Labour Law and Cybersecurity in Higher Education

Klemen Drnovšek
University of Maribor, Faculty of Law, Maribor, Slovenia
klemen.drnovsek@um.si

Abstract In this chapter, labour law aspects of cybersecurity in the higher education sector are presented. Labour law regulations set the rights and obligations of employees both in the case of typical and atypical labour relations. The worker can also work remotely (teleworking) or in home office (homeworking), respectively, whilst in this case, they must respect legislative provisions and instructions by their employer. Internet development and digitalisation essentially influenced the field of labour law. Due to the consequences of the pandemic disease COVID-19, drastic changes also appeared in the field of higher education practically overnight. The use of e-mail, data clouds, e-learning environments, video conference ways of conducting the study process, the examination and other internet activities of performance of study programmes represent different risks that must be tackled by higher education institutions. Aiming to lower security risks, educational institutions must constantly recognise these and train their employees in proper ways to provide for cybersecurity.

Keywords:
labour law;
employment law,
cybersecurity,
higher education,
COVID-19,
security policy,
diligence,
liability,
mitigation of risks

University of Maribor Press

DOI https://doi.org/10.18690/um.1.2023.4
ISBN 978-961-286-693-8

1 General

Labour can be performed on the basis of various legal bases, whereby the choice of the appropriate legal basis depends primarily on the nature of the work that the individual performs. In higher education, labour is done by scholars, higher education employees, researchers and students, who perform pedagogical and research labour, as well as by administrators performing technical, administrative, professional and other tasks. Despite the very varying nature of work of people employed in higher education institutions, practically all do their labour based on an employment contract. Due to specific work, the labour of scholars steps out. However, relations towards higher education institution still remains such that by performing their labour scholars meet the basic elements of a labour relation. A labour relation exists, when an individual does labour in a way that he or she is included in an organised labour process and does labour for payment, personally and without interruption, in line with instructions and under supervision by the employer, in our case – the higher education institution. Only exceptionally, the base of labour may be another contract of civil law (e.g., copyright agreement) or another legal base appearing especially in cases of short-term and occasional labour, for example when a certain lecturer conducts only an individual lecture or module at some higher education institution and obtains payment for that.

For all employees who have concluded employment contracts, or whose nature of work meets the elements of an employment relationship (Darja Senčur Peček & Franca, 2019: 114-132), special rights and obligations apply, which are grouped under the term "Labour Law". On the one hand, there are rules relating to the individual relationship between the employee and the employer (Employment Law). These include, in particular rules on the conclusion of employment contracts, their termination, remuneration, distribution of working time, breaks and rest periods, annual leave, protection of certain categories of workers, liability of the employee and the employer, etc. On the other hand, Labour Law consists of rules that regulate the relationship between workers' associations (unions) and employers or employers' associations (Collective Labour Law). In this case, these are autonomous rules that are not set by the legislator but are the result of negotiations and mutual agreement between the various stakeholders in the employment relationship. Consequently, the rules of labour law are regulated in various heteronomous and autonomous legal

acts. The basic source of any employment relationship is the employment contract, which must not contradict cogent regulations.

At the European Union level, a set of rules and arrangements have been adopted governing various areas of labour law and must be considered in the national laws of the Member States[1]. Among the autonomous sources, in addition to collective agreements at various levels (at the level of the employer – e.g., Harvard University & Harvard Union of Clerical and Technical Workers Agreement[2], at the branch level - e.g., Collective Labour Agreement for Dutch Universities[3], and general (unilateral) acts of the employer by which the employer regulates the organization of work - e.g., Rules on the protection of personal and confidential data at the University of Ljubljana[4]).

Labour law is a relatively young industry that began to develop in the early 19th century during the Industrial Revolution. The purpose of the first acts was in particular to improve working conditions (e.g., adequate ventilation of premises), to limit working hours (e.g., a maximum of 10 hours per day), to set restrictions on the work of children and women, etc. Over time, the rules of labour law have spread to virtually every area of our lives. It is characteristic of a classic employment relationship that the employee performs work on the employer's premises, whereby the employer must provide appropriate working conditions, working means, providing protective equipment and a safe and healthy working environment. Initially, the requirement to ensure a safe and healthy environment was mainly related to material circumstances (e.g., machinery, hazardous substances, etc.), but today the emphasis is on intangible assets such as online security, mental health, etc.

