017, p. 76).

O propósito desta investigação é responder a seguinte pergunta: Como o empregado dentro do ambiente laboral está sendo tratado em relação à proteção de seus dados pessoais?

Deste modo, serão abordados no decorrer dos capítulos deste artigo aspectos relacionados ao *compliance*, LGPD, armazenamento de dados, privacidade das informações pessoais dos trabalhadores, dentre outros assuntos relevantes.

Em se tratando da metodologia, a presente pesquisa é exploratória, adotando-se uma abordagem dedutiva, bibliográfica, com um compilado de doutrinas; sendo ainda, empírica, pois, houve, uma coleta de dados concretos colhidos através de pesquisa realizada *in loco*.

A pesquisa de campo foi realizada na loja C&A com o intuito de observar como a referida empresa aplica a Lei nº 13.709/2018 - Lei Geral de Proteção de Dados e demais legislações conexas que versam sobre o direito do trabalho, *compliance*, direito do consumidor, direito civil, direito constitucional, dentre outros ramos do direito, que visam garantir a inviolabilidade dos direitos fundamentais da liberdade, privacidade e intimidade dos titulares das informações pessoais que estão sob o domínio da empresa ou empresário individual.

O desenvolvimento deste trabalho está dividido da seguinte forma: O primeiro capítulo trata da “Tutela normativa dos dados pessoais dos trabalhadores”, trazendo as principais legislações em vigor que abordam sobre a matéria de proteção de dados; O segundo capítulo aborda acerca do “Direito comparado e a proteção de dados”, relembrando a contribuição jurídica de outros países da Europa na elaboração da nossa lei geral de proteção de dados; O terceiro capítulo trata do “Estudo empírico da política de privacidade dos dados utilizados pela C&A na relação laboral”, a pesquisa de campo aborda o tema *compliance* realizado na loja física da C&A e também no *site* do seu *e-commerce*; este último capítulo está dividido em dois subtópicos; o 3.1 relata sobre “O *compliance* no ambiente laboral da C&A” e o 3.2 aborda sobre “A vulnerabilidade das informações pessoais disponibilizadas pelos empregados”.

Por fim, nas conclusões, faz-se um arremate geral sobre todo o estudo realizado através das doutrinas, legislações, revistas jurídicas e pesquisa *in loco*, respondendo ao problema principal desta pesquisa e demonstrando como as empresas privadas e os empresários individuais estão aplicando as normas de *compliance* e proteção de dados no ambiente laboral.

TUTELA NORMATIVA DOS DADOS PESSOAIS DOS TRABALHADORES

A Lei Geral de Proteção de Dados (LGPD), lei nº 13.709/2018, teve inspiração nas legislações da União Europeia e especialmente na atual Regulamentação Geral de Proteção de Dados Europeu (GDPR - *General Data Protection Regulation*) em vigor desde 2018.

A LGPD contempla em seu bojo uma variedade de legislações sobre o tema de proteção de dados, possuindo normas jurídicas do nosso Código civil (Lei nº 10.406/2002), do Código de defesa do consumidor (Lei 8.078/90) e do Marco civil da *internet* (Lei nº 12.965/2014), estabelecendo garantias, direitos e deveres para a utilização da *web* no Brasil, determinando modos de atuação da União, Estados, Distrito Federal e Municípios quanto à matéria, tendo como um dos fundamentos principais a observância do princípio da liberdade de expressão.

Na seara do Direito do Trabalho, a Organização Internacional do Trabalho (OIT), no ano de 1997, passou a adotar recomendações básicas de proteção de dados pessoais dos trabalhadores, dispondo no item 5.11: “Os empregadores, os trabalhadores e seus representantes devem cooperar na proteção de dados pessoais e na elaboração de uma política de empresa que respeite a vida privada dos trabalhadores (...)”. (OIT, p. 02).

A Lei nº 12.965/2014, em seu art. 3º, traz alguns princípios, dentre eles; a proteção da privacidade dos dados pessoais, a estabilidade da rede, a segurança técnica conforme padrões internacionais, o estímulo às boas práticas, a responsabilização dos agentes infratores, a liberdade de escolha nos negócios realizados pela *web*, dentre outros, já que o rol é meramente exemplificativo, não excluindo outros princípios previstos no ordenamento jurídico.

O art. 10º, da supracitada lei, prevê que: “A disponibilização dos registros (...) de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas”.

A nossa Constituição Federal de 1988 em seu art. 5º, inciso X, trata sobre a privacidade: “São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação”.

O conceito de *internet* está no art. 5º da Lei nº 12.965/2014: “Conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes”.

No Decreto nº 8.771/2016 há previsão de situações de discriminação de dados pela *web* e aponta métodos para o armazenamento e preservação de informações através do uso de provedores de acesso à *internet*, orientando formas de transparência no requerimento de bases cadastrais pelos órgãos públicos, editando medidas de fiscalização e controle das infrações.

A LGPD, em seu art. 52 traz um rol, exemplificativo, de sanções administrativas, tais como: advertência (com prazo para adequação de medidas corretivas), multa simples chegando até 2% do faturamento da empresa privada (limitada no valor de cinquenta milhões de reais por infração), multa diária, publicização da infração nos meios de comunicações, após a sua ocorrência ter sido devidamente comprovada; bloqueio dos dados pessoais pertinentes à infração até a sua completa regularização; eliminação dos dados pessoais a que se refere a infração; suspensão parcial do banco de dados a que se refere a infração pelo período de até seis meses, podendo ser prorrogável, pelo mesmo período, dentre outras sanções.

As sanções somente serão aplicadas após o devido procedimento administrativo em que seja disponibilizado à outra parte o contraditório e a ampla defesa.

As penalidades citadas neste capítulo podem ser aplicadas individual ou cumulativamente, de acordo com os danos ocasionados, tendo como parâmetro: a gravidade do ilícito, a natureza e reincidência da infração, a vantagem pecuniária obtida, a situação financeira do infrator, a cooperação, a boa-fé e a proporcionalidade na aplicação da sanção.

As sanções administrativas previstas na LGPD e demais legislações que tratam sobre a matéria de proteção de dados, não anulam a aplicabilidade, também, de sanções civis ou penais, conforme tenha sido a natureza jurídica do ilícito perpetrado.

