İSTANBUL UNIVERSITY PRESS

Annales de la Faculté de Droit d'Istanbul, 75: 225–253

DOI: 10.26650/annales.2024.75.0009
http://annales.istanbul.edu.tr/

Annales de la Faculté de Droit d'Istanbul

Submitted: 16.07.2024
Revision Requested: 05.08.2024
Last Revision Received: 21.08.2024
Accepted: 21.08.2024
Published Online: 27.09.2024

RESEARCH ARTICLE

Implementation of the Concept of "Bring Your Own Device" (BYOD) within the Scope of Labour Law

Hasan Alparslan Ayan*

Abstract

The process of digitalisation has a profound impact on the global landscape. The ramifications of this phenomenon on the workforce are inescapable. Technological developments exert an influence on employment relationships. From this point forward, information technology (IT) devices will become a requisite component for employees in order to fulfil the obligations inherent to an employment contract. It is therefore becoming more common for employees to use the devices they bring to the workplace. The concept of BYOD (Bring Your Own Device) refers to the use of an employee's personal IT devices for work-related purposes. Concurrently, this situation leads to issues within the employment relationship. To resolve these issues, it is essential to consider the BYOD concept within the context of labour law. The aim of this study is to evaluate the characteristics of the BYOD concept in employment relationships in comparison with German and Turkish labour law. In consideration of the nature of BYOD, only situations of the utilisation of IT devices will be addressed, and the use of other work resources will not be subject to evaluation. Although there is no direct court decision on the BYOD, the decisions of the Turkish Constitutional Court and the Court of Cassation, as well as the German Federal Labour Court and the Court of Justice of the European Union, which pertain to this concept, will be included in this study. As the primary focus of this article is on the BYOD concept, a concise overview of alternative concepts is provided. After this juncture, the employer's right of the management and workplace practises will be analysed within the context of BYOD. In the context of the use of personal IT devices within the framework of the employment relationship, certain issues emerge that affect the work and rest periods of employees. In addition, the BYOD application is inextricably linked to the issue of personal data. It is an inevitable consequence of the BYOD that an employee's personal data, in conjunction with third parties, will be on the IT devices. Therefore, measures have been developed to protect personal data on IT devices. These topics will be explained under mobile device management (MDM) tools. The final issue to be addressed is the legal status of software on the employee's IT devices. In this context, the issues of intellectual property rights and licencing agreements will also be discussed in a separate section dedicated to the BYOD.

Keywords

BYOD, Types of BYOD, Employment Contract, Employer's Liability, Employee Claims, Appropriate Remuneration, Mobile Device Management (MDM)

***Corresponding Author:** Hasan Alparslan Ayan (Res. Asst. Dr.), Necmettin Erbakan University, Law Faculty, Department of Labour and Social Security Law, Konya, Turkiye. E-mail: hayan@erbakan.edu.tr ORCID: 0000-0002-9991-9492
To cite this article: Ayan HA, "Implementation of the Concept of "Bring Your Own Device" (BYOD) within the scope of Labour Law", (2024) 75 Annales de la Faculté de Droit d'Istanbul 225. https://doi.org/10.26650/annales.2024.75.0009

Introduction

The utilisation of information technologies (IT), including computers, tablets, and smartphones, has become an indispensable aspect of contemporary working practises. Previously, there was a clear delineation between the technological resources provided by the employer and those of the employee. However, this boundary is becoming blurred, as an increasing number of employees prefer to use personal IT devices in their workplaces[1]. Research indicates that candidates expect their potential employers to permit them to use their existing personal IT devices for work[2]. The widespread acquisition and leasing of these devices, coupled with employers' efforts to reduce investment costs, have integrated these tools into the operational processes of workplaces[3].

On the whole, this approach may appear to be advantageous to both parties to the employment contract. However, the concept of BYOD in employment relationships causes some legal conflicts, few of which have been analysed to date. In the absence of legal regulations regarding the BYOD, the parties to the employment contract should shape the framework for its use. This leads to unresolved issues. Issues are of central importance and encompass a number of key areas, including cost, liability, maintenance/repair, working/resting periods, the limits on the usage rights of employees' devices, data protection, intellectual property rights and licence agreements[4].

I. Concepts

A. BYOD: "Bring Your Own Device"

In the United States, the utilisation of personal IT devices in the workplace is discussed under the concept of *"Bring Your Own Device" (BYOD)*[5]. Similarly, in Germany, the concept is referred to as *"Bring dein eigenes Gerät mit (und nutze es für*

1 Gerlind Wisskirchen and Jan Peter Schiller, 'Aktuelle Problemstellungen im Zusammenhang mit „Bring Your Own Device"' [2015] Der Betrieb 1163, 1163; Dirk Pollert, 'Arbeitnehmer-Smartphone als Betriebsmittel – ein kostensparendes Modell?' NZA-Beilage 152, 152.

2 For further details regarding the results of the study, please refer to the following. Jin Hwa Lee and Hasan Tinmaz, 'A Perceptional Analysis of BYOD (Bring Your Own Device) for Educational or Workplace Implementations in a South Korean Case' (2019), 6 Participatory Educational Research, 51, 61. See also Christian Hoppe, 'Bring your own device (BYOD)' in Stefan Kramer (ed), *IT-Arbeitsrecht* (3rd edn, CH BECK 2023) para 726.

3 Oliver Zöll and Jacek B Kielkowski, 'Arbeitsrechtliche Umsetzung von „Bring Your Own Device" (BYOD)' [2012] Betriebs-Berater, 2625, 2625.

4 Wisskirchen and Schiller (n 1) 1163; Ferdinand Grieger, 'Bring Your Own Device in Der Unternehmenspraxis' [2023], MMR 168, 168.

5 Shefiu Olusegun Ganiyu and Rasheed Gbenga Jimoh, 'Characterising Risk Factors and Countermeasures for Risk Evaluation of Bring Your Own Device Strategy' (2018) 7 International Journal of Information Security Science, 49, 49.

die Arbeit)"[6]. The concept is also prevalent in Turkish law as *"Kendi Cihazını Getir"*[7]. The focus is on employees using their own devices for work-related purposes, both within and outside the workplace, and reaching an agreement with their employer on this matter[8]. The term "IT device" should be understood to encompass a broad range of technical work tools capable of inputting and outputting information, such as smartphones, laptops, tablets, wearable technologies, in as well as computer programs/softwares, databases, internet services, and digital platforms installed on these devices[9].

The BYOD can be defined in a variety of ways. First, it refers to an employee using his/her own IT devices to replace workplace tools[10]. Although the employer is legally obliged to provide the necessary tools for the job, the parties may agree that the employee will provide his/her own equipment. In this case, the employer avoids the cost of maintaining IT devices in the workplace[11]. Second, BYOD can be applied on an optional basis. In this case, the employer does not relinquish their responsibility to provide devices; instead, the employer allows the employee to use his/her own devices within the work organisation[12]. Third, the parties may not regulate BYOD practises. This implies that although the employer tolerates the use of personal devices, no binding conditions are set forth in the employment contract. This practise is known as *"BYOD Wildwuchs"* and is not recommended due to the significant risks it poses to company data[13].

The consequences of implementing a BYOD policy are contingent on the specific types of BYOD models selected. The utilisation of BYOD as a replacement for workplace tools may reduce costs, electronic waste, and energy consumption.

6 Wolfgang Däubler, *Digitalisierung und Arbeitsrecht* (7th edn, Bund Verlag 2020) 99; Stefan Bartz and Marco Grotenrath, '„Bring Your Own Device"-Geräte in internen Ermittlungen' [2019] CCZ 184, 184; Burkard Göpfert and Elena Wilke, 'Nutzung privater Smartphones für dienstliche Zwecke' [2012] NZA 765, 765.

7 Ulaş Baysal, 'İşçiye Ait Taşınabilir İletişim Cihazlarının İş Amaçlı Kullanılması' [2018] Sicil İş Hukuku Dergisi 65, 66.

8 Hoppe (n 2) para 726; Ganiyu and Jimoh (n 5) 49; Däubler (n 6) 99. The concept of bring-your-own-device (BYOD) inherently pertains to the utilisation of personal IT devices by employees. See, Christine Monsch, *Bring Your Own Device (BYOD): Rechtsfragen der dienstlichen Nutzung arbeitnehmereigener mobiler Endgeräte im Unternehmen* (Duncker & Humblot 2017) 22; Wisskirchen and Schiller (n 1) 1163; Pollert (n 1) 153. For an explanation of the BYOD types, see COPE, POCE, and CYOD concepts.

9 Alexander Raif and Philipp Nann, 'Arbeitsrecht 4.0 – Möglichkeiten und Hürden in der digitalen Arbeitswelt' [2016] GWR 221, 222; Isabell Conrad and Jochen Schneider, 'Einsatz von „privater IT" im Unternehmen Kein privater USB-Stick, aber „Bring your own device" (BYOD)?' [2011] ZD 153, 153. For the relationship between Industry 4.0 and BYOD, see Jens Günther and Matthias Böglmüller, 'Arbeitsrecht 4.0 – Arbeitsrechtliche Herausforderungen in der vierten industriellen Revolution' [2015], NZA 1025, 1030.

10 Falk Müller, 'Bring Your Own Device (BYOD) im öffentlichen Dienst' [2021], öAT 23, 23. One perspective on the literature addresses the issue under two headings: real BYOD (allowing the use of a private devices for work purposes) and unreal BYOD (consenting to the private use of a workplace IT devices). See, Grieger (n 4) 168. For the concept of workplace tools (Arbeitsmittelbegriff), see Daniel Klocke and Sophia Hoppe, 'Der Anspruch auf essenzielle Arbeitsmittel' [2022], NZA-RR 515, 516.

11 Wisskirchen and Schiller (n 1) 1163; Stefan Kascherus and Martin Pröpper, 'Bring your own device (BYOD) - Mitbestimmung bei der Nutzung privater technischer Geräte' [2021], Betriebs-Berater 756, 756.

12 This option represents the most prevalent form of BYOD in Germany, as not all employees are willing or able to use personal IT devices for work-related purposes. See Monsch (n 8) 24; Hoppe (n 2) 729.