[1] See https://eur-lex.europa.eu/summary/chapter/1717.html.
[2] Harvard University & Harvard Union of Clerical and Technical Workers Agreement, available at: https://hr.harvard.edu/union-contracts.
[3] Collective Labour Agreement for Dutch Universities, available at: https://www.vsnu.nl/en_GB/cao-universiteiten.html
[4] Rules on the protection of personal and confidential data at the University of Ljubljana, available at: https://www.uni-lj.si/university/organization_legal_framework_and_reports/statutes_of_ul_and_regulations/

2 Teleworking

There are several types of employment relationships. A typical employment relationship is based on a full-time employment contract, which depends on national law and is between 35 and 40 hours per week. A typical employment contract is concluded for an indefinite period (it can only be terminated in the case of specific conditions), and the work is performed at the employer's premises. There are several types of atypical employment contracts, e.g., part-time contracts, fixed-term contracts, and atypical employment contracts also include employment contracts for homeworking or teleworking.

Although cybersecurity issues occur in virtually all employment relationships, they are most common in the case of teleworking, so the focus of this paper will be on this atypical form of employment.

In order to establish a general framework for teleworking and to ensure greater protection for employees, the European Trade Union Confederation (ETUC), the Union of Industrial and Employers' Confederations of Europe / the European Union of Crafts and Small and Medium-Sized Enterprises (UNICE / UEAPME), and the Center of Enterprises with Public Participation (ECPE) signed Framework Agreement on Telework (July 2002)[5]; The agreement defined telework as a form of organizing and/or performing work, using information technology, in the context of an employment relationship, where work, which could also be performed at the employer's premises, is carried out away from those premises on a regular basis. The following basic characteristics of teleworking are derived from the agreement: it is voluntary (it cannot be unilaterally ordered), workers have the same rights as those working at the employer's premises, the employer must provide adequate equipment and personal data protection, respect the employee's privacy. provide him or her with all the necessary equipment and check that the worker meets the conditions for safety and health at work. In 2008, a Report on the implementation of the European social partners' Framework Agreement on Telework was published, which found

[5] Framework Agreement on Telework, available at: https://resourcecentre.etuc.org/sites/default/files/2020-09/Telework%202002_Framework%20Agreement%20-%20EN.pdf

that the Framework Agreement on Telework had been successfully implemented in most EU Member States and EEA Countries[6].

Although the rules on teleworking have been implemented in virtually all national legislation in recent years and the development of the Internet and other forms of digitalisation has had a significant impact on all employment relationships (give source of this affirmation), it can be seen that (until recently) teleworking was rarely done (give source of this affirmation). It is true that workers used machines, computers, robots and other smart devices at work, but the work was still done traditionally on the employer's premises and in relatively strictly defined work frames. The latter was also common for business meetings and other gatherings. Although technology has long enabled remote access to work computers and machines, cloud use, data transfer to private environments, real-time video conferencing meetings, electronic document signing, etc., these tools have been virtually unused in the context of employment law (give source of this affirmation).

In the first half of 2020, however, there was a significant change that had a significant impact on the further development of teleworking. The COVID-19 pandemic has caused, at minimum, temporary drastic transformations in work processes and introduced virtually 100% work from home in most sectors, at least for a limited period of time (give source of this affirmation). Due to several measures to prevent the spread of COVID-19, the work process ~~has~~ moved into different online environments. As in other sectors, people were forced to adapt to new working conditions practically overnight in higher education institutions and to carry out the entire pedagogical process, as well as all administrative and organizational work, remotely via the electronic network. Prior to the COVID-19 pandemic, employees at higher education institutions used e-mails and some learning environments in which they uploaded teaching materials. Those who were more technologically "advanced" may have published a short video of the lecture. In the post-Covid-19 era, the picture is completely different. Many lecturers publish various recordings and other video content, use remote access, collect electronic applications, seminar papers and keep various electronic records. For lectures and meetings (and in some

[6] Commission of the European Communities, Commission Staff Working Paper, Report on the implementation of the European social partners' Framework Agreement on Telework, {COM (2008) 412 final}, Brussels, 2.7.2008.

cases even for knowledge testing) they use various tools that enable real-time face-to-face online communication, such as Zoom, MS Teams, Skype and others.