A Lei de acesso à informação pública (Lei nº 12.527/2011) dispõe sobre os mecanismos a serem seguidos pela União, Estados, Distrito Federal e Municípios, com o fim de garantir o acesso às informações; estando tal previsão, na nossa CF, no art. 5º, inciso XXXIII, que aduz: “Todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado”.

O termo inglês *compliance* deriva do verbo *to comply*, que quer dizer: “o agir humano em conformidade com algo, pautado na ética e na observância de regras”.

A Lei nº 9.507/1997 regula o direito de acesso a informações e disciplina o rito processual do *habeas data* no seu art. 7º, inciso I, esta previsão legal aplica-se também à LGPD e ao *compliance*: “Para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registro ou banco de dados de entidades governamentais ou de caráter público”.

Conforme preleciona o art. 64 da LGPD: “Os direitos e princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte”.

Observa-se pela simples leitura da Lei Geral de Proteção de Dados que há expresso no art. 41, inc. III, a previsão de pertinência com o programa de conformidade visando a observância de proteção da tutela dos dados pessoais da pessoa natural.

O art. 46, *caput*, da LGPD, relata que: “Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados (...) ou qualquer forma de tratamento inadequado ou ilícito”.

O *compliance* deve ser estruturado para aplicação às pessoas jurídicas de direito privado, tais como, as organizações e as instituições, devendo, também, estarem em conformidade com o tratamento de dados pessoais das pessoas jurídicas de direito público (art. 23 da LGPD).

A LGPD em seu art. 50, § 3º, prevê: “As regras de boas práticas e de governança deverão ser publicadas e atualizadas periodicamente e poderão ser reconhecidas e divulgadas pela autoridade nacional”.

Já o art. 5º, inciso XII, da CF/88 prevê sobre a inviolabilidade do sigilo das comunicações telegráficas e de dados, sendo uma garantia constitucional.

As legislações vigentes que tratam sobre proteção de dados preveem o direito do requerente às informações solicitadas aplicando-se o princípio da transparência. Além deste, há os princípios da finalidade, necessidade, adequação e não discriminação.

Há, também, assegurado direito de acesso aos dados, retificação e descarte de informações equivocadas (conforme art. 6º, 17º e 18º da LGPD)³, sendo formas de garantias dos direitos fundamentais.

A Lei do Cadastro Positivo, Lei nº 12.414/2011: “Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito”.

O art. 6º da referida lei aduz que: “Ficam os gestores de bancos de dados obrigados, quando solicitados, a fornecer ao cadastrado: I - todas as informações sobre ele constantes de seus arquivos, no momento da solicitação”.

Neste contexto, o fato de utilizarmos uma comunicação digital é determinante para que suportemos constante vigilância em nossa privacidade, através da utilização de câmeras de segurança, máquinas com detectores de metais, reconhecimento facial, impressão digital na entrada e saída do trabalho, senhas para utilização de *sites* e sistemas operacionais e etc.

Voluntária ou involuntariamente, vivemos sob o constante monitoramento de dados pessoais ou de informações devido ao uso controlado das tecnologias de inteligência artificial.

3. Art. 6º da Lei nº 13.709/2018: As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios (...).

Art. 18º da Lei nº 13.709/2018: O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição (...).

Art. 2º da Lei nº 13.709/2018: 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.

O DIREITO COMPARADO E A PROTEÇÃO DE DADOS

Em relação ao direito comparado, na Europa, a previsão acerca da tutela dos dados pessoais está presente no art. 35 da Constituição Portuguesa de 1976 e inserida, também, no art. 18 e art. 105 da Constituição Espanhola de 1978.

A Constituição Portuguesa de 1976 em seu art. 35, dispõe: “1. Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua retificação e atualização, e o direito de conhecer a finalidade a que se destinam (...)”.

Há tutelas jurídicas sobre dados pessoais que extrapolam os meros interesses individuais das pessoas naturais, alcançando o direito empresarial disposto no art. 2º da lei nº 13.709/2018, prevendo acerca dos direitos fundamentais e individuais constitucionalmente assegurados pela nossa Constituição Federal de 1988, dentre eles: o direito à privacidade, à honra, à imagem, à intimidade, à proteção do direito do consumidor, à livre concorrência, à livre iniciativa e ao desenvolvimento tecnológico.

O art.35 da Constituição Portuguesa de 1976, aduz que: “3. A informática não pode ser utilizada para tratamento de dados referentes a convicções políticas, filiação partidária (...), fé (...), vida privada e origem étnica, salvo mediante consentimento expresso do titular(...)”.

Conforme Doneda et al. (2018): “O desenvolvimento dos mecanismos de inteligência artificial com a maior disponibilidade de informação deixou seus reflexos na regulação que começou a ser concebida em relação à proteção de dados pessoais”.

Sobre os dados pessoais a Constituição Portuguesa de 1976 em seu artigo 35º preleciona que: “4. É proibido o acesso a dados pessoais de terceiros, salvo em casos excepcionais previstos na lei”.

De acordo com Rodotà (2008), Norris (2003), Lianos e Douglas (2000), um dos pontos mais relevantes quanto à disponibilização de dados pessoais é a utilização das informações coletadas com o objetivo de criar perfis de usuários formando vários bancos de dados.

A supracitada Constituição Espanhola de 1978 prevê no seu artigo 18 matéria de teor semelhante: “4. *La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos*”.

A Constituição Espanhola de 1978 trouxe no bojo do seu artigo 105 previsão legal acerca do acesso e cuidado dos arquivos e registro contendo dados pessoais: “b) *El acceso de los ciudadanos a los archivos y registros administrativos, salvo en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas*”.

Já nas legislações brasileiras a previsão legal de *compliance* está expressa no art. 5º, inciso XVII, da LGPD, que dispõe acerca do relatório de impacto visando a proteção de dados pessoais contendo descrições de processos de tratamento de dados e mecanismos de diminuição de riscos.⁴

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

Em um contexto geral, vemos o “abismo entre os desenvolvedores desses tipos de tecnologias e aqueles que são impactados por ela” (Bioni; Luciano, 2019, p. 208), o que tem demonstrado a necessidade de normas legais específicas sobre este tema, além da aplicação da transparência e vigilância no uso de programas dotados de inteligência artificial com o fim de reduzir as incertezas quanto aos riscos de proteção às informações (Floridi et al., 2017).

