Monitoring of Business Email and Internet Use During Corporate (Internal) Investigations vs. Employees' Right to Privacy

Author: Dundović, D.

Abstract

Digitalization of business presents new challenges for companies and employees daily. While the digitalization of business undoubtedly affects business performance, it can also impact employee privacy. Although business digitalization brings numerous benefits to companies—such as increased efficiency, reduced operating costs, improved and faster communication and collaboration among employees and with other companies, and the possibility of remote work—it also carries significant risks.

One of the main risks from the company's perspective is security risk, which manifests itself through an increased likelihood of cyberattacks[1], data theft, and information misuse. Equally important, particularly from the employees' standpoint, is the right to privacy when employees using company IT networks and information systems[2] within the digital workplace.

The growing digitalization of business, as a prerequisite for successful operations, does not necessarily pose a threat to employee privacy. However, this threat can be avoided only if high standards of privacy protection are unconditionally upheld throughout all business processes within the company, including during corporate (internal) investigations.

Keywords: business digitalization, employee privacy, corporate (internal) investigations.

[1] "Cybersecurity" means all activities necessary to protect network and information systems, their users and other persons affected by them from cyber threats. (Article 2(1) of Regulation (EU) 2019/881, Official Journal of the European Union, L 151/15)

[2] Definition of "network and information systems" in: Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, Official Journal of the European Union L 194/1

1. Privacy as a Protected Human Right in International and Croatian Legislation

1.1. International Regulations

One of the most important documents governing and protecting human rights at the international level is the Universal Declaration of Human Rights, proclaimed by the United Nations General Assembly on 10 December 1948. Article 12 of the Declaration states: *"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."* (Universal Declaration of Human Rights, Official Gazette 12/2009, Art. 12). As can be seen, the right to privacy is explicitly recognized in this document as one of the fundamental human rights. Among other international legal instruments that refer to the protection of privacy, it is necessary to mention Article 17 of the International Covenant on Civil and Political Rights, adopted by the United Nations General Assembly on 16 December 1966 (United Nations, 1966). Privacy protection is also enshrined in the legal framework of the European Union, particularly within the Convention for the Protection of Human Rights and Fundamental Freedoms (1999), Article 8(1), as well as in the Charter of Fundamental Rights of the European Union (2000). Article 7 of the Charter, titled "Respect for private and family life", provides that: *" Everyone has the right to respect for his private and family life, his home and his correspondence."*. The same document further elaborates the protection of personal data in Article 8, which states:"1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority.". A particular emphasis in privacy protection within the EU legal order is placed on protection of personal data. Article 39 of the Treaty on European Union (European Union, 2016) requires all Member States to adopt "rules relating to the protection of individuals with regard to the processing of personal data." This and other EU documents, combined with the previously insufficient regulation of personal data protection, highlighted the need for a comprehensive instrument addressing privacy and data protection in greater detail at the EU level. These developments ultimately led to the adoption of the General Data Protection Regulation (GDPR) in 2016 (General Data Protection Regulation, 2016). It is important to note that the GDPR is directly applicable and binding in all EU Member States, taking precedence over national legislation.

In addition to the GDPR, it is also worth mentioning the Resolution 1986 on improving user protection and cybersecurity (Council of Europe, 2014). Rapid technological development,

the widespread use of the Internet, digital platforms, mobile devices, and other information systems have enabled communication among a vast number of individuals, along with the exchange and storage of large volumes of diverse data. While such technological advancements have undoubtedly facilitated communication and business operations, they have also increased the risk of privacy breaches—not only for those directly using these technologies but also for individuals whose data are being shared or processed. At the same time, the growing number of online services and social media platforms—where users voluntarily enter their personal data or leave digital traces simply by accessing a website or using a service—further amplifies privacy risks. Moreover, the rapid advancement of artificial intelligence[3] (AI) significantly contributes to the potential violation of privacy through surveillance and interception of communications. This global concern was recognized by the United Nations General Assembly in 2013 through the adoption of Resolution 68/167 titled "The Right to Privacy in the Digital Age" (United Nations, 2013), calling upon states to review their policies, practices, and legislation regarding communication surveillance, interception, and personal data collection. To enhance oversight of the implementation of these principles, in 2015 the UN established the position of Special Rapporteur on the Right to Privacy (United Nations, 2015). The Special Rapporteur's mandate is to promote and protect the right to privacy by examining government policies and laws on digital communication interception and data collection, identifying unjustified intrusions into privacy, assisting governments in developing best practices to ensure lawful oversight of surveillance activities, articulating the responsibilities of the private sector in upholding human rights, and ensuring that national laws and procedures comply with international human rights obligations. In addition to the extensive privacy protections provided under EU law, legal entitys are also entitled to the right to privacy. The European Court of Human Rights guarantees such protection under Article 8 (Right to respect for private and family life) of the European Convention on Human Rights, extending not only to persons but also to legal entities in cases where their "correspondence" or "premises" are not respected. This interpretation has been confirmed through several judgments of the European Court of Human Rights.