13 Monsch (n 8) 24; Zöll and Kielkowski (n 3) 2625.

Nevertheless, if it has an adverse effect on productivity, it will cease to be a viable option. Similarly, in the case of optional BYOD practises, additional expenses may be incurred, such as those associated with the protection of company data or the updating of software on personal devices. It is therefore unsurprising that certain concepts were developed to mitigate the disadvantages associated with the BYOD[14]. It is crucial to engage in discourse on these related concepts to gain a deeper understanding of the matter at hand.

B. COPE – "Corporate-Owned, Personally-Enabled"

This alternative model is distinct from BYOD, where the employer is responsible for providing the IT device. The employee is permitted to use the device for personal purposes and to configure it according to personal preferences[15].

In this model, the employee is responsible for ensuring that software is updated and that the technical functionality of the device is maintained. This includes the performance of maintenance and repair tasks. To safeguard the confidentiality of company data, the employer is responsible for installing the software on the device in advance. As the employee does not own the device, it is more convenient to monitor, remotely control, and ensure data security. Nevertheless, since the employer retains the financial responsibility for the purchase of the device and the employee is unable to utilise their own device, the anticipated cost savings and employee satisfaction that are purported to be achieved through the implementation of the BYOD policy are not realised[16].

C. POCE – "Personally-Owned, Corporate-Enabled"

In contrast to the COPE model, the IT device in question is owned by an employee. Although the employee utilises the device for work-related purposes, the operating system and software remain the property of the employee. Nevertheless, the employer is obliged to pay a lump sum in advance for the provision of the device, and the employee is obliged to grant the employer the necessary permission for remote access to the device[17].

D. CYOD – "Choose Your Own Device"

In this model, the employee is afforded a discretionary right regarding the IT device they will use; however, there are also predetermined IT devices provided by

14 Raif and Nann (n 9) 222; Grieger (n 4) 169; Göpfert and Wilke (n 6) 766; Däubler (n 6) 99.

15 Thomas Faas, 'WhatsApp & Outlook auf dem beruflichen Smartphone: Haftungsrisiken und Auswege' [2018] ArbRAktuell 594, 594; Baysal (n 7) 73; Ganiyu and Jimoh (n 5) 49.

16 As a prerequisite for COPE is the possession of the requisite technical expertise in support and maintenance, its use is recommended solely for employees with technical backgrounds in these fields. See Hoppe (n 2) para 727.

17 Bartz and Grotenrath (n 6) 184–185.

the employer[18]. As the tools used for work are the property of the employer, the employer is entitled to set usage conditions and limits, even if the employee uses the device for personal purposes[19]. In contrast to COPE, an employer is also responsible for providing device support and maintenance, thereby eliminating the need for an employee to possess specific technical expertise to operate the device[20]. The option to use personal devices may enhance employee satisfaction and productivity[21].

II. Legal basis for BYOD and contractual parties' agreement

A. Employer's right to management

Turkish law does not regulate the use of personal devices for work. The utilisation of IT devices for work purposes raises many concerns related to privacy, personal data protection, and the condition of the work. To obviate uncertainty and avoid litigation, it is imperative to establish a legal framework for BYOD and to delineate the obligations of the relevant parties[22].

In the event that the work assigned to the employee is only broadly outlined in the employment contract, as stipulated by Article 399 of the Turkish Code of Obligations No. 6098 (TCO), the employer must specify the content, place, and time of the work to be performed in a concrete manner[23]. In general, an employer is entitled to exercise his/her managerial prerogatives to determine and modify working conditions without the consent of the employee, provided that this does not constitute a significant alteration and does not contravene the legal standards[24]. Therefore, the determination right of the employer is applicable only in instances where the working conditions have not been determined by legal provisions, collective bargaining, employment contracts, or workplace practises[25].

18 Regarding CYOD, see Hoppe (n 2) para 727; Wisskirchen and Schiller (n 1), 1163.

19 Baysal (n 7) 73.

20 Any use of the IT device for purposes other than work can be defined as private use. For a detailed delineation of the distinctions between private and work-related use, see: Zeki Okur, *İş Hukuku'nda Elektronik Gözetleme* (Legal Yayıncılık 2013) 147.

21 Monsch (n 8) 27; Hoppe (n 2) para 726; Günther and Böglmüller (n 9) 1030.

22 Unlike Turkish legislation, German law allows for regulating BYOD in employment contracts with the involvement of the work council in accordance with 87 BetrVG. For further insight, see Kascherus and Pröpper (n 11) 756; Günther and Böglmüller (n 9) 1031; Conrad and Schneider (n 9) 157; and Däubler (n 6) 102.

23 Sevgi Dursun Ateş, *İşverenin Yönetim Hakkı* (Seçkin Yayıncılık 2019) 54. In terms of Turkish law, on the legal consequences of an employer's right to management, see Tankut Centel, *Introduction to Turkish Labour Law* (Springer 2017) 15; Ömer Ekmekçi, M Refik Korkusuz and Ömer Uğur, *Turkish Individual Labour Law* (2nd edn, Onikilevha Yayıncılık 2023) 33–34. See also, Şebnem Kılıç, 'Employment Law' in Şebnem Kılıç (ed), *Introduction to Turkish Business Law* (Peter Lang 2022) 165.

24 Dursun Ateş (n 23) 29. In accordance with the employer's orders, the employee is duty-bound to adhere to the instructions provided. For a comprehensive examination of this topic within the context of Turkish law, see Toker Dereli, Yeşim Pınar Soykut Sarıca and Aslı Taşbaşı, *Labour Law in Turkey* (3rd edn, Kluwer Law International 2023) 141.

25 Nuri Çelik and others, *İş Hukuku Dersleri* (36th edn, Beta Yayınevi 2023) 312; Mollamahmutoğlu Hamdi, Muhittin Astarlı and Ulaş Baysal, *İş Hukuku* (7th edn, Lykeion 2022) 85; Sarper Süzek, *İş Hukuku* (23rd edn, Beta Yayınevi 2023) 85. In accordance with Gewerbeordnung 106, the onus falls upon the employer to provide a more detailed delineation of the specific content, location and time of the tasks to be performed. See also Kascherus and Pröpper (n 11) 757.

It is evident that an employer's management rights do not constitute a legal basis for BYOD[26]. IT devices owned by the employee are not subject to the employer's instructions. In accordance with Article 413/I of the TCO, unless otherwise agreed or customary, the employer is obliged to provide the necessary tools and materials for work. Otherwise, the employer will be in default for failing to perform preparatory acts necessary for the execution of the work, which will result in continuing payment obligations under Article 408 of the TCO[27]. Furthermore, in accordance with Article 24/II-f of the Labour Act No. 4857 (LA), failure to comply with the stipulated working conditions will entitle the employee to terminate the contract without further notice[28]. Consequently, the extent to which the employee will use personal tools for work purposes and the manner in which such use will be undertaken is a matter for agreement between the parties[29].

Instructions to employees to use their own IT devices instead of those in the workplace is an extension of management rights. However, this does not concretise existing obligations; rather, it expands them and transfer employer responsibilities to the employee. This exceeds the limits of the legitimate authority to issue instructions[30]. The implementation of a BYOD policy requires a clear delineation of the respective responsibilities associated with the use of personal IT devices at work[31].

B. Agreement with the Employment Contract

It can be argued that the most crucial tool in regulating the implementation of BYOD is, in fact, employment. The prevailing view in the literature is that the BYOD must be explicitly agreed upon in the employment contract or addendum[32]. This perspective posits that establishing a BYOD model through legal relationships outside the employment relationship, such as through lease agreements, is never in the interests of the employee. This is because a legal relationship outside an employment contract lacks the principles and protections intended to protect the employee[33].

26 Müller (n 10) 23; Kascherus and Pröpper (n 11) 761.

27 Baysal (n 7) 67; Süzek (n 25) 500. A similar conclusion can be reached regarding German law. See Däubler (n 6) 99.

28 For a decision on this topic, please see. Court of Cassation, 9th Division, 8.12.2020, 2016/29695, 2020/17632, (lexpera.com.tr), accessed 09.07.2024.

29 Hoppe (n 2) para 729; Grieger (n 4) 169; Baysal (n 7) 68; Efe Yamakoğlu, *Bilişim Teknolojilerinin Kullanımının İş Sözleşmesi Taraflarının Fesih Hakkına Etkisi* (Onikilevha Yayıncılık 2020) 104.

30 Wisskirchen and Schiller (n 1) 1166; Zöll and Kielkowski (n 3) 2626; Däubler (n 6) 100.

31 Hoppe (n 2) para 729.

32 For a detailed examination of the characteristics of the employment contract, see M. Refik Korkusuz and Ömer Uğur, 'Turkish Individual Labour Law' in M Refik Korkusuz and Ferna İpekel Kayalı (eds), Turkish Private Law (3rd edn, Seçkin Yayıncılık 2024) 114; Centel (n 23) 67; Dereli and others (n 24) 81; Kılıç (n 23) 177. Parties to the employment contract may deviate from the principle of the provision of work equipment by the employer and may agree on the use of the employee's own work equipment in accordance with the BYOD concept. On this subject, see Katja Chandna-Hoppe, 'Essentielle Arbeitsmittel und mobile Arbeit' [2023], RdA 152, 157. For those who adhere to this viewpoint, see Monsch (n 8) 31; Pollert (n 1) 154; Däubler (n 6) 101.

33 Müller (n 10) 23; Grieger (n 4) 169.

The agreement, whether incorporated into the employment contract or presented as an addendum, may be addressed by the parties during the hiring process. Should the intention be to implement the aforementioned agreement during employment, note that this constitutes a significant alteration to the working conditions. The provisions of BYOD must diverge from the conventional notion that an employer provides tools as a fundamental aspect of work. Consequently, the consent of the employee is required in accordance with Article 22/I of the LA[34].

Furthermore, if a collective labour agreement contains a stipulation requiring employees to use their personal devices, this provision is in the interests of the employer. However, Article 36/I of the Act on Trade Unions and Collective Labour Agreements No. 6356 stipulates that the employment contract provision that is more beneficial to the employee should prevail. Therefore, if the individual employment contract explicitly stipulates that the employer will provide IT devices, the collective labour agreement provision will not be applicable[35].

