

**II CONGRESSO INTERNACIONAL DE
DIREITO, POLÍTICAS PÚBLICAS,
TECNOLOGIA E INTERNET**

RELAÇÕES DE TRABALHO E TECNOLOGIA

R382

Relações de trabalho e tecnologia [Recurso eletrônico on-line] organização II Congresso Internacional de Direito, Políticas Públicas, Tecnologia e Internet: Faculdade de Direito de Franca – Franca;

Coordenadores: Iara Marthos Aguila, Presleyson Plínio de Lima e Rogerio Borba da Silva – Franca: Faculdade de Direito de Franca, 2024.

Inclui bibliografia

ISBN: 978-65-5274-013-7

Modo de acesso: www.conpedi.org.br em publicações

Tema: Regulação do Ciberespaço.

1. Relações de Trabalho. 2. Teletrabalho. 3. Subordinação Algorítmica. 4. Políticas Públicas de Desenvolvimento. 5. Efetividade do Direito. I. II Congresso Internacional de Direito, Políticas Públicas, Tecnologia e Internet (1:2024 : Franca, SP).

CDU: 34

II CONGRESSO INTERNACIONAL DE DIREITO, POLÍTICAS PÚBLICAS, TECNOLOGIA E INTERNET

RELAÇÕES DE TRABALHO E TECNOLOGIA

Apresentação

Entre os dias 27 e 30 de agosto de 2024, a Faculdade de Direito de Franca recebeu o Congresso Internacional de Direito, Políticas Públicas, Tecnologia e Internet. O evento reuniu acadêmicos, profissionais, pesquisadores e estudantes, promovendo o debate interdisciplinar sobre o impacto das inovações tecnológicas no campo jurídico e nas políticas públicas. A programação envolveu Grupos de Trabalho (GTs) organizados para aprofundar temas específicos, abordando desde o acesso à justiça até as complexidades da regulação tecnológica, com ênfase na adaptação do sistema jurídico aos avanços da inteligência artificial e da automação.

O GT 4 – Relações de Trabalho e Tecnologia explorou as profundas mudanças nas relações de trabalho provocadas pelo avanço tecnológico. O debate incluiu a automação e os desafios da proteção dos empregos na Indústria 4.0, além do impacto da subordinação algorítmica no trabalho gerido por aplicativos. A reforma trabalhista e a expansão do teletrabalho, impulsionada pela pandemia, foram temas de destaque, assim como as novas formas de contratação no ambiente digital e os desafios do BYOD ("Bring Your Own Device"). As discussões também abordaram a Data Economy, o crowdsourcing, as novas profissões e as formas emergentes de organização do trabalho, como o cooperativismo de plataforma e a organização coletiva de trabalhadores em rede. As contribuições deste GT propõem uma análise crítica e reflexiva sobre a adaptação do Direito do Trabalho às inovações tecnológicas e seus impactos sociais e jurídicos.

**A POLÍTICA DO BYOD NAS EMPRESAS: APLICAÇÃO DO COMPLIANCE
TRABALHISTA DIGITAL NA PROTEÇÃO DOS DADOS PESSOAIS**

**THE BYOD POLICY IN COMPANIES: IMPLEMENTING DIGITAL LABOR
COMPLIANCE FOR PERSONAL DATA PROTECTION**

**Maria Eduarda Marçal Vilela
Guilherme Lanzoni Martinelli**

Resumo

É indubitável que a sociedade se encontra em constantes evoluções em todos os seus aspectos. No âmbito trabalhista, a busca por flexibilidade e lucratividade, tanto por parte dos funcionários, quanto das organizações empresariais, tem levado à adoção do sistema “Bring Your Own Devices” (BYOD). O BYOD permite que os funcionários utilizem seus próprios dispositivos para acessar recursos corporativos, proporcionando flexibilidade e mobilidade no trabalho. Contudo, essa prática apresenta riscos significativos à segurança dos dados corporativos. Dessa forma, o presente estudo analisa a importância do Compliance Trabalhista Digital, na mitigação desses riscos, garantido conformidade com as leis de proteção de dados.

Palavras-chave: Byod, Dados pessoais, Compliance

Abstract/Resumen/Résumé

It is indubitable that society is in constant evolution in all its aspects. In the labor sphere, the pursuit of flexibility and profitability by both employees and business organizations has led to the adoption of the “Bring Your Own Devices” (BYOD) system. BYOD allows employees to use their own devices to access corporate resources, providing flexibility and mobility at work. However, this practice presents significant risks to corporate data security. Therefore, this study analyzes the importance of Digital Labor Compliance in mitigating these risks, ensuring compliance with data protection laws.