[3] " AI is the ability of a machine to display human-like capabilities such as reasoning, learning, planning and creativity.AI enables technical systems to perceive their environment, deal with what they perceive, solve problems and act to achieve a specific goal. The computer receives data - already prepared or gathered through its own sensors such as a camera - processes it and responds. AI systems are capable of adapting their behaviour to a certain degree by analysing the effects of previous actions and working autonomously. https://www.europarl.europa.eu/topics/en/article/20200827STO85804/what-is-artificial-intelligence-and-how-is-it-used

1.2. Legislation in the Republic of Croatia

Articles 36 and 37 of the Constitution of the Republic of Croatia guarantee the right to freedom and confidentiality of correspondence and all other forms of communication (Art. 36), as well as the security and confidentiality of personal data, which may be collected, processed, and used without the consent of the data subject only under conditions prescribed by law (Official Gazette 85/2010, 2010). On 25 May 2018, the Republic of Croatia ratified the aforementioned Convention for the Protection of Human Rights and Fundamental Freedoms and simultaneously began the implementation of the General Data Protection Regulation (GDPR). To ensure the implementation of the Regulation, the Act on the Implementation of the General Data Protection Regulation (Official Gazette 42/18) was adopted, designating the Croatian Personal Data Protection Agency as the competent authority responsible for supervising the application of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of persons with regard to the processing of personal data. According to Dragičević Prtenjača and Zagorec (2023), privacy in the Republic of Croatia is protected either through the general right to privacy or through the protection of personal data regulated by various national laws. In addition to the aforementioned Act on the Implementation of the General Data Protection Regulation, the authors cite the following acts: the Labour Act (Zakon o radu, Official Gazette 93/14, 127/17, 98/19), Article 29; the Family Act (Obiteljski zakon, Official Gazette 103/15, 98/19, 47/20); the Media Act (Zakon o medijima, Official Gazette 59/04, 84/11, 81/13, 114/22); the Electronic Media Act (Zakon o elektroničkim medijima, Official Gazette 111/21, 114/22); the Consumer Protection Act (Zakon o zaštiti potrošača, Official Gazette 19/22); the Electronic Communications Act (Zakon o elektroničkim komunikacijama, Official Gazette 76/22); the Juvenile Courts Act (Zakon o sudovima za mladež, Official Gazette 84/11, 143/12, 148/13, 56/15, 126/19); and the Criminal Code (Kazneni zakon, Official Gazette 125/11, 144/12, 56/15, 61/15, 101/17, 118/18, 126/19, 84/21), specifically Article 146, Unauthorized Use of Personal Data. Each of these laws contains provisions that, in different ways, address the protection of privacy and personal data. A detailed analysis of the individual articles of these acts could certainly be undertaken; however, given the scope and focus of this paper, such an analysis falls outside its primary objectives.