C. Agreements Other than Employment Contracts

The minority view posits that the use of personal IT devices for work-related purposes should be regulated through legal relationships with individuals other than employment contracts. In such cases, the existence of obligations independent of the employment relationship becomes crucial, particularly regarding whether additional compensation will be provided to the employee. It is also necessary to consider the circumstances in which an employee shares his/her IT device with other colleagues or where the employer exercises partial control over the device. In such cases, it may be necessary to categorise the arrangement under other legal relationships[36].

In our opinion, not regulating the BYOD implementation within the scope of the employment contract but rather establishing it through other legal relationships is not conducive to protecting the interests of the employee. Therefore, it is appropriate to regulate specific provisions regarding BYOD within the framework of the employment contract terms rather than through other legal relationships.

34 Kılıç (n 23) 207; Ömer Ekmekçi, M Refik Korkusuz and Ömer Uğur (n 23) 132; Halûk Hâdi Sümer, *İş Hukuku Uygulamaları* (7th edn, Seçkin Yayıncılık 2019) 151; Dursun Ateş (n 23) 230. It is evident that the employer's decision to cease providing employees with IT devices represents a significant alteration to the established working conditions. For further insight into this topic, see Court of Cassation, 9th Division, 10.11.2020, 2017/18389, 2020/15521, (lexpera.com.tr), accessed 09.07.2024.

35 For conditions for the application of the benefit (more favourable) principle in collective agreements, see Dereli and Others (n 24) 373-374; Seda Ergüneş Emrağ, *Yararlılık İlkesi* (Onikilevha Yayıncılık 2022) 91. This is also the opinion in German labour law. See Hoppe (n 2) para 733.

36 Zöll and Kielkowski (n 3) 2626.

D. Workplace Practises

In general, employees are not entitled to use their own IT devices to fulfil their work obligations without the employer's consent. Nevertheless, given that employees frequently express a preference for working with their personal devices, the practise of BYOD is a prevalent reality within the context of employment relationships. Should an employer permit such a practise, the question of whether employees have the right to BYOD based on workplace practises becomes debatable.

The workplace practise is defined as the formation of a specific act by an employer in the workplace that is repeated regularly. The continuous provision of a benefit unilaterally provided by the employer, with the implicit acceptance of employees, constitutes a workplace practise that becomes a contractual provision under the employment contract. It is sufficient for employees to understand that such a benefit is provided unilaterally by the employer in accordance with the principle of good faith[37]. In order for a valid workplace practise to exist, several conditions must be met. Primarily, the practise must be of a general nature and provided by the employer to all employees or a specific section. Furthermore, the practise must be repeated if it becomes customary in the workplace[38].

In the literature, there is no consensus regarding whether a BYOD agreement can arise through a workplace practise. One perspective posits that if an employer permits the use of private IT devices for work purposes in accordance with the German Civil Code (Bürgerliches Gesetzbuch/BGB) 151, the employee may benefit from BYOD without the necessity of a separate agreement due to the existence of the workplace practise[39]. However, an opposing perspective maintains that BYOD cannot be based on a workplace practise, as its use primarily concerns the employer's interests[40].

The practise of BYOD should not emerge as a workplace practise. As a rule, BYOD serves the interests of the employer, for example, by reducing operating costs. The bringing of personal IT devices to the workplace may also entail certain burdens for the employee, which could disrupt the balance between the obligations set forth in the employment contract. Therefore, any such agreement must be explicitly agreed upon by the contracting parties.

37 Ömer Ekmekçi, M Refik Korkusuz and Ömer Uğur (n 23) 32; Sümer (n 34) 117. In accordance with the established case law of the Geman Federal Labour Court, workplace practise is defined as the regular repetition of certain behaviours by an employer that may lead employees to conclude that they will be permanently benefited. For further insight, direct to following judgments; BAG, 28.06.2006, 10 AZR 385/05, NZA 2006, 1174; BAG, 28.05.2008, 10 AZR 274/07, NZA 2008, 941, (beck-online), accessed 16.07.2024. For an examination of the role of workplace practises in the hierarchy of sources of labour law in the context of Turkish legislation, see Centel (n 23) 14.

38 Hamdi, Astarlı and Baysal (n 25) 85; Çelik and others (n 25) 270; Süzek (n 25) 80. See also, Ömer Ekmekçi, M Refik Korkusuz and Ömer Uğur (n 23) 32-33; Centel (n 23) 14. For the role of entrenched workplace practises, see Dereli and Others (n 24) 84. For entrenched workplace practises versus customary in labour law, see Kılıç (n 23) 164.

39 For the perspective that BYOD in the workplace may emerge through workplace practise, see Dirk M Barton, 'Betriebliche Übung und private Nutzung des Internetarbeitsplatzes „Arbeitsrechtliche Alternativen" zur Wiedereinführung der alleinigen dienstlichen Verwendung' [2006] NZA 460, 461.

40 The perspective that BYOD in the workplace does not emerge from the workplace (see Monsch (n 8) 43.

III. Regulation of BYOD Provisions in Employment Contracts

A. Prohibiting the Private Use of Devices

As stated previously, any provisions related to the use of BYOD must be incorporated into the employment contract or an addendum. The question of whether employees must accept prohibitions on the private use of IT devices during and outside working hours is raised in the employment contract. In addition, the use of unlicensed software on the device or the allowing of third parties, such as family members, to use it for private purposes presents a risk to the security of work-related data[41].

Employers may restrict the personal use of IT devices during working hours regardless of the characteristics of BYOD usage, if it jeopardises the performance of duties[42]. However, in private time, the situation remains debatable.

In the literature, *Lipp* posits that a prohibition that extends beyond working hours would constitute a restriction on an employee's property rights. She further argues that such a prohibition would only be valid if significant compensation is provided to the employee[43]. *Koch* holds that insofar as the device in question remains the property of the employee, its personal use cannot be prohibited[44]. *Monsch* also posits that the nature of the BYOD model, where the integration of work and personal use of IT devices is inherent, renders the prohibition of personal use incompatible with the BYOD concept[45].

The prohibition on personal use of IT devices constitutes disproportionate interference with the fundamental rights of employees. In lieu of an outright prohibition on personal use, as outlined below, the segregation of personal and work-related data on the device would prove a more effective means of safeguarding the employee's fundamental rights.

B. Effects of Work and Resting Periods

The advent of portable devices has enabled employees to contact each other at any time and from any location. The distinction between work and resting time is becoming increasingly indistinct[46]. In light of the fact that BYOD entails the utilisation of IT

41 Conrad and Schneider (n 9) 159.

42 Zöll and Kielkowski (n 3) 2627.

43 Katharina Lipp, 'Bring Your Own Device (BYOD) – Das neue Betriebsmittel', *Law as a service (LaaS): Recht im Internet- und Cloud-Zeitalter [Tagungsband Herbstakademie 2013]* (OlWIR, Oldenburger Verlag für Wirtschaft, Informatik und Recht 2013) 747.

44 Frank A Koch, 'Arbeitsrechtliche Auswirkungen von „Bring your own Device" – Die dienstliche Nutzung privater Mobilgeräte und das Arbeitsrecht' [2012], ITRB 35, 35. For a similar opinion, see Däubler (n 6) 101.

45 Monsch (n 8) 46.

46 Grieger (n 4) 171. Alongside its advantages, BYOD carries the risk of an increasing mix of work and resting time. See

devices owned by employees and that these devices are likely to remain operational for the purpose of engaging in personal activities, the implementation of specific regulations pertaining to working hours is imperative. It is therefore necessary to consider whether personal IT devices should be used during periods of free time during work hours[47].

Working time refers to the hours an employee spends performing their occupational duties. In addition, in accordance with Article 66 of the LA, the period spent awaiting work is considered working time. In this context, the primary motivation of the legislator in legally limiting working hours is to protect employee health. The advent of modern flexible working models has facilitated the flexibilisation of working times[48]. Nevertheless, when establishing working hours in the context of BYOD usage, it is imperative to consider the health of employees and respect their *right to disconnect*[49].

At this point, it is essential to consider whether the implementation of a BYOD policy will result in employees having extended accessibility for work-related purposes. In the German literature, this issue has been examined in the context of standby duty[50]. According to the literature, if an employer requires an employee to be accessible via an IT device outside of work, this should be regarded as working time, given that the employee is constantly on call and therefore unable to use their free time as they wish[51]. An alternative perspective posits that if the employee, while maintaining the IT device for the employer's use, can determine when to perform the tasks, it cannot be classified as working time[52]. Similarly, in the absence of explicit regulation concerning accessibility via the IT device and in the absence of the employer's directive, the reason for the working hours cannot be attributed to the employer. Consequently, no working time or wage payment obligation arises[53]. Furthermore, in consideration of the evolving of European labour law, it is imperative to underscore the employer's obligation to maintain accurate documentation of working periods in the context of BYOD practises. In this regard, it is incumbent upon the employer to implement a monitoring system that will record and document working hours regularly[54].

Hoppe (n 2) para 726.

47 Zöll and Kielkowski (n 3) 2628; Pollert (n 1) 154; Göpfert and Wilke (n 6) 768; Baysal (n 7) 73.

48 Centel (n 23) 137; Süzek (n 25) 800. For an examination of the concept of working time, see Ömer Ekmekçi, M Refik Korkusuz and Ömer Uğur (n 23) 107. For information on the regulation of working time within the context of workplace organisation, see Toker and Others (n 24) 157; Kılıç (n 23) 196-197.

49 Müller (n 7) 25. For suggestions on the employee's right to disconnect, see Deniz Ugan Çatalkaya, 'Kişisel Yaşamı Kapsamında İşçinin, İşverence "Ulaşılabilir Olmama" Hakkı' (2016) 74 Journal of Istanbul University Law Faculty 737, 743. See also F Burcu Savaş Kutsal, *İşçinin Ulaşılabilir Olmama Hakkı* (Seçkin Yayıncılık 2024), 102.