O art. 35 da Constituição Portuguesa de 1976 já tratava no seu artigo 35º acerca da utilização da informática, vejamos: “1. Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua retificação e atualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei”.

Observa-se que a Constituição Portuguesa mesmo sendo do ano de 1976 traz em seu texto previsão legal do conceito de dados pessoais, deliberando sobre quais devem ser os requisitos utilizados na conexão, no tratamento e transmissão de dados através do uso da rede mundial de computadores e aparelhos eletrônicos similares de modo a garantir a proteção jurídica.

O direito de acesso às informações é um dos mais importantes elementos de proteção que diz respeito ao direito da pessoa em tomar conhecimento de quem possui acesso a seus dados pessoais e como estes são ou foram utilizados devendo haver um controle social (Rodotà, 2013).

Na nossa Constituição Federal Brasileira de 1988 não há, explicitamente, previsão legal de que as pessoas jurídicas são titulares de direitos fundamentais. Contudo, a doutrina especializada no assunto de proteção de dados e a jurisprudência, possuem entendimento no sentido de que há possibilidade de aplicação dos direitos fundamentais, às pessoas jurídicas de direito privado e também aos entes despersonalizados, tendo em vista a tutela da personalidade.

Já a Lei Fundamental Alemã de 1949, em seus artigos 19 e 321, e também, a Constituição Portuguesa de 1976, em seus artigos 12 e 2, trazem a previsão normativa de que as pessoas jurídicas são titulares de direitos.

Deste modo, em todas as atividades, seja na esfera pública ou privada, é necessário que haja a transparência dos atos da Administração Pública, de acordo com a Lei 12.527/2011, e também, que seja feito o controle dos dados pessoais pelo titular, conforme a LGPD.

As informações pessoais da pessoa natural ou jurídica são atributos da personalidade e da honra, devendo haver o controle destes dados a fim de garantir a privacidade na atual sociedade da informação.

Atualmente o termo privacidade tem passado por uma reconceituação, dentro do direito do consumidor e da LGPD, pois, a privacidade deve respaldar-se no “direito do indivíduo de escolher aquilo que está disposto a revelar aos outros” (Rodotà, 2008, p. 74).

O conceito de dados pessoais está inserido no art. 5º, I, da LGPD e no art. 4º, IV, da Lei de Acesso a Informações Públicas (LAI) ao tratar acerca dos dados das pessoas naturais identificáveis.

Há uma pluralidade de dados ligados à pessoa natural, como os que dizem respeito à qualificação, dentre eles; o nome, nacionalidade, estado civil, naturalidade, profissão, RG, CPF, extrato de imposto de renda, certidão de nascimento ou casamento e comprovante de residência.

Nesse contexto, existem dados sensíveis, pertencentes à pessoa natural, que merecem um tratamento mais cuidadoso, tendo em vista dizerem respeito a informações: étnica, racial, religiosa, política, saúde, herança genética, fator sanguíneo, doença, orientação sexual, e etc., (art. 5º, inciso II, da LGPD).⁵

Existem, ainda, dados referentes às declarações ou opiniões manifestadas em redes sociais, sendo também considerados como dados pessoais, por analogia. Assim, o objeto de proteção legal visa garantir a tutela sobre a personalidade, dados e informações identificáveis relacionadas a determinada pessoa.

O art. 12, § 2º, da LGPD, leciona que: “Poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada.

A lei de proteção de dados traz determinações específicas acerca, também, da segurança dos dados pessoais de titularidade das pessoas jurídicas.

Devido a relevância do tema, na 108ª Conferência Internacional do Trabalho, foi promulgada a Declaração do Centenário da OIT, referindo-se ao ser humano como sendo o centro das políticas de melhorias laborais estando prevista a garantia de tutela à privacidade dos dados pessoais (OIT, 2019).

O Parlamento Europeu promulgou em 20/06/2019 um regulamento referente à efetivação da justiça e da transparência para os profissionais de serviços de intermediação, tendo como meta implementar normas que possibilitem às empresas agirem com mais equidade e eficiência.

O art. 35 do supracitado regulamento da União Europeia dispõe: “o tratamento dos dados pessoais deverá respeitar o regime jurídico da União relativo à proteção das pessoas singulares, ao respeito pela vida privada e à proteção dos dados pessoais nas comunicações eletrônicas”.

Muito embora o referido regulamento esteja restrito à circunscrição da União Europeia, sua base legal serve como um norte para que as plataformas digitais relatem, por exemplo, os motivos pelos quais estão suspendendo um motorista de aplicativo.

5. Art. 5º da Lei nº 13.709/2018: Para os fins desta Lei, considera-se:

I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Art. 4º, IV, da Lei de Acesso a Informações Públicas - informação pessoal: aquela relacionada à pessoa natural identificada ou identificável.

Assim, legislações de diferentes países que tratam sobre a matéria de proteção de dados traçam diretrizes de normas norteadoras para a elaboração de programas de *compliance*.

Rodotà relata acerca do aumento incontido do uso da *internet*, atrelado à intensa coleta de dados pessoais, somada à interconexão entre diversos bancos de dados que realizam o cruzamento de informados usuários, para o autor, a atual sociedade da informação “ameaça sombrear o crescimento igualmente intenso dos bancos de dados mais tradicionais, aqueles com finalidade de segurança, que também são modificados pelas tecnologias e pela realidade de um mundo sem fronteiras” (Rodotà, 2008, p. 146).

ESTUDO EMPÍRICO DA POLÍTICA DE PRIVACIDADE DOS DADOS UTILIZADOS PELA C&A NA RELAÇÃO LABORAL

Neste presente trabalho foi realizada uma pesquisa empírica, *in loco*, na loja C&A à fim de observar como a referida empresa aplica a Lei nº 13.709/2018 - Lei Geral de Proteção de Dados e demais legislações conexas que garantem a inviolabilidade dos direitos constitucionais da intimidade, honra e liberdade de seus funcionários, sendo estes também, titulares do direito à privacidade em relação às suas informações pessoais que estão sob o domínio da empresa.

Nas lojas físicas da C&A há um sistema acústico de som em que dentre os anúncios dos produtos e serviços ofertados é informado, também, sobre a Lei Geral de Proteção de Dados e a Política de Privacidade adotada pela empresa em relação aos dados pessoais dos usuários.