Keywords/Palabras-claves/Mots-clés: Byod, Personal data, Compliance

1. INTRODUÇÃO

A sociedade se encontra em constante evolução frente ao uso da tecnologia e meios de trabalho. Na última década, a adoção do sistema “*Bring Your Own Devices*” (*BYOD*) tem sido amplamente discutida e aceita pelas empresas que têm a possibilidade de implementar tal política a seus funcionários.

O conceito do BYOD refere-se à prática de permitir ou solicitar que seus funcionários desenvolvam suas tarefas e acessem os recursos da empresa através de seus próprios dispositivos pessoais, sejam eles *smartphones*, *laptops*, *tablets*, etc.

A ascensão e constante aplicação concreta de tal política laboral se deve ao fato de que, em um mundo cada vez mais conectado e globalizado, a flexibilidade e principalmente, a mobilidade no trabalho, tem sido impulsionadores frente os funcionários e, conseqüentemente, às empresas. O ideal de poder realizar suas tarefas de maneira remota e em qualquer localidade, bem como o equilíbrio entre profissional e pessoal são argumentos incentivadores e atrativos aos empregados, primordialmente na procura por vagas de emprego.

Ademais, pela visão da empresa, a adoção do BYOD pode trazer diversos benefícios, podendo-se citar maior lucratividade e rendimento dos funcionários, dinamização e flexibilidade, bem como economia de custos em relação à equipamentos.

Contudo, existem também riscos inerentes à política do BYOD nas redes corporativas, primordialmente quanto à segurança dos dados pessoais em posse da empresa e seu tratamento adequado, os quais podem ser frutos da ausência de estratégias corretas e que permitam a dinamização da política no âmbito legal.

Não pairam dúvidas de que ao permitir a utilização de dispositivos alheios à empresa, a vulnerabilidade frente à ataques e ameaças cibernéticas, capazes de ocasionar vazamento de informações e dados em responsabilidade da pessoa jurídica, é exponencialmente aumentada, principalmente quando tratamos da riqueza e poder que um dado pessoal é capaz de gerar.

É nesse cenário que a empresa adotante do sistema BYOD pode socorrer-se através do Compliance Trabalhista Digital, aplicando políticas e regulamentos a fim de reduzir a possibilidade de ataques aos dados pessoais corporativos, podendo ser uma medida extremamente viável ao ente empresarial se aplicado e elaborado corretamente frente a realidade da pessoa jurídica e seus funcionários ao caso concreto.

O Compliance envolve a implementação de políticas e procedimentos que garantam a conformidade com leis e regulamentações, como no caso da proteção de dados, aplicando-se corretamente legislações como a GDPR na Europa ou a LGPD no Brasil. Isso inclui a adoção de medidas de segurança robustas, como criptografia, autenticação multifator e gestão de dispositivos móveis (MDM), além de programas de treinamento contínuo para os funcionários sobre práticas seguras de uso de tecnologia.

A implementação das políticas do Compliance não só protegem os dados sensíveis da empresa, mas também preserva a reputação da organização e evita possíveis penalidades legais, garantindo assim, o sucesso do sistema BYOD, o qual será objeto de estudo do presente resumo.

Para tanto, a metodologia utilizada consiste em uma revisão de literatura, com extensa pesquisa bibliográfica, documental e exploratória, a partir de legislação, doutrinas, jurisprudências, artigos científicos, revistas e relatórios nacionais e internacionais, jornais, tabelas estatísticas, e todo material que agregue fundamentação teórica sobre o tema.

Dessa forma, o presente trabalho teórico debruça-se sobre a análise em temas relevantes ao estudo da importância do Compliance em empresas que adotam o sistema BYOD com a finalidade de assegurar a efetividade da proteção de dados pessoais sob posse da pessoa jurídica.

2. DESENVOLVIMENTO

2.1 O SISTEMA BYOD

O termo BYOD, sigla para “*Bring Your Own Devices*” (Traga Seu Próprio Dispositivo), dentro de um ambiente empresarial, refere-se à prática de permitir que os funcionários utilizem seus próprios dispositivos tecnológicos para realizarem as tarefas, pelas quais são responsáveis.

No cenário empregatício atual, a demanda por empregos que ofereçam maior flexibilidade e liberdade para a realização das funções é alta e tende a crescer exponencialmente, assim como a demanda por lucratividade e redução de gastos. Diante desse contexto, o BYOD oferece diversas vantagens e tem sido amplamente aceito tanto pelas empresas, que buscam melhores resultados e maior lucratividade, quanto pelos

funcionários, que valorizam a flexibilidade e liberdade no modo de trabalho, sendo capaz de conciliar interesses de todas as partes envolvidas em uma relação trabalhista (Moretti, 2013).

