Scientific Bulletin
of the Politehnica University of Timisoara, Romania

TRANSACTIONS on ENGINEERING AND MANAGEMENT

Volume 9, Number 1&2, 2023

An Analysis of the Legal Implications of Data Security Risks of Teleworking in Romania

Mirabela METZLER [1], Caius Tudor LUMINOSU[2] and Valentina TAUCEAN [3]

Abstract – In March 2020 with the spread of the COVID-19 pandemic employees were forced to continue working office hours from their own homes and sometimes even on their own technological devices. The purpose of this article is to identify the legal implications of specific data security risks in the case of teleworking, from both the perspective of the organization and the individual, thereby facilitating managerial decision regarding privacy compliance and protection of intellectual property. Furthermore, the study opens to new research directions in the attempt to provide insights into the new challenges for Romanian management, that current work trends pose.

Keywords: Teleworking, data security, legal liability, critical review, implications

I. INTRODUCTION

In March 2020 with the spread of COVID-19 pandemic, in Romania, teleworking became the type of remote work most common within organisations, having employees working remotely from home using ICT, as opposed to working from an employer's workplace. During this time, the rules of teleworking have been temporarily amended to ensure that employers have been able to unilaterally change the work agreement and order their employees to telework. Home confinement was imposed by law and teleworking suddenly became a mandatory full-time practice. Employees were forced to continue working office hours from their own homes and sometimes on their own technological devices, with little preparation time.

Eurofound's unique e-survey administrated in 2020 in relation to "Living, working and COVID-19", offers some much-needed facts and figures regarding teleworking [1]. Over three-quarters of EU employees in July want to continue working from home at least occasionally, even without COVID-19 restrictions, but very few people wish to telework all the time, with the preferred option being a mix of teleworking and presence at the workplace. Analysing results regarding Romania, the survey found that 55% employees continued working from employer's premises during the pandemic and 30% worked from their homes. These results would lead us to believe teleworking does not have a strong presence in Romania, but we must account for the fact that data is available for the June/July 2020 round only, when society and economies were slowly re-opening, compared to the harsh legal restrictions imposed during spring 2020. Not surprisingly, 60% of employees expressed the desire to occasionally work from home if there were no restrictions due to COVID-19. Regarding devices used, 66% respondents said that their personal equipment where enough to do the work properly but unfortunately the survey fails to provide the results for measuring whether the employer provided the equipment needed to work from home.

Remote working brings several data protection and intellectual property challenges because data is being generated, processed, and stored in/from multiple offsite locations. We believe a more focused approach on legal implications when teleworking is needed, to better illustrate the intricacy and complexity of law and IT, from both the perspective of the organization and the individual. This would help managerial decision regarding privacy compliance and protection of intellectual property in the case of teleworking even beyond COVID-19.

To address this, the article is structured in three sections comprising of literature review regarding teleworking aspects and terminology, an analysis of the legal framework of teleworking in Romania and an exposition of common security risks associated with teleworking. The article finishes with the analysis of

[1] Lawyer, Timis Bar Association, Romania, mirabela.metzler@gmail.com
[2] Politehnica University of Timișoara, Romania, caius.luminosu@upt.ro
[3] Politehnica University of Timișoara, Romania, valentina.taucean@student.upt.ro

the legal implications associated with identified risks, followed by conclusions.

II. LITERATURE REVIEW

1. A brief overview of teleworking

According to Oxford Languages, two words that have seen a huge surge in use since March 2020 are "remote" and "remotely", as well as distinct changes in the words used in collocation with these two (remote/remotely studying, teaching, meeting, and voting) [2].

The terms "remote working" and "teleworking" each relate to the spatial distribution of work, however "remote work" can be considered the broadest concept and "telework" would be a subcategory [3]. Before the term "teleworking" permeated in our work arrangements, the first documented form of telecommunications-augmented decentralized work – also known as "telecommuting", has emerged in the 1970's in the USA [4] but the adoption of teleworking practices across Europe was much slower than anticipated, due to various human, social and organizational factors [5].