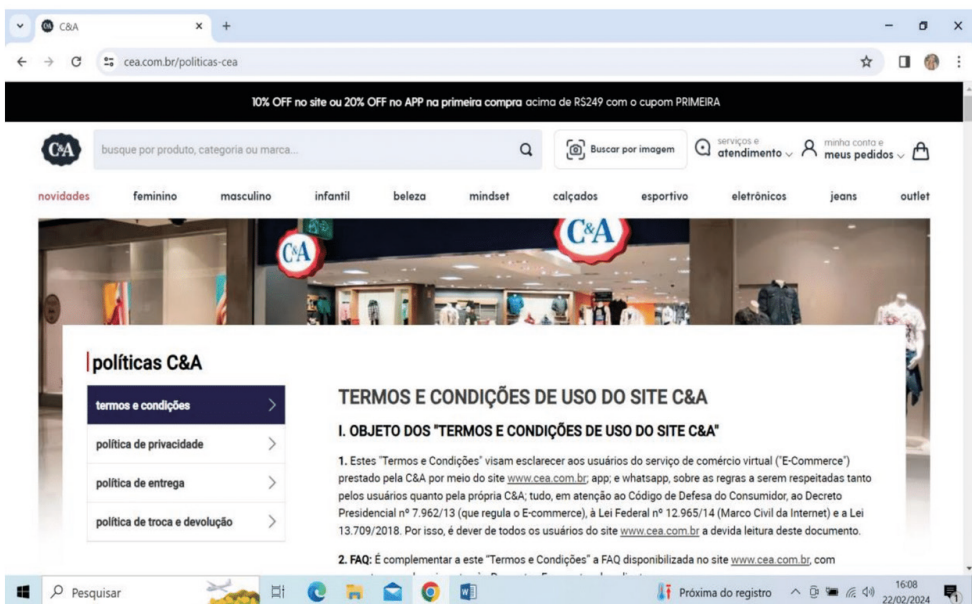
Foi realizada, no dia 10/11/2023, uma pesquisa de campo na loja C&A do *Shopping Aldeota*, localizado na cidade de Fortaleza/CE.

Nesta visita, *in loco*, foi solicitado a um dos funcionários, informações sobre como a C&A atua de modo a garantir o bom armazenamento dos dados pessoais fornecidos, não apenas por seus clientes, mas também, por seus funcionários.

Diante da pergunta, o funcionário imprimiu um papel em que constava o termo de “Aviso de Privacidade para Clientes e Usuários de Canais C&A e C&A Pay”, sendo este, um regulamento da empresa que prevê sobre a responsabilidade das informações prestadas pelos clientes das lojas físicas ou virtuais, além de ser uma política de segurança utilizada, também, no tratamento de banco de dados dos seus funcionários, vejamos:



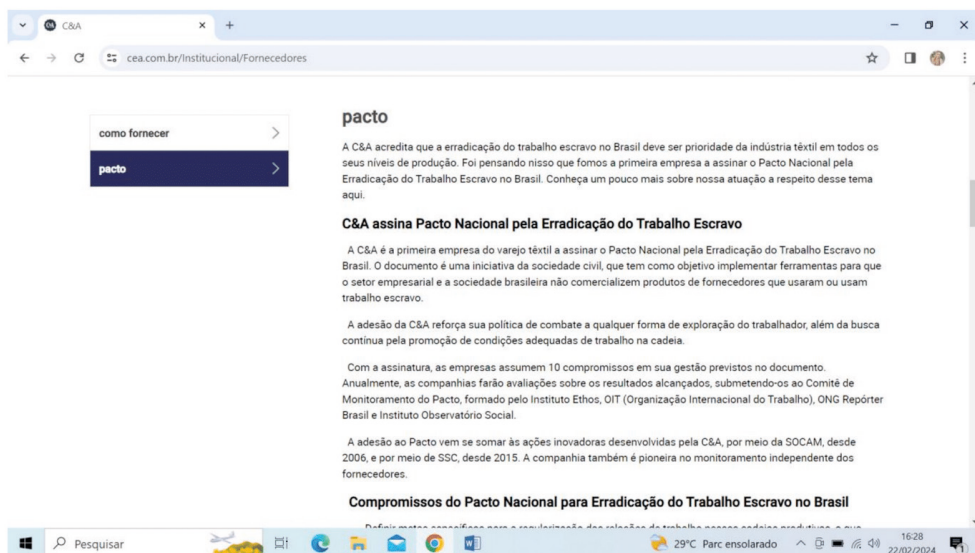
Na mesma oportunidade da pesquisa de campo realizada na loja C&A verificou-se que a empresa comunica aos seus usuários acerca da existência, não apenas da LGPD, mas também, disponibiliza no *site* do seu *e-commerce* outras legislações como o marco civil da *internet*, o código de defesa do consumidor, o decreto presidencial nº 7.962/13 e etc., conforme abaixo:



Em um segundo dia de pesquisa de campo realizada na C&A, em 17/11/2023, ao adentrar na loja, verificou-se que se encontrava trabalhando, uma operadora de caixa, transexual, que apesar de ter nascido com o gênero masculino se vê como mulher e é tratada no ambiente de trabalho e pelos clientes da empresa no feminino, atendendo pelo nome de “Yvi”.

Com isso, houve uma boa impressão na visita *in loco* realizada na referida empresa tendo em vista que a mesma está adotando, adequadamente, medidas de *compliance* dentro do seu ambiente laboral.

No *site* da C&A há a menção de um pacto contra o trabalho escravo tendo sido a referida empresa a primeira a assinar o “Pacto Nacional pela Erradicação do Trabalho Escravo no Brasil”, sendo este, um exemplo da utilização do *compliance* em sua atuação, senão vejamos:



Há também na loja virtual da C&A informações acerca das garantias dos direitos fundamentais trabalhistas do empregado, vejamos:



Percebe-se que as regras de *compliance* vieram para beneficiar a todos, sejam: clientes, consumidores, empresas parceiras, empregados da empresa, pessoas portadoras de deficiência física, cromossômicas, transgêneros, transexuais e etc; fazendo com que haja um ambiente mais igualitário e justo, para todos, sem discriminação ou preconceitos quanto à raça, cor, orientação sexual, etnia, ideologia de gênero, religião, política e etc.