As organizações reconhecem que esta prática pode ser benéfica, especialmente em termos de flexibilidade e eficiência, uma vez que funcionários que utilizam seus próprios dispositivos tendem a ser mais confortáveis e eficientes, já que estão familiarizados com o equipamento. Além disso, o sistema pode facilitar o trabalho remoto e a colaboração, especialmente em tempos de pandemia, quando o trabalho a distância se tornou uma necessidade. (Yeboah-Boateng; Boaten, 2021).

Embora sejam translúcidos os diversos benefícios gerados pela adoção do sistema BYOD, a implementação do mesmo acarreta diversos desafios, principalmente quando relacionados à segurança dos dados pessoais que estão em posse da empresa adotante.

2.2 A PROTEÇÃO DOS DADOS PESSOAIS NO SISTEMA BYOD

É sabido que a sociedade contemporânea está inserida no contexto da supervalorização dos dados pessoais, tendo em vista a grande riqueza e quantidade de informações que os mesmos podem gerar, sendo até mesmo taxados como “novo petróleo” (Parkins, 2017).

A busca pela proteção dos dados pessoais tem sido cenário de grandes debates e pesquisas, trazendo mudanças no mundo legislativo, como a criação da Lei Geral de Proteção de Dados (LGPD) no Brasil, inspirada no modelo da *General Data Protection Regulation* (GDPR), legislação digital da União Europeia.

Ambas as legislações versam sobre como devem ser coletados, tratados, protegidos e até mesmo descartados os dados pessoais oriundos de uma empresa, independente de seu caráter público ou privado, sendo prevista a aplicação de sanções aos casos de descumprimento das leis.

Diante disso, adentrando ao âmbito da proteção de dados pessoais no sistema BYOD, é possível perceber que a utilização de dispositivos pessoais dos funcionários para a realização das tarefas profissionais, são capazes de gerar uma grande vulnerabilidade na tutela dos mesmos, uma vez que os riscos de vazamento e ciberataques são maiores quando comparados ao método tradicional de trabalho presencial.

Isso pois, tais incidentes podem decorrer de práticas inseguras, como a utilização de redes Wi-Fi públicas ou a falta de atualização dos dispositivos. A ausência de controle centralizado sobre os dispositivos pessoais limita a ação das empresas em garantir a segurança de suas informações sensíveis, como os dados pessoais.

Dessa forma, para mitigar esses riscos, as empresas devem implementar políticas robustas de segurança e privacidade no contexto do BYOD.

2.3 APLICAÇÃO DO COMPLIANCE DIGITAL TRABALHISTA FRENTE À POLÍTICA BYOD NAS EMPRESAS

A adoção do programa de Compliance deve ser implementada frente à realidade de cada ente empresarial, sob a análise do perfil e riscos da pessoa jurídica, adotando-se medidas e regras a fim de prevenir problemáticas, detectando falhas e aperfeiçoando programas que facilitem o monitoramento contínuo da empresa.

Nesse ínterim, não há obrigatoriedade de medidas a serem adotadas, devendo sempre ser analisada a realidade da empresa ao caso concreto, como no caso da política do BYOD, na qual a prioridade é a preservação dos dados corporativos, em consonância ao direito à privacidade e proteção de dados pessoais dos funcionários e os limites do poder diretivo do empregador (Gularte, 2021).

O programa de Compliance voltado à política BYOD deve estabelecer diretrizes claras, definindo em contrato os tipos de dispositivos que podem ser utilizados pelos funcionários, as aplicações que podem ser acessadas e os procedimentos a serem adotados no caso de furto e perda dos dispositivos pessoais, demonstrando a responsabilidade e expectativas dos empregados em relação aos dados.

Ademais, a empresa possui sua responsabilidade quanto ao fornecimento de ferramentas de segurança aos funcionários, como VPNs, antivírus, sistema de gestão de criptografia de dados, promovendo atualizações e treinamentos de capacitação aos obreiros.

Uma estratégia deve ser traçada como o *Mobile Device Management* (MDM), a gestão de dispositivos móveis, na qual infere-se o gerenciamento centralizado do que é permitido acessar na empresa, os dados a serem infiltrados nos dispositivos móveis dos empregados, valendo-se do monitoramento dos aparelhos individuais de forma remota e integrada (Cunha; Castro, 2014).

Nesse sentido, o Compliance corporativo deve traçar estratégias eficazes e pragmáticas entre empresa e funcionário, entre profissional e pessoal, na qual o compartilhamento de dados seja estrito aos interesses do ente empresarial e do cumprimento dos direitos inerentes à privacidade dos seus empregados.