50 Regarding the duration of standby duty under German law, see Sevil Doğan, *İş Hukukunda İşçinin İş ve Aile Yaşama Uyumunun Sağlanması* (Seçkin Yayıncılık 2022) 366.

51 Monsch (n 8) 52; Hoppe (n 2) para 756; Pollert (n 1) 154.

52 Wisskirchen and Schiller (n 1) 1167.

53 Wisskirchen and Schiller (n 1) 1167.

54 For further information regarding the judgement of the Court of Justice of the European Union dated 14/05/2019 on

In the Turkish legal literature, as in European labour law, the argument is put forth that the working time of employees using IT devices should be documented[55]. This approach is of particular significance for employees in the context of BYOD. As the literature indicates, documentation of working periods is crucial for the protection of employee rights and the substantiation of claims in the event of a dispute between an employee and employer. Similarly, the documentation of working periods is of vital importance in terms of determining the employee's overtime work and ensuring a work-life balance[56].

Documentation of working periods is indirectly regulated in our legislation. Since the Labour Act does not directly regulate the documentation of working periods, the regulations issued pursuant to Articles 63 and 41 of the Labour Act (Article 9 of the Regulation on Working Periods Pursuant to the Labour Law and Article 10 of the Regulation on Overtime Work and Working for Excessive Periods Pursuant to the Labour Law) obligate the employer to document the working periods. Nevertheless, there is no stipulation regarding the manner in which the work should be documented. This matter shall be at the discretion of the employer[57]. Thus, the question of how to document working periods should be addressed by the contractual parties within the framework of the BYOD agreement[58].

An evaluation of the impact of BYOD usage on rest periods is also required[59]. In general, rest periods are defined as the time between the conclusion of the daily workday and the start of the subsequent work period. In accordance with Article 69/V of the LA, in workplaces where shift work is in operation, it is not permissible to require an employee to commence the next shift without a minimum of 11 consecutive hours of rest. In accordance with Article 46 of the LA, the employer is obliged to provide the employee with a minimum of 24 consecutive hours of rest within a 7-day period, with full remuneration provided that the employee has worked on the previous working days[60].

---

the recording and documentation of working periods, refer to the Judgement in Case C-55/18 Federación de Servicios de Comisiones Obreras (CCOO) v Deutsche Bank, (https://curia.europa.eu/jcms/jcms/j_6/en/), accessed on 08.08.2024. A recent decision by the Federal Labour Court established that employers are now required to record and document all working periods of their employees. This obligation is not contingent on the size of the workplace or the existence of a work council. For the related judgement, see BAG, 13.09.2022, 1 ABR 22/21, (https://www.bundesarbeitsgericht.de), accessed on 09.08.2024. However, according to two recent rulings of the BAG (04.05.2022, 5 AZR 359/21 and 5 AZR 474/21), the obligation to record working periods does not increase the burden of proof in overtime proceedings.

55 For an evaluation of the Case C-55/18 Federación de Servicios de Comisiones Obreras (CCOO) v. Deutsche Bank judgement in terms of Turkish labour law, see Namık Hüseyinli and Emre Ünal, 'Avrupa Birliği Adalet Divanı Kararı Işığında, Türk İş Hukuku'nda Çalışma Sürelerinin Kayıt Altına Alınması' (2024), 7 Necmettin Erbakan Üniversitesi Hukuk Fakültesi Dergisi 44, 47.

56 Hüseyinli and Ünal, (n 55), 64.

57 Hüseyinli and Ünal, (n 55), 51.

58 It can also be posited that when the use of personal IT devices outside the workplace is involved, the determination of working periods should be based on the employee's autonomy in structuring the standby period and the extent to which the employer's instructions impinge upon the employee's freedom during their free time.

59 Hoppe (n 2) para 756; Zöll and Kielkowski (n 3) 2628; Baysal (n 7) 73. For an examination of the concept of rest periods, see Ömer Ekmekçi, M Refik Korkusuz and Ömer Uğur (n 23) 116; Toker and others (n 24) 189; Kılıç (n 23) 203-204.

60 Centel (n 23) 149; Süzek (n 25) 860.

In the context of BYOD, it is our opinion that activities such as sending emails or making phone calls should not be considered interruptions to the rest periods, provided they do not require prolonged and strenuous preparation[61]. In other words, from an equity standpoint, an employee's use of a personal IT device for brief communication, such as making phone calls or preparing e-mail texts, should not be considered a cessation of the resting period. Conversely, a work-related activity that necessitates a prolonged preparatory period and is of a nature that precludes the benefit of a rest period should be regarded as an interruption to the resting period.

In conclusion, it would be prudent to regulate working and resting periods when drafting contractual provisions related to BYOD to prevent disputes[62]. Although there is no specific legal regulation on this issue in Turkish law, it is of particular importance to respect the employee's right to disconnect. For example, precautions may be implemented, such as deactivating software on an employee's personal IT devices at the end of the work or preventing email server activation during rest periods. Similarly, it is possible to pre-plan which employees can be contacted in the event of an emergency in a predetermined order and how such contact will be made in order to minimise the workload[63].

C. Occupational Health and Safety Precautions

The advent of digitalisation and the concomitant increase in the use of BYOD have resulted in a shift towards flexible forms of work. Despite this, the onus remains on the employer to ensure that requisite precautions are taken and risk assessments are conducted within the context of occupational health and safety[64]. In accordance with Article 4 of the Occupational Health and Safety Act No. 6331, it is the responsibility of the employer to ensure the health and safety of employees in relation to their work.

Considering the inherent risks associated with the distinctive structure of BYOD implementation, employers must implement occupational health and safety precautions in accordance with Article 417/2 of the TCO[65]. With this regulation, employers are obliged to guarantee the availability of requisite health and safety precautions and to provide suitable equipment. In addition, employees must adhere to these stipulations[66]. In this context, it is essential to consider the working conditions

61 Those who espouse a comparable perspective on this matter concerning German labour law, see Monsch (n 8) 59; Wisskirchen and Schiller (n 1) 1167.

62 Baysal (n 7) 73.

63 Further information that may be taken within the scope of the employee's right to disconnection is available in Savaş Kutsal (n 49) 111. In accordance with the principle of employee protection, the following measures should be taken by the employer. For further details see Ugan Çatalkaya (n 49) 750.

64 Müller (n 11) 24. Regarding the identification of factors and precautions for the risk assessment of BYOD use, see Ganiyu and Jimoh (n 5) 50.

65 Regarding health risks arising from long periods of time spent in front of IT devices, see Savaş Kutsal (n 49) 41.

66 Dereli and Others (n 24) 145; Ömer Ekmekçi, M Refik Korkusuz and Ömer Uğur (n 23): 209; Sümer (n 34): 459.

(such as illumination, screen quality and size) and ergonomic postures. Furthermore, the issue of mental stress on employees, such as burnout, and increased accessibility and psychosocial risks should be addressed. In addition, employees should be required to stop working and immediately inform their employer if they notice any health-threatening effects from IT device use[67].

D. Appropriate Payment to the Employer

When an employee uses his/her own IT device for work-related purposes, questions arise regarding whether the employer will compensate for this use and who will bear the costs associated with the support, maintenance, software, and repair of the devices. It is necessary to distinguish between the use of BYOD as a replacement for workplace IT devices and its optional application[68].

In German law, the use of BYOD as a substitute for workplace tools, as delineated in 670 of the BGB, is contingent upon 675[69]. In such cases, an employee who has incurred expenses on behalf of the employer is entitled to claim reimbursement. Expenses eligible for reimbursement include those incurred by the employee during fulfilling their work duties, as well as costs that are a direct consequence of fulfilling the contract. The provision of IT devices without appropriate compensation would result in the cost burden being shifted to the employee, which would render such a provision invalid under 307/I of the BGB[70]. The compensation should be based on the IT device's current value. In accordance with German law, such compensation may be claimed either on the basis of receipts or a pre-determined lump sum[71].

In Turkish law, in accordance with Article 413/II of the TCO, an employee is permitted to dedicate his/her tools or materials to work provided that such an arrangement is agreed upon by the employer[72]. In the absence of an agreement or customary practise to the contrary, the employer must provide the employee with appropriate compensation. This encompasses the device itself (work tools), software

According to the Turkish Court of Cassation, occupational health and safety rules must be strictly followed by employees. In this regard, in addition to the precautions to be taken by the employer, the employee also has obligations. See Court of Cassation, 9th Division, 12.6.2023, 2023/10610, 2023/8946, (lexpera.com.tr), accessed on 09.07.2024. Obligation to take measures for occupational health and safety (see Centel (n 23) 123-124.

67 Kascherus and Pröpper (n 11) 759.

68 Pollert (n 1) 154.

69 Hoppe (n 2) para 728. See also Chandna-Hoppe, (n 32), 153.

70 Wisskirchen and Schiller (n 1) 1166.

71 Monsch (n 8) 69–70. For decisions of the Federal Labour Court (Bundesarbeitsgericht-BAG) concerning the payment of appropriate compensation, see BAG, 12.01. 2005, 5 AZR 364/04, NZA 2005, 465; BAG, 11.10.2006, 5 AZR 721/05, 28, (beck-online), accessed 15.07.2024. In cases where equipment is required to fulfil an obligation, the question arises of whether and to what extent the employee can demand the provision of such resources. Aside from old rulings and in light of the changing conditions of new work models (such as BYOD), the Federal Labour Court addressed this issue in a landmark judgement and concluded that employees have the right to demand the provision of work equipment. For the decision, see BAG 10.11.2021, 5 AZR 334/21, NZA 2022, 401 ff., (beck-online), accessed 08.08.2024. For an evaluation of the decision, see Klocke and Hoppe (n 10) 515; Chandna-Hoppe (n 32) 153.

72 Centel (n 23) 133; Süzek (n 25) 499.

used on the device (materials), connection and subscription fees, electricity costs, technical support, and repair expenses. Article 414 of the TCO provides the relevant provision for establishing the requisite expenses. In accordance with this stipulation, the employer is obliged to bear all costs associated with the completion of assigned tasks, as well as any expenses incurred by the employee in the course of their duties, if they are carried out outside the usual place of work[73]. In the event that the expenses are deemed necessary for the satisfactory completion of the work, they may be compensated in a lump sum in accordance with the provisions laid down in Article 414/II of the TCO. However, as stipulated in Article 414/III of the TCO, agreements where compulsory expenses are partially or completely covered by the employee are invalid. In accordance with Article 416/I of the TCO, payment for expenses shall be provided with each salary payment, unless a shorter period is agreed upon or is customary practise.

