

Adrienn Lukács
University of Szeged
Faculty of Law and Political Sciences
lukacs.adrienn@juris.u-szeged.hu

WORKING FROM HOME AND EMPLOYEES' RIGHT TO DATA PROTECTION DURING THE COVID-19 PANDEMIC IN HUNGARY

Abstract: *The COVID-19 pandemic shook the globe, and also had a great impact on the world of work. Due to the different restrictions and lockdowns, many employees started to work from their homes. What had been a relatively marginal phenomenon before, became widespread. However, the sudden proliferation of working from home came together with increased need for employee monitoring – raising several data protection questions. In Hungary, several acts regulate the protection of (employees') personal data, however, they were adopted with mainly keeping in mind the “traditional” employment relationship, when the employee works from the employer's premises. Nevertheless, working from home can have certain characteristics which raise specific data protection challenges. By reviewing the relevant legal literature and legal provisions, the article presents the applicable Hungarian legal framework and examines the data protection challenges in relation to working from home. The aim of the article is to examine, compared to data processing in the traditional employment relationship, the specific characteristics of working from home which make it increasingly important to ensure employees' right to data protection.*

Keywords: *data protection, employee monitoring, telework, home office, COVID-19.*

1. Introduction

The COVID-19 pandemic gave rise to new kinds of data processing in the employment context. On the one hand, employers had the interest to ensure the continuous and effective functioning of the workplace – which led to various kinds of data processing: collecting information about the employees' health status, infection or vaccination, as well as monitoring whether employees work efficiently

while they work from home. However, on the other hand, the employees' rights, notably the right to privacy and the right to data protection must be respected.

As many employers sent home their employees due to the lockdowns, telework and home office went on the rise. Although the general data protection rules also adequately apply to the control of employees working from home, the different place of work leads to different data protection challenges. In addition, as a consequence of the pandemic, it was an additional challenge that the spread of telework and home office was extensive, rapid and in certain cases they were introduced against the will of the party or parties, as a result of mandatory lockdowns. This led to several employers compensating the unpreparedness and/or the lack of trust in employees working from home with increased monitoring – resulting in data protection challenges. Thus the importance of identifying the sensitive points of this monitoring is crucial in order to ensure the employees' right to data protection.

The article focuses on the relevant Hungarian legal regulations regarding working from home during the 1st-3rd waves (March 2020 – June 2021) of COVID-19. By reviewing the relevant legal literature and legal provisions, first, the article presents the applicable Hungarian legal framework, then examines the data protection challenges in relation to working from home. The aim of the article is to examine, compared to data processing in the traditional employment relationship, the specific characteristics of working from home which make it increasingly important to ensure employees' right to data protection.

2. The right to data protection and employees working from home

Regarding the applicable legal framework, in Hungary the right to data protection is regulated by different general and sector specific norms. Concerning the general norms, the constitution (*Fundamental Law*) declares the protection of the right to privacy and the right to data protection, providing a constitutional protection to these rights.¹ The *Hungarian Civil Code* (Act V of 2013) affords protection to the right to data protection (and to the right to respect for private life) on the ground of personality rights. The primary objective of personality rights is to ensure protection to rights which make humans human, which are parts of human personality, without examining the societal circumstances – excluding from their scope political, cultural and social rights.² *Act LIII of 2018 on the Protection of*

¹ Subsection (1) of Article VI of the Fundamental Law states that “[e]veryone shall have the right to respect for his or her private and family life, home, communications and reputation” and Subsection (3) states that “[e]veryone shall have the right to the protection of his or her personal data, as well as to have access to and disseminate information of public interest.” However, the right to data protection is not an absolute right, it can be limited by the application of the necessity and proportionality test.

² Tamás Fézer, “Harmadik rész: személyiségi jogok”, *A Polgári Törvénykönyvről szóló 2013. évi V. törvény és a kapcsolódó jogszabályok nagykommentárja. I. kötet.* (ed. András Osztovits) Opten Informatikai Kft., Budapest 2014, 250.