2. Monitoring of Business Email and Internet Use During Corporate (Internal) [4]Investigations

2.1. Corporate Investigations as a Component of Corporate Security Operations

Every company strives to achieve the highest possible level of success in its business operations. According to Dundović (2022), one of the key prerequisites for successful business performance in today's environment is security. The security of employees, company assets, business partners, and internal processes is a legitimate subject of protection by the company. Certain companies implement such protection through various technical security systems—most commonly through video surveillance, alarm systems, and access control systems—by engaging security guards (physical protection) and deploying measures to safeguard IT infrastructure against cyberattacks. Companies typically define in their internal documents how they will ensure a high level of security for their employees, assets, business processes, and all elements contributing to operational success. A Security Policy is one of the fundamental documents that every company, regardless of its size, should adopt. Depending on the specific nature of their activities, size, number of employees, and operational locations, companies may also adopt additional documents that enhance corporate security. One such document may be the Security Regulations, which consolidate all important security procedures and protocols in a single place. Some companies—particularly large ones (for the purpose of this paper, company size classification follows Article 5 of the Accounting Act, Official Gazette 85/2024)—have dedicated organizational units responsible for the overall security system. Depending on the company's internal organization, these units may be referred to as Security Departments, Security Services, or Security Teams. Considering the variety of business activities, these structures are commonly referred to under the general term corporate security. Micro, small, and some medium-sized companys typically lack specialized organizational structures for security and instead rely on designated employees (e.g., security managers) or ad hoc teams for such tasks. Dundović (2022) emphasizes that the scope and nature of corporate security functions depend significantly on the company's size, number of employees, type of business activity, operational locations, and the overall security risk profile of the business environment. Given the scope of this paper, a detailed analysis of the potential tasks and organizational structures of corporate security in different companies will not be undertaken. However, within corporate security activities, there often arises a need to conduct corporate or internal investigations. Every company has the right to monitor certain aspects of employee behavior and to investigate specific incidents, but such actions must

[4] For the purposes of this work, the terms "corporate investigation", "internal investigation" and "corporate (internal) investigation" have the same meaning

take into account certain limitations. When conducting corporate investigations, these limitations primarily relate to legitimacy, subsidiarity, proportionality, and the right to privacy (Meerts, 2016). According to Dundović (2022), regardless of whether a company has a separate function dedicated to corporate investigations, an individual employee or an ad hoc team within the corporate security framework may perform investigative activities. Nonetheless, each company should have a document—or detailed provisions within another internal document, such as a Security Policy or Security Regulations—that governs the internal investigation process. In contemporary business environments, most activities take place within a digital framework, which involves the use of digital platforms, tools, technologies, and processes that enable or enhance business operations through the use of the internet, software solutions, artificial intelligence (AI), cloud computing, social networks, email communication, and other digital technologies that contribute to efficiency and success. Consequently, it is sometimes necessary to monitor the use of certain or all of these technologies by employees in the course of their work. If an employer suspects that an employee is not adhering to established rules and procedures regarding the use of such technologies, the employer has the right to investigate such conduct. According to the author of this paper, such investigations should primarily be conducted within the framework of a corporate (internal) investigation, provided that the process is properly defined in the company's internal documents. Given the subject of this paper, the following sections will focus primarily on the monitoring of email and, to a lesser extent, internet usage—specifically, access to websites. Certain procedures discussed herein may also be applicable to the monitoring of other forms of data within the digital environment, such as specific business applications, data storage (including potential private data) in cloud environments, and data sharing through shared folders and similar systems.

2.2. Use of Corporate IT Infrastructure for Private Purposes

According to Komanovics (2023), employees have the right to private communication in the workplace, even when such communication takes place using the employer's equipment or during working hours. The author supports this position by referencing the judgment of the European Court of Human Rights in Bărbulescu v. Romania (European Court of Human Rights, 2017), where the Court held that "an employer's instructions cannot reduce private social life in the workplace to zero" (para. 80 of the judgment). Furthermore, the Court emphasized that most people develop significant, if not the majority of, relationships with the outside world during their working life (para. 71). Most companies regulate the use of corporate IT infrastructure through internal documents—such as an Information Security Policy, Information Security Regulations, or Guidelines on IT Security—that clearly define the purpose, terminology, usage rules, responsibilities, and other details related to the use of company information systems. In general, there are two main