In the optional BYOD implementation, the employer is typically responsible for providing the necessary work tools. Nevertheless, in this context, the employee may opt to use their own IT device due to its familiarity and ease of use. In the absence of a contrary agreement, the employee bears the costs associated with the use of BYOD[74].

E. Liability Clauses

1. Regarding employer claims

The implementation of the BYOD concept within the context of labour law gives rise to questions about the field of legal liability. In the context of BYOD implementation, employer liability claims against employees frequently relate to the safeguarding of information infrastructure or the protection of company data and secrets[75]. In particular, significant financial losses may result if third parties, such as clients or commercial partners, submit compensation claims against the employer due to data losses caused by incidents such as a cyber attack, jailbreak[76], or the use of outdated antivirus software on the IT system[77].

In German law, an employer's compensation claim is based on the provisions laid down in BGB 280/I and 241/II[78]. These provisions stipulate that in the event of a debtor breaching an obligation arising from a contractual relationship, the creditor is

73 Baysal (n 7) 68.

74 Pollert (n 1) 154.

75 Kascherus and Pröpper (n 11) 758.

76 Jailbreak bypasses the device's protection mechanisms and security infrastructure to instal unlicensed software, especially applications that are not officially available in the app store. Applicable to iOS-based devices. See this topic, Ganiyu and Jimoh (n 5) 56.

77 Zöll and Kielkowski (n 3) 2627; Däubler (n 6) 108.

78 Kascherus and Pröpper (n 11) 758.

entitled to demand compensation for the resulting damage. To establish liability on the part of the employee, the employer is required to prove fault in accordance with the stipulations set forth in BGB 280/II and 619a. The extent of damage is determined on the basis of the specific circumstances of the case, the seriousness of the fault, and the employee's duty of loyalty. In this context, it is incumbent upon the employer to regulate the requirements of access to the network and the security settings of IT devices with a view to safeguarding work-related data. Furthermore, the employer must inform the employee about these measures[79].

In accordance with Turkish legislation, the realisation of these possibilities causes employee liability under Article 400 of the TCO. In accordance with the stipulations of this regulatory framework, the employee bears responsibility for any damages incurred by the employer due to the employee's actions or omissions. In liability, the second paragraph of the regulation requires an evaluation of the nature of the work, its inherent dangers, the necessity for expertise and training, and the employee's abilities and qualifications, both as they are known or expected by the employer[80]. If the IT device utilised by an employee has caused damage, consideration should be given to the employee's training and expertise. Furthermore, if the employee's role (for example that of a data security specialist) entails a significant degree of responsibility, it can be concluded that the work is risky and prone to loss[81].

2. Regarding employee claims

A claim by an employee against their employer may arise in the event of the theft, loss, or damage of an IT device. It is recommended that employers insure these devices to prevent disputes; however, there is no legal obligation for employers to do so[82].

Nevertheless, the employer bears the responsibility of safeguarding the devices that the employee brings to the workplace for work-related purposes, as stipulated in the employment contract. In German law, this obligation is based on BGB 241/II[83]. In Turkish law, in consideration of the protective purpose of Article 413 of the TCO, it is stated that the onus is on the employer to bear the risks associated with the equipment during the performance of the work[84]. Consequently, it is incumbent

79 Monsch (n 8) 79; Conrad and Schneider (n 9) 158.

80 Centel (n 23) 106; Gaye Baycık, *Türk-İsviçre Hukukunda İşçinin Hukuki Sorumluluğu* (Yetkin Yayınları 2015) 160. For the legal liability of the employee to be accepted, it is clear that there must be an unintended decrease in the employer's assets, an appropriate causal link between the employee's act contrary to the contract, loss (damage), and the employee's fault. See, Court of Cassation, 9th Division, 23.11.2022, 2022/14705, 2022/15027, (lexpera.com.tr), accessed 09.07.2024.

81 Baysal (n 7) 70.

82 Zöll and Kielkowski (n 3) 2628; Baysal (n 7) 69. For an overview of employers' legal liability in general, see Centel (n 23) 38.

83 Monsch (n 8) 82.

84 Centel (n 23) 133; Baysal (n 7) 69.

upon the employer to take all reasonable measures to protect the devices from loss or damage. For example, in the event of loss or theft, it is necessary to remotely erase company data. However, this should not automatically erase personal data. Lockable cabinets should also be provided to reduce the risk of theft. The specific measures to be implemented are contingent on the context, scale of the workplace, and objectives associated with the adoption of BYOD[85].

It is important to highlight that the implementation of a policy that replaces working tools with personal IT devices increases the necessity for additional precautions because such devices require use for the fulfilment of work duties. However, in optional BYOD usage, the question of employer responsibility remains open to debate. In instances where the use of the device for professional purposes is not obligatory for the completion of work tasks, it is proposed that the onus of responsibility for potential loss or damage should fall upon the employee[86]. Similarly, Turkish legislation has established that damages resulting from risks unrelated to the performance of work duties do not fall under the purview of employer liability[87].

Failure by an employer to comply with the aforementioned obligations may result in damages for which the employee is entitled to claim compensation. In German law, the basis for such claims is established by the provisions of BGB 276/I and 280/I. In contrast to employee liability, the provisions laid down in BGB 619a do not apply in this context[88].

In Turkish law, the protection of devices brought by employees to the workplace can be seen to arise from an employer's duty of care towards the employee. If this obligation is not fulfilled and it results in harm, the employer may be held liable under the contractual liability provisions, allowing the employee to claim compensation for the damages incurred[89].

F. Obligation to Deliver Personal BYOD Devices

It is possible that, during an employment relationship, the employer may have a legitimate interest in requesting the employee's personal IT device and stored data. Such circumstances may include, for example, suspicion of misconduct (in the context of internal investigations), device maintenance and software updates, installation programmes, device disposal, and compliance checks related to BYOD agreements[90].

85 Hoppe (n 2) para 752; Zöll and Kielkowski (n 3) 2627.

86 Monsch (n 8) 93. For decisions of the Federal Labour Court in this direction, see BAG, 22.06.2011, 8 AZR 102/10, NZA 2012, 91; BAG, 23.11.2006, 8 AZR 701/05, NZA 2007, 870, (beck-online), accessed 15.07.2024.

87 Baysal (n 7) 70.

88 Göpfert and Wilke (n 6) 767.

89 Orhan Ersun Civan, *İşçinin Yan Yükümlülükleri* (Beta Yayınevi 2021) 95.

90 Raif and Nann (n 9) 222.

In light of the fact that BYOD does not affect device ownership, it has been observed that a specific agreement is required for an employee to be bound by an obligation to deliver the device to the employer[91]. The aforementioned obligation should be limited to the exceptional circumstances mentioned above, and the conditions under which the employee is required to deliver the device and its data should be clearly defined. Furthermore, it would be prudent to determine whether the employer will provide a comparable device during the aforementioned return period[92].

In the context of internal investigations or the termination of an employment contract, the obligation to deliver the device is of particular significance. In accordance with German legislation, as set forth in BGB 667, even in the absence of a specific agreement between the parties, an employee is obliged to deliver all work-related communication data, documents and records stored on his/her personal computing devices[93]. Following termination of the employment contract, the employer is entitled to delete the remaining work-related data on the device and is also obliged to safeguard any third-party data[94]. In cases where there is a suspicion of misconduct, a comparable interpretation is applicable. In such cases, depending on the circumstances of the specific case, the employer may request the BYOD device on the grounds of the employee's obligation. Ultimately, an employee may invoke defences of property law in accordance with BGB 858 and 861[95].

In accordance with Turkish legislation, if the parties have consented to a delivery obligation under the terms of the contract, the employee is bound by law to deliver the device to the employer. Nevertheless, in the absence of an agreement between the parties, it is our opinion that the obligation to deliver should only be considered justified in exceptional cases where the predominant interests of the employer justify the device's return, based on the specific circumstances of the individual case. In balancing interests, factors such as the seriousness of a suspicion of miscorruption, the potential extent of harm incurred if the device is not returned, or the duration of deprivation from the device can be considered. In addition to the aforementioned considerations, Article 443 of the TCO provides that employees are obliged to return any items they have received from their employers during their employment[96]. Based on this provision, in alternative models in which device ownership is retained by the employer (such as COPE or CYOD), upon termination of the employment contract, the employee is obliged to deliver the devices to the employer[97].

91 Monsch (n 8) 95; Bartz and Grotenrath (n 6) 187.

92 Kascherus and Pröpper (n 11) 759.

93 Monsch (n 8) 96; Däubler (n 6) 110. In essence, this relates to agency agreements and associated payment services. However, given the absence of a regulatory framework within the context of BGB §§ 611-630.

94 Hoppe (n 2) para 740.

95 Bartz and Grotenrath (n 6) 186.

96 Centel (n 23) 169; Hamdi, Astarlı and Baysal (n 25) 617.

97 In a case that was the subject of a trial, the employee did not deliver the computer provided by the employer and the software

IV. Protection of Personal Data in BYOD

A. Protection of Personal Data of Third Parties

In accordance with the legislation in question, the employer is bound by law to act as the data controller when collecting, processing and storing personal data during the employment relationship[98]. In the context of the implementation of a BYOD policy, the presence of personal data on an employee's private devices gives rise to considerations under data protection legislation[99]. Although the BYOD devices belong to the employee, they do not solely contain the employee's personal data due to their use for work. Instead, these devices may also process or store personal data related to third parties, such as company, business partners, employees, and customers[100]. Consequently, the use of BYOD poses significant risks, particularly in professions where third-party personal data are frequently processed for example finance, healthcare, and legal sectors[101].

In the literature concerning the relationship between IT devices and personal data, it is emphasised that sensitive data should not be stored on BYOD devices. This implies that employers should refrain from using employees' personal IT devices, particularly when processing sensitive personal data[102].