Before the current pandemic crisis, research conducted over a large amount of data collected in 2015 from 15 European countries concluded (amongst others) that most teleworkers were self-employed and there was a weakening connection between telework and permanent contracts, full-time jobs, and living in urban areas [6]. Since the start of the pandemic, legally imposed home confinement blurs the line within remote work and many aspects of "teleworking" can be assimilated to "working from home". A teleworker does not always work from home, he can use a "hot desk" in a co-working place or travel as a "nomad worker" [7]. The present paper refers only to employed teleworkers that forcefully became home-based (hereafter, teleworkers), as this is congruent with the current recommendation in the prevention of the coronavirus disease. Moreover, self-employment and informal telework practices are beyond this analysis.

2 The Legal frameworks for teleworking in Romania

Teleworking is determined by the specific mechanisms of communication between teleworkers and employers that resulted from acceptance and use on a large, global scale of added information and communication technologies. The first definition of teleworking in Europe was adopted in 2002 with the European Framework Agreement on Telework. It was intentionally broad, to cover both mobile and home-based telework, so that it can be adapted flexibly to technological advancements and new forms of work [8].

Following the European framework, teleworking was regulated for the first time in Romania by Law no. 81/2018. Teleworking is not just a form of home working regulated by art. 108 of the Romanian Labour Code, Law no. 53/2003. Besides having a different legal basis, the characteristic features of telework are the voluntary character, the legal context of an employment contract/relationship and the use of computers and telecommunications to change the usual location of work, away from employer's premises, on a regular basis.

The Romanian legal definition of teleworking follows entirely the essential elements regarding agreement, place, and modality agreed in the European Framework, but its implementation was confusing and problematic. A recent study confirmed that, despite some differences between countries teleworking is regulated in Europe quite uniformly because of EU regulations. However, same study found that in Romania there are certain problems with regards to the issue of occupational safety and health and the recording and checking of working hours [9].

Discussions in Romanian legal literature ranged from practical aspects in relation to flexible work [10] and digitalization [11] to the meaning and legal terminology used by the legislator [12]. A controverse can be observed regarding specificity and distinction from other forms of work, especially working at home [13, 14, 15]. Other authors analysed the particularities of teleworking regarding the penalty for the non-compliance with legal provisions regarding work, as well as fiscal aspects [16]. Considering the current work trends, [17] expressed concerns that teleworking is not comprehensively regulated and suggested some improvements for future regulations in favour of the teleworker. An interesting opinion claims that teleworking is a form of "virtual migration" that implies movement not only of employee from the employer's premises, but also movement of data from teleworkers to the organisation and vice versa [18].

3. Some preliminary studies and facts on teleworking

The lack of time for preparation became a particularity of telework induced by epidemic. This situation was noticed across many countries and not all were prepared. In France it reinforced the pressing need for a telework policy and rules regarding work at home equipment, professional IT tools access and costs compensation [19]. Spanish researchers noticed that an increasing number of companies have been adopting teleworking as an urgent solution to ensure their employees' safety and to provide continuity to economic activity, with low costs of implementation [20]. A survey in Portugal found that adapting to teleworking was easy or extremely easy and that it happened very quickly, but with a lack of resources related to technical support infrastructures at home, such as the internet or a printer [21]. But switching to teleworking was not smooth especially for those organizations with no or limited prior experience with teleworking, especially because of lack of appropriate ICT devices and tools, lack of skilled and trained employees to support the transition to telework practices and data security concerns [22]. In fact, a joint EC-Eurofound report discussing the extent of teleworking in the EU before and during the COVID-

19 outbreak, observed that organizations that had to move to telework may feel the need to adapt to this arrangement by trying to introduce increasingly intrusive forms of remote control and surveillance of the work carried out from home [3].

4. Security risks in teleworking

Besides organisational challenges with a remote workforce, finding a solution to protect data across several infrastructures and environments is still quite challenging and more critical than in the past. The most common security objectives for telework and remote access technologies are known as the "CIA Triad" consisting of confidentiality - ensure that remote access communications and stored user data cannot be read by unauthorized parties; integrity - detect any intentional or unintentional changes to remote access communications that occur in transit; and availability- ensure that users can access resources through remote access whenever needed [23].