Conforme mencionamos no primeiro capítulo deste estudo, devido ao cenário atual do mercado de trabalho e de consumo, pequenas, médias e grandes empresas precisaram se moldar às legislações do *e-commerce* e às regulamentações de *compliance*.

Há o Decreto Presidencial nº 7.962/13 que regimenta a Lei nº 8.078/1990 e delibera acerca das transações efetivadas no comércio *online* sendo um verdadeiro manual de compilados de requisitos legais que servem de base para a efetivação do *compliance*.

O COMPLIANCE NO AMBIENTE LABORAL DA C&A

Sites de comércio eletrônico como a C&A estão investindo, cada vez mais, em políticas de proteção às informações pessoais não apenas de seus clientes, mas também, de seus empregados, como meio de resguardar o banco de dados e a privacidade dos mesmos.

O art. 5º, inciso I, da LGPD, traz o conceito de dado pessoal: “informação relacionada a pessoa natural identificada ou identificável”.

Já o inciso IV do art. 5º da LGPD define o que seria banco de dados: “conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico”.

Partindo do exemplo da loja C&A, vemos que, atualmente, há um maior comprometimento por parte das empresas com a responsabilidade e transparência em sua relação interpessoal com os consumidores que compram produtos, nas lojas físicas, no *e-commerce* e no *marketplace*, assim como há também o cuidado com as informações pessoais dos funcionários da empresa, sendo todos os usuários considerados como titulares de direitos, estando protegidos pela Lei nº 13.709/2018, Lei Geral de Proteção de Dados (LGPD).

O art. 5º, inciso V, da Lei nº 13.709/2018, traz o conceito de quem é considerado titular: “pessoa natural a quem se referem os dados pessoais que são objeto de tratamento”.⁶

Ao manusearmos o *site* de comércio eletrônico da C&A percebemos que até para a oferta de emprego o candidato à vaga precisa preencher algumas informações constando os seus dados pessoais, antes mesmo de ser contratado para trabalhar na empresa, conforme ver-se abaixo:

The image shows a web browser window displaying the registration page of C&A. The browser's address bar shows the URL 'cea.com.br/trabalhe-conosco'. The page has a light blue header with the text 'Trabalhe Conosco | C&A'. Below the header, there are two dropdown menus: 'Como trabalhar na C&A?' and 'Privacidade de Dados (LGPD)'. The main content area is titled 'Cadastre-se' with the subtitle 'e fique por dentro de todas as novidades'. It features an 'email' input field containing 'exemplo@ex.com', a 'seleção seu gênero' section with radio buttons for 'feminino' (selected) and 'masculino', and an 'enviar' button. A small note below the button reads 'Ao clicar em "enviar" você aceita os termos de uso da C&A'. Below the registration form, there are six columns of product categories: 'feminino', 'masculino', 'infantil', 'plus size', 'beleza', and 'eletrônicos'. Each column lists various items such as blusas, macacões, vestidos, saias, moda praia, biquínis, moda íntima, camisas, bermudas, calças, cuecas e meias, jaquetas e casacos, moda praia, bodies, conjuntos, vestidos, shorts e bermudas, calçados, calças, moda praia, vestidos, moda íntima, casacos e jaquetas, calças, blusas, shorts e bermudas, perfumes, maquiagem, cosméticos masculinos, perfume feminino, acessórios, corpo e banho, celulares, kindle, tablets, fones de ouvido, caixa de som, and carregadores. The browser's taskbar at the bottom shows the search bar, task icons, system tray with temperature (29°C), location (Parc ensolarado), and date/time (16:13, 22/02/2024).

Vamos adentrar agora no plano do consentimento dado pelo titular quanto à disponibilização de seu dados e informações pessoais ao controlador, permitindo a este a utilização dos mesmos.

No *sítio* eletrônico da C&A há várias informações sobre a importância do aceite do titular quanto ao consentimento da utilização de seus dados pessoais, informando quais dados serão coletados.

O art. 5º, VI, da LGPD, traz o conceito de controlador: “pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais”.

6. Aviso de Privacidade para Clientes e Usuários de Canais C&A e C&A Pay. Disponível em: <https://www.cea.com.br/politica-de-privacidade>. Acesso em: 10/11/23.

Já o art. 5º, XII, da LGPD relata por sua vez o que é considerado consentimento: “manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada”.

Percebemos que há uma certa imposição ao titular, condicionando o fornecimento do produto ou serviço somente após obter-se seus dados pessoais. O art. 9º, § 3º, da LGPD, traz o alerta de que o usuário deverá ser informado sobre os seus direitos previstos no art. 18 do mesmo dispositivo legal.

Com isso, podemos dizer que o consentimento do titular vem da liberdade deste em manifestar o seu aceite ou não. Por sua vez, o operador fica atrelado à utilização dos dados pessoais apenas para a finalidade informada.⁷

A VULNERABILIDADE DAS INFORMAÇÕES PESSOAIS DISPONIBILIZADAS PELOS EMPREGADOS

No momento do aceite do usuário na página do *e-commerce* da C&A são coletadas diversas informações cadastrais de cunho pessoal do titular, tais como: nome e endereço completo, CPF, RG, carteira de habilitação, *e-mail*, gênero, data de nascimento, e etc; além de fotos dos respectivos documentos, o que gera uma certa insegurança jurídica.

O alerta está na autorização que foi dada ao controlador quanto ao compartilhamento dos dados pessoais do usuário, pois, com isso, empresas como a C&A, no nosso exemplo, poderão repassar informações pessoais para terceiros ou empresas parceiras, tais como: Cyamprev - sociedade de previdência privada, C&A Modas S.A, Instituto C&A, cartão de crédito C&A, envio de propagandas da C&A por *e-mail*, *smartphone*, algoritmos de *instagram*, e etc.

Outro alerta é que esses dados pessoais disponibilizados pelo usuário à C&A podem ser transferidos às prestadoras de serviços associadas localizadas fora do Brasil, conforme disposto no tópico 5, itens 5.1, 5.2 do termo de política de privacidade da C&A.

A preocupação está no fato de que tendo em vista que a C&A é uma empresa transnacional, presente não apenas no Brasil, mas também em outros países, como Alemanha, Holanda, Espanha, México, Portugal, dentre outros, fortalece o dever de cuidado destas empresas com o armazenamento e tratamento desse banco de dados pessoais em relação à dimensão extraterritorial que o compartilhamento mundo a fora de informações pode causar.