3 Individual Aspects of Cybersecurity

With the introduction of the Internet in labour law proceedings, questions were initially raised regarding the (in)permissibility of the use of the Internet and webmail for private purposes. Especially in the initial phase, many employees could not resist the temptation and played online games during working hours, read the news, visited adult websites, online stores, sent e-mails with entertainment content, etc. This kind of behaviour led to lower productivity that could jeopardize the work process of the employer. Namely, by inappropriate use of the Internet, employees could cause many problems to the employer in the initial phase of using the Internet, such as criminal and compensatory liability for downloading illegal content, harassment and other inappropriate behaviour, violation of copyright law, damage to the reputation of the employer. process due to the transmission of computer viruses and other malicious programs, etc. As a result, employers have had to establish certain rules regarding the level of tolerance regarding private internet browsing or the admissibility of private emailing and warn employees in various ways about the risks and dangers of using the Internet (Malte Niemann, 2002: 114-116). In addition to strict rules, some employers have also technically disabled access to private content on work computers.

With regards to the private use of the Internet and e-mail, the question of the admissibility of online supervision has been raised from the outset, as the employer can strongly interfere with the employee's right to privacy by controlling the use of the Internet and e-mail. The European Court of Human Rights in Bărbulescu v. Romania ~~has~~ decided that the employer has the right to control the private use of the Internet and e-mail, but not based on the adoption of a general policy permitting monitoring. This means that the employer must set out precise rules, outlining why, how and where employees may be monitored and explaining how any information gathered through monitoring may be used[7].

[7] Bărbulescu v. Romania, The European Court of Human Rights, Grand Chamber, (Application no. 61496/08, 5 September 2017.

If at first the threat to online security and negative consequences for the employer could be caused mainly by consciously inadmissible actions of employees (non-compliance with the rules regarding the use of the Internet for private purposes), telecommuting began to create completely new risks and challenges. Technological development and globalization have brought new challenges, especially in the field of personal data protection. The volume of collection and exchange of personal data has increased significantly, and individuals are rarely aware of the consequences of their actions. To protect individuals with regard to the processing of personal data, a General Data Protection Regulation has been adopted[8], regulating detailed rules regarding data protection.

Online tools have significantly simplified the way people work, but they pose a serious security risk to the employer in the event of violation or misconduct. Namely, the employer can suffer great damage in the form of financial loss, negative consequences due to unwanted transmission of documents, business secrets and other data, and sanctions due to violations of personal data protection rules. Even the smallest error or deficiency in the system can pose a major security risk. Individual aspects of online security in connection with the employment relationship in higher education institutions can be divided into the following sections: 1) deletion or transmission of data due to error, 2) cyberattacks, 3) inadmissible control, and 4) unauthorized use of data.

We will briefly explain the above-mentioned sets of online security in the case of an employee of a higher education institution, and the above applies to professional as well as to pedagogical and scientific-research workers. Web clouds and e-learning environments allow employees to store a variety of data. In the case of professional staff, these are various financial, academic and administrative data, and in the case of pedagogical and research staff, especially personal data on students, teaching materials, student works, records of applicants for examinations, records of grades, etc. If the listed documents and data are located in the web cloud, there is a high risk of unwanted data deletion (especially if proper data backup is not provided) or unwanted transmission of data to ineligible persons. The risk is even greater in the case of joint documents (a document that can be edited by several people at the same

[8] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regards to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance).

time) and joint folders. The more people have access to the data, the greater the security risk.

The risk of online attacks (data intrusion and encryption) occurs especially in the case of remote access or in the case of downloading malicious software. Employees are the target of various (personalized) ways of stealing user data, phishing attacks, social engineering attacks, distributing malware, etc. Recently, attacks with data encryption for the purpose of extortion have become particularly common. Thus, we can read about many cases of employees confronted with a message on the screen: "*All your files are encrypted with RSA-2048 encryption. … It's not possible to recover your files without a private key. … You must send us 0.7 Bitcoin for each affected PC or 3 Bitcoins to receive ALL Private Keys for ALL affected PCs.*" (Chuang, 2018). If an employee works on the premises of a higher education institution and uses a business computer, internet connection, licensed software with appropriate protection, etc. and at the same time respects generally known facts and employer policy (e.g., the fact that we do not open suspicious emails, do not transmit suspicious files, we do not open unknown and suspicious websites, etc.), cyberattacks should not occur in principle. However, working remotely is more problematic, as in this case, people use their own internet connections, in some cases also private computers, mobile phones and other devices that are not sufficiently secured.