Data security risks have been documented for more than two decades, like systems being used for multiple purposes, user's systems not being directly controlled by the IT department, Internet connection sharing that may allow others to access corporate resources [24]. Present teleworking scenarios start from an ideal situation where the employer provides employees with data processing equipment for processing data securely; a riskier situation is when the teleworker uses his own devices (such as computers, tablets or mobile phones) and the employer cannot control the security of the data processed on the employee's system; a third situation is using cloud technology, meaning that both the teleworker and the employer are connected to a cloud platform where they find all necessary resources [25]. As a result, ensuring full security of computer systems has become the great challenge of any organization because security vulnerabilities arising from remote working increase the risk of cyber-attacks and is considered one of the main enemies of any organization, from SMEs to large corporations [26].

A literature review identified three triggers of risks: the teleworkers, the data /information, and the software, hardware, and network assets [27]. In the same lines, major security concerns for telework and remote access technologies include a lack of physical security controls of mobile devices that can be lost or stolen, unsecured networks used for remote access over the internet, as well as providing external access to internal-only resources that increases the risk of that resource being compromised [28]. Guidelines and reports confirmed that the use of technology for teleworking can present higher risks of cyber-attacks and confidentiality breaches, especially if employees are using personal laptops or devices for teleworking [28]. IT solution vendors added other risks like VPN brute-force attacks, phishing campaigns, and man-in-the-middle attacks [29].

Also, people's behaviour has long been a weak link in the security of any business, responsible for careless use of passwords and keeping confidential documents filled in paper form or unsecured equipment such as USB flash drives or accessing links to suspicious emails [30, 31, 32]. Without firewalls, proxies, BNS filtering and VPNs to protect them, it's a "perfect storm for human error" [33].

When asked in a survey, employees teleworking said their top tech-specific concern is how it makes their companies more vulnerable to data breaches and expressed concerns around security and being heavily reliant on tech at home to get the job done [34]. Another research found that employees are confident in their company's ability to keep personal identifiable information secure while working remotely [35] and are trusting of the cybersecurity protocols that their organizations implemented for teleworking during the COVID-19 crisis (like VPNs and teleconferencing platforms), but they consider these protocols to be vulnerable [36].

III. METHODOLOGY

In the context of the present research, the following methods were used: Scientific research; Comparative analysis; Systematic analysis; Logical analysis. This study employs document analysis to unravel the legal characteristics of teleworking agreements, data security risks and their legal implications. The analysis considers both review of the contemporary academic and non-academic literature, because teleworking has been widely covered in government regulatory guidelines and technical reports of IT companies. The research included all countries but was limited to those cases presented in papers published in English and Romanian languages.

IV. ANALYSIS OF LEGAL ASPECTS OF TELEWORK

The purpose of the paper is to explore legal implications of specific data security risks of teleworking in Romania, to support managerial decision regarding privacy compliance and protection of intellectual property in a teleworking situation. This section provides an analysis of the legal component of

1. The legal framework of telework

A textual analysis of the laws governing teleworking reveals the following key elements that define telework on a legal level:

i) work is performed based on a specific teleworking agreement between the employer and employee,

ii) telework always implies the use of computers and telecommunications in a work relation,

iii) the employer is responsible for all expenses necessary to set-up and maintain home-based offices,

iv) the employer will provide access to company-valuable information on technology or on any other

aspect of the business – that can be or already is being protected as intellectual property (IP),

v) as in any employment situation, within a teleworking arrangement, data and privacy protection are the employer's responsibility under the General Data Protection Regulation (GDPR) and

vi) the employer must explicitly inform the teleworker of regulations in matters relating to the protection of personal data (and the teleworker must comply).

The teleworker is an employee under the Labour Code and disciplinary actions can be taken against him, in certain conditions. This is a specific situation that only exists within a work agreement and not applicable if the teleworker is freelancing. Other types of legal liability that can affect both parties are administrative (includes GDPR fines), criminal, and civil/tortious liability, that are derived from general law principles.

It is also important to recall the fact that, according to the Labour Code, the employee has specific rights which he must be informed of. These labour rights include providing the employee correct and sufficient information regarding the handling of data and tools for doing so.

2. Legal aspects of data security in telework

We identified specific data security risks in teleworking such as physical security attacks on devices, unsecure or vulnerable internet connection and user's level of access to company systems. To keep business continuity during the pandemic, and without any time to prepare for teleworking, it is unlikely that all companies provided their employees with a work computer having a degree of cyber protection equal to company environments. Thus, employees would have used their personal devices for remote access to company IT-infrastructure, as well as their private Wi-Fi networks that create potential entry points for security threats, if insufficiently secure.