Private Life (hereinafter: Privacy Act) is a “national curiosity” because, since the adoption of this act, the protection of private life is not only ensured by the Fundamental Law and the Civil Code but also constitutes the subject of a separate act. The aim of the right to respect for private life is to protect especially the right to bear a name, personal data, private secrets, image and voice recordings, honour and good reputation. Its infringement can occur especially through the abuse of personal data, secret, image and voice recording intended to be protected by the individual in relation to his/her private life and through the infringement of honour and good reputation.^{3, 4}

Besides these general norms, attention should be paid to the sector specific regulations. These sector specific norms either focus on data protection exclusively or on workplace data protection. Among these specific regulations, the data protection act (Act CXII of 2011 on the Informational Self-determination and the Freedom of Information, hereinafter referred to as: HDP, standing for Hungarian Data Protection Act) in line with the European Union’s General Data Protection Regulation (hereinafter referred to as: GDPR) should be mentioned. Specific rules are to be found in the Labour Code (Act I of 2012, hereinafter referred to as HLC), which contains employment specific data protection rules.

2.1. The general data protection framework

Since 2004 Hungary has been a Member State of the European Union, which means that it has to meet the legal requirements arising from its membership. The data protection rules are to be found in the HDP. However, as the previous EU data protection directive⁵ was replaced in 2018 by the GDPR, significant changes occurred in the Hungarian data protection system as well.

As the GDPR is directly applicable in the Member States, it is not possible for the HDP to repeat or transpose the provisions of the GDPR. For this reason, the HDP had to be significantly amended⁶ – which, prior to the EU data protection reform, regulated the issue of personal data protection comprehensively, in the form of a code. Thus, with the GDPR, the role of the HDP was significantly changed, as a general rule, the GDPR should apply in the field of data protection.⁷ The

³ Subsections (1)-(2) of Section 8 of the Privacy Act

⁴ On the general rules regarding the right to respect for private life and the right to data protection in Hungary see more in: Adrienn Lukács, *Employees’ Right to Privacy and Right to Data Protection on Social Network Sites: with Special Regard to France and Hungary*, Iurisperitus Kiadó, Szeged 2021, 44ff.

⁵ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, 31–50.

⁶ By Act XXXVIII of 2018.

⁷ Attila Péterfalvi, Balázs Révész, Péter Buzás (eds.), *Magyarázat a GDPR-ról*. Wolters Kluwer Hungary, Budapest 2018, 42.

HDPa is applicable in particular in the following cases: when it *complements the GDPR* upon the authorization of the GDPR (e.g. Article 9 on the processing of special categories of personal data); when it *implements the GDPR* (e.g. rules relating to the composition and functioning of the data protection authority) or when *the GDPR does not cover a question* (e.g. post-mortem data protection.) Also, the GDPR does not regulate freedom of information, which is regulated by the HDPa.

The GDPR has also introduced significant changes to *processing in the employment context*. Although having a regulation instead of a directive indeed leads to more uniformity, it does not mean that no differences exist between Member State regulations, as in certain questions the GDPR empowers Member States to adopt specific rules. Particularly, Article 88 of the GDPR contains *special provisions* regarding processing in the employment context, stating that Member States can provide for more specific rules in order to ensure employees' right to data protection.⁸ Such rules should include suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights, with particular regard to, amongst others, monitoring systems at the workplace.⁹ This means – as there is no unified “EU labour law” – that some differences between Member State regulations still exist in the field of employment monitoring.

The HDPa contains the detailed rules regarding the functioning of Hungary's data protection supervisory authority, the Hungarian National Authority for Data Protection and Freedom of Information (“Nemzeti Adatvédelmi és Információszabadság Hatóság”, hereinafter referred to as: NAIH). The NAIH is responsible for monitoring and promoting the enforcement of two fundamental rights: the right to the protection of personal data and the right to freedom of information (access to data of public interest and data accessible on public interest grounds) in Hungary, as well as promoting the free movement of personal data within the European Union. Regarding the organisational perspective, the NAIH is an autonomous public administration organ; it may not be instructed in its functions and shall operate independently of other organs and of undue influence.¹⁰

2.2. Employee data protection

As regards the number of employees working from home, it greatly increased during the pandemic.¹¹ In parallel with the sudden spread of telework and home

⁸ Catherine Schultis, “Le traitement de données dans le cadre des relations de travail dans le règlement sur la protection des données personnelles”, *Dalloz IP/IT*, (5) 2017, 266.