approaches to regulating the use of corporate IT infrastructure for private purposes. The first approach is a complete prohibition of private use of corporate systems, while the second involves defining the conditions and scope under which such use is permitted. The author of this paper considers that an absolute prohibition on occasional private use of company IT infrastructure is not an optimal solution, except perhaps in organizations engaged in security or military-related activities. Supporting this view is the fact that modern technology allows a high level of IT system protection even when such systems are used for limited private purposes. Regulating the private use of corporate IT infrastructure requires the adoption of appropriate internal company documents governing this area, as well as procedures ensuring that all employees are adequately informed of the applicable rules. Some companies explicitly allow the limited private use of corporate email accounts, provided that such use does not include the exchange of advertising materials, politically oriented messages, disturbing images or videos, or any other content contrary to the company's Code of Ethics. Additionally, automatic forwarding of official business emails to private accounts is typically prohibited. Other companies employ technical solutions that block access to private email accounts from the corporate network, and they may also regulate the storage of data on portable media or private devices. Employers should clearly state in such documents that they will fully respect employee privacy, while also reserving the right to carry out periodic monitoring to verify compliance with internal procedures and legal obligations, particularly where non-compliance could harm the company's legitimate interests. The purpose of monitoring must be clearly defined and communicated to employees. In addition to the requirement for clear internal policies on IT use—including private use—it is common practice for employees to sign a consent form acknowledging that they have been informed of potential monitoring measures. From the perspective of the General Data Protection Regulation (GDPR), consent is defined as: "Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her." (Article 4(11), GDPR). The request for consent must be presented in an intelligible and easily accessible form, using clear and plain language, and employees must be informed of their right to withdraw consent at any time. However, the Article 29 Working Party and the European Data Protection Board (EDPB) have consistently maintained that employees are rarely in a position to freely give, refuse, or withdraw consent due to the inherent dependency arising from the employer–employee relationship (Working Party[5], 2017). The same body adopted Guidelines on Consent (revised in 2018), emphasizing

[5] The Article 29 Working Party is an advisory group composed of representatives of the data protection authorities of the EU Member States, which acts independently and is tasked, among other things, with examining all issues relating to the application of national measures adopted pursuant to the Data Protection Directive in order to contribute to the uniform application of such measures.

that it is unlikely that an employee can freely refuse consent to data processing without fear or risk of adverse consequences. The Working Party further argued that it is problematic for employers to process personal data of current or prospective employees based solely on consent, as such consent is unlikely to be truly voluntary. Therefore, in most cases of employee data processing, the lawful basis cannot and should not be consent, given the imbalance of power in the employment relationship. The GDPR (2016) does not prescribe a specific form for providing information necessary to ensure informed consent. This means that information may be presented in various ways, such as written or oral statements, or through audio or video messages. Nonetheless, workplace monitoring should not rely solely on consent, given the inherent imbalance of power between employers and employees. In the employment context, consent generally cannot be assumed to constitute a valid legal basis; rather, the most appropriate basis for data processing is the employer's legitimate interest in protecting corporate assets and ensuring a secure work environment (Komanovics, 2023). Conversely, in the Danish context, employee consent has not been interpreted as strictly as in the Article 29 Working Party's opinion (2017). In Denmark, consent may be considered freely given despite the power imbalance, reflecting the country's longstanding tradition of balanced employer–employee relations and mutual trust between the parties. The absence of employee notification or consent regarding email monitoring was also addressed in the case of Copland v. the United Kingdom (European Court of Human Rights, 2007). The Court held that the applicant had not been warned that her telephone calls and emails might be monitored, and therefore she had a reasonable expectation of privacy in relation to the calls and messages made from her work phone and business email account. The Court found a violation of her rights and ordered the United Kingdom to compensate her for non-pecuniary damages (Copland v. the United Kingdom 2007). Ray and Rojot, writing nearly three decades ago (1995), observed that employers traditionally perceived employees in a parental manner, such that an employee enjoyed no more privacy than a child did within the parent–child relationship (Ray & Rojot, 1995, p. 61). This comparison underscores the significant progress made in the protection of employee rights in recent decades. It should be emphasized that workplace monitoring differs substantially in its scope and intensity from the information gathering to which individuals are exposed in other contexts—such as when conducting daily transactions or personal activities in public. Mobile phones track our movements, credit cards record our transactions, and loyalty cards used in stores and services monitor our consumption habits. However, it would be incorrect to view workplace monitoring as merely an extension of this general data collection. Data collected in the workplace are held exclusively by the employer, with whom the employee is almost always in a position of dependence. This contrasts with other contexts, where individuals generally have more freedom to decide with whom they share their personal information. Therefore, any monitoring of employees in the

workplace must be conducted with particular caution and in strict compliance with fundamental principles and legal standards — as will be discussed in the following sections.