An employer may assign employees to perform data processing activities. This employee may also be employed under the BYOD scheme. The presence of third-party personal data on personal IT devices does not make an employee data processor. They are only part of the data controller organisation.[103] As the data controller, the employer bears the responsibility of ensuring compliance with personal data protection regulations while continuing commercial activities and supervising data processors. In the context of a workplace where BYOD is permitted, it is of paramount importance for the employer to implement the necessary measures to

dongle required for the use of the programme; as a result, the employer was compensated. The Turkish Court of Cassation, however, ruled that the cost of the lease and the new system provided by the employer as a result of an employee's action can be claimed from the employee. See here, Court of Cassation, 9th Division, p. 24.3.2015, 2013/15795, 2015/11674, (lexpera.com.tr), accessed 09.07.2024.

98 Ömer Ekmekçi, M Refik Korkusuz and Ömer Uğur (n 23) 99-100. For the main legal actors in the protection of personal data within the framework of the employment contract, see Centel (n 23) 125-126; Nazlı Elbir, *Kişiliğinin Korunması Bağlamında İşçiye Ait Kişisel Verilerin Korunması* (Yetkin Yayınları 2020) 157; Elif Küzeci and Şebnem Kılıç, '6698 Sayılı Kişisel Verilerin Korunması Kanunu'nun İş Sözleşmesi Çerçevesinde Değerlendirilmesi: Veri Sorumlusu, Veri İşleyen ve Diğer Aktörler' (2019) 16 Legal İş Hukuku ve Sosyal Güvenlik Hukuku Dergisi 947, 962.

99 Wisskirchen and Schiller (n 1) 1163; Pollert (n 1) 154; Günther and Böglmüller (n 9) 1030.

100 Axel Bertram and Roland Falder, 'Datenschutz im Home Office-Quadratur des Kreises oder Frage des guten Willens?' [2021] ArbRAktuell 95, 97.

101 Bernd Schmidt and Anna-Kristina Roschek, 'Datenschutz Im Anwaltlichen Home- Und Mobile-Office' [2021], NJW 367, 370; Conrad and Schneider (n 9) 154. Regarding finance professions, see Grieger (n 4) 169.

102 Bertram and Falder (n 100) 97; Kascherus and Pröpper (n 11) 759; For sensitive personal data, see Elbir (n 98) 134.

103 Regarding the discussion of the concepts of data controllers and data processors in the employment relationship, see Küzeci and Kılıç (n 98) 970-971. See also Baysal (n 7) 71; Däubler (n 6) 104.

ensure compliance with data protection regulations[104]. If an employee is granted access to a company's IT resources, the focus should be on the measures that need to be implemented under the BYOD framework[105]. At this juncture, the role of *Mobile Device Management (Mobilgeräteverwaltung)* becomes particularly salient[106].

Mobile Device Management (MDM) tools are software that facilitate secure registration, configuration, updating, monitoring of compliance with data policies, and remote data wiping of devices[107]. Before implementing a BYOD, the employer may investigate whether the employee's device meets the requirements of mobile device management and prohibit the use of noncompliant devices. Consequently, the employee must consent to the installation of such software on the device[108].

It is also incumbent upon the employer to ensure the separation and protection of work-related and personal data in the context of BYOD[109]. Solutions have been developed to address this issue. In accordance with the *container solution (Containerlösung/ Sandboxing)*, work-related data are segregated from other applications on the device and stored in an encrypted data container[110]. The separation of work-related and personal data is achieved without any restriction on the personal use of the BYOD device[111]. Implementing the container solution necessitates employee consent because the employer is prohibited from storing work-related data on an employee's IT device without permission due to property rights. In this regard, it may be necessary for employees to undergo training to become familiar with the software[112].

In contrast, in *virtualisation solutions*, work-related data are not stored locally on the BYOD device; rather, they remain on the company's server. This implies that the BYOD device is only a conduit for data visualisation[113]. In the absence of storage activity, the necessity to obtain employee consent is obviated. Although it increases the costs of data security, virtualisation is the optimal mobile device management solution for BYOD devices because it prevents the mixing of personal data belonging to employees in the workplace, business partners and customers with employees' private data[114].

104 Müller (n 10) 23. Regarding the concept of a data processor and the fact that it can be a separate person (employee) who performs data processing activities on behalf of the data controller (employer), see Elbir (n 98).

105 For the measures taken by the employer, see Hoppe (n 2), para 736.

106 Däubler (n 6) 104.

107 Ganiyu and Jimoh (n 5) 50.

108 Bartz and Grotenrath (n 6) 185.

109 Hoppe (n 2) para 736; Zöll and Kielkowski (n 3) 2625; Elbir (n 98) 318.

110 Conrad and Schneider (n 9) 156.

111 Bertram and Falder (n 100) 97; Wisskirchen and Schiller (n 1) 1164; Raif and Nann (n 9) 222; Müller (n 10) 24; Kascherus and Pröpper (n 11) 757.

112 Pollert (n 1) 153.

113 Zöll and Kielkowski (n 3) 2625; Bartz and Grotenrath (n 6) 185.

114 Monsch (n 8) 137; Grieger (n 4) 171.

Conversely, safeguarding work-related data on BYOD devices requires certain responsibilities for the employee. It would be prudent to explicitly delineate these obligations in the BYOD agreement. The most notable of these obligations pertain to device access and usage controls.[115]

In order to ensure *access control* of a BYOD device, it is essential that the employee assumes responsibility for restricting any unauthorised individuals, such as family members and friends, from accessing the device[116]. It is important that employees do not leave the BYOD device unattended. Furthermore, the employee must comply with any security scans predetermined by the employer within a reasonable timeframe. If the employee does not consent to such an intervention, the employer is entitled to exclude the device from the BYOD. In such a scenario, the employer is bound by law to provide the necessary IT equipment for the employee to fulfil their professional obligations[117].

Usage control for a BYOD device is aimed at preventing potential data loss and mitigating cyber-risks and crimes in the workplace network. Employees must use antivirus software on their BYOD devices and avoid actions such as rooting[118], which involves significant alterations to the IT device's operating system[119]. Such manipulated devices can create opportunities for attacks against mobile device management. In addition, employment contracts may impose restrictions on using other cloud computing systems or copying business data via a BYOD device[120]. It is suggested in the literature that the employer should have the authority to remotely wipe work-related data from the device in case of loss or theft to prevent data and reputational damage to clients[121]. Consequently, it can be stated that in the event of loss or theft, an employee is obliged to immediately inform the employer in accordance with his/her duty of loyalty[122].

A further measure that can be adopted by employers within the context of a BYOD policy is the implementation of a *blacklist*. In accordance with management rights, the employer is responsible for establishing the minimum technical specifications that a device must adhere to for it to be utilised within the scope of a BYOD initiative. Conversely, some devices and software have functions that may compromise the confidentiality, integrity, or availability of work-related data. The employer is

115 Hoppe (n 2) para 736.

116 Hoppe (n 2) para 737; Grieger (n 4) 170.

117 Däubler (n 6) 107.

118 Root can be used to make system changes to IT devices. Pre-installed programmes can be uninstalled, and, in some cases, the entire operating system can be changed. It can be used on Android-based devices. See Ganiyu and Jimoh (n 5) 56.

119 Raif and Nann (n 9) 222; Zöll and Kielkowski (n 3) 2627; Müller (n 10) 24.

120 Hoppe (n 2) para 758; Kascherus and Pröpper (n 11) 759.

121 Monsch (n 8): 144; Wisskirchen and Schiller (n 1): 1164; Müller (n 10): 24; Kascherus and Pröpper (n 11): 760; Ganiyu and Jimoh (n 5): 61.

122 Hoppe (n 2) para 741; Pollert (n 1) 154.

entitled to prohibit the use of programmes and devices that are classified as critical for security[123]. Once the list has been made public in the workplace, employees are required to cease using the devices and software in question within a reasonable timeframe and to delete the software.

Moreover, it is observed in the legal literature that a *whitelist* application, which stipulates that employees can only use devices and applications that have been explicitly permitted, is invalid. Such a prohibition, which applies to all existing devices and applications without consideration of their respective risks, constitutes an undue infringement of employees' rights to possess and utilise their personal IT devices, thereby violating their fundamental rights[124].

B. Protection of Personal Data of the Employee

When BYOD devices are used in an employment relationship, it is inevitable that personal data belonging to third parties, such as the business partners and customers, as well as the employee's personal data, will be present on the device, given that it belongs to the employee. Consequently, the scope of an employer's intervention and control authority is constrained by the employee's right to privacy, which is enshrined in fundamental rights. It is evident that data of the use of the device must be safeguarded[125].

In Turkish labour law, the protection of personal data belonging to employees is governed by two distinct legal instruments: the TCO and the Personal Data Protection Act No. 6698 (PDP). In accordance with Article 419 of the TCO, personal data processing is permitted if necessary for an employment contract or related to the employee's suitability for the position under consideration. Moreover, in accordance with Article 4 of the PDP, personal data processing on an employee's device must adhere to principles of good faith, accuracy, and up-to-dateness when necessary; it must be processed for specific, explicit, and legitimate purposes; it must be relevant, limited, and proportionate to the purposes for which it is processed; and it must be retained for the duration prescribed by law or necessary for the purposes for which it is processed[126].

In this context, the employer is permitted to access work-related data on the employee's personal device, which the employee has chosen to use for work purposes, from a remote location. Nevertheless, such an intervention may prove to be disproportionate and potentially harmful to the employee's data. It is therefore argued

123 Grieger (n 4) 171; Däubler (n 6) 106.

124 According to German law, contractual provisions forcing employees to comply with the white list are invalid pursuant to 307 BGB. See, Monsch (n 8) 146.

125 Bertram and Falder (n 100) 97; Wisskirchen and Schiller (n 1) 1164; Baysal (n 7) 72; Däubler (n 6) 105; Elbir (n 98) 229.

126 Centel (n 23) 126; Baysal (n 7) 72; Elbir (n 98) 86.

in the literature that for a BYOD application to be legally compliant, there must be a clear separation between work-related and personal data[127]. Consequently, one of the most crucial measures to protect employee personal data is the implementation of effective mobile device management[128].