⁹ Article 29 Data Protection Working Party, *Opinion 2/2017 on data processing at work*, 17/EN WP 249, 2017, 9.

¹⁰ NAIH, *About the Authority*, <https://www.naih.hu/about-the-authority> (Accessed: 30. 08. 2021.)

¹¹ European Commission, *Telework in the EU before and after the COVID-19: where we were, where we head to*, https://ec.europa.eu/jrc/sites/default/files/jrc120945_policy_brief_-_covid_and_telework_final.pdf (Accessed: 25. 06. 2021.)

office, there was an increase in employers' need for monitoring of employees,¹² which intensified the question of protection of employees' rights (in particular the right to the protection of personal data). Even though the data protection requirements are applicable both to "traditional" work performed in the workplace and in the home, these requirements were adopted to mainly regulate data processing *in the workplace*. This raises the question whether working from home has characteristics which would make the adoption of specific data protection rules necessary.¹³ In the following, these general rules relating to the processing of personal data will be presented, then the specific challenges in relation to working from home will be discussed.

2.2.1. Employee data protection and the Hungarian Labour Code

In Hungary, the employment specific data protection rules are to be found in the HLC. The HLC came into force in 2012 and it brought fundamental changes to workplace data protection. Declaring the protection of personality rights is also a novelty of the HLC in force: the previous Labour Code (1992) contained only very brief provisions regarding workplace privacy and data protection, it did not set the general protection of these rights.¹⁴ After the entering into application of the GDPR, the Hungarian legislator adopted Act XXXIV of 2019 on legislative amendments required for the implementation of the European Union's data protection reform (hereinafter referred to as: Enforcing Act) in April 2019, aiming to adapt the Hungarian

According to the Hungarian Central Statistical Office, in 2020, 8.6% of employees worked in home office or telecommuting, compared to 2.9% in the previous ten years. Source: Központ Statisztikai Hivatal, *Felértékelődött a távmunka a Covid19 árnyékában*, <http://www.ksh.hu/docs/hun/xftp/idoszaki/koronavirus-tavmunka/index.html> (Accessed: 25. 06. 2021.)

¹² Manuela Samek Lodovici (ed.), *The impact of teleworking and digital work on workers and society: Special focus on surveillance and monitoring, as well as on mental health of workers*, European Union, Luxembourg 2021, 55-56.

¹³ The pandemic did not only create challenges for processing personal data outside the workplace, but also raised new questions regarding employees working in the workplace – such as whether and how employers could process information about the employees' health status, infection or vaccination. Employers had the interest to ensure the continuous and effective functioning of the workplace in spite of the pandemic. Also, the responsibility for the implementation of occupational safety and occupational health requirements lies with the employers. Collecting information about the employees' health status, infection or vaccination can contribute to achieving these objectives. Thus, many employers have contacted the NAIH regarding what their options are, what data they can process. In March 2020, the NAIH issued an information notice on processing data related to the coronavirus epidemic. (NAIH, *Tájékoztató a koronavírus járvánnyal kapcsolatos adatkezelésekről*, NAIH/2020/2586) and later its standpoint was refined in various documents (see, for example: NAIH, *Tájékoztató az új típusú koronavírus járványra (Covid-19) tekintettel az egészségügyi válsághelyzet elrendelésével bevezetett járványügyi készültség időtartama alatt a testhőmérséklet mérésével összefüggő egyes adatkezelések kapcsán*, NAIH/2020/7465).