2.3. General Principles Applicable to the Monitoring of Employees Email and Internet Use

A report on workplace surveillance by the Trades Union Congress[6] (2018) in London shows that more than half of workers (56%) believe it is likely that they are monitored at work, while 66% express concern that workplace monitoring could be used in a discriminatory manner if not properly regulated. According to the same study, 70% of employees believe that monitoring is likely to become even more common in the future. The Working Document on the Surveillance of Electronic Communications in the Workplace (2002), adopted by the European Commission (hereinafter – the Working Document), sets out seven fundamental principles applicable to the monitoring of employees email and internet use:

1. Necessity

Under this principle, the employer must determine whether any planned monitoring activity is absolutely necessary for a specific, legitimate purpose before initiating such activity. Traditional forms of supervision that are less intrusive to individual privacy should be carefully considered and, where appropriate, implemented prior to any electronic communications monitoring. Monitoring employees email or internet use should be considered necessary only in exceptional circumstances. An example would be monitoring employee email to collect evidence of involvement in criminal activity—but only to the extent required to protect the employer's legitimate interests, particularly where the employer may be indirectly liable for the employee's conduct.

2. Finality

Data must be collected for a specific, explicit, and legitimate purpose and must not be further processed in a way incompatible with that purpose. In this context, the principle of "compatibility" means that, for example, if data processing is justified on the grounds of system security, those data may not subsequently be used for another purpose, such as monitoring employee behavior.

[6] The Trades Union Congress is a federation made up of the majority of trade unions in England and Wales. They publish guidance on workplace health and safety, equality and diversity, education and training, employment law and workers' rights.

3. Transparency

This principle requires employers to act openly and clearly in relation to their monitoring activities. Secret monitoring of employees' electronic communications is not permitted, except where explicitly authorized by national law and necessary for the protection of significant public interests such as national security or the prevention, investigation, detection, and prosecution of criminal offences. A good example of transparency in practice is the employer's obligation to inform and/or consult employee representatives prior to introducing monitoring policies and rules. Moreover, transparency encompasses several sub-principles:

3.1. The obligation to provide information to the dana subject

Employers must provide employees with clear, accessible, and accurate information regarding their policies on email and internet monitoring. Employees should be fully informed of the specific circumstances that may justify such exceptional measures, as well as the scope and extent of the monitoring. This information should include:

- The company's email/internet policy, specifying the extent to which communication tools owned by the company may be used for personal purposes (e.g., time limits and usage duration).
- The reasons and purposes for which monitoring, if any, is conducted. If private use is permitted, such communications may be monitored only in very limited circumstances, e.g., to ensure information system security (virus checking).
- Details of the monitoring measures: who conducts them, what data are processed, how, and when.
- Details of any enforcement procedures outlining how and when workers will be notified of breaches of internal policies and be given the opportunity to respond to any such claims against them.

The Working Document (2002) emphasizes that employers should, as a rule, immediately notify employees of any detected misuse of electronic communications, unless compelling reasons justify continued monitoring — which is rarely the case.

3.2. The obligation to notify supervisory authorities before carrying out any wholly or partly automatic processing operation or set such processin operations

Before conducting any fully or partially automated data-processing operation, employers are required to notify the competent data protection authority. This further ensures transparency, as employees can verify—through public data protection registers—which

categories of data, for what purposes, and to which recipients their employer processes personal information.

3.3. Right of Access

Employees have the right to access personal data relating to them that are processed by their employer, and, where appropriate, to request the rectification, erasure, or restriction of processing where such data are inaccurate or unlawfully processed, in accordance with Directive[7] (2016).

4. Legitimacy

Any data-processing operation must pursue a legitimate purpose. Employer monitoring activities must serve the employer's legitimate interests and must not infringe upon employees fundamental rights. For instance, the employer's need to protect its business from serious threats—such as preventing the unauthorized transfer of confidential information to competitors—constitutes a legitimate interest.

5. Proportionality

This principle requires that personal data, including those processed through monitoring, be adequate, relevant, and not excessive in relation to the intended purpose. A company's monitoring policy should correspond to the nature and level of risk it faces. The proportionality principle excludes general, continuous monitoring of employees individual emails or internet use, except where necessary to ensure system security. If the same goal can be achieved in a less intrusive manner, the employer should choose that alternative (for example, by avoiding systems that automatically and continuously track employee activity).

6. Accuracy and retention of data

All data lawfully stored by the employer—after applying the aforementioned principles—relating to employee email accounts or internet use must be accurate, up-to-date, and retained no longer than necessary for the stated purpose.

7. Security

This principle obliges the employer to implement appropriate technical and organizational measures to ensure that all personal data are secure and protected against unauthorized access or external intrusion. It also includes the employer's right to protect its systems against malware, which may involve automated scanning of email and network traffic data.