All data security risks involve one of the three outcomes: disclosure of data – which leads to loss of confidentiality; modification of data – which will result in the loss of information integrity; destruction of data – resulting in loss of availability of that data. Legal liability is engaged either way if the data is affected because of physical or software attacks, has been intercepted, accessed in an unauthorized way, or accidentally deleted. From a legal point of view, we can approach data from perspective of personal data (protected under GDPR), trade secrets and confidential information (protected under IP law, commercial and civil law).

3. Personal data breach

Companies are under threat of GDPR fines if the cyber-attack results in a personal data breach because integrity and confidentiality of data are fundamental principles for data processing. According to art. 4 (12) GDPR a personal data breach refers to a security breach leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed. Employers, as data controllers, stay liable for any personal data processed by teleworkers on company or personal devices used for work purposes, shared devices, or unsecure Internet connections. For example, what starts with a simple email click in case of phishing attacks or a transmission over an unsecured network might engage the company in administrative liability. Liability of employer is questionable, however, if the company fulfilled (and can prove) the obligation to implement appropriate technical and organizational security measures to avoid personal data breaches [37], like the case of losing a laptop containing encrypted personal data if the data is still available in a back-up system [38].

In certain situations, the employer may also take legal action against the persons – even employees – who caused the incident, based on the contractual, civil, or disciplinary liability of these persons. During the first half of 2020, insufficient technical and organisational measures to ensure information security held second place in a top of reasons for fines and penalties in EU, that could be avoided by training of personnel, with little costs and avoiding high fines [39]. If the company has internal rules and regulations regarding data processing in place, an employee disregarding them is liable for disciplinary action. However, employee's tortious liability could be limited by the nature of telework that always implies the use of computers and telecommunications, making the management of data security risks a regular job aspect in the sense of art. 254 Labour Code. For these reasons we believe it crucial that employers assess the activity of their employees working from home, to determine whether this activity may be considered teleworking and amend the employment contracts accordingly.

4. Breach of intellectual property rights

Potential security breaches may put the confidential work files of companies at risk. Teleworkers need access to diverse types of documents that are either digital or digitalised, making them easily copied, modified, shared, or deleted. These documents are at least confidential if not secret, forming the pool of information and know-how that is not protectable or cannot be protected properly through patents, such as early-stage inventions, manufacturing processes, lists of suppliers and clients, recipes, the results of marketing studies, brand names, prices, and dates of launching of new products or the price offered in a public procurement or bidding procedure. When such documents are intercepted and stolen through attacks like ransomware, companies might have to pay to retrieve them from cyber criminals without a real possibility to sue for damages because it is difficult (although possible) to impose the liability for actions over the Internet, especially because of the presence foreign elements in legal proceedings [40]. Teleworking relies on computers and data rather than

paper, making these unintended consequences more frequent, and, while organizations often look to their general liability policies to cover them for accidental losses, an insurance policy might be the only way to mitigate the risk, including when the attack is happening through an employee-owned device. Moreover, lost or corrupted documents could lead to missing deadlines on ongoing contracts and open the company to damaging their clients.

Company data is not always their own, like data provided by business partners and clients, especially when we think Romania's economy is mainly centred on the services sector. We can imagine that employees might start downloading company files on their personal computers instead of working in the company's cloud, to be able to continue to work if remote access should be suddenly interrupted. Even accidental disclosure of confidential client information to a party outside the workplace, puts the company in breach of contract with their client. As such, based on civil or commercial law, the company would be responsible for paying compensation to the client for damages they faced due to this breach.

Employees could be held responsible for IP breaches, especially if they signed a non-disclosure agreement. When using their preferred file sharing systems or devices that are shared with family members, the employee is still responsible for the company data and even criminal charges can be brought if malicious intent can be proven.

V. CONCLUSIONS

Data security is a much wider issue that covers more than only the aspect of technology. From the legal point of view, the challenge is two-fold: protecting the teleworker through the security of personal data & privacy as well as protecting the employer by ensuring preservation of business data & proprietary information. Managing teleworking means balancing safeguarding personal data of employees and the need of securing business sustainability through protection of intellectual property.