Conversely, if the employer does not implement effective mobile device management, whereby work-related data are stored alongside personal data on the BYOD device, the employer is required to intervene in the personal data to gain regular access to the work-related data. In practise, this situation can arise, particularly in the context of *email monitoring*[129]. Nevertheless, in the absence of compelling and legitimate interest on the part of the employer and not coupled with the employee's consent, the employer is not entitled to access the email system on the BYOD device. Given the inherent imbalance of power and dependency in the employment relationship between employers and employees, it is not feasible to consider employee consent as a valid basis for all actions[130]. It follows that only explicit consent, which is informed and based on the employee's free will regarding the employer's intervention in personal data, should be recognised[131].

In BYOD practises, the protection of an employee's personal data encompasses the safeguarding of data stored on their mobile device against remote wiping by the employer, which is facilitated through the use of MDM tools. In accordance with the Federal Data Protection Act 35/II, employers are obliged to delete data stored on IT devices located outside the workplace under specific circumstances. If a data container method is employed, only work-related data are subject to remote deletion; thus, personal data are not affected. Nevertheless, in the event that both work-related and personal data are not separated and are subject to deletion, the employee is entitled to claim damages in accordance with BGB 280/I, 241/1, and 823/1. It has been observed that in instances where a data container method is not employed, the principle of proportionality dictates that access to data should be prevented rather than deleted entirely[132].

127 Monsch (n 8) 149; Ganiyu and Jimoh (n 5) 53. For the opinion that, in addition to the employer, the employee also has an obligation to separate work-related and private data on the device, see Bartz and Grotenrath (n 6) 185.

128 Bartz and Grotenrath (n 6) 185.

129 In a decision of the Turkish Constitutional Court, it was emphasised that the e-mail data of the employee is personal data and must be protected. According to this decision, it should be determined whether there are legitimate grounds that justify the examination of the communication tools and content that the employer makes available to the employee. In this inspection, a distinction should be made between examining the communication flow and the content, and more serious grounds should be sought for the examination of the content. See, Constitutional Court, App no 2016/13010, 17/9/2020, § 70, (kararlarbilgibankasi.anayasa.gov.tr), accessed on 09.07.2024.

130 Wisskirchen and Schiller (n 1) 1165.

131 Baysal (n 7) 72; Elbir (n 98) 238.

132 Monsch (n 8) 150.

V. Licences and Intellectual Property Rights in BYOD Devices

The defining characteristic of BYOD models, irrespective of whether they are replacing existing workplace devices or are optional, is the utilisation of licenced software by employees for work-related purposes, or conversely, the incremental adoption of company-owned software for personal use[133]. It is established that the transfer of usage rights from intellectual property rights on computer programmes is typically conducted through licence agreements[134]. It is therefore imperative to consider licence agreements in the context of employment relationships involving BYOD use to avoid violations of intellectual property rights[135].

In German law, the regulations of licence agreements are primarily governed by the provisions set forth in the German Intellectual Property Rights Code (UrhG), specifically 69a and the subsequent sections. In accordance with Article 99 of the legislation, an employer is held accountable for infringements of intellectual property rights, even in instances where the employer is not aware that an employee is using unlicensed software or employing software for work-related (commercial) purposes that are prohibited[136]. The employer is held liable for such infringements if they occur within the context of the work-related activities[137]. To illustrate, if an employee utilises a personally owned device with unlicensed software (i.e. pirated copies) for the fulfilment of work duties, thereby conferring a commercial benefit upon the work, the employer becomes liable[138]. However, it should be noted that this provision does not extend to situations involving the private use of software[139].

In Turkey, the possibility of licencing agreements concerning intellectual property rights is regulated under Article 48/II of the Code of Intellectual Property Rights and Artistic Works (as an abbreviation: Intellectual Property Act/IPA). Computer programmes (software) and databases (databank) used on BYOD devices are regarded as intellectual property rights and are thus subject to licencing agreements in accordance with Article 2/I-1 of the IPA. Furthermore, the licensee is obliged to utilise the licenced subject matter in accordance with the terms of the contract. The use of the licenced subject matter is determined by the parties in accordance with the provisions of the contract (Article 48/I of IPA)[140]. Consequently, licencing agreements may stipulate whether the relevant software may be used exclusively for private or work-related purposes or for both. In the event of non-compliance with the

133 Zöll and Kielkowski (n 3) 2625; Göpfert and Wilke (n 6) 767.

134 Gökhan Şahan, *Bilgisayar Programı İmâl Sözleşmesi* (Yetkin Yayınları 2016) 167.

135 Hoppe (n 2) para 754; Pollert (n 1) 153; Kascherus and Pröpper (n 11) 757.

136 Georg Herrnleben, 'BYOD – die rechtlichen Fallstricke der Software-Lizenzierung für Unternehmen' [2012] MMR 205, 206.

137 Hoppe (n 2) para 754.

138 Conrad and Schneider (n 9) 157.

139 Monsch (n 8) 154.

140 Ömer Arbek, *Fikir, and Sanat Eserlerine İlişkin Lisans Sözleşmesi* (Yetkin Yayınları 2005) 186.

terms of the contract, such as the utilisation of software prohibited for work-related use on a BYOD device for work purposes, this constitutes a breach of contract. In such instances, the stipulations of the legislation safeguarding the right holder are invoked, and the licensee is held accountable for the right holder.

A thorough examination of Turkish labour law revealed no explicit provisions addressing the ramifications of using intellectual property materials without a licence or for work-related purposes within the context of work-related activities. In the context of BYOD, it is essential to differentiate between scenarios where software licenced to the employer is used on an employee's personal IT device and instances where software licenced to the employee is employed for work-related purposes[141].

The utilisation of licenced software on an employee's personal IT device is contingent on the stipulations set forth in the licence agreement. In light of the possibility of licences being allocated to specific individuals in the workplace, conducting a review of the licence terms in order to prevent any potential violations and ensure that the necessary licencing is in place, should it be required. Conversely, employees may use software for which they hold a licence for work purposes. In some cases, the licence terms for software on devices may stipulate that software is intended for personal use only and is therefore not suitable for work-related applications. Such restrictions are binding on third parties in accordance with Article 48/I of the IPA. Consequently, the utilisation of licenced software intended for employee use for work-related purposes, namely the commercialisation of the programme, would necessitate the employer obtaining a licence.

In legal literature, it is observed that if the licensee is a legal entity, the licence right is intended for use by natural persons employed within the legal entity. In the event that employees act in contravention of the terms of the licence agreement and cause damage to the rights holder, the legal entity is held responsible under Article 116 of the TCO for the actions of its agents[142]. Nevertheless, in the event that an employee uses pirated software on a BYOD device in the absence of a licence agreement between the employer and the rights holder, it is our opinion that the employer's liability would be subject to the provisions set forth in Article 66 of the TCO, which pertains to the liability of employers for the actions of their employees.

To preclude the potential for legal disputes, contract provisions relating to the use of personal IT devices for work-related purposes should explicitly stipulate that licenced software may be employed without a reservation for work-related applications. It is recommended that a blacklist approach be employed to determine which software is prohibited. In addition, the presentation of evidence demonstrating

141 Monsch (n 8) 152.

142 Şirin Aydıncık, *Fikri Haklara İlişkin Lisans Sözleşmeleri* (Arıkan 2006) 176.

the status of software licences may be required regularly for verification. In instances where uncertainty persists, the employment contract may require the delivery of devices for conducting necessary inspections.

Conclusion

A review of the legislation on Turkish labour law reveals the absence of any explicit provisions regulating the practise of BYOD. It is closely linked to the protection of personal data and intellectual property law. It can thus be argued that the legislative burden on legislators is intensifying. The issues addressed within the BYOD context apply to other models provided they are compatible with their inherent characteristics. The following conclusions can be drawn regarding labour law.

1. In the employment relationship, the use of employees' personal IT devices for work-related purposes necessitates the existence of a specific agreement, such as provisions set forth in the employment contract or an addendum. Implementing mobile device management systems to segregate and control data on IT devices is essential. Thus, it follows that workplace practises or the employer's management rights do not constitute the basis for BYOD. The regulation of this model through legal instruments other than an employment contract is at odds with the fundamental principles in place to protect employees.

2. The BYOD encompasses an employee's personal IT devices. Given the continuous accessibility of such devices for personal use, special regulations regarding working hours need to be established. When considering the issue of working hours in the context of BYOD, it is necessary to consider the periods of standby duty for employees. In cases where there is a dispute regarding these periods, the decision of the Court of Cassation is often dependent on whether the employee is allowed to move freely during the standby period. In determining working hours for employees using BYOD devices outside of the workplace, it is necessary to consider the extent to which the employee is able to structure their standby duty freely, as well as the degree to which employer instructions restrict their activities during this time. Regarding periods of rest, it is of the utmost importance to strike a balance between the utilisation of BYOD devices and the respect of employees' private lives. In this context, in our opinion, it is incumbent upon the employer to consider the employee's right to disconnect from constant access, although the employee's right to disconnect has not yet been regulated.

3. In the BYOD policies, where employees use their personal IT devices for work-related purposes, Article 413/II of TCO allows them to claim expenses related to their work. This includes the device itself, connection and subscription fees, electricity costs, technical support, and repair expenses. However, in the case of optional BYOD,

the onus is generally laid down on the employer to provide the necessary working tools. Nevertheless, in this scenario, due to the employee's familiarity with and ease of use of their own IT device, unless otherwise agreed, the employee assumes the financial responsibility for BYOD.

4. The utilisation of BYOD may cause liabilities. It is essential to consider the respective responsibilities of both the employee and the employer in relation to these liabilities. From the standpoint of the employee, the source of liability is determined by the provisions of Article 400 of TCO. In accordance with this stipulation, the employee is held accountable for any damages incurred by the employer because of negligence. In accordance with paragraph 2 of this article, consideration should be given to an employee's training and expertise if an IT device used by an employee causes harm. If the role performed by an employee (for example a data security specialist) requires a high level of responsibility, it may be inferred that the work is inherently prone to loss. On the other hand, from the perspective of the employer, the obligation to safeguard the devices brought by employees to the workplace arises from the employer's duty to supervise the employee. Failure to fulfil this obligation, which would result in harm, could lead to the employer's liability under contractual liability provisions, allowing the employee to claim compensation for the damages incurred.