---

[7] Directive (EU) 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union

The Working Document (2002) highlights that maintaining system security is of paramount importance; therefore, automated email scanning should not be considered a violation of employees privacy rights, provided adequate safeguards are in place. Regarding the private use of Internet for private purporses at the company's IT infrastructure, the Working Document (2002) states that it is up to each company to decide whether employees may use the internet for personal purposes and to what extent. It also observes that a complete ban on personal internet use is generally impractical and unrealistic. When addressing internet monitoring, the Working Document outlines several applicable principles, emphasizing prevention over detection. Employers should prioritize preventive technical measures to reduce misuse, rather than investing resources in post-incident detection. Where reasonably possible, corporate internet-use policies should rely on technical access restrictions rather than direct behavioral surveillance. For example, some companies use configurable software tools to block access to pre-defined categories of websites. Employers may then review aggregated data on visited sites and decide to expand or adjust the list of restricted domains. A good practice example includes notifying employees in real time when their internet use violates the company's policy. As with email monitoring, the principle of proportionality must be observed—any monitoring must represent a proportionate response to the level of risk faced by the employer. In most cases, internet misuse can be detected without examining the content of websites visited.

All of the above principles should be carefully considered and incorporated into company policies governing the use of employee email and internet resources—both for business and for limited private purposes.

2.4. Basic Preconditions for Monitoring Employee Email and Internet Use During Corporate (Internal) Investigations

In the previous section of this paper, we outlined the fundamental principles that must be applied when monitoring employee email and internet usage. This section provides a more detailed description of the circumstances under which corporate (internal) investigations are conducted, including the monitoring of employee email and internet activity. The key question is: What general conditions must be met for such actions to be lawfully and appropriately carried out as part of a corporate investigation? As previously stated, every company has the right to undertake activities aimed at protecting its employees, assets, business partners, and clients, as well as to implement preventive measures to reduce risks that may impact security. One such activity is the conduct of corporate investigations. According to the author of this paper, in order to carry out activities such as accessing employee email or internet usage data within the framework of a corporate investigation, the following preconditions must be met:

- The company must have a **document regulating the use of email and internet** (including private use, if permitted), clearly specifying the purposes for which the company's IT infrastructure may be used and what is prohibited.
- The company must have a **document regulating the conduct of corporate (internal) investigations**[8], or include such provisions in another document (e.g., Security Policy, Security Guidelines, etc.).
- The company must have a **document regulating personal data protection**, which is also a legal requirement.

These documents must be drafted in accordance with the principles previously discussed and the relevant legal provisions concerning the monitoring of employee email and internet use. All employees must be informed of the contents of these documents and must sign a consent form[9] confirming their awareness and agreement to such data processing or at least acknowledging that monitoring may be conducted.

The consent form should specify:

- The **purpose** of the monitoring,
- The **types of data** to be monitored,
- The **possibility of withdrawing consent**.

Notification that the employer may conduct such activities must be provided to employees **before** any monitoring begins. A fundamental precondition for accessing an employee's email should be the **existence of an officially initiated and approved corporate investigation**. Accessing employee email without such an investigation should not be permitted.

The document regulating corporate investigations should include provisions related to email monitoring, clearly specifying:

➤ **Who authorizes** such activity (the authorizing person should not be the same individual who authorized the investigation itself),

[8] More about corporate (internal) investigations in Dundović D., (2022), Corporate Investigations – An Indispensable Part of Corporate Security. Velika Gorica University of Applied Sciences, Republic of Croatia, ISSN: 2706-3720, Velika Gorica 2022.

[9] For more information on consent, see 2.2. Use of business IT infrastructure for private purposes in this paper.

➤**Who conducts** the monitoring (e.g., investigation team leader, team member, or another designated person),

➤ **Justification** explaining why the necessary data for corporate investigation cannot be obtained through less intrusive means[10]. Before deciding to monitor email, alternative methods that are less invasive of employee privacy should be considered,

➤ **Scope of monitoring**, which should generally be limited to metadata such as sender information, subject line, keywords, timestamps of sent/received emails, and recipient addresses,

➤ **Monitoring plan**, including time, location, responsible personnel, specific email addresses, search parameters, data extraction methods, and other relevant details.

It is important to emphasize that **reviewing the content** of email communication should be an **exception**, due to the privacy rights of individuals or companies outside the organization who may be communicating with the monitored employee. The aforementioned Working Document (2002) recommends that, in cases where content is accessed, the employer should make reasonable efforts to inform external parties about the existence of monitoring activities (in this case, email monitoring), to the extent that such monitoring may affect them. One example is the inclusion of a disclaimer in all outgoing company emails indicating that communications may be monitored.