¹⁴ Zsolt Györg Balogh et al., "Munkahelyi adatvédelem a gyakorlatban", *Infokommunikáció és Jog*, 9(3), 2012, 99.

legal system to the GDPR, by amending more than 80 acts. The Enforcing Act also concerned the HLC, as in accordance with Article 88 of the GDPR, specific rules were introduced.

The Enforcing Act introduced some important changes in the field of data protection, considerably increasing the number of provisions dealing with this matter. Now these matters are regulated under a separate title (“Title 5/A: Data processing”) containing three Sections: *Section 10* regulating employee statements, disclosure of information and aptitude tests, *Section 11* on the processing of sensitive data (biometric and criminal personal data) and *Section 11/A* relating to employee monitoring. Section 10 and Section 11/A existed before the amendment as well, although the Enforcing Act modified them and extended them with additional rules. Section 11 on sensitive data is completely new.

Regarding employee data protection, the activity of the NAIH should be mentioned, which considerably shaped employment data protection through investigating the complaints, as well as through publishing different recommendations or information notices. Notably, the NAIH issued a comprehensive information notice on the general requirements of workplace data processing in 2016,¹⁵ providing detailed insight into the NAIH’s approach to the most common employment-related data processing operations. The NAIH also emphasised that the approach outlined in this guidance remained mostly the same even after the GDPR became applicable in 2018.¹⁶

2.2.2. *Working from home and employee data protection*

Before addressing the specific characteristics of data protection in the case of working from home, it must be discussed how an employee can work from home from a labour law point of view. Considering the “traditional” pre-pandemic forms of working from home, the employee had the opportunity to work outside the employer’s premises even before the COVID-19 pandemic. The HLC regulates teleworking and outworking, and although the HLC does not regulate it *expressis verbis*, home office is also known in practice. Although in common parlance these terms (especially telework and home office) are often used interchangeably, they are by no means identical legal institutions. Besides, during the COVID-19 pandemic, the importance of telework and home office increased, while outworking was mainly unaffected by the pandemic. Thus, the focus of the article will be put on the examination of telework and home office.

¹⁵ NAIH, *A Nemzeti Adatvédelmi és Információszabadság Hatóság tájékoztatója a munkahelyi adatkezelések alapvető követelményeiről*, 2016

¹⁶ Dóra Petrányi, Márton Domokos, *Hungary: Comprehensive and strict guidance on workplace privacy*, 2017, <https://www.lexology.com/library/detail.aspx?g=602076fa-cdc1-4642-aa98-dc21c-508ce85> (Accessed: 30. 08. 2021.)

2.2.2.1. Telework and home office

Working from home is possible in the frame of several legal institutions. On the one hand, among the atypical forms of work, the HLC regulates telework and outwork – which differ from the typical forms of employment regarding the place of work. Subsection (1) of Section 196 of the HLC regulates *telework*. One of its most important characteristics is that work activities are performed *on a regular basis* at a place other than the employer’s facilities. Such a place might be the home of the employee, a satellite office or a telework centre or it can even be performed as mobile telework.¹⁷ Another important feature is that the employee works through using computing equipment and delivers the end product by way of electronic means. *Outwork* differs from teleworking (Sections 198-200 of the HLC) as in this case the place of work is the employee’s home (or another place designated by the parties), the contract is concluded to provide a job that can be performed independently, and it is remunerated exclusively on the basis of the work done.

On the other hand, although it is not specifically mentioned in the HLC, the institution of *home office* is also known in practice. Unlike teleworking and outworking, working in a home office is not considered as an atypical form of employment, but an exceptional variation/change in the place of work. Namely, the employer may exceptionally allow work to be carried out in a place other than the place of work, usually in the employee’s home.¹⁸ Working in home office takes place on an *ad hoc* and non-regular basis, and the employee’s work schedule remains unchanged. While in teleworking, as a general rule, the employee’s work schedule is flexible, the work schedule of the employee working in home office does not change compared to the work schedule of the work performed at the employer’s premises.¹⁹

2.2.2.2. Data protection challenges regarding telework and home office

In relation to working from home (either in the case of telework or home office) several *data protection challenges* arise, especially in the field of employee monitoring. Although the data protection regulations examined above are also adequately applicable to the monitoring of employees working from home, the different place of work may lead to specific data protection challenges.