Quanto aos direitos dos usuários em relação à vigilância no manuseio dos seus dados pessoais, o tópico 7 do Termo de Política de Privacidade da C&A, presente no *site* da empresa, este não traz maiores detalhes sobre o prazo em que a C&A terá, por exemplo, para retificar quaisquer informações incorretas ou desatualizadas, disponibilizando apenas números de contato e preenchimento de formulário *online* de atendimento ao cliente.

7. Aviso de Privacidade para Clientes e Usuários de Canais C&A e C&A Pay. Disponível em: <https://www.cea.com.br/politica-de-privacidade>. Acesso em: 10/11/23.

No item 9 do Termo de Política de Privacidade da empresa, há a afirmação de que a C&A não se responsabiliza por conteúdos ou *links* repassados através de interações com *sites* de terceiros, não monitorando o modo como esses sítios eletrônicos coletam, armazenam e transferem informações do titular dos dados, o que dá margem à insegurança jurídica.

Por fim, no final do item 12 do referido termo, há a informação de que caso o usuário cadastre o seu *e-mail* no *site* da C&A e clique em enviar estará aceitando todos os termos de uso da C&A.

Nota-se, por todo o contexto, que ainda existe uma acentuada vulnerabilidade quanto à disponibilização de dados pessoais nos cadastros físicos das empresas ou dentro do ambiente virtual, restando uma certa margem de insegurança jurídica.

CONCLUSÃO

O presente artigo tratou sobre mecanismos de proteção de dados pessoais dos empregados dentro do ambiente de trabalho. Utilizou-se como base de pesquisa, legislações específicas sobre a política de governança e privacidade das informações personalíssimas fornecidas no meio laboral, possuindo como objetivo principal mostrar alguns programas de *compliance* utilizados na empresa C&A onde fora realizada uma pesquisa *in loco*.

O Conselho Administrativo de Defesa Econômica (CADE) dispõe que: “pequenas e médias entidades podem implementar programas de *compliance*, ainda que eles sejam mais modestos e contem com orçamentos muito reduzidos em face dos programas de grandes companhias” (CADE, 2016).

Podemos afirmar que a nova era digital, requer cuidado quanto ao tratamento normativo que se refere a proteção de dados pessoais, pois, envolve direitos fundamentais, constitucionalmente protegidos, como a vida privada, a intimidade, a honra, a imagem e a liberdade humana. Assim, tendo em vista a relevância dos direitos protegidos, tenta-se dirimir a utilização desenfreada dos dados pessoais do titular seja pelas instituições públicas ou privadas. (Silveira, 2023).

De acordo com Barros e Venturini, atividades estatais são pouco sujeitas a terem a veiculação de seus dados sem a devida autorização, no entanto, os particulares são alvos constantes de importunação às suas informações confidenciais, estando cada vez mais expostos à propagação de seus dados pessoais, sem o devido consentimento, seja por ato de agente público ou privado (Barros; Venturini, 2018, p. 43).

Diante desse cenário, observamos que deve-se haver zelo e cuidado com os dados pessoais dos usuários da *web*, pois, só é legalmente autorizado disseminar as informações do titular com o consentimento deste.

Dentro deste cenário as empresas privadas estão se utilizando do *compliance* adotando ações dentro do seu ambiente corporativo que visam garantir que as atividades prestadas não violem as normas vigentes, sendo uma política de comportamento adotada, também, pelas sociedades empresariais, organizações e instituições, como meio de prevenir a ocorrência de danos ou riscos, no ambiente empresarial, agindo conforme valores éticos.

Na política de *compliance*, caso não haja o consentimento livre do usuário, o controlador estará agindo de forma abusiva, desrespeitando as normas do CDC, conforme previsão do art. 39, inciso IX, e desobedecendo, também, os art. 5º, inciso XVII, art. 46 a 50 e art. 52, § 1º, incisos VIII a X, todos da LGPD, podendo ser penalizado com sanções administrativas.

A lei visa tutelar a privacidade e a liberdade do indivíduo. A norma jurídica tem por titular os direitos constitucionais e fundamentais da pessoa física, brasileira ou estrangeira, que digam respeito à proteção de dados tratados dentro do território nacional brasileiro.

Podemos dizer que o tema sobre proteção de dados pessoais faz parte, hoje, do processo evolutivo do direito digital, sendo considerado um direito fundamental autônomo (Mendes, 2014).

Com isso, a pessoa jurídica de direito privado deverá atuar de modo diligente, gerenciando os riscos no processo de tratamento, coleta e armazenamento dos dados de seus funcionários, evitando a ocorrência de danos e violação às normas contidas na LGPD, dirimindo riscos aos direitos fundamentais da pessoa humana em decorrência da desconformidade no tratamento dos dados pessoais por parte do controlador.

REFERÊNCIAS

ANDRADE, Flávio Carvalho Monteiro de; FERREIRA, Isadora Costa. *Compliance* trabalhista: compreendendo a prevenção de risco trabalhista por meio de programa de integridade. **Revista Síntese:** trabalhista e previdenciária. São Paulo, v. 28, n. 331, p. 73-84, jan. 2017.

ANTONIK, Luis Roberto. **Compliance, ética, responsabilidade social e empresarial:** uma visão prática. Rio de Janeiro: Alta Books, Edição do Kindle, 2016.

AMARAL, João Ferreira do. **Economia da informação e do conhecimento.** Coimbra: Almedina, 2009.

Aviso de Privacidade para Clientes e Usuários de Canais C&A e C&A Pay. Disponível em: <https://www.cea.com.br/politica-de-privacidade>. Acesso em: 10/11/23.

BAIÃO, Kelly Sampaio; GONÇALVES, Kalline Carvalho. **A garantia da privacidade na sociedade tecnológica:** um imperativo à concretização do princípio da dignidade da pessoa humana. *Civilistica*. com. Rio de Janeiro, a. 3, n. 2, jul./dez. 2014. Disponível em: Acesso em: 23 jun. 2019.

BENVENISTI, E. **The Law of Global Governance.** Hague Academy of International Law [s.l.]. AIL-Pocket, p.118, 2014.

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, p. 70-77, 2019.