In the case of higher education institutions, the issue of inadmissible supervision arises particularly in connection with the monitoring of the implementation of lectures, exercises, examinations and other obligations of study obligations. These are especially cases where a certain person (e.g. superior, student or a third party) is secretly involved in real-time communication. Perhaps less frequently, however, even in the case of higher education institutions, there is a risk of scrutiny in relation to meetings on business and other important decisions.

By publishing their own products (e.g. seminar work, examination papers, etc.) in online e-learning environments or sending them via e-mail, unauthorized use of data for various purposes may occur. Regarding the unauthorized use of copyrighted products, pedagogical and scientific or research workers are even more exposed, as their products (e.g. study materials, videos of lectures, research results, etc.) are even more sought after. In the case of distance learning, the risk of unauthorized use of

data is even greater, as participants in study programs can obtain data relatively easily (e.g. by inadmissible recording, storage of data from e-learning environments, etc.).

4 Mitigation of Risks

Regarding the stated risks in the field of labour law aspects of online security of higher education institutions, the question arises how to minimize individual risks and thus improve the online security of employees, students and other participants. We can consider that the existing rules and institutes of labour law adequately address this area, with the need to apply them appropriately. Workers must perform the work for which they have concluded an employment contract in accordance with the applicable legislation and with the required level of diligence. They must follow the instructions of the employer unless they lead to wrongdoing or omission. They must refrain from any action which, given the nature of the work they do, could harm the stated interests of the employer. They must protect business secrets and are liable for damages if the employer causes material or non-material damage resulting from their fault.

As a result, measures to mitigate security risks are primarily in the hands of the employer. By measures, however, we do not mean so many binding legal rules that would be included in an employment contract or in collective agreements at various levels, but rather in the preventive actions of the employer. A prerequisite for adequate online security in the workplace is the identification of security risks and the development of appropriate protocols. It is recommended that every employer (including in the field of higher education) adopt an appropriate security policy, which addresses the most common security risks related to the use of the Internet and electronic devices and provides ways (security protocols) to prevent or mitigate the consequences.

Even more important than the adoption of the security policy is the education of employees, e.g. knowledge of GDPR, constant warning of possible risks and mistakes, and the ongoing identification of new security risks. The fact is that employees do not (yet) have the appropriate knowledge to ensure online security, so it is even more important that they know the employer's security policy in detail, understand it and "take it for granted". It should be pointed out that cybersecurity professionals, who specialize in the field of online security, have an increasing role

in work environments, and it is expected that certain knowledge about online security due to the needs in work environments will be acquired in the educational process (De Zan & Di Franco, 2019).

5 Conclusion

We can conclude that the risks in the field of labour law aspects of online security are usually the result of careless or unwitting or deliberate behaviour of employees or the result of inappropriate business processes. We must be aware that in the age of digital technology, just one wrong or careless "click" can cause great damage and irreparable consequences. To reduce security risks, we must constantly identify hazards and educate employees on appropriate ways to use the Internet and electronic devices. In addition to knowing the security policy and security risks, it is extremely important that we are very careful and attentive when performing work, especially if we perform with a large amount of (personal) data, and if we perform work remotely. What future implications of labour law with the rise of artificial intelligence, notably (unsupervised) "deep learning"? For example, can one envisage a link between labour law and the need for an audit of algorithms and IA? e.g., https://www.businessofgovernment.org/sites/default/files/Algorithmic%20Auditing.pdf

References

Chuang, Tamara, Pay us bitcoin or never see your files again: Inside the highly profitable underworld of ransomware, The Denver Post, 8 March 2018.

Commission of the European Communities, Commission Staff Working Paper, Report on the implementation of the European social partners' Framework Agreement on Telework, {COM (2008) 412 final}, Brussels, 2.7.2008.

De Zan, Tommaso, Di Franco, Fabio, Cybersecurity Skills Development in the EU, European Union Agency for Cybersecurity (ENISA), 2019.

Malte Niemann, Jan, Monitoring Internet and Email Usage - Germany: Surfing into Unemployment? Private Internet Use and Emailing under German Labour Law, Computer Law & Security Review, Volume 18, Issue 2, 2002.

Senčur Peček, Darja, Franca, Valentina, From student work to false self-employment: how to combat precarious work in Slovenia? in: Kenner, Jeff (ed.), Florczak, Izabela (ed.), Otto, Marta (ed.). Precarious work: the challenge for labour law in Europe. Cheltenham; Northampton: E. Elgar. 2019.