5. In the BYOD, it is necessary to address the issue of delivering devices to the employer as a separate matter. If the parties have stipulated a delivery obligation within the contract, the employee is bound by the terms of the agreement to deliver the device to the employer. In the absence of an agreement between the parties, the delivery obligation should be considered only in exceptional cases, which are justified by the employer's main interests in light of the specific conditions of the case. In balancing interests, factors such as criminal suspicion, the potential extent of harm incurred if the device is not returned, or the duration of its deprivation may be considered. Furthermore, in accordance with Article 443 of the TCO, an employee must return any items received from the employer in connection with the work. In the alternative models (COPE or CYOD), upon termination of the employment contract, the employee is also required to return the relevant devices to the employer.

6. To ensure adequate protection of personal data, it is of the utmost importance to segregate data stored on BYOD devices. In this regard, it is the employer to implement the necessary technical measures, including the use of data containers and virtualisation solutions. Furthermore, an additional measure that an employer may implement in accordance with a BYOD policy is the creation of a blacklist. In accordance with the stipulations of management rights, the employer is vested with the authority to determine the minimum technical prerequisites that must be

satisfied for the device to be utilised in a BYOD. Nevertheless, certain devices and software may possess functions that could compromise the confidentiality, integrity, or availability of work-related data. It is within the prerogative of the employer to prohibit the use of such programmes and devices that are classified as critical for security reasons.

7. The practise of BYOD is a prominent feature of the utilisation of computer programmes installed on IT devices for the fulfilment of duties. The transfer of usage rights over intellectual property rights in programmes is subject to the terms set forth in licencing agreements. It is therefore imperative that attention be paid to licencing agreements in order to avoid infringements of intellectual property rights in employment relationships involving BYOD use.

Peer-review: Externally peer-reviewed.
Conflict of Interest: The author has no conflict of interest to declare.
Financial Disclosure: The author declared that this study has received no financial support.

Bibliography

Arbek Ö, *Fikir ve Sanat Eserlerine İlişkin Lisans Sözleşmesi* (Yetkin Yayınları 2005)

Aydıncık Ş, *Fikri Haklara İlişkin Lisans Sözleşmeleri* (Arıkan 2006)

Barton DM, 'Betriebliche Übung und private Nutzung des Internetarbeitsplatzes „Arbeitsrechtliche Alternativen" zur Wiedereinführung der alleinigen dienstlichen Verwendung' [2006] NZA 460

Bartz S and Grotenrath M, '„Bring Your Own Device"-Geräte in internen Ermittlungen' [2019], CCZ 184.

Baycık G, *Türk-İsviçre Hukukunda İşçinin Hukuki Sorumluluğu* (Yetkin Yayınları 2015)

Baysal U, 'İşçiye Ait Taşınabilir İletişim Cihazlarının İş Amaçlı Kullanılması' [2018] Sicil İş Hukuku Dergisi 65

Bertram A and Falder R, 'Datenschutz im Home Office-Quadratur des Kreises oder Frage des guten Willens?' [2021], ArbRAktuell 95.

Centel, T. 2017. *Introduction to Turkish Labour Law* (Springer 2017)

Chandna-Hoppe K, 'Essentielle Arbeitsmittel und mobile Arbeit' [2023] RdA 152

Çatalkaya DU, 'Kişisel Yaşamı Kapsamında İşçinin, İşverence "Ulaşılabilir Olmama" Hakkı' (2016) 74 Journal of Istanbul University Law Faculty 737

Çelik N, and others, *İş Hukuku Dersleri* (36th edn, Beta Yayınevi 2023)

Civan OE, *İşçinin Yan Yükümlülükleri* (Beta Yayınevi 2021)

Conrad I and Schneider J, 'Einsatz von „privater IT" im Unternehmen Kein privater USB-Stick, aber „Bring your own device" (BYOD)?' [2011] ZD 153

W. Däubler, *Digitalisierung und Arbeitsrecht* (7th edn, Bund Verlag 2020)

Dereli T, Soykut Sarıca YP and Taşbaşı A, *Labour Law in Turkey* (3rd edn, Kluwer Law International 2023)

Doğan S, *İş Hukukunda İşçinin İş ve Aile Yaşama Uyumunun Sağlanması* (Seçkin Yayıncılık 2022)

Dursun Ateş S, *İşverenin Yönetim Hakkı* (Seçkin Yayıncılık 2019)

Ekmekçi Ö, Korkusuz MR and Uğur Ö, *Turkish Individual Labour Law* (2nd edn, Onikilevha Yayıncılık 2023)

Elbir N, *Kişiliğinin Korunması Bağlamında İşçiye Ait Kişisel Verilerin Korunması* (Yetkin Yayınları 2020)

Emrağ SE, *Yararlılık İlkesi* (Onikilevha Yayıncılık 2022)

Faas T, 'WhatsApp & Outlook auf dem beruflichen Smartphone: Haftungsrisiken und Auswege' [2018] ArbRAktuell 594

Ganiyu, S.O. and Jimoh RG, 'Characterising Risk Factors and Countermeasures for Risk Evaluation of Bring Your Own Device Strategy' (2018) 7 International Journal of Information Security Science, 49

Göpfert B, Wilke E. 'Nutzung privater Smartphones für dienstliche Zwecke' [2012]. NZA 765.

Grieger F. 'Bring Your Own Device in Der Unternehmenspraxis' [2023], MMR 168.

Günther J and Böglmüller M (2015) 'Arbeitsrecht 4.0 – Arbeitsrechtliche Herausforderungen in der vierten industriellen Revolution' [2015] NZA 1025

Hamdi M, Astarlı M and Baysal U, *İş Hukuku* (7th edn, Lykeion 2022)

Herrnleben G, 'BYOD – die rechtlichen Fallstricke der Software-Lizenzierung für Unternehmen' [of] MMR 205

Hoppe C (2023) 'Bring your own device (BYOD)' in Stefan Kramer (ed), IT-Arbeitsrecht (3rd edn, CH BECK 2023)

Hüseyinli N and Ünal E, 'Avrupa Birliği adalat Divanı Kararı Işığında, Türk İş Hukuku'nda Çalışma Sürelerinin Kayıt Altına Alınması' (2024) 7 Necmettin Erbakan Üniversitesi Hukuk Fakültesi Dergisi 44

Kascherus S and Pröpper M, 'Bring your own device (BYOD) - Mitbestimmung bei der Nutzung privater technischer Geräte' [2021], Betriebs-Berater 756

Kılıç Ş, 'Employment Law' in Şebnem Kılıç (ed), *Introduction to Turkish Business Law* (Peter Lang 2022)

Klocke D and Hoppe S (2022) 'Der Anspruch auf essenzielle Arbeitsmittel' [2022] NZA-RR 515

Koch FA, 'Arbeitsrechtliche Auswirkungen von „Bring your own Device" – Die dienstliche Nutzung privater Mobilgeräte und das Arbeitsrecht' [2012] ITRB 35

Korkusuz MR and Uğur Ö, 'Turkish Individual Labour Law' in M Refik Korkusuz and Ferna İpekel Kayalı (eds), Turkish Private Law (3rd edn, Seçkin Yayıncılık 2024) 114

Küzeci E and Kılıç Ş, '6698 Sayılı Kişisel Verilerin Korunması Kanunu'nun İş Sözleşmesi Çerçevesinde Değerlendirilmesi: Veri Sorumlusu, Veri İşleyen ve Diğer Aktörler' (2019) 16 Legal İş Hukuku ve Sosyal Güvenlik Hukuku Dergisi 947

Lee JH and Tinmaz H, 'A Perceptional Analysis of BYOD (Bring Your Own Device) for Educational or Workplace Implementations in a South Korean Case' (2019) 6 Participatory Educational Research 51

Lipp K, 'Bring Your Own Device (BYOD) – Das neue Betriebsmittel', *Law as a service (LaaS): Recht im Internet- und Cloud-Zeitalter [Tagungsband Herbstakademie 2013]* (OlWIR, Oldenburger Verlag für Wirtschaft, Informatik und Recht 2013)

Monsch C, *Bring Your Own Device (BYOD): Rechtsfragen der dienstlichen Nutzung arbeitnehmereigener mobiler Endgeräte im Unternehmen* (Duncker & Humblot 2017)

Müller F. 'Bring Your Own Device (BYOD) im öffentlichen Dienst' [2021] öAT 23

Okur Z, *İş Hukuku'nda Elektronik Gözetleme* (Legal Yayıncılık 2013)

Pollert D. 'Arbeitnehmer-Smartphone als Betriebsmittel–ein kostensparendes Modell?' NZA-Beilage 152

Raif A and Nann P, 'Arbeitsrecht 4.0 – Möglichkeiten und Hürden in der digitalen Arbeitswelt' [2016] GWR 221

Şahan G, *Bilgisayar Programı İmâl Sözleşmesi* (Yetkin Yayınları 2016)

Savaş Kutsal FB, *İşçinin Ulaşılabilir Olmama Hakkı* (Seçkin Yayıncılık 2024)

Schmidt B and Roschek A-K, 'Datenschutz Im Anwaltlichen Home- Und Mobile-Office' [2021], NJW 367.

Sümer HH, *İş Hukuku Uygulamaları* (7th edn, Seçkin Yayıncılık 2019)

Süzek S, *İş Hukuku* (23rd edn, Beta Yayınevi 2023)

Wisskirchen G, Schiller JP. 'Aktuelle Problemstellungen im Zusammenhang mit „Bring Your Own Device"' [2015]. Der Betrieb 1163

Yamakoğlu E, *Bilişim Teknolojilerinin Kullanımının İş Sözleşmesi Taraflarının Fesih Hakkına Etkisi* (Onikilevha Yayıncılık 2020)

Zöll O and Kielkowski JB, 'Arbeitsrechtliche Umsetzung von „Bring Your Own Device" (BYOD)' [2012] Betriebs-Berater, 2625.