With regard to *working time*, one of the main obligations of an employee is to spend his/her working time working [Subsection (1) of Section 52 of the HLC], and at the same time it follows from the employer’s power of control that he/she is

¹⁷ Zoltán Bankó, *Az atipikus munkajogviszonyok*, Dialóg Campus Kiadó, Budapest – Pécs 2010, 162.

¹⁸ György Kiss (ed.), *Munkajog*, Dialóg Campus, Budapest 2020, 359.

¹⁹ Bálint Vargha (ed.), *Elemzés. Távmunka, otthoni munkavégzés, lehetőségek, kockázatok*, Állami Számvevőszék, Budapest 2020, 15.

entitled to control whether the employees actually comply with this contractual obligation. The employer has several means to control: although difference must be made between what is technologically possible and what is in compliance with the law/legally possible. According to the HLC – and this applies to all methods of control which involve data processing, regardless of the exact method – a restriction of the employee's personality rights must be deemed strictly necessary for reasons directly related to the intended purpose of the employment relationship and if proportionate for achieving its objective. Another important requirement is that employees must be informed in advance about the restriction of their personality rights, about data processing and about the monitoring of the computer device [Subsection (2) of Section 9, Subsection (5) of Section 10, Subsection (1) of Section 11/A of the HLC] – excluding the lawful use of covert surveillance.

In contrast to working from the employer's premises – in which case the workplace serves as a place dedicated to perform work – in the case of telework and home office, the physical boundaries of professional life and personal life are completely blurred, possibly having an effect on the respect of working hours as well. In the context of the mass ordering of working from home due to the pandemic, it is necessary to draw attention to the differences between teleworking and home office, and to the specificities of quarantine affecting the lives of the individuals in several regards. *On the one hand*, it does matter whether the work is done as telework or as home office: while in the case of home office the work schedule is the same as in the workplace, telework, as a main rule, comes with a flexible work schedule. Consequently, strictly monitoring the work schedule of such a teleworker would not be in accordance with the law. *On the other hand*, the question arises as to what extent, given the changed circumstances, the worker can be expected to adhere to a strict working schedule and to its strict monitoring, with regard to the specific characteristics of working from a “quarantine office”. In contrast to “traditional” home office, during quarantine the employees' home might be used by other people who have to work from home themselves as well, or their children have to study from home – not making it possible to create a proper working environment, where the employee can focus only on his/her work. All these exceptional “quarantine” situations might make it increasingly difficult for the employee to adhere to the established strict work schedule. Consequently, the question arises – if the nature of the employee's job allows it – whether instead of a strict monitoring of the working hours, emphasis should be put on performing the task instead.

As regards the *equipment used for work*, it is an important factor whether it is owned by the employer or the employee. As a main rule, the employee can use the information technology and computing equipment provided by the employer for the performance of work solely [Subsection (2) of Section 11/A of the HLC], while it is not subject to such an obligation as regards his/her own computing equipment. Ownership might have an impact on the possible extent of monitoring: the employer

shall be entitled to inspect only information which is related to the employment relationship. [Subsection (3) of Section 11/A of the HLC] If the computing equipment can be used for both official and personal purposes, increased attention should be paid to the data protection requirements.

The question arising in the case of telework and home office is whether the employer was capable of providing computer equipment to employees who suddenly *en masse* started to work from their homes, and how often employees working from home had to use their own devices. With the sudden introduction of telework or home office, employers and employees might not have had the time to prepare for the different working conditions. If an employee uses his/her own device for work, it can be more difficult not to use the device for personal purposes during working hours. Consequently, it is extremely important to train or educate employees regarding the use of the equipment and to provide them guidance regarding the effective separation of personal and professional life.