Not all employees will be accessing sensitive information while they are working from home. For the management, the legal implications should be part of the risk assessment. This should start by asking the right questions: How is data being generated? Where is it stored? Which physical devices are storing data? How are documents being secured according to their classification? Is all data (no matter where it is located) being backed up? Is the device or devices the employee uses for work used for other purposes? Are employees aware of cyber-risks? As one senior practitioner said, the new remote-working reality calls for an "urgent rethinking of general security training" [41].

The contribution of this study, aimed at practitioners and managers, is seen as threefold: it can help organisations to successfully manage the introduction of teleworking for employees, create and implement appropriate policies and also, assist the employees to learn about the legal risks related to remote work.

REFERENCES

[1] Eurofound. (2020). Living, working and COVID-19 data | Eurofound. https://www.eurofound.europa.eu/data/covid-19.

[2] Oxford Languages. (2020). Oxford Word of the Year 2020 | Oxford Languages. https://languages.oup.com/word-of-the-year/2020/.

[3] Sostero, M., Milasi, S., Hurley, J., Fernandez-Macías, E., & Bisello, M. (2020). *Teleworkability and the COVID-19 crisis: a new digital divide?* (No. 2020/05). JRC working papers series on labour, education and technology.

[4] Nilles, J. (1975). Telecommunications and organizational decentralization. *IEEE Transactions on Communications*, *23*(10), 1142-1147.

[5] Eurofound and the International Labour Office. (2017). Working anytime, anywhere: The effects on the world of work. https://doi.org/10.2806/425484.

[6] López-Igual, P., & Rodríguez-Modroño, P. (2020). Who is teleworking and where from? Exploring the main determinants of telework in Europe. *Sustainability*, *12*(21), 8797.

[7] Sfetcu, N. (2011). Ce este telelucrul (telemunca, telework)? MultiMedia Publishing. https://www.setthings.com/ro/e-books/ce-este-telelucrul-telemunca-telework/.

[8] Gschwind, L., & Vargas, O. (2019). Telework and its effects in Europe. *Telework in the 21st Century*, 36-75.

[9] Sládek, P., & Sigmund, T. (2021). Legal Issues of Teleworking. SHS Web of Conferences, 90, 01020.

[10] Popescu, R. R. (2018). Aspecte controversate cu privire la noua reglementare a telemuncii. *Revista Romana de Dreptul Muncii*, (3).

[11] Georgescu, L. (2020). Solutions with Respect to Employment Relations in the Context of Their Digitalization and Flexibilization. *Rev. Romana Drept. Muncii*, 26.

[12] Zainea, E. (2020). Individual Employment Contract in Telework Regime. Individual Work Contract at Home. Specific Clauses. *Revista Drept Social*, 3.

[13] Ciochina-Barbu, I. (2019). Aspecte legislative privind reglementarea muncii în biroul virtual (telemunca-teleworking). *Acta Universitatis George Bacovia. Juridica*, *8*(2), 545-572.

[14] Dub, A. D. (2018). Teleworking. Context of Occurrence. Differences compared to Homework. *Revista Drept Social*, 8.