_____; LUCIANO, Maria. O princípio da precaução na regulação de inteligência artificial: seriam as leis de proteção de dados o seu portal de entrada? In: FRAZÃO, Ana; MULHOLLAND, Caitlin (Org.). **Inteligência artificial e Direito: ética, regulação e responsabilidade**. São Paulo: Thomson Reuters Brasil, 2019.

BLUM, Renato Opice; ZAMPERLIN, Emelyn. **Compliance, responsabilidade empresarial e segurança da informação**. Lex Magister, Porto Alegre, 23 jun. 2016. Disponível em: [www.lex.com.br/doutrina_27159943_compliance_responsabilidade_empresarial_e_seguranca_da_informacao.aspx]. Acesso em: 26.10.2019.

CALIESS, Graf-Peter; RENNER, M. **Between law and social norms: the evolution of global governance**. Ratio Juris, v. 22, n. 2, p. 260-280, 2009.

CAMARGO, Coriolano Almeida; SANTOS, Cleorbete. **Fundamentos do compliance**. Edição do Kindle, 2019.

CANOTILHO, J.J. Gomes; SARLET, Ingo Wolfgang; STRECK, Lenio Luiz; MENDES, Gilmar Ferreira (Org.). **Comentários à Constituição da Brasil**. 2. ed. São Paulo: Saraiva, 2018.

CASTELLS, Manuel. **A sociedade em rede**. 3. ed. São Paulo: Paz e Terra, 2000.

CASTRO, Catarina Sarmiento e. **Direito da Informática, privacidade e dados pessoais**. Coimbra: Almedina, 2005.

COMPLIANCE TOTAL. **Pilares de um mecanismo de integridade e sistema de compliance**. Texto baseado no conteúdo do livro “*Compliance – A excelência na prática*” de Wagner Giovanini. 2014. Disponível em: [www.compliancetotal.com.br/compliance/pilares]. Acesso em: 14.10.2019.

CONSELHO ADMINISTRATIVO DE DEFESA ECONÔMICA (CADE). **Guia para programas de compliance**. Brasília, 2016. Disponível em:[www.cade.gov.br/aceso-a-informacao/publicacoes-institucionais/guias_do_Cade/guia-compliance-versao-oficial.pdf]. Acesso em: 11.01.2019.

CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana (Coord.). **Compliance: perspectivas e desafios dos programas de conformidade**. Belo Horizonte: Fórum, 2018.

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

_____. et al. **Considerações iniciais sobre inteligência artificial, ética e autonomia pessoal**. Pensar, Fortaleza, v. 23, n. 4, p. 1-17, out./dez. 2018.

EGGERS, W.; SCHATSKY, D.; VIECHNICKI, P. **AI-augmented government: using cognitive technologies to redesign public sector work**. [s.l.], 2017. Disponível em:. Acesso em: 5 ago. 2018.

FLORIDI, L. Soft ethics, the governance of the digital and the General Data Protection Regulation. **Philosophical transactions of the royal society a mathematical physical and engineering sciences**. Disponível em: Acesso em: 23 jun. 2019.

FRAZÃO, Ana; MEDEIROS, Ana Rafaela Martinez. Desafios para a efetividade dos programas de *compliance*. In: CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana (Coord.). **Compliance: perspectivas e desafios dos programas de conformidade**. Belo Horizonte: Fórum, p. 71, 2018.

_____ et al. **Artificial intelligence and the “Good Society”**: the US, EU, and UK approach. *Science and Engineering Ethics*, Springer, p. 1-24, 2017.

FRAZÃO, Ana; OLIVA, Milena Donato; ABILIO, Vivianne da Silveira. *Compliance* de dados pessoais. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (Coords.). *A lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters, **Revista dos Tribunais**, p. 677-715, 2019.

GOULART, Guilherme Damasio. Limites do BYOD: entre o poder do empregador e a proteção dos direitos da personalidade do empregado. **Revista de direito do trabalho**, São Paulo, v. 40, n. 159, p. 71-86, set.-out. 2014.

GUZMAN, Andrew T. **International Law: a compliance-based theory**. UC Berkeley Public Law and Legal Theory. Working Paper Series, Berkeley, CA, Paper n. 47, 2001.

HAN, Byung-Chul. **No exname: perspectivas do digital**. Trad. Lucas Machado. Petrópolis: Vozes, 2018.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. **Código das melhores práticas de governança corporativa**. 5. ed. São Paulo, SP: IBGC, 2015.

JANONI, Daniella; GIEREMEK, Rogéria. **Relações de trabalho e compliance: parceria necessária**. São Paulo, 01 fev. 2013. Disponível em: [www.administradores.com.br/noticias/carreira/relacoes-de-trabalho-e-compliance-parceria-necessaria/73122/]. Acesso em: 26.10.2019.

JOBIM, Rosana Kim. **Compliance e trabalho: entre o poder diretivo do empregador e os direitos inespecíficos do empregado**. Florianópolis: Tirant Lo Blanch, 2018.

KARAM-SILVEIRA, Marco Antonio. Lei de Acesso a Informações Públicas (Lei nº 12.527/2011) – Democracia, República e Transparência no Estado Constitucional. **Revista dos Tribunais**, v. 102, n. 927, p. 131-155, jan. 2013.

LAZZARIN, Sonilde Kugel; CAVAGNOLI, Fernanda Onzi. *Compliance* trabalhista. **Revista Fórum Justiça do Trabalho**. Belo Horizonte, v. 35, n. 417, p. 95-110, set. 2018.

LIMA MARQUES, Cláudia. **Contratos no Código de Defesa do Consumidor: o novo regime das relações contratuais**. 9. ed. São Paulo: Ed. RT, p. 884-885, 2019.

MADDEN, Mary. **Privacy, security, and digital inequality: how technology experiences and resources vary by socioeconomic status, race, and ethnicity**. Acesso em: 23 jun. 2019.

MAGALHÃES JUNIOR, Danilo Brum de. Gerenciamento de risco, *compliance* e geração de valor: os *compliance programs* como ferramenta para mitigação de riscos reputacionais nas empresas. **Revista dos Tribunais**, v. 997, n. 107, p. 575-594, nov. 2018.

MARQUES, Cláudia Lima. **Contratos no Código de Defesa do Consumidor: o novo regime das relações contratuais**. 9. ed. rev., atual. ampl. São Paulo: Ed. RT, 2019.