In the employer's premises, it is not uncommon to use camera surveillance *to monitor the workplace* and/or the employees. In extreme cases, it may also happen that, by analogy with camera surveillance at work, the employer would like to resort to the use of webcam surveillance of employees working from home. As an example to illustrate such a measure, the programs *Pragli* and *Sneek* can be mentioned. *Pragli*, on the one hand, allows the employer to measure online activity (active or idle) and, on the other hand, allows employees to call a colleague *at any time* via video call – analogous to when they go into a colleague's office in the workplace. For this reason, *Pragli* encourages employees to keep their microphones and cameras on at all times. *Sneek* takes a snapshot of the employee with the webcam every minute, making it visible whether the employee is working. Such measures raise the issue of privacy with particular intensity, as webcams do not only constitute processing of the employees personal data, but can also provide a glimpse into one of the most fundamental "areas" of their privacy, their home. In addition, it is important to note that in the case of working from home, other persons using the property (e.g. family members, roommates, etc.), who have no legal connection to the employment relationship, may also be subject to such monitoring.

According to the relevant practice of the NAIH, camera surveillance at work must not violate human dignity, must not be directed to a room where the worker spends his/her rest time, and must not be used to monitor only one worker and his/her activities.²⁰ Although these rules have been developed for "traditional" electronic monitoring systems (which were applied in the workplace), working from home can increasingly raise issues of human dignity, besides, the home has traditionally been a major place to spend one's leisure time. Monitoring the home

²⁰ NAIH, *A Nemzeti Adatvédelmi és Információszabadság Hatóság ajánlása a munkahelyen alkalmazott elektronikus megfigyelőrendszer alapvető követelményeiről*, 2013, NAIH-4001-6/2012/V)

would be an intrusion into one of the most private spheres of the employee. In view of all this, the use of webcams as surveillance cameras is not compatible with Hungarian law.

Although the rules outlined above set out expectations regarding “general” data protection requirements, attention should be drawn to the *legislation adopted in response to the pandemic* and to the state of danger which was ordered due to the COVID-19 crisis. These rules not only made it easier to order telework and home office, but also allowed the parties to agree on rules different from the ones laid down in the HLC. On the one hand, *Government Decree 47/2020. (III. 18.) on immediate measures to mitigate the impact of the coronavirus pandemic on the national economy* contained changes affecting the HLC: first, the parties could agree to derogations from any provision of the HLC, second, the employer could unilaterally order telework for thirty days after the end of the state of danger. On the other hand, *Government Decree 487/2020. (XI. 11.) on the application of telework during the state of danger* – which specifically regulated telework but not home office – is another important piece of legislation of the state of danger. According to Decree 487/2020, during the state of danger, the employee’s and the employer’s agreement may deviate from Section 196 of the HLC (Section 3); it contained rules on the reimbursement of the employees’ expenses (Section 2) and on different workplace safety and health. The legislation adopted during the state of danger provided unprecedented flexibility to unilaterally order telework/home office and to adapt the rules governing telework/home office to the agreement of the parties, including rules on the control of employees, potentially allowing derogation from the above-presented rules. However, as there is a hierarchal relation between the parties due to the employee’s vulnerability, the voluntary nature of the agreement might be questioned.

4. Conclusion

In conclusion, although the data protection challenges related to teleworking had existed before the pandemic, the pandemic intensified these challenges by contributing to their mass spread. Teleworkers/Home office workers’ right to data protection can be affected increasingly and to a greater extent compared to working from the employer’s premises. This is especially true in the case when many employees were obliged to work from home due to state regulations, as the employer might try to compensate the lack of physical presence by increased electronic monitoring. However, the rules regulating employee data protection are applicable even to such monitoring. Monitoring working time and the employees’ equipment were identified as especially sensitive areas as the workplace and the home become physically the same, and it is also not uncommon that the same electronic device is used for personal and for professional purposes as well.