[15] Țiclea, A. (2018). Telemunca–modalitate modernă și flexibilă de desfășurare a activității salariatului. *Revista „Dreptul”*, (11), 181-194.
[16] Stănciulescu, E. (2020). Teleworking and Working from Home in the Current Environment. *CECCAR Business Review*, *1*(10), 52-60.
[17] Vartolomei, B. O. T. (2020). Considerations regarding work from home and telework. In *Proceedings of the International Conference on Business Excellence* (Vol. 14, No. 1, pp. 1217-1221).
[18] Predut, S. N., Ipate, F., Gheorghe, M., & Campean, F. (2018, June). Formal modelling of cruise control system using Event-B and Rodin platform. In *2018 IEEE 20th International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th International Conference on Data Science and Systems (HPCC/SmartCity/DSS)* (pp. 1541-1546). IEEE.
[19] Carillo, K., Cachat-Rosset, G., Marsan, J., Saba, T., & Klarsfeld, A. (2021). Adjusting to epidemic-induced telework: Empirical insights from teleworkers in France. *European Journal of Information Systems*, *30*(1), 69-88.
[20] Belzunegui-Eraso, A., & Erro-Garcés, A. (2020). Teleworking in the Context of the Covid-19 Crisis. *Sustainability*, *12*(9), 3662.
[21] Tavares, F., Santos, E., Diogo, A., & Ratten, V. (2021). Teleworking in Portuguese communities during the COVID-19 pandemic. *Journal of Enterprising Communities: people and places in the global economy*, *15*(3), 334-349.
[22] Abulibdeh, A. (2020). Can COVID-19 mitigation measures promote telework practices?. *Journal of Labor and Society*, *23*(4), 551-576.
[23] Samonas, S., & Coss, D. (2014). The CIA strikes back: Redefining confidentiality, integrity and availability in security. *Journal of Information System Security*, *10*(3).
[24] Robinson, C. (2002, August 2). Addressing Teleworker Network Security Risks. CSO Online. https://www.csoonline.com/article/2113195/addressing-teleworker-network-security-risks.html.
[25] Bucşa, R. C. (2020). Teleworking and Securing Data with VPN Technology. *Economy Transdisciplinarity Cognition*, *23*(1), 78-85.
[26] Chávez, J. D. (2020). Key considerations for ensuring the security of organisational data and information in teleworking from home.
[27] Yang, H., Zheng, C., Zhu, L., Chen, F., Zhao, Y., & Valluri, M. (2013). Security risks in teleworking: A review and analysis. *The University of Melbourne*.
[28] IOE. (2020). IOE Guidance on teleworking in the times of Covid-19 (Issue April).
[29] Varonis. (2020, August 12). Top 5 Remote Work Security Threats. Inside Out Security Blog. https://www.varonis.com/blog/top-5-remote-work-security-threats/.
[30] Pyöriä, P. (2011). Managing telework: risks, fears and rules. *Management Research Review*, *34*(4), 386-399.
[31] Safa, N. S., Von Solms, R., & Futcher, L. (2016). Human aspects of information security in organisations. *Computer Fraud & Security*, *2016*(2), 15-18.
[32] Warkentin, M., McBride, M., Carter, L., & Johnston, A. (2012). The role of individual characteristics on insider abuse intentions.
[33] Evangelakos, G. (2020). Keeping critical assets safe when teleworking is the new norm. *Network security*, *2020*(6), 11-14.
[34] Lenovo. (2020). Technology and the Evolving World of Work. https://news.lenovo.com/wp-content/uploads/2020/07/Technology-and-the-Evolving-World-of-Work_Lenovo-IDG-Global-Research-Report_FINAL.pdf.
[35] IBM. (2020). IBM Security Study Finds Employees New to Working from Home Pose Security Risk - Jun 22, 2020. IBM. https://newsroom.ibm.com/2020-06-22-IBM-Security-Study-Finds-Employees-New-to-Working-from-Home-Pose-Security-Risk, 2020.
[36] Turner, C., Turner, C. B., & Shen, Y. (2020). Cybersecurity Concerns & Teleworking in the COVID-19 Era: A Socio-Cybersecurity Analysis of Organizational Behavior. *Journal of Advanced Research in Social Sciences*, *3*(2), 22-30.
[37] Škiljić, A. (2020). Cybersecurity and remote working: Croatia's (non-) response to increased cyber threats. *International Cybersecurity Law Review*, *1*, 51-61.
[38] Taeger, J. (2020). Obligaţia de informare şi de notificare în cazul încălcării securităţii datelor cu caracter personal conform art. 33, 34 GDPR. *Revista română pentru protecţia şi securitatea datelor cu caracter personal*, (01), 13-27.
[39] Dumitrescu, M., & Cireaşă, D. (2020). *Sinteza amenzilor GDPR aplicate la nivel european, în primele cinci luni ale anului 2020*, Revista Română Pentru Protecţia Şi Securitatea Datelor Cu Caracter Personal, 02, p. 126-146.
[40] Ionel, G. (2011). Dreptul internetului sau dreptul la internet. *Revista Română de Dreptul Proprietăţii Intelectuale*, (02), 66-70.
[41] Lueck, M. (2020). GDPR in the new remote-working normal. *Computer Fraud & Security*, *2020*(8), 14-16.