When it comes to monitoring employee internet usage or access to various websites, it is advisable to use technical solutions that block access to specific websites or restrict access to internal company pages only, rather than conducting active monitoring. A good practice is to implement on-screen warnings that appear whenever an employee attempts to access a restricted website or a site for which they lack authorization. Another option is to display a login warning message each time the employee starts the computer. An example of such a message might be: *"This computer is the property of the company. Use of this computer is intended solely for authorized users and for strictly defined purposes. Unauthorized access or modification of settings may result in disciplinary action and/or legal prosecution. All company IT systems may be monitored to ensure secure and appropriate use. For questions, please contact..."* The Working Document (2002) also warns that employers must be cautious when interpreting internet usage data, as websites can be accessed

[10] The Personal Data Protection Agency of the Republic of Croatia believes that monitoring e-mail without a specific explanation and reason (i.e. a legitimate and particularly justified purpose) constitutes a violation of employee privacy. Available at: https://azop.hr/nadzor-poslovne-elektronicke-poste/

unintentionally (e.g., via hyperlinks, ads, or typing errors). Employees should be given the opportunity to explain or contest any conclusions drawn by the employer.

As indicated in the title of this paper, the primary focus has been on monitoring employee email and internet usage during corporate investigations. However, it is also important to mention other forms of monitoring, such as:

- Tracking the location of company mobile phones,
- Using GPS data from company vehicles,
- Monitoring access to wireless networks,
- Tracking the location of company smartwatches used by employees.

These types of monitoring become even more complex when conducted during remote work or when employees use such devices during personal time. These topics were not the subject of this paper and may be explored in future research. Additionally, this paper does not address the technical methods of accessing email (e.g., remote access, direct access to device memory, cloud data), as these depend on the technical solutions implemented by each company.

Conclusion

The advancement of technology, which will be increasingly applied in the daily digitalization of business operations, will further complicate the monitoring of employee email and internet usage, while simultaneously increasing the risks companies face when engaging in such activities. It is reasonable to expect that, due to the continuous development of technology and the growing difficulty in clearly distinguishing between private and professional life, there will be a stronger emphasis on the protection of employee privacy. At the same time, employers will increasingly justify the intensification of threats to their interests to legitimize (and implement) restrictions on employees' rights to respect for their private life and personal communications in the workplace.

In conducting such activities, companies expose themselves not only to reputational risks but also to potential financial risks, including fines resulting from lawsuits filed by supervisory authorities or employees themselves. Companies are required to demonstrate that such monitoring is lawful, necessary, and proportionate in relation to the legitimate interests they seek to protect—namely, the security of employees and the protection of company assets.

The need for companies to conduct corporate investigations will continue to grow—not only for the purpose of establishing facts in specific incidents but also to develop and propose

measures to prevent the recurrence of such incidents. This can be viewed as a preventive activity. It is important to emphasize that every investigation disrupts regular business operations and consumes company resources. Therefore, the preventive effect of conducting corporate investigations should be a priority.

Literature

Articles and books

1. Dragičević Prtenjača, M., & Zagorec, M. (2023). Ponešto o privatnosti, pravu na privatnost i njezinoj zaštiti u Hrvatskoj kroz kazneno djelo Nedozvoljene uporabe osobnih podataka. Godišnjak Akademije pravnih znanosti Hrvatske, 14(1), 57–85.
2. Dundović, D. (2022). Korporativne istrage – Nezamjenjiv dio korporativne sigurnosti. In XV Međunarodno stručna konferencija Dani kriznog upravljanja, Zbornik radova (pp. 285–296). Veleučilište Velika Gorica.
3. Komanovics, A. (2023). Workplace privacy in the EU: The impact of emerging technologies on employees' fundamental rights. EU and Comparative Law Issues and Challenges Series (ECLIC), 7, 443–474.
4. Meerts, C. (2016). A world apart? Private investigations in the corporate sector. Erasmus Law Review, Vol. 9, No. 4, 2016, (December 31, 2016).
5. Ray, J. E., & Rojot, J. (1995). Worker privacy in France. Comparative Labour Law & Policy Journal, 17, 61–74.