The article drew attention to the importance of ensuring the respect of employees' right to data protection when working from home. Ensuring employees' personal data when working from home is not just a temporary obligation: it is very likely that even after the end of the pandemic, telework and home office are not going to disappear from the world of work. Telework/home office can present many advantages for both parties, but in order to use these advantages, both the employer and the employee must take certain measures. From the employer's perspective, the article encouraged the application of a more flexible approach (putting emphasis on the work done and not on when it is done) instead of strictly monitoring every minute of employees' working hours. From the employees' perspective it is important to adopt measures as well: it is recommended to adopt a cautious conduct, aiming to separate personal and professional life (e.g. create a designated work space within the home, if possible, use virtual backgrounds for video calls, try to set up periods for work and for non-work, etc.). Through providing trainings or guidance to employees, the employer can contribute to achieving these objectives. Such measures can also contribute to the respect of the right to data protection.

Lukács Adrienn
Szegei Tudományegyetem
Állam-és Jogtudományi Kar
lukacs.adrienn@juris.u-szeged.hu

Otthonról történő munkavégzés és a munkavállalók személyes adatok védelméhez való joga a covid-19 pandémia alatt Magyarországon

***Absztrakt:** A COVID-19 világjárvány megrázta az egész világot, és nagy hatással volt a foglalkoztatásra is. A különböző korlátozások és lezárások miatt rengeteg munkavállaló otthonról kezdett munkát végezni: ami korábban viszonylag marginális jelenség volt, az széles körben elterjedtté vált. Az otthoni munkavégzés hirtelen elterjedése azonban a munkavállalók ellenőrzésének megnövekedett igényével járt, ami számos adatvédelmi kérdést is felvet. Magyarországon több törvény is szabályozza a (munkavállalók) személyes adatainak védelmét, azonban ezeket elsősorban a „hagyományos” munkaviszony szem előtt tartásával fogadták el, amikor a munkavállaló a munkáltató telephelyéről végez munkát. Mindazonáltal az otthoni munkavégzésnek lehetnek bizonyos jellemzői, amelyek különös adatvédelmi kihívásokat vetnek fel. A cikk a vonatkozó jogirodalom és jogszabályi rendelkezések áttekintésével bemutatja a magyar jogszabályi keretrendszert, és megvizsgálja az otthoni munkavégzéssel kapcsolatos adatvédelmi kihívásokat. A cikk célja, hogy megvizsgálja a hagyományos munkaviszonyban történő adatkezeléshez képest az otthoni munkavégzés azon sajátosságait, amelyek kiemelten fontosá teszik a munkavállalók személyes adatok védelméhez való jogának biztosítását.*

***Kulcsszavak:** adatvédelem, munkahelyi ellenőrzés, távmunka, home office, COVID-19.*

Адриен Лукач
Универзитет у Сеједину
Правни факултет
lukacs.adrienn@juris.u-szeged.hu

Заштита података о личности запослених који раде код куће услед пандемије вируса COVID-19 у Мађарској

Сажетак: Пандемија вируса COVID-19 променила је свет око нас, а посебно значајан утицај имала је на свет рада. Због различитих ограничења и заштита, многи запослени су почели да раде у својим домовима. Тако је рад код куће од једне маргиналне појаве, постао широко распрострањен облик рада. Ипак, ова изненадна распрострањеност рада код куће резултирала је повећаном употребом за спровођењем надзора над радом запослених што је отворило низ питања у вези са заштитом података о личности запослених. Области заштите података о личности у Мађарској уређена је са неколико различитих закона. Међутим, сви они су базирани на традиционалном имању радног односа, који подразумева да запослени раде у просторијама послодавца. Ипак, рад код куће, због својих карактеристика, поставља специфичне изазове за заштиту података о личности запослених. Прећедом релевантне правне литературе и законских одредаби, у овом раду је најпре представљен важећи правни оквир заштите личних података запослених у Мађарској, а потом се скреће пажња на отворена питања која са тим у вези узрокује вршење рада код куће. Циљ овог рада је да се истражују специфичности заштите података о личности запослених који раде код куће.

Кључне речи: заштита података о личности, надзор над радом запослених, рад код куће, COVID-19.