3. CONCLUSÃO

A política do BYOD está inserida em diversas empresas brasileiras, sendo fomentada pelo avanço tecnológico e as novas tendências de trabalho, optando os entes empresariais pela maior liberdade, flexibilização e mobilidade da atividade laboral em relação aos seus funcionários.

Observa-se que com o advento do BYOD, há uma inovação não só na relação entre empresa e funcionário, visto que há a utilização de equipamentos pessoais para uso laboral, mas também um novo cenário quanto à proteção do direito à privacidade do usuário e informações gerais e dados da pessoa jurídica.

A nova política laboral, embora apresenta sua respectiva vantagem em relação à custos com equipamentos por parte da empresa e proporcionando maior liberdade e dinamismo na execução de atividades, também conduz a responsabilidade do compartilhamento e tratamento dos dados pessoais de empregados e da próprio ente empresarial, conflitando entre o meio profissional e pessoal.

Nesse ínterim, o presente resumo expôs a importância de programas internos nas empresas que sejam capazes de regulamentar e fiscalizar o tratamento e condicionamento dos dados pessoais no sistema BYOD, como objeto de estudo, os programas de Compliance, os quais são essenciais a fim de estabelecer medidas eficazes frente à proteção de dados, em consonância à legislação vigente e a redução de possíveis danos face à pessoa jurídica.

Para tanto, foram expostas medidas que podem ser adotadas pelas empresas, organizando diretrizes claras e capazes de centralizar o tratamento dos dados pessoais de modo seguro e que possam ser hábeis a neutralizar e prevenir qualquer risco inerente ao uso de equipamentos próprios em relação aos dados fornecidos pela empresa, seja quanto ao uso para trabalho; delimitar quais dados são permitidos acessar; procedimentos em caso de furto ou estrago do aparelho; fornecimento de ferramentas de segurança; gestão de dispositivos móveis, dentre outras estratégias.

Destacou-se que não há obrigatoriedade em quais medidas devem ser adotadas pela empresa, devendo sempre analisar as possibilidades ao caso concreto e perante a realidade da empregadora, detectando possíveis falhas e aplicando medidas proporcionais a fim de conduzir a menor exposição e risco dos dados pessoais frente à execução das atividades laborais.

Desse modo, a pesquisa em comento debruçou-se frente a política do BYOD nas empresas e a relevância dos programas de Compliance com o finalidade de prevenir riscos e violações aos direitos pessoais entre pessoa jurídico e física, proporcionando o equilíbrio entre relação profissional e pessoal, adotando medidas que cumpram as determinações legais e que atendam a realidade da empresa no cenário econômico, jurídico e social.

REFERÊNCIAS

CUNHA, Ilane KB; CASTRO, Rita CC. Gestão da Segurança da Informação em ambientes BYOD: Um mecanismo de apoio baseado nas boas práticas ITIL. **Anais do Encontro Anual de Tecnologia da Informação**, v. 4, n. 1, p. 32-32, 2014.

GULARTE, Caroline de Melo Lima. **A proteção de dados pessoais no uso de tecnologia na relação de emprego: efeitos do Compliance Trabalhista Digital nas negociações Coletivas – PUC/RS**. Londrina, PR. Editora Thoth, 2021.

MORETTI, João. **BYOD: como as empresas devem avaliar e se precaver**. Disponível em: <https://www.tiespecialistas.com.br/byod-como-as-empresas-devem-avaliar-e-se-precaver/> Acesso em: 05 jul. 2024.

PARKINS, David. *The world's most valuable resource is no longer oil, but data*. The Economist, London, v. 425, n. 9075, p. 20-22, 6 mai. 2017. Disponível em: <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>. Acesso em: 10 jul. 2024.

UZ, Gabriel; RICCI, Gabriel; FERREIRA, Lucas. **BYOD e DLP: Implementando soluções de segurança para Prevenção de perda de dados. Trabalho de conclusão de curso (Curso Superior de Tecnologia em Segurança da Informação) - Faculdade de Tecnologia de São Caetano do Sul - Antonio Russo, São Caetano do Sul, 2020.**

YEBOAH-BOATENG, Ezer Osei; BOATEN Francis Edmund. *Bring-Your-Own-Device (BYOD): An Evaluation of Associated Risks to Corporate Information Security*. International Journal in IT and Engineering, Impact Factor - Vol. 4, nº 5.343, Agosto de 2016. Disponível em: <https://arxiv.org/abs/1609.01821>. Acesso em: 05. jul. 2024.