International Acts and Official Documents

1. Council of Europe. (2014). Parliamentary Assembly Resolution 1986: Improving user protection and security in cyberspace. Retrieved February 3, 2025, from http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=20791&lang=en (Accessed 3.2.2025.)
2. European Parliament and Council. (2016). Directive (EU) 2016/1148 on measures for a high common level of security of network and information systems across the Union. Official Journal of the European Union, L 194/1.
3. Konvencija za zaštitu ljudskih prava i temeljnih sloboda Official Gazette, international agreements, no.18/97., 6/99., 14/02., 13/03., 9/05., 1/06., 2/10.
4. United Nations. (1966). International Covenant on Civil and Political Rights. Resolution 2200 A (XXI), From https://pravamanjina.gov.hr/UserDocsImages/arhiva/pdf/medjunarodni/medjunarodni_pakt_o_gradjanskim_i_politickim_pravima.pdf (Accessed 30.1.2025.)

5. United Nations. (1948). Opća deklaracija o ljudskim pravima, from https://narodne-novine.nn.hr/clanci/medunarodni/2009_11_12_143.html (Accessed 30.1.2025.)
6. European Union. (2010). Charter of Fundamental Rights of the European Union. Official Journal of the European Union, C 83/389, from https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex%3A12007P (Accessed 30.1.2025.)
7. United Nations General Assembly. (2013). The right to privacy in the digital age (A/RES/68/167), from https://undocs.org/A/RES/68/167 (Accessed 5.2.2025.)
8. United Nations. (n.d.). Special Rapporteur on the right to privacy, from https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx (Accessed 5.2.2025.)
9. European Parliament and Council. (2019). Uredba (EU) 2019/881 o ENISA-i i certifikaciji kibernetičke sigurnosti [Regulation (EU) 2019/881 on ENISA and cybersecurity certification]. Official Journal of the European Union, L 151/15.
10. European Parliament and Council. (2016). Uredba (EU) 2016/679 o zaštiti osobnih podataka (General Data Protection Regulation). Official Journal of the European Union, L 119/1C, from https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:32016R0679 (Accessed 3.2.2025.)
11. European Court of Human Rights. (2017). Bărbulescu v. Romania [GC], Application no. 61496/08, from https://hudoc.echr.coe.int/fre#{"itemid":["001-177082"]} (Accessed 13.2.2025.)
12. European Court of Human Rights. (2007). Copland v. United Kingdom, Application no. 62617/00. Retrieved March 15, 2025, from http://hudoc.echr.coe.int/eng?i=001-79996 (Accessed 15. 3. 2025).
13. European Court of Human Rights. (2002). Société Colas Est and Others v. France, Application no. 37971/97, from https://hudoc.echr.coe.int/eng#{"itemid":["001-60431"]} (Accessed 4.2.2025.)
14. European Commission. (2017). Article 29 Data Protection Working Party, Opinion 2/2017 on data processing at work (17/EN, WP 249, para. 6.2).
15. European Commission. (2002). Article 29 Data Protection Working Party, Working Document on the Surveillance of Electronic Communications in the Workplace, From https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2002/wp55_en.pdf (Accessed 11.2.2025)

Croatian Legislation

Kazneni zakon (NN, br. 125/11, 144/12, 56/15, 61/15, 101/17, 118/18, 126/19, 84/21).

Ustav Republike Hrvatske (NN, br. 85/2010).

Zakon o elektroničkim komunikacijama (NN, br. 76/22).

Zakon o elektroničkim medijima (NN, br. 111/21, 114/22).

Zakon o medijima (NN, br. 59/04, 84/11, 81/13, 114/22).

Zakon o provedbi Opće uredbe o zaštiti podataka (NN, br. 42/18).

Zakon o računovodstvu (NN, br. 85/2024).

Zakon o radu (NN, br. 93/14, 127/17, 98/19), čl. 29.

Zakon o sudovima za mladež (NN, br. 84/11, 143/12, 148/13, 56/15, 126/19).

Zakon o zaštiti potrošača (NN, br. 19/22).

Internet sources

1. Agencija za zaštitu osobnih podataka. Nadzor poslovne elektroničke pošte. https://azop.hr/nadzor-poslovne-elektronicke-poste/ (Accessed 14.2.2025.)
2. Trades Union Congress. (2018). I'll be watching you: A report on workplace monitoring. https://www.tuc.org.uk/research-analysis/reports/ill-be-watching-you (Accessed 11.2.2025)