MATHIES, Anaruez. **Assédio moral e *compliance* na relação de emprego**: dos danos e dos custos e instrumentos de prevenção. Curitiba: Juruá, p. 131-181, 2018.

MEHR, H. **Artificial intelligence for citizen services and government**. [s.l.], 2017. Disponível em: Acesso em: 5 ago. 2018.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. **Curso de Direito Constitucional**. 13. ed. rev. e atual. São Paulo: Saraiva, p. 172-173, 2018.

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

_____. **Decisão histórica do STF reconhece direito fundamental à proteção de dados pessoais**. Jota, [s.l.], 10 maio 2020. Disponível em: Acesso em: 27 jun. 2020.

MILLER, Geoffrey P. **The compliance function**: an overview. NYU Law and Economics Research Paper, p. 14-36, nov. 2014.

MIRAGEM, Bruno. A Lei Geral de Proteção de Dados (Lei nº 13.709/2018 (LGL\2018\7222)) e o Direito do consumidor. **Revista dos Tribunais**, v. 1009, n. 108, p. 173-222, nov. 2019.

_____; FRAJHOF, Isabella Z. Inteligência artificial e a Lei Geral de Proteção de Dados Pessoais: breves anotações sobre o direito à explicação perante a tomada de decisões por meio de *machine learning*. In: FRAZÃO, Ana; MULHOLLAND, Caitlin (Org.). **Inteligência artificial e Direito**: ética, regulação e responsabilidade. São Paulo: Thomson Reuters Brasil, 2019.

MULHOLLAND, Caitlin. A tutela da privacidade na internet das coisas (IOT). In: MAGRANI, Eduardo (Org.). **Horizonte presente**: debates de tecnologia e sociedade. 1. ed. Rio de Janeiro: Letramento, v. 1, 2019.

MUNIZ, Mirella Karen de Carvalho Bifano; DIAS, Ronaldo Mayrink de Castro Garcia. **Compliance e direito do trabalho**: novas práticas para mitigar novos riscos. LTR Suplemento Trabalhista, São Paulo, v. 52, n. 094, p. 529-537, nov. 2016.

NEGRI, S. M. C. de Ávila; DE OLIVEIRA, S. R.; COSTA, R. S. **O uso de tecnologias de reconhecimento facial baseadas em inteligência artificial e o direito à proteção de dados**. *Direito Público*, [S. l.], v. 17, n. 93, 2020.

NORRIS, Clive. From personal to digital CCTV, the panopticon, and the technological mediation of suspicion and social control. In: LYON, David. **Surveillance as social sorting**: privacy, risk, and digital discrimination. Routledge: New York, 2003.

OLIVA, Milena Donato; SILVA, Rodrigo da Guia. Origem e evolução histórica do *compliance* no direito brasileiro. In: CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana (Coord.). **Compliance**: perspectivas e desafios dos programas de conformidade. Belo Horizonte: Fórum, p. 40-43, 2018.

ORGANIZACIÓN INTERNACIONAL DEL TRABAJO (OIT). **ILO Centenary Declaration**. Geneva: International Labour Office, 2019. Disponível em: [www.ilo.org/wcmsp5/groups/public/---ed_norm/---relconf/documents/meetingdocument/wcms_700622.pdf]. Acesso em: 03.11.2019.

ORWELL, George. 1984. Trad. Alexandre Hubner. São Paulo: **Companhia das Letras**. 2009.

PINHEIRO, Patrícia Peck Garrido. Nova lei brasileira de proteção de dados pessoais (LGPD) e o impacto nas instituições públicas e privadas. Sociedade da informação: inquietudes e desafios. **Revista dos Tribunais**, São Paulo, v. 1000, ano 108, p. 309-323, fev. 2019.

PURTOVA, Nadezhda. **The law of everything. Broad concept of personal data and future of EU data protection law.** Law, Innovation and Technology, v. 10, n. 1, p. 40-81, 2018.

REUTERS, Thomson. A cultura de *compliance* em matéria de proteção de dados e sua adoção no âmbito laboral. **Revista dos Tribunais Online**. vol. 214, p. 323 – 340, 2020.

RICHARDS, N. M.; SMART, W. D. **How should the law think about robots?**, 2013. Disponível em: Acesso em: jan. 2018.

RODOTÁ, Stefano. **A vida na sociedade de vigilância: a privacidade hoje.** Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

_____. **Some Remarks on Surveillance today.** European Journal of Law and Technology, Vol. 4, No. 2, 2013. Disponível em: Acesso em: 20 ago. 2019.

SILVEIRA, Marco Antonio Karam. Lei Geral de Proteção de Dados Pessoais e seu *compliance* para empresas privadas. **Revista de Direito Civil Contemporâneo**. vol. 35. ano 10. p. 247-285. São Paulo: Ed. RT, abr./jun. 2023.

SOUZA, Renato Rocha. Sobre a ética humana e a ética dos algoritmos. In: MAGRANI, Eduardo (Org.). **Horizonte presente: debates de tecnologia e sociedade**. 1. ed. Rio de Janeiro: Letramento, v. 1, 2019.

SPRATLING, Gary R. The experience and views of the enforcement community. In: **Corporate Crime in America: Strengthening the “good citizen” Corporation**. United States Sentencing Commission (Simpósio), p. 303-309, 1995.

STUCKE, Maurice. **In search of effective ethics & compliance programs.** The Journal of Corporation Law – University of Tennessee, v. 39, n. 4, p. 769-832, dez. 2013.

UNIÃO EUROPEIA. **Regulamento do Parlamento Europeu e do Conselho. Relativo à promoção da equidade e da transparência para os utilizadores profissionais de serviços de intermediação em linha.** Disponível em: [<https://data.consilium.europa.eu/doc/document/PE-56-2019-INIT/pt/pdf>]. Acesso em: 04.11.2019.

VERBEEK, P. Morality in design: design ethics and the morality of technological artifacts. In: VERMAAS, Pieter E.; KROES, Peter; LIGHT, Andrew; MOORE, Steven A. (Eds.). **Philosophy and Design: from Engineering to Architecture**. Dordrecht: Springer, p. 91-103, 2008.

WEBER, Rolf H. Internet of Things – New security and privacy challenges. **Computer Law & Security Review**, v. 26, n. 1, p. 23-30, 2010.

WECHSLER, H. **Reliable face recognition methods: system design, implementation and evaluation.** Springer, 2007.