UNIVERZITET U SARAJEVU
EKONOMSKI FAKULTET

ZAVRŠNI RAD

PRAVNA I ETIČKA PITANJA NADZORA ZAPOSLENIKA

Sarajevo, septembar 2024. godine HANADI ŽELJO

ZAHVALNICA

Ovim se putem želim zahvaliti svojoj mentorici, prof. dr. Fatimi Mahmutćehajić, koja mi je bila velika inspiracija i podrška tokom pisanja ovog rada, i bez čijih smjernica ovaj istraživački rad bi bilo nemoguće dovesti do kraja.

Najiskrenije riječi zahvalnosti upućujem svojoj porodici koja me je bodrila, razumjela i podržavala u toku sticanja novih znanja i vještina.

U skladu sa članom 54. Pravila studiranja za I, II ciklus studija, integrisani, stručni i specijalstički studij na Univerzitetu u Sarajevu, daje se

I Z J A V A O A U T E N T I Č N O S T I R A D A

Ja, **Hanadi Željo**, studentica drugog (II) ciklusa studija, broj index-a **6053 HRM/22** na programu **Ekonomija**, smjer **Menadžment ljudskih resursa i upravljanje znanjem** izjavljujem da sam završni rad na temu:

PRAVNA I ETIČKA PITANJA NADZORA ZAPOSLENIKA

pod mentorstvom **prof. dr. Fatima Mahmutćehajić** izradila samostalno i da se zasniva na rezultatima mog vlastitog istraživanja. Rad ne sadrži prethodno objavljene ili neobjavljene materijale drugih autora, osim onih koji su priznati navođenjem literature i drugih izvora informacija uključujući i alate umjetne inteligencije.

Ovom izjavom potvrđujem da sam za potrebe arhiviranja predao/predala elektronsku verziju rada koja je istovjetna štampanoj verziji završnog rada.

Dozvoljavam objavu ličnih podataka vezanih za završetak studija (ime, prezime, datum i mjesto rođenja, datum odbrane rada, naslov rada) na web stranici i u publikacijama Univerziteta u Sarajevu i Ekonomskog fakulteta.

U skladu sa članom 34. 45. i 46. Zakona o autorskom i srodnim pravima (Službeni glasnik BiH, 63/10) dozvoljavam da gore navedeni završni rad bude trajno pohranjen u Institucionalnom repozitoriju Univerziteta u Sarajevu i Ekonomskog fakulteta i da javno bude dostupan svima.

Sarajevo, 09. 09. 2024. godine

Studentica
Hanadi Željo

Potpis studentice

SAŽETAK

Razvojem modernih tehnologija, jedno od područja koje je suočeno sa nužnim prilagođavanjima, u skladu sa pravnim i etičkim dilemama, a posljedično i sporovima je - radno mjesto - odnosno prava zaposlenika na jednoj i prava poslodavca na drugoj strani. Ovaj rad istražuje pravna i etička pitanja nadzora zaposlenika. Istraživanje analizira pravni okvir za praćenje zaposlenika unutar Europske unije pokazujući nijansirane pristupe nadzoru u različitim jurisdikcijama, kao i prikaz rješenja u vezi sa nadzorom zaposlenika u pravu Bosne i Hercegovine. Uz navedeno, sistematično su prikazani relevantni pravni dokumenti koji su zastupljeni u svim pojedinačnim zemljama Evropske unije (uzimajući u obzir i Norvešku i Veliku Britaniju), same specifičnosti svake o zemalja Evropske unije, te ograničenja korištenja nadzora zaposlenika uvažavajući pravnu regulativu za obradu osobnih podataka, transparentnost poslodavaca i prava zaposlenika na pristup i izmjene svojih podataka. Na osnovu provedenih istraživanja, uz analizu relevantnih sudskih slučajeva, moguće je zaključiti da pravni okvir u Evropskoj uniji koji regulira pitanja nadzora zaposlenika, adekvatno štiti prava zaposlenika. Pored navedenoga, u funkciji postavljene izvedene i pomoćne hipoteze, u radu su analizirani i proučavani pravni okvir nadzora zaposlenika u Bosni i Hercegovini, te odredbe Zakona o zaštiti ličnih podataka Bosne i Hercegovine, kojima su jasno određeni načini i mogućnosti nadzora zaposlenika u Bosni i Hercegovini. Etički izazovi nadzora zaposlenika adresirani su kroz diskusiju o balansiranju između sigurnosti i privatnosti zaposlenika. Raspravlja se o etičkim dilemama koje proizlaze iz savremenih tehnika nadzora, te se posebna pažnja posvećuje debatama o produktivnosti, sigurnosti, odgovornosti, privatnosti, kreativnosti, paternalizmu i društvenoj kontroli. Interakcija prava i etike u kontekstu nadzora istražuje se kroz analizu slučajeva sukoba između pravnih rješenja i etičkih standarda, s posebnim osvrtom na mišljenja, smjernice i dobre prakse u nadzoru zaposlenika u EU. U ovom završnom radu predstavljeno je istraživanje koje uključuje studiju slučaja Adriatic Metalsa. Rezultati istraživanja u vezi sa praksama nadzora među zaposlenicima potvrđuju složenu dinamiku nadzora. Prepoznajući potencijalne koristi za sigurnost i učinkovitost, zabrinutost zbog invazivne prirode određenih praksi praćenja, poput praćenja internetske komunikacije i videonadzora u vozilu, sugerira značajne etičke i moralne izazove. Rad potvrđuje glavnu hipotezu da trenutni pravni okvir u EU adekvatno štite prava zaposlenika. Uz glavnu, potvrđena je i izvedena hipoteza ovog završnog rada, odnosno da su tehnološka rješenja često u koliziji sa važećim pozitivno-pravnim propisima i praksama, pa je u skladu s tim u savremenim uvjetima poslovanja nužno naći pravu ravnotežu između prava zaposlenika, na jednoj i prava nadzora od strane poslodavca, na drugoj strani, što bez nužnog uvažavanja i etičkih principa nije moguće.

Ključne riječi: pravni okvir nadzora, etičnost nadzora, kompanije, zaposlenici, pravni okvir u Evropskoj uniji

ABSTRACT

With the development of modern technologies, one of the areas that is faced with necessary adjustments, in accordance with legal and ethical dilemmas, and consequently disputes, is - the workplace - i.e. the rights of employees on the one hand and the rights of the employer on the other. This paper explores the legal and ethical issues of employee supervision. The research analyzes the legal framework for monitoring employees within the European Union, showing nuanced approaches to supervision in different jurisdictions, as well as presenting solutions related to employee supervision in the law of Bosnia and Herzegovina. Furthermore, the relevant legal documents that are represented in all individual countries of the European Union (taking into account Norway and Great Britain), the specifics of each country of the European Union, and the limitations of the use of employee supervision are systematically presented, taking into account the legal regulations for the processing of personal data, the transparency of employers and the rights of employees to access and change their data. Based on the conducted research, with the analysis of relevant court cases, it is possible to conclude that the legal framework in the European Union that regulates the issues of employee supervision adequately protects the rights of employees. Moreover, in the function of the derived and auxiliary hypotheses, the paper analyzes and studies the legal framework of employee supervision in Bosnia and Herzegovina, as well as the provisions of the Law on Personal Data Protection of Bosnia and Herzegovina, which clearly define the ways and possibilities of employee supervision in Bosnia and Herzegovina. The ethical challenges of employee supervision are addressed through a discussion on balancing employee security and privacy. Ethical dilemmas arising from modern surveillance techniques are discussed, and special attention is paid to debates on productivity, security, responsibility, privacy, creativity, paternalism and social control. The interaction of law and ethics in the context of supervision is explored through the analysis of cases of conflict between legal solutions and ethical standards, with special reference to opinions, guidelines and good practices in the supervision of employees in the EU. In this final paper, a research involving a case study of Adriatic Metals is presented. The results of the survey regarding supervisory practices among employees confirm the complex dynamics of supervision. Recognizing the potential benefits for safety and efficiency, concerns about the invasive nature of certain surveillance practices, such as monitoring internet communications and in-vehicle video surveillance, suggest significant ethical and moral challenges. The paper confirms the main hypothesis that the current legal framework in the EU adequately protects the rights of employees. In addition to the main one, the hypothesis of this final paper was confirmed and derived, that is, that technological solutions are often in collision with valid positive legal regulations and practices, and accordingly, in modern business conditions, it is necessary to find the right balance between the rights of the employee, on the one hand, and the right of supervision by the employer, on the other, which is not possible without the necessary respect and ethical principles.

Keywords: legal framework of supervision, ethics of supervision, companies, employees, legal framework in the European Union

SADRŽAJ

POPIS TABELA

POPIS ILUSTRACIJA

POPIS GRAFIKONA

POPIS SKRAĆENICA

BIH Bosna i Hercegovina

CRM Upravljanje odnosima sa kupcima

EC Evropska Komisija

ESLJP Evropski Sud za Ljudska Prava

EU Evropska unija

GDPR Opšta uredba o zaštiti podataka

GPS Globalno položajni sistem

ICT Informacijske i komunikacijske tehnologije

OECD Organizacija za ekonomsku suradnju i razvoj

SAD Sjedinjene Američke Države

1. UVOD

Stalna evolucija tehnologije mijenja naše metode komunikacije, interakcije i rada u društvu. Jedno od područja koje je suočeno sa nužnim prilagođavanjima, u skladu sa pravnim i etičkim dilemama, a posljedično i sporovima je - radno mjesto - odnosno prava zaposlenika na jednoj i prava poslodavca na drugoj strani. Ovo naročito dolazi do izražaja primjenom novih tehnologija, posebno u vezi s praćenjem osoblja putem elektroničkih uređaja (Ball, 2021). Tehnologija danas omogućava povećanje produktivnosti poslodavcima, ali pored toga donosi i niz pravnih i etičkih izazova. Neki od najznačajnijih pravnih izazova su pravo na privatnost (Solove i Schwartz, 2021), zakonski pristanak na aktivnosti nadzora (Kuner *et al.*, 2013), te da prikupljanje ličnih podataka zaposlenika mora biti u skladu sa zakonom o zaštiti podataka (Cate i Mayer-Schönberger, 2013). S druge strane, kao najznačaniji etički izazovi navode se smanjenje povjerenja i transparentnosti zaposlenika (Baase, 2012), pravednost i jednakost nadzora zaposlenika (Nissenbaum, 2009), te autonomija i sloboda zaposlenika (Tursunbayeva, Di Lauro i Pagliari, 2018). Predmet ovog rada nastoji da pruži kritički pregled literature i analizira praksu pravnih i etičkih problema poslovanja, a naročito prilikom nadzora zaposlenika.

U ovom radu bit će artikulirani akademski naučni radovi, odnosno teorijski okvir i primjeri iz prakse, kako bi bili detaljno istraženi izazovi koje tehnologija predstavlja za poslodavce u upravljanju produktivnošću. Naročito će biti analizirani pravni i etički aspekti i dimenzije koje će uključivati prava radnika kao što su pravo na privatnost i slobodu komuniciranja i kretanja.

Pravni i etički okviri za praćenje zaposlenika u središtu su ovog istraživanja. S obzirom na brzi napredak tehnologije, postoji hitna potreba da se istraži jesu li "moderne" prakse nadzora, naročito imajući u vidu savremene uvjete poslovanja i digitalnu transformaciju, kompatibilne sa pozitivno pravnim propisima (Ball, 2021).

Ti se izazovi mogu bolje razumjeti kroz perspektive kao što su deontološka i teleološka. Kada je riječ o moralnim dužnostima i pravilima, deontološka razmatranja su ključna, dok se teleološka razmatranja više usredotočuju na posljedice i krajnje ciljeve. Međutim, u području nadzora ova se dva pristupa često sukobljavaju, stvarajući jaz između zakona i etike (Alder, 1998).

Analizirajući teoretske koncepte, poput onih koji se nalaze u dokumentu "Etička pitanja u elektroničkom praćenju učinka", i scenarije iz stvarnog svijeta koje daje Ball (2021), koji će biti osnova za analizu pravnih i etičkih nedoumica koje okružuju praćenje zaposlenika primjenom tehnologije. Savremeno praćenje zaposlenika suočava se s nizom etičkih i pravnih problema zahvaljujući napretku digitalne tehnologije. Prema izvještaju Eurofound (2020), pokazalo je da više od jedne četvrtine (27%) organizacija na nivou EU koristi analitiku podataka za praćenje učinka zaposlenika i da će korištenje takvih tehnika ići samo uzlaznom putanjom u godinama koje dolaze. Spomenuto istraživanje također pokazuje da je

praćenje učinka zaposlenika najčešće u Hrvatskoj i Rumuniji, a najmanje u Njemačkoj i Švedskoj. Najviše su ga primjenjivale velike kompanije s 250 ili više zaposlenika, a najmanje male kompanije s 10 do 49 zaposlenika (Eurofound, 2020).

Međutim, važno je sagledati i povijesni kontekst. Čak i tokom industrijske revolucije, menadžeri su imali politike za praćenje ponašanja i produktivnosti radnika (Zuboff, 1988). Međutim, savremene digitalne tehnologije pružaju bez presedana mogućnosti za nadzor, stvarajući niz novih pravnih i etičkih izazova u savremenim uslovima poslovanja.

Jedan od ključnih izazova je pitanje privatnosti. Zaposlenik ima pravo na privatnost, ali kako se to odnosi paralelno na poslovne interese poslodavca i na njegovo pravo nadzora poslovanja, a posljedično i zaposlenika, na nivou Evropske unije postoje brojne sudske odluke koje istražuju ovu vezu i koje će biti predstavljene u ovom radu. Prema *Regulation (EU) 2016/679* (Direktivi o zaštiti podataka EU (2016/679)OJ L 119, 4.5.2016, p. 1–88), poslodavci moraju imati opravdan razlog za prikupljanje i obradu ličnih podataka zaposlenika, a nadzor mora biti "nužan i razmjeran" (European Parliament, 2016). Odnos između prava zaposlenika na privatnost i interesa poslodavca u nadzoru i obradi ličnih podataka zaposlenika istražuje se u kontekstu EU prema Direktivi o zaštiti podataka 2016/679. Neke države članice EU mogu imati zahtjeve o privatnosti i radu koji su čak strožiji od rješenja sadržanih u *General Data Protection Regulation,* (Opštoj uredbi o zaštiti podataka, u nastavku GDPR) (European Parliament, 2016) što dopušta državama članicama da uspostave vlastita posebna pravila za obradu ličnih podataka u okviru zapošljavanja. Zemlje poput Belgije, Francuske, Italije i Španije, na primjer, uspostavile su pravo na prekid veze (right to disconnect). Sudska praksa, kao što je presuda u slučaju "Bărbulescu protiv Rumunije" (European Parliament, 2016), naglašava da nadzor komunikacija zaposlenika od strane poslodavca mora biti nužan i razmjeren, uz prethodno obavještenje zaposlenika.

Također, postoji i pitanje informirane privole. Kako navodi Moor (2005), tehnološki napredak često napreduje brže od razvoja odgovarajućih etičkih smjernica i zakonskih regulativa, što dovodi do stvaranja "sive zone". Zaposlenici bi trebali biti jasno informirani o prirodi, opsegu i svrsi nadzora, kao i o tome kako će se prikupljeni podaci koristiti. Bez transparentnosti i privole, elektronski nadzor može se smatrati neetičnim i potencijalno nezakonitim.

Nadalje, postoji rizik od zloupotrebe informacija prikupljenih kroz elektronski nadzor. Baš kao što Zuboff (1988) sugerira da tehnologija može biti korištena kako za osnaživanje, tako i za dominaciju, postoji potreba za strožijim smjernicama kako bi se spriječila zloupotreba nadzornih tehnologija. Na nivou EU donesena je *General Data Protection Regulation* (Opštoj uredbi o zaštiti podataka) koja je postala obvezujuća u maju 2018. godine. Prema odredbama GDPR osnažena su prava zaposlenika u vezi s obradom njihovih ličnih podataka na radnom mjestu. Pristanak zaposlenika rijetko se prihvaća kao pravna osnova za obradu podataka zbog neravnoteže moći. Umjesto toga, GDPR postavlja stroge smjernice za transparentnost, informiranje zaposlenika i zaštitu njihovih prava u vezi s obradom podataka,

što ima ključnu ulogu u zaštiti privatnosti zaposlenika i poslovnih interesa poslodavaca prema Article 29 17/EN WP 249 Opinion 2/2017 (European Commission, 2017).

Za razumijevanje cjeline ovog rada, valja razmotriti i kulturološke razlike u percepciji nadzora. Ono što je prihvatljivo u jednom okruženju možda nije u drugom. Kako svjetsko tržište rada postaje globalno, potrebno je proučavati i razumijevati ove razlike kako bi se pravilno usmjeravali i razvijali i pravna rješenja ali i etički standardi (Hofstede, 2001).

Razvoj modernih tehnologija donosi mnoge prednosti, i otvara nove načine i mogućnosti za praćenje nadzora zaposlenika. Takve tehnologije mogu unaprijediti produktivnost i poboljšati ukupnu ekonomsku aktivnost kompanija. Pored toga, moderne tehnologije često su u koliziji sa važećim regulativama i praksama shodno tome treba ih balansirati i naći pravu ravnotežu između prava zaposlenika i prava nadzora od strane poslodavca. S obzirom na brzi tehnološki razvoj, kontinuirano istraživanje i revizija, a potom i razvoj pravnih rješenja bit će ključna stavka u budućnosti.

1.1. Predmet rada

Nadzor zaposlenika je često opravdan na temeljima povećanja produktivnosti zaposlenika, te promoviranja odgovornosti i efikasnosti među zaposlenicima (Attewell, 1987; Ball, 2010). No s druge strane, nadzor zaposlenika ima i svoje negativnosti, kao što su povećano nezadovoljstvo poslom i fluktuacija, aktivni otpor, pa čak i odmazda zaposlenih (Anteby i Chan, 2018; Bernstein, 2012). Prema tome, velika je važnost ovog pitanja za uspješno poslovanje kompanija, naročito sa pravnog i etičkog aspekta (Yerby, 2013).

Predmet rada su pravna i etička pitanja nadzora zaposlenika. Kroz rad se teorijskim osvrtom bavi pitanjem kako etika nadzora zaposlenika utiče na istog. Pored navedenog objašnjen je fenomen pravnog nadzora zaposlenika u EU. U istraživačkom dijelu prikazano je kako i na koji način kompanija Adriatic Metals reguliše pitanja nadzora zaposlenika.

1.2. Hipoteze

U kontekstu pravnih i etičkih pitanja vezanih za ciklus zaposlenika i nadzor na radnom mjestu, predložene su sljedeće hipoteze.

Glavna hipoteza: Pravni okvir u Evropskoj uniji koji regulira pitanja nadzora zaposlenika, adekvatno štiti prava zaposlenika.

Izvedena hipoteza: Tehnološka rješenja često su u koliziji sa važećim pozitivno-pravnim propisima i praksama, pa je u skladu s tim u savremenim uvjetima poslovanja nužno naći pravu ravnotežu između prava zaposlenika, na jednoj i prava nadzora od strane poslodavca, na drugoj strani, uz nužno uvažavanje etičkih principa.

Pomoćna hipoteza: Odnosi u pravu Evropske unije prema pitanju prava zaposlenika, na jednoj i pravu nadzora od strane poslodavca, na drugoj strani su na višoj razini razvoja nego u Bosni i Hercegovini. Tako određeni odnos bit će osnova za izvođenje zaključaka o mogućnosti i dinamici promjena u pravu Bosne i Hercegovine, ali i poslovnoj praksi.

1.3. Ciljevi

Nagle promjene u radnom okruženju, s posebnim osvrtom na elektronski nadzor, su osnova za postavljanje istraživačkih ciljeva kako bi bila provedena sveobuhvatna analiza pravnih i etičkih pitanja u radnom ciklusu zaposlenika, istražujući implikacije tih promjena na zaštitu privatnosti i prava koja proizilaze iz radnog odnosa. Na osnovu dostupne literature iz područja poslovanja, prava i etike, ali i s navednim područjima povezanih empirijskih istraživanja, ciljevi ovog rada su:

1. Analiza povijesnog konteksta elektronskog nadzora zaposlenika: Razumijevanje kako su se prakse nadzora zaposlenika razvijale, kao i njihova pravna i etička obilježja (Smith, 2008);
2. Deontološki i teleološki pristupi etici nadzora: Analiza ovih dvaju etičkih pristupa kako bi se razumjele njihove specifične implikacije za elektronski nadzor zaposlenika (Alder, 1998);
3. Pravna regulativa i njeni izazovi: Ispitati važeće zakonske okvire na nivou EU vezane za elektronski nadzor, kao i identificirati "sive zone" i izazove u primjeni postojećih pravnih rješenja, te mogućim i nužnim unaprjeđenjima (Ball, 2021);
4. Stavovi zaposlenika prema elektronskom nadzoru: Cilj je istražiti kakvi su stavovi, osjećaji i percepcije zaposlenika o nadzoru u svrhu poboljšanja produktivnosti i efikasnosti. (Johnson, 2010) Studija slučaja u BiH –„Adriatic Metals“https://www.adriaticmetals.com/;
5. Preporuke za pravno-etički održive prakse nadzora: Cilj rada je analizirati teorije, prakse i empirijska istraživanja i na osnovu njih dati odredniceza pravno-etički održive prakse nadzora u Bosni i Hercegovini (Ball, 2021).

1.4. Metodologija istraživanja

U sferi metodološkog okvira za izradu završnog rada izdvajaju se primarni i sekundarni podaci. Bit će korištena teorijska i empirijska istraživanja iz recentnog perioda koja su usko povezana sa istraživačkim područjem, tačnije sa komparativnom analizom postojeće pravne

regulative i novih pravnih i etičkih izazova povezanih sa nadzorom zaposlenika, s jedne strane, te načina na koji primjena postojećih pravnih rješenja i digitalne transformacije utiče na zaštitu prava zaposlenika, s druge strane.

Metodologija završnog rada najvećim dijelom će se oslanjati na empirijska istraživanja koja su navedena u popisu literature za izradu završnog rada, iako ne obuhvata isključivo navedenu literaturu. Teorijska znanja iz literature poslužiti će kao osnova za donošenje zaključaka vezanih za analiziranje postavljenih ciljeva i dokazivanje postavljenih hipoteza. Bit će korišteni izvori iz dostupnih i relevantnih međunarodnih baza podataka.

Pored navedenog, metodologija završnog rada također obuhvata implementaciju spektra naučno-istraživačkih metoda, *inter alia*, općih naučnih metodu dedukcije i indukcije, te analize i sinteze, Uz njih bit će primijenjeni i posebni pravni metodi - historijski, normativni i uporedno-pravni metod.

2. POJAM NADZORA ZAPOSLENIKA I PRAVNI KONTEKST

Nadzor od strane "moćnih aktera" u društvu, bilo da se radi o vladama, kompanijama ili drugima, ima dugu historiju (Igo, 2018). Usprkos tome, nove informacijske i komunikacijske tehnologije (u nastavku ICT) i njihova sve veća zastupljenost u društvima širom svijeta omogućuju sve detaljniji nadzor nad sve većim brojem grupa, aktivnosti i prostora (Lyon, 2015; Nissenbaum, 2009). Od upotrebe kamera postavljenih na gotovo svakoj većoj ulici u Evropi i sve veće upotrebe softvera za prepoznavanje lica od strane policijskih tijela (McCahill i Norris, 2003; Harmon 2019), do masivnog digitalnog nadzornog aparata vlada (Mozur, 2019), do sve više priznatih nadzornih aktivnosti privatnih tehnoloških kompanija (Fowler, 2019.; Kwet, 2019; Zuboff, 2019), gotovo svaka osoba danas iskusi neki oblik nadzora u svom svakodnevnom životu.

Kompanije sve više koriste ICT za nadzor zaposlenika (Stark, Stanhaus, i Anthony, 2020), najčešće koristeći analitiku lica, snimki zaslona radne stanice, analizu e-pošte, te praćenja ponašanja na mreži (Solon, 2017). Svaka tehnologija koja nadzor i komunikaciju čini učinkovitijima olakšava nadzor (Rule, 1973), a ICT omogućuje nadzornim aktivnostima da prošire opseg nadzora, na nove prostore, nove aktivnosti, nove grupe i nove vrste informacija, uključujući i na radnom mjestu (Ullmann-Margalit, 2008). ICT ne samo da povećavaju kanale kroz koje se nadzor može odvijati, već i njegov opseg i sveprisutnost (Levy i Barocas, 2018), povećavajući kapacitete poslodavaca da nadziru i oblikuju svakodnevicu radne prakse (Rosenblat i Stark, 2016). Procjenjuje se da gotovo 75 posto američkih kompanija nadzire komunikaciju radnika i aktivnosti na poslu te da se nadzire 27 milijuna online zaposlenika širom svijeta (Ball, 2010).

2.1. Historijski kontekst nadzora

Praćenje radnog mjesta nije nova praksa u smislu da kompanije na razne načine pokušavaju doći do informacija o sebi i zaposlenicima u različite svrhe. Findlay i McKinlay (2003) navode da nema sumnje da je konvergencija kompjuterskih i telekomunikacijskih tehnologija otvorila nove mogućnosti, između ostalog, za nadzor radnika, potrošača i građana. Više od toga, teorija nadzora tvrdi da te mogućnosti nadzora također nude neviđene prilike za centralizaciju ličnih podataka, dopuštajući sve opsežnije i intimnije praćenje svih aspekata društvenog života (Findlay i McKinlay, 2003).

Na radnom mjestu, nadzor proizlazi iz "sposobnosti poslodavca da prati, bilježi i evidentira učinak zaposlenika, ponašanja i lične karakteristike", ponekad u stvarnom vremenu (Ball, 2010). Historija ranih velikih kompanija naglašava kako je razvoj "informacijskih sistema" dao menadžerima kompanija mogućnost da nadziru svoje unutrašnje strukture, što se obično opravdavalo u ime produktivnosti i kontrole kvalitete (Attewell, 1987). Dok je "nadzor na radnom mjestu" termin koji se koristi kao sinonim za "monitoring zaposlenika" (Ball, 2010., str. 88), prastara praksa, njegove savremene metode u Sjedinjenim Američkim Državama (nastavku SAD) imaju svoje korijene u transformaciji radne snage sredinom 19. do početka 21. stoljeća, kada su se radnici počeli seliti u gradove kako bi zaradili veću platu, fokus rada i radnog mjesta pomaknuo se s rada za preživljavanje na farmama na rad po satu i plaćen rad u tvornicama industrijske revolucije (Rosenblat, Kneese i Boyd, 2014).

Krajem 19. stoljeća, kako su željeznice širile svoj organizacijski doseg, trgovci s lokaliziranim trgovinama i poznavanjem tržišta morali su se spojiti kako bi ostali konkurentni na rastućem tržištu. Spajanja nisu automatski proizvela jedinstvene organizacijske jedinice, a načini proizvodnje i računovodstva unutar kompanija često su bili u neredu (Saval, 2014). Nakon što su proizvodnja dobara i metode njihova prijevoza nadmašili sporiji, ljudski tempo rada, pojavila se kriza kontrole za poslodavce koji su iznenada trebali obraditi mnogo više informacija kako bi držali korak s industrijskim tempom proizvodnje (Beniger, 1989).

Samim time, goruće pitanje postalo je koje strukture i tehnologije mogu osigurati učinkovitost i integritet u organizaciji poslovanja i rada (Zureik, 2003). Inovacije u obradi informacija i komunikacijskim tehnologijama koje su se razvile za rješavanje ovog pitanja bile su uglavnom usmjerene na upravljanje radnicima (Beniger, 1989).

Pitanjem učinkovitosti i integriteta u kompaniji počinje se baviti Frederick Winslow Taylor koji je radio kao savjetnik za učinkovitost u kompanijama na prijelazu 20. stoljeća (Saval, 2014). Njegova misijabila je mapirati znanje o tome kako je zadatak obavljen identificiranjem, fragmentiranjem i reguliranjem radnih tokova te primijeniti metode "praćenja učinka" za postizanje proizvodnih ciljeva (Sewell, 2005). Radnikovo znanje i kontrola nad radom na taj se način uklanjaju od radnika, a njegovo se izvršavanje

racionalizira u diskretni rad po komadu koji organizira i nadzire menadžer u sve više naučnom procesu (Braverman, 1998).

Pravilo Taylorističkog sistema je da je neopaženi radnik neučinkovit (Saval, 2014). Praćenje ima za cilj spriječiti radnike da usporavaju ili sabotiraju načine proizvodnje, kako u tvornicama tako i u kancelarijama. U Taylorovo doba neki su menadžeri pokušavali postići voljnu usklađenost tako što su praćenje vremena pretvorili u igru, koristeći štopericu za poticanje prijateljskog takmičenja među radnicima (Saval, 2014). Savremeni menadžeri nastavljaju koristiti različite metode, poput sistema nagrađivanja, kako bi potaknuli svoje zaposlenike da se pridržavaju nadzora na radnom mjestu.

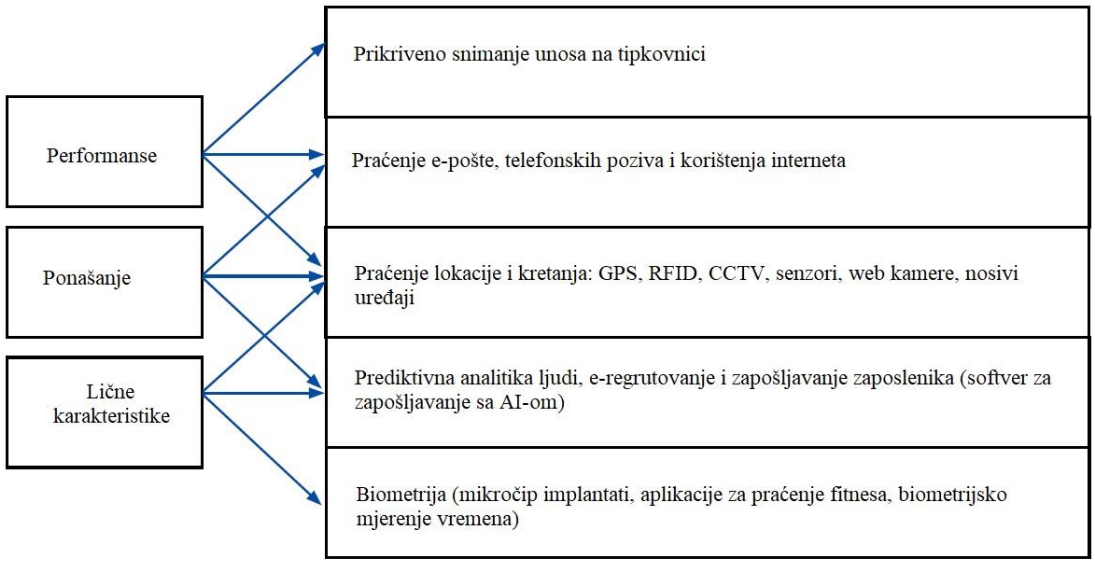
Promjena tehnologije otvorila je širok raspon opcija za praćenje aktivnosti radnika. Prije samo deset godina većina nadzora zaposlenika morala se obavljati lokalno u kancelarijama. Kako su se vremena promijenila, s promjenom u načinu obavljanja posla, menadžeri kompanija sada moraju promisliti kako i zašto se praćenje zaposlenika implementira i koristi (Rosenblat, Kneese i Boyd, 2014).

Savremeni menadžerski nadzor postao je osjetno lakši jer su nove tehnologije omogućile raznovrsnije, prodornije i raširenije prakse nadzora koje uključuju rutinsko testiranje na droge i praćenje e-pošte (Sewell, 2005). Štoviše, granice onoga što čini radno mjesto postaju sve poroznije, posebno jer digitalni uređaji i tehnologije posreduju u velikom dijelu našeg radnog sadržaja i komunikacije, kako na daljinu tako i na radnom mjestu. Elektronički nadzor može se dogoditi direktno na poslu ili kao funkcija pristupa zaposlenika poslodavcima putem njihovih uređaja izvan kancelarija.

Potom se pregovara o granicama nadzora na radnom mjestu u kontekstu šire rasprave između onoga što je javno i onoga što je privatno (Dash, 2014.).

Tehnološki razvoj proširio je obim praćenja zaposlenih izvan tradicionalnih metoda kao što su sigurnosne kamere, e-mail, telefon i internet nadzor. Poboljšani digitalnim inovacijama, novi alati za nadzor sada mogu pratiti performanse, ponašanje i lične osobine zaposlenih, potencijalno postajući sastavni dio sistema upravljanja (Ilustracija 1) (Eurofond, 2020).

Ilustracija 1. Tehnike i uređaji za praćenje i nadzor zaposlenih



Izvor: Autor završnog rada prilagođeno prema Ball (2010)

Pandemija COVID-19 ubrzala je usvajanje novih digitalnih alata za praćenje. Prelazak na daljinski rad tokom ovog perioda doveo je do povećane potražnje za softverom *keylogger* za praćenje korištenja kompjuterazaposlenika koji rade od kuće, kao i drugim aplikacijama koje snimaju slike web kamere u redovnim intervalima kako bi provjerile dostupnost i prisutnost zaposlenika na njihovim kompjuterima (Business Insider, 2020; Washington Post, 2020). Podaci o Google trendovima pokazuju da su pretraživanja za „nadzor zaposlenika na daljinu" porasla na početku karantina zbog COVID-19 u proljeće 2020. godine. Kako se rad na daljinu normalizira, očekuje se da će sve više kompanija nastaviti ulagati u tehnologije za praćenje rezultata zaposlenih (Sostero *et al*., 2020).

Iako se na primjenu tehnologija digitalnog nadzora često gleda negativno, ona može biti opravdana ovisno o zahtjevima posla i može čak ponuditi pogodnosti zaposlenima. Ipak, razlikovanje između legitimne upotrebe i potencijalnog kršenja privatnosti može biti izazovno. Na primjer, globalno položajni sistem (eng: *Global Positioning System*, u nastavku GPS) već dugo koriste kompanije za transport i dostavu ne samo za olakšavanje zadataka zaposlenima, već i za nametljivo praćenje njihovog učinka, uključujući trajanje njihovih pauza i njihovo kretanje van radnog vremena (Eurofond, 2020).

2.2. Evolucija pravnih rješenja nadzora

Brojni poslodavci su mišljenja kako nadzor radnoga okruženja utiče na produktivnost radnika i sigurnost kompanije, no neovisno o kakvoj se vrsti nadzoraradi, poslodavci trebaju paziti da ne zloupotrijebenadzor i time naruše prava zaposlenika (Pivčević i Erceg Ćurić, 2022). Pravni okviri nadzora različito su se razvijali u različitim dijelovima svijeta. Za potrebe ovoga rada, uzimajući u obzir kontekst u kojem je rad napisan, geografske

pripadnosti, mi ćemo se prvenstveno fokusirati na područje Evrope, odnosno zemalja članica EU.

Nadzor na radnom mjestu se prvenstveno može vezati za *Convention for the Protection of Human Rights and Fundamental Freedoms* (Konvenciju za zaštitu ljudskih prava i temljenih sloboda) iz 1950. godine, koja je međunarodni ugovor o zaštiti ljudskih prava i sloboda u Evropi (Pivčević i Erceg Ćurić, 2022).

Preambula Konvencije za zaštitu ljudskih prava i osnovnih sloboda (poznate i kao Evropska konvencija o ljudskim pravima), koja je usvojena 1950. godine (Council of Europe, 1950):

„Vlade potpisnice ove Konvencije, članice Savjeta Evrope,

s obzirom na Univerzalnu deklaraciju o ljudskim pravima koju je Generalna skupština Ujedinjenih nacija proglasila 10. decembra 1948. godine;

s obzirom da je cilj Savjeta Evrope postizanje veće saradnje među svojim članicama i da se jedan od načina za ostvarenje tog cilja može naći u zaštiti i razvoju ljudskih prava i osnovnih sloboda;

potvrđujući svoju duboku vjeru u ove osnovne slobode koje su temelj pravde i mira u svijetu i koje se najbolje održavaju, s jedne strane, kroz stvarno političko demokratsko uređenje i, s druge strane, kroz zajedničko razumijevanje i poštovanje ljudskih prava na koja se oni oslanjaju;

ponovo potvrđujući svoje čvrsto opredeljenje za ove slobode kao osnovni stub Evropske pravne zajednice, koju oni stvaraju u zajedničkom interesu i za zajedničko dobro; saglasni su na donošenje ovih mjera koje će obezbediti kolektivne garancije za neka prava navedena u Univerzalnoj deklaraciji.“

U članu 8. Konvencija za zaštitu ljudskih prava i temeljnih sloboda propisuje da svako ima „pravo na poštovanje svog privatnog i porodičnog života, doma i dopisivanja; da se javna vlast neće miješati u ostvarivanje tog prava, osim u skladu sa zakonom i ako je u demokratstkom društvu nužno radi interesa državne sigurnosti, javnog reda i mira, ili ekonomske dobrobiti zemlje te radi sprečavanja nereda ili zločina, radi zaštite zdravlja ili morala ili radi zaštite prava i sloboda drugih“ . Zaštita prema čl. 8. Konvencije odnosi se na sadržaj komunikacije pri čemunije bitno na koji se način komunicira, putemtelefona, interneta ili e-pošte (Harris, O'Boyle i Warbrick, 2014).

Naredni korak u razvoju pravnih rješenja učinjen je nakon osnivanja EU, uvođenjem Direktive 95/46/ECo zaštiti pojedinaca u vezi s obradom ličnih podataka i slobodnom kretanju takvih podataka. Direktiva 95/46/EC, uvedena 24.10.1995. godine, imala je za cilj uskladiti zakone o zaštiti podataka u državama članicama EU i uspostaviti zajednički skup načela za obradu ličnih podataka. Direktiva je prepoznala važnost zaštite temeljnog prava pojedinaca na privatnost, istovremeno olakšavajući slobodan protok ličnih podataka unutar

EU-a. Ova Direktiva je stavljena van snage 24.05.2018 godine kada je uvedena Uredba 2016/679 Europskog parlamenta i Vijeća od 27.4.2016. o zaštiti pojedinca uvezi s obradom ličnih podataka i o slobodnomkretanju takvih podataka.

Pravnim aktom 2016/679, općepoznata kao GDPR[1], ima za cilj ojačati zaštitu podataka i prava na privatnost za pojedince unutar evropskog ekonomskog prostora, uključujući države članice EU. Uredba poslodavcima nameće stroge zahtjeve u pogledu obrade ličnih podataka, uključujući podatke prikupljene mjerama nadzora. Prema odredbama GDPR, poslodavci moraju osigurati da sve aktivnosti nadzora budu u skladu s načelima zakonitosti, poštenja i transparentnosti te da zaposlenici budu adekvatno obaviješteni o svrsi i opsegu nadzora. Osim toga, GDPR daje zaposlenicima prava kao što su pravo na pristup svojim ličnim podacima, pravo na ispravak i pravo na brisanje (poznato kao "pravo na zaborav")[2]. U narednom poglavlju bit će dat prikaz i analiza pravnihrješenja u Evropskoj uniji.

2.3 Temeljna prava zaposlenika u pravu EU

Prema Evropskoj Komisiji (u nastavku EC), svaki radnik u EU ima određena minimalna prava koja se odnose na (European Commission, 2024):

- zdravlje i sigurnost na radu: opća prava i obaveze, radna mjesta, oprema za rad, specifični rizici i ranjivi radnici (Direktiva 89/391/EEC);
- jednake mogućnosti za žene i muškarce: jednako postupanje prema muškarcima i ženama pri zapošljavanju i zanimanju, uključujući programe socijalne sigurnosti (Direktiva 2006/54/EC);
- zaštita od diskriminacije na temelju spola, rase, vjere, dobi, invaliditeta i seksualne orijentacije (Direktiva 2000/78/EC);
- radno pravo: nepuno radno vrijeme, ugovori na određeno, radno vrijeme, zapošljavanje mladih, informiranje i savjetovanje zaposlenika (Direktiva 2003/88/EC).

Council Directive of 12 June 1989 on the introduction of measures to encourage improvements in the safety and health of workers at work (89/391/EEC) (Direktiva 89/391/EEC) je uvedena 12.06.1989. godine i odnosi se na uvođenje mjera za poticanje poboljšanja sigurnosti i zdravlja radnika na radu. Osnovna svrha direktive (European

[1]Uredba 2016/679 Evropskog parlamenta i Vijeća od 27. aprila 2016. o zaštiti fizičkih osoba u vezi s obradom ličnih podataka i slobodnom kretanju takvih podataka, dostupna na: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679

[2] Uredba 2016/679 Evropskog parlamenta i Vijeća od 27. aprila 2016. o zaštiti fizičkih osoba u vezi s obradom ličnih podataka i slobodnom kretanju takvih podataka, dostupna na: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679

Commission, 1989) jeste da osigura zaštitu zdravlja i sigurnosti radnika postavljanjem općih načela za sprječavanje profesionalnih rizika, zaštitu sigurnosti i zdravlja, pružanje informacija, osposobljavanje i savjetovanje radnika, te promicanje kultura prevencije na radnom mjestu.

Directive 2006/54/EC of the European Parliament and of the Council of 5 July 2006 on the implementation of the principle of equal opportunities and equal treatment of men and women in matters of employment and occupation (recast) OJ L 204, 26.7.2006, p. 23–36 (Direktiva 2006/54/EC) je uvedena 05.07.2006. godine i odnosni se na provedbu načela jednakih mogućnosti i jednakog tretmana muškaraca i žena u pitanjima zapošljavanja i zanimanja. Osnovna svrha Direktive jeste da se nastoji boriti se protiv diskriminacije na temelju spola na radnom mjestu i promicati ravnopravnost spolova osiguravanjem jednakog tretmana za muškarce i žene u pitanjima zapošljavanja i zanimanja.

Council Directive 2000/78/EC of 27 November 2000 establishing a general framework for equal treatment in employment and occupationOJ L 303, 2.12.2000, p. 16–22 (Direktiva 2000/78/EC) usvojena je 27.11.2000. godine i predstavlja generalni okvir za jednaki tretman pri zapošljavanju i zanimanju. Direktiva ima za cilj suzbijanje diskriminacije na posebnim osnovama, naime vjeri ili uvjerenju, invaliditetu, dobi ili seksualnoj orijentaciji, u područjima zapošljavanja i zanimanja. Njime se uspostavlja pravni okvir za osiguranje jednakog tretmana pojedinaca na radnom mjestu, bez obzira na te karakteristike.

Directive 2003/88/EC of the European Parliament and of the Council of 4 November 2003 concerning certain aspects of the organisation of working timeOJ L 299, 18.11.2003, p. 9–19 (Direktiva 2003/88/EC) je uvedena 04.11.2003. godine i utvrđuje minimalne standarde za radno vrijeme, odmore i godišnji odmor za radnike u EU. Direktiva ima za cilj zaštititi zdravlje i sigurnost radnika uspostavljanjem minimalnih standarda za radno vrijeme, odmore i godišnji odmor. Nadalje, Direktiva nastoji osigurati da radnici imaju dovoljno vremena za odmor, opuštanje i slobodno vrijeme, a istovremeno promiče bolju ravnotežu između poslovnog i privatnog života.

3. PRAVNI OKVIR NADZORA ZAPOSLENIKA U EVROPSKOJ UNIJI I BOSNI I HERCEGOVINI

Analizirajući važeće zakonodavstvo u EU, moguće je zaključiti da se izričito ne govori o nadzoru zaposlenika, ali se neupitno ističu prava na privatnost i zaštitu podataka koja mogu biti ugrožena nadzorom zaposlenika. Najvažniji dio zakonodavstva EU u tom smislu je GDPR (Uredba 2016/679), koja zamjenjuje Direktivu 95/46/EZ. Stupanjem na snagu u maju 2018. i primjenjivim u svim državama članicama EU, GDPR regulira prikupljanje, korištenje i prijenos ličnih podataka i utvrđuje odredbe koje se primjenjuju na sve postupke obrade podataka, uključujući praćenje zaposlenika. Za uvođenje nadzora zaposlenika potreban je, primjerice, prethodni informirani pristanak zaposlenika. Međutim, pojedinačne države članice imaju u nadležnosti uvođenje posebnih odredbi u vezi sa obradom podataka o

zaposlenicima uključujući različite svrhe, od zapošljavanja, do zdravlja i sigurnosti (Eurofound, 2020)[3].

Prema navodima *European Union Agency for Fundamental Rights* (Evropske agencije za temeljna prava), GDPR je modernizirao zakonodavstvo EU o zaštiti podataka tako da ono odgovara novim izazovima privatnosti koje postavlja razvoj digitalnih tehnologija (Eurofound, 2020), ali ističući da posebna se pažnja mora ukazati na valjanost privole kao pravne osnove za obradu podataka o zaposlenicima, s jedne strane, i zabrinutost što se tiče opsega podataka koje kompanije prikupljaju o zaposlenicima, naročito u kontekstu veće povezanosti uređaja s omogućenim internetom stvari i poboljšanim mogućnostima obrade, s druge strane. Prema tome, nacionalna tijela za zaštitu podataka do sada su zauzela stajalište da veliki podaci spadaju u djelokrug zakona o zaštiti podataka i stoga moraju biti u skladu sa zakonodavstvom o zaštiti podataka (Eurofound, 2020).

Pored navedenoga, Eurofound (2020) navodi dva područja koja su jasno pogođena tehnološkim promjenama na radnom mjestu:

1. Zaštita i sigurnost na radu;
2. Neuronadzor na poslu.

Okvirna direktiva EU-a za sigurnost i zdravlje na radu (Direktiva 89/391/EEZ) utvrđuje opća načela i obaveze u vezi s prevencijom profesionalnih rizika i zaštitom sigurnosti i zdravlja radnika. Direktiva se, međutim, izričito ne bavi novim izazovima koje postavljaju digitalne tehnologije – uključujući tehnologije nadzora – ili pojavom novih vrsta zdravstvenih problema i rizika koje takve tehnologije mogu proizvesti (European Parliament, 2019).

Neuronadzor na poslu odnosi se na pozive na priznavanje novih ljudskih prava koja bi obuhvatala mentalnu privatnost i integritet. Prema tome, Organizacija za ekonomsku saradnju i razvoj (Organisation for Economic Co-operation and Development, u nastavku OECD) usvojila je 2019. godine prvi međunarodni pravni instrument o neurotehnologiji, definišući lične podatke o mozgu kao *„podatke koji se odnose na funkcioniranje ili strukturu ljudskog mozga identificiranog ili pojedinca koji se može identificirati i koji uključuje jedinstvene podatke o njegovoj fiziologiji, zdravlju ili mentalnom stanju“* (OECD, 2019). Nadalje, OECD (2019) preporučuje promicanje politika koje *„štite lične podatke o mozgu*

[3]Prema članu 88, GDPR navodi: „Države članice mogu, zakonom ili kolektivnim ugovorima, predvidjeti konkretnija pravila kako bi se osigurala zaštita prava i sloboda u pogledu obrade ličnih podataka zaposlenika u kontekstu zapošljavanja, posebno u svrhu zapošljavanja, izvršavanje ugovora o radu, uključujući ispunjavanje obveza utvrđenih zakonom ili kolektivnim ugovorima, upravljanje, planiranje i organizaciju rada, jednakost i različitost na radnom mjestu, zdravlje i sigurnost na radu, zaštitu imovine poslodavca ili stranke i za u svrhu ostvarivanja i uživanja, na individualnoj ili kolektivnoj osnovi, prava i pogodnosti vezanih uz radni odnos, te u svrhu prestanka radnog odnosa.“

od upotrebe za diskriminaciju ili neprikladno isključivanje određenih osoba ili populacija, posebno u komercijalne svrhe ili u kontekstu pravnih procesa, zapošljavanja ili osiguranja".

3.1. Pravni okvir Evropskoj uniji za nadzor zaposlenika

Zakonodavstvo većine država članica slijedi tehnološki neutralan pristup, postavljajući opća pravila široke primjene koja, barem u načelu, pokrivaju sve vrste praćenja i obrade. GDPR je kreiran s namjerom pokrivanja tehnološkog razvoja, posebno se pozivajući na činjenicu da je „opseg prikupljanja i dijeljenja ličnih podataka značajno porastao" i da „tehnologija dopušta ... korištenje ličnih podataka u neviđenom opsegu" (GDPR, uvodna izjava 6).

Analizirajući pravna rješenja u zemljama Evropske unije (Francuska, Portugal, Španija, Belgija, Italija), moguće je uočiti da je jedno od specifičnih područja koje se obrađuje – i u određenoj mjeri regulira – upotreba nametljivih digitalnih tgehnologija kao što su GPS praćenje i biometrija (čitači ruku, čitači otiska prsta ili uređaji za prepoznavanje lica). Na primjer, relativno recentno izmijenjeni francuski *Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles* - Zakon o zaštiti podataka (zakon 2018-493 od 20. juna 2018.) regulira neke oblike nadzora zaposlenika, uključujući one koji koriste naprednije digitalne tehnologije. Prema odredbama navedenog zakona, biometrijski uređaji za kontrolu pristupa moraju biti u skladu s takozvanim „modelom uredbe" koju je izradila Francuska uprava za zaštitu podataka. Na primjer, poslodavci moraju opravdati i dokumentirati svoj izbor biometrijskog uređaja i objasniti zašto korištenje drugih, standardnijih mjera (primjerice bedževa i šifri) nije dostatno s obzirom na potrebnu razinu sigurnosti.

Osim toga, portugalski *Lei n.º 58/2019, de 8 de agosto* (Zakon o zaštiti podataka (zakon 58 od 8. augusta 2019.)) ima posebne odredbe o obradi biometrijskih podataka na radnom mjestu i navodi da je obrada biometrijskih podataka zaposlenika dopuštena samo u svrhu praćenja prisutnosti i kontrole pristup prostorijama poslodavca. Nadalje, portugalski *Lei n.º 7/2009, de 12 de fevereiro* (Zakon o radu (zakon 7 od 12. februara 2009.)) propisuje da poslodavac može koristiti mehanizme daljinskog nadzora na radnom mjestu putem tehnološke opreme samo u svrhu zaštite radnika, klijenata i imovine – a ne za praćenje učinka zaposlenika.

Novi regulatorni pristup uveden je u Španiji, s *Organic Law 3/2018, of December 5, Protection of Personal Data and Guarantee of Digital Rights* (Organskim zakonom 3/2018 o zaštiti ličnih podataka i jamčenju digitalnih prava), koji uvodi novi koncept „digitalnih prava", postavljajući ograničenja za korištenje digitalno omogućenog praćenja. Ovim zakonom priznaje se pravo zaposlenika na privatnost pri korištenju digitalnih uređaja koje im osigurava poslodavac te se propisuje da su poslodavci dužni utvrditi kriterije za korištenje digitalnih uređaja za nadzor zaposlenika u skladu sa zakonom. Spomenuta digitalna prava uključuju pravo na prekid veze i prava zaposlenika na odmor, dopust, praznike, ličnu privatnost i privatnost porodice. Zakon prepušta provedbu prava na isključenje i dodatna

jamstva u vezi s obradom ličnih podataka radnika i zaštitu digitalnih prava stranama kolektivnog ugovora na razini sektora ili kompanije.

Kao i u Španiji, pravo na prekid veze također je uključeno u zakonodavstvo u Belgiji, Francuskoj i Italiji, a o njemu trenutačno raspravljaju politički sudionici u nizu drugih zemalja (Eurofound, 2020b). Međutim, valja napomenuti da od decembra 2019. u dostupnom nacionalnom zakonodavstvu nisu pronađene nikakve posebne odredbe o pravu na prekid veze u vezi s upotrebom novih digitalnih tehnologija za praćenje radnika na daljinu.

Tabela 1 prikazuje pregled najrelevantnijih nacionalnih zakona koji se bave praćenjem i nadzorom zaposlenika.

Tabela 1. Relevantno nacionalno zakonodavstvo koje se bavi praćenjem i nadzorom zaposlenika

Zemlja	Relevantni pravni dokumenti	Specifičnosti zemlje	Ograničenja korištenja nadzora zaposlenika
Austrija	Austrijski zakon o radnom ustavu i austrijski Zakon o zaštiti podataka.	Vrlo široka definicija koja pokriva mehaničko upravljanje, upravljanje korištenjem nadzornih tehnologija i upravljanje od strane drugih ljudi. Suodlučivanje i sudjelovanje radničkog vijeća obavezno je ako poslodavac želi uvesti nadzor radnika za koji smatra da zadire u ljudsko dostojanstvo.	Privremeni pregled i pristup sadržaju na računaru (primjerice poslovni e-mailovi) i GPS praćenje predmet su suodlučivanja. Video nadzor u svrhu praćenja performansi zaposlenika je zabranjen.
Belgija	Član 8. Evropske konvencije o ljudskim pravima i član 22. belgijskog ustava potvrđuju pravo na privatnost zaposlenih. Kolektivnim ugovorima regulišu se posebni oblici praćenja (npr. kolektivni ugovor br. 68 od 16. juna 1998. o korištenju kamera za nadzor na radnom mjestu i kolektivni ugovor br. 81 od 26. aprila 2002. o elektronskom praćenju interneta i elektronske pošte).	Primjenjuju se principi zakonitosti, legitimnosti i proporcionalnosti.	Praćenje elektronskih komunikacija dozvoljeno je samo u svrhe navedene u kolektivnom ugovoru br. 81. Nadzor kamerom na radnom mjestu dozvoljen je samo za ciljeve predviđene Kolektivnim ugovorom br. 68. GPS praćenje mora biti opravdano. Zaposleni moraju biti unaprijed obaviješteni o postojanju, svrsi i trajanju monitoringa.
Bugarska;	Bugarski zakon o zaštiti ličnih podataka i bugarski ustav.	Postoje dodatne odredbe općih GDPR pravila koje postavljaju zahtjeve u cilju pojašnjenja	Posebna pravila u pogledu obrade podataka važe za poslodavce koji

	Postoje i posebni zakoni koji regulišu video nadzor u određenim kontekstima.	obima praćenja zaposlenih, obaveza i metoda implementacije.	uspostavljaju sisteme video nadzora na radnom mjestu. Mora postojati pravni osnov za korištenje takvog praćenja. Video nadzor je, međutim, obavezan u određenim kontekstima (na primjer, banke i postrojenja za sagorijevanje). Postoji opšta ustavna zabrana praćenja e-pošte. GPS sistemi za praćenje su prihvaćeni u određenim slučajevima iu legitimne svrhe.
Hrvatska;	Zakon o radu, Zakon o zaštiti na radu, Nacionalni zakon o implementaciji (sprovođenje GDPR) i sektorski zakoni (za obavezni video nadzor).	Naglasak je u zakonodavstvu na video i telefonskom nadzoru. Prilikom uvođenja nove tehnologije na radno mjesto ili promjene načina rada obavezno je učešće radničkog vijeća ili sindikalnog predstavnika. Ako je praćenje kontinuirano, potrebna je saglasnost radničkog vijeća ili predstavnika sindikata. Ako nije kontinuirano, i dalje su potrebne prethodne konsultacije, ali negativno mišljenje nije obavezujuće.	Nije dozvoljeno postavljanje uređaja za nadzor u svlačionicama, toaletima ili drugim određenim prostorima za odmor. Tajni video i telefonski nadzor nije dozvoljen.
Kipar;	Zakon o zaštiti fizičkih lica u pogledu obrade podataka o ličnosti i slobodnog kretanja tih podataka iz 2018. godine (Zakon 125(I)/2018) Povjerenik za zaštitu	Sistemi praćenja zaposlenih moraju biti proporcionalni cilju kojem se teži. Elektronski	Upotreba biometrije u svrhu praćenja općenito je zabranjena. Sistemi časovnika koji koriste otiske prstiju ili druge biometrijske podatke nisu dozvoljeni

	podataka o ličnosti donio je smjernice o korištenju video nadzora i biometrijski sistemi praćenja na radnom mjestu.	sistemi nadzora na radnom mjestu mogu se instalirati samo u legitimne svrhe.	samo u svrhu praćenja prisustva ili radnog vremena zaposlenih. Tajno praćenje je protivzakonito. Zabranjen je pristup sadržaju ličnih e-mailova i ličnih telefonskih poziva zaposlenih.
Češka Republika	Građanski zakonik (Zakon 89/2012), Zakon o radu (Zakon 262/2006), Češki Zakon o zaštiti podataka (Zakon 101/2000).	U češkom Zakonu o zaštiti podataka nisu propisana posebna pravila ili ograničenja u vezi sa pristankom koji zaposleni daje poslodavcu. Zakon ne poznaje posebnu kategoriju ličnih podataka zaposlenih. Opšta pravila o pristanku primjenjuju se na lične podatke zaposlenika. Zaposleni moraju biti propisno informisani o specifičnim metodama praćenja koje koristi poslodavac.	Metode praćenja zaposlenih mogu se smatrati zakonitim samo u slučajevima u kojima poslodavac ima legitimne razloge za njihovu primjenu.
Danska	Krivični zakonik, Zakon o ličnim podacima, Zakon o televizijskom nadzoru (za video nadzor) i kolektivni ugovori.	Praćenje zaposlenih je dozvoljeno sve dok ne vrijeđa ili ne šteti zaposlenima ili ne narušava njihovo ljudsko dostojanstvo i osnovna prava. Zaposleni moraju biti informisani o mjerama praćenja i kontrole prije nego što se primjene na radnom mjestu.	Propisi o zaštiti podataka i kolektivni ugovori navode ograničenja za praćenje zaposlenih. Video nadzor je u određenoj mjeri dozvoljen i generalno se smatra da narušava uslove razumnog i pristojnog postupanja prema zaposlenima.
Estonija	Zakon o ugovorima o radu i Zakon o zaštiti podataka o ličnosti.	Ne postoje detaljne upute u vezi s pravima poslodavca na nadzor, ali smjernice je izdala estonska inspekcija za zaštitu podataka.	Upotreba opreme za nadzor (na primjer, kamera) dozvoljena je samo u svrhu zaštite osoba i imovine, ali njena upotreba

		Zakon o ugovorima o radu prilično općenito precizira da je poslodavac dužan poštivati privatnost zaposlenika i provjeravati izvršavanje njihovih dužnosti na način koji ne krši osnovna prava radnika.	mora biti što je moguće minimalnija i što manje utjecati na zaposlene.
Finska;	Zakon o zaštiti privatnosti u radnom životu, Zakon o saradnji u kompanijama, Zakon o saradnji u vladinim službama i agencijama, Zakon o saradnji unutar opština i Zakon o zaštiti podataka.	Poslodavac je po zakonu dužan da informiše zaposlene o metodama praćenja i da se dogovori o pravilima praćenja u pregovorima o saradnji. Poslodavci mogu obrađivati samo lične podatke koji su direktno neophodni za radni odnos, čime se ograničava obim aktivnosti praćenja, bez obzira na obim informacija datih zaposlenima.	Praćenje elektronske korespondencije zaposlenih je nezakonito osim ako nije motivisano posebnim pravnim razlozima. Za korištenje video nadzora važe strogi uslovi. Nije dozvoljena njegova upotreba u svrhu praćenja određenih zaposlenih na radnom mjestu. Praćenje GPS praćenjem dozvoljeno je samo tokom radnog vremena. Pregovori o saradnji su potrebni i za video nadzor i za GPS praćenje.
Francuska	Francuski građanski zakonik, zakon o radu i francuski zakon o zaštiti podataka.	Potrebno je striktno poštovanje principa transparentnosti ili lojalnosti, proporcionalnosti i relevantnosti.	Posebni zahtjevi se odnose na korištenje video nadzora, GPS praćenja i biometrijskih sistema.
Njemačka	Njemački zakon o zaštiti podataka, Zakon o ustavu o radu i njemački zakon o telekomunikacijama.	Postoje stroge granice za zaštitu privatnosti zaposlenih.	Potpuni nadzor upotrebe interneta i/ili e-pošte dozvoljen je samo u slučaju

		Uvođenje i korištenje nadzora zaposlenih podliježe odobrenju radničkog vijeća.	konkretne sumnje na kriminalnu aktivnost ili ozbiljne zloupotrebe.
Grčka	Zakon 4624/2019, Direktiva br. 115/2001 i grčki ustav (član 9a).	Grčka jurisdikcija ne pravi razliku između vrsta nadzora zaposlenih. Kontrola i nadzor se odnose na upotrebu uređaja za nadzor, posebno kompjutera, kola za nadzor, snimanja zvuka, video snimanja i metoda praćenja komunikacije ili kretanja zaposlenih za kontrolu istih i/ili njihovih radnih mjesta i radnih prostorija. Nadgledanje na radnom mjestu je dozvoljeno pod određenim uslovima.	Pojašnjenja su data u smjernicama koje je izdalo grčko tijelo za zaštitu podataka kako je detaljno opisano u nastavku. Praćenje e-mailova i korištenja interneta dozvoljeno je samo u izuzetnim okolnostima i kada je to neophodno radi odbrane legitimnih interesa poslodavca. Video nadzor se ne smije koristiti za praćenje zaposlenih, osim ako je to opravdano prirodom profesionalne djelatnosti. GPS praćenje se može implementirati radi optimizacije poslovanja i ne smije narušiti privatnost zaposlenika. Upotreba biometrije je dozvoljena samo radi osiguranja sigurnosti na radnom mjestu; ne postoje drugi slučajevi u kojima se biometrija može koristiti.
Mađarska	Mađarski zakon o radu i mađarski zakon o implementaciji GDPR-a.	Pravni osnov za praćenje zaposlenih je, u većini slučajeva, kada poslodavac ima legitiman interes. Poslodavac mora provesti test ravnoteže, odmjeravajući svoje legitimne interese u odnosu na prava i slobode radnika.	Tajno praćenje je nezakonito, korištenje video nadzora mora biti opravdano, praćenje korištenja interneta i e-pošte podliježe ograničenjima, biometrijski sistemi unosa su dozvoljeni samo u izuzetnim slučajevima, a GPS praćenje

			nije dozvoljeno da bi se utvrdilo gdje se zaposleni nalaze izvan radnog vremena.
Irska;	Zakon o zaštiti podataka iz 2018.	Svako praćenje zaposlenika mora biti proporcionalno i neophodno kako bi se zaštitio legitimni interes poslodavca, ali ne dovodeći u pitanje prava i slobode zaposlenika.	Nema podataka.
Italija	Radnički statut (član 4 italijanskog zakona 300/1970) izmijenjen reformom rada 2015. (član 23 zakonske uredbe 151 od 14. septembra 2015.) i Kodeks o privatnosti (zakonodavna uredba 196/2003) izmijenjen zakonodavnom uredbom 1/2010.	Uređaji za daljinsko upravljanje mogu se koristiti samo u legitimne svrhe i posebne razloge, kao što su organizacione i proizvodne potrebe, sigurnost na radu i zaštita imovine kompanija. Njihova upotreba mora biti pokrivena posebnim kolektivnim ugovorima ili administrativnim odobrenjem i moraju biti u skladu sa zakonima o zaštiti podataka.	Bez izuzetka je zabranjeno direktno praćenje radnih aktivnosti koje se sprovode na daljinu pomoću instaliranih uređaja. Sudska praksa i administrativna praksa uveli su posebna ograničenja u zavisnosti od oblika praćenja.
Latvija	Zakon o obradi ličnih podataka, usvojen 21.06.2018.	Primjenjuju se principi legitimnosti i proporcionalnosti između prava radnika i interesa poslodavca. Prilikom postavljanja video nadzora i drugih vidova nadzora potrebno je uzeti u obzir pravo zaposlenika na privatnost.	Video nadzor i audio snimanje treba da budu eksplicitno navedeni. Sistemi video nadzora mogu se koristiti za praćenje rada radnika samo u vrlo specifičnim slučajevima.
Litvanija	Član 27 Zakona o radu br. XII-2603 koji reguliše zaštitu prava zaposlenih na privatni život i lične podatke i zakon XIII-1426 o izmenama i dopunama Zakona I-1374 o pravnoj zaštiti ličnih podataka.	U principu, poslodavci imaju pravo da koriste mjere kontrole za praćenje rada zaposlenih na radnom mjestu, ali samo ako je to pravo jasno utvrđeno i opravdano internim aktima kompanije.	Nema podataka.

		Poslodavac je dužan da upozna zaposlene sa internim propisima o praćenju zaposlenih (uz potpis ili na drugi način dokaza).	
Luksemburg	Zakon o radu (član L 261-1) i zakon od 1. augusta 2018. o organizaciji Nacionalne komisije za zaštitu podataka i opštim pravilima o zaštiti podataka.	Ne postoji zakonska definicija nadzora. Poslodavci mogu preduzeti nadzor u bilo koju svrhu, pod uslovom da ispunjavaju niz uslova utvrđenih zakonom. Poslodavac mora unaprijed obavijestiti dotične radnike i njihove predstavnike. Zaposleni imaju pravo žalbe Nacionalnoj komisiji za zaštitu podataka ako se sumnja u usklađenost i legitimnost obrade.	Nema podataka.
Malta	Zakon o zaštiti podataka zakona Malte (Cap 440) i njegove podzakonske akte, te smjernice koje je izdao Ured povjerenika za informacije i zaštitu podataka.	Ne postoji poseban propis o praćenju i nadzoru zaposlenih na radnom mjestu. Primjenjuju se pravila i principi zaštite podataka utvrđeni postojećim zakonodavstvom. Praćenje je stoga dozvoljeno pod uslovom da je adekvatno, relevantno i ne pretjerano i da se provodi na najmanji mogući način. Štetne posljedice praćenja moraju biti opravdane njegovom dobrom za poslodavca i/ili druge. Iako izričita saglasnost za praćenje obično nije potrebna, poslodavac treba da obavesti zaposlene o sljedećem: (1) da se praćenje sprovodi, (2) svrhe takvog praćenja i kako se njihovi lični podaci mogu koristiti, (3) kome će biti dostavljeni lični	Savjetuje se da, prije implementacije biometrijskih sistema, treba izvršiti procjenu uticaja na privatnost kako bi se osiguralo da je upotreba biometrije neophodna.

		podaci (4) ako određeno ponašanje zaposlenog može dovesti do disciplinskog postupka.	
Nizozemska	GDPR.	Ne postoji određena definicija praćenja i/ili nadzora zaposlenih. Pristanak zaposlenika ne smatra se valjanim osnovom za obradu ličnih podataka. Praćenje zaposlenih nije zabranjeno, ali poslodavci moraju voditi računa o privatnosti zaposlenih. Praćenje zaposlenih je dozvoljeno ako ispunjava uslove GDPR-a. Ovi uslovi se tiču legitimnog interesa poslodavca koji ima prednost nad privatnošću zaposlenih, dokazanu neophodnost praćenja, prethodnu saglasnost zaposlenih i dozvolu radničkog savjeta.	Tajno praćenje zaposlenih je dozvoljeno samo pod određenim uslovima. Video nadzor i nadzor (uključujući korištenje tehnologija za prepoznavanje lica) za utvrđivanje obrazaca ponašanja općenito nisu dozvoljeni. GPS praćenje je dozvoljeno samo da bi se osigurala sigurnost zaposlenika, spriječila krađa ili u slučaju sumnje na kriminalnu aktivnost.
Poljska	Zakon o radu i Građanski zakonik i Zakon o zaštiti ličnih podataka.	Monitoring se odnosi samo na radno mjesto (ne i na praćenje zaposlenih). Odredbe Zakona o radu izričito se odnose na video nadzor i praćenje e-pošte, ali su također primjenjive i na „druge oblike nadzora“. Poslodavac je dužan da kolektivnim ugovorima ili internim aktima definiše obim, način i svrhu praćenja.	Praćenje e-mailova ne može narušiti tajnost prepiske i druga lična prava zaposlenih. Zabranjeno je praćenje privatnih emailova. Video nadzor je dozvoljen u određenim okolnostima i kada je to opravdano.
Portugal	Zakon o radu (zakon 7/2009 od 12. februara) i portugalski Zakon o zaštiti podataka (zakon 58/2019 od 8. augusta).	Primjenjuje se opći princip da zaposleni imaju pravo na privatnost. Sistemi daljinskog nadzora mogu se koristiti samo u svrhu zaštite radnika, klijenata i imovine, a ne za kontrolu profesionalnog rada radnika. Poslodavac je	Nije dozvoljeno praćenje aktivnosti zaposlenih putem elektronske pošte, interneta i/ili biometrijskih uređaja. Poslodavcu je zabranjeno korištenje pristanka svojih zaposlenika za obradu

		dužan da obavesti zaposlene o uslovima i ograničenjima korišćenja opreme kompanije i obrade podataka.	ličnih podataka kada takva obrada za njih rezultira pravnom ili ekonomskom prednosti.
Rumunija	Zakon o radu (zakon 53/2003), zakon 190/2018 o mjerama za implementaciju Uredbe (EU) 2016/679 i Odluka 99/2018 Nacionalnog nadzornog tijela za obradu ličnih podataka.	Zakon 190/2018 propisuje da je nadzor zaposlenih dozvoljen ako je ispunjen skup kumulativnih uslova. Ovi uslovi obuhvataju (1) legitimne interese koje teži poslodavac, koji moraju biti u potpunosti opravdani i prevladati nad interesima ili pravima i slobodama zaposlenih, (2) preliminarne informacije date zaposlenima, (3) konsultacije sa sindikata ili predstavnika zaposlenih prije uvođenja sistema praćenja, (4) iscrpljenost drugih, manje nametljivih, oblika i modaliteta nadzornih sredstava i (5) period skladištenja, koji mora biti proporcionalan svrsi obrade, ali ne duže od 30 dana.	Prema zakonima koji su trenutno na snazi, poslodavac nema pravo da vrši nadzor nad svojim zaposlenima na radnom mjestu. Međutim, ako se djelatnost obavlja na otvorenim prostorima, gdje radi više desetina zaposlenih, u industrijskim halama ili u supermarketima, poslodavac može iz sigurnosnih razloga postaviti nadzorne kamere. Međutim, oni moraju biti na vidljivom mjestu, a zaposleni moraju znati za njihovo postojanje.
Slovačka	Zakon o radu (Zakon 311/2011), Zakon o zaštiti podataka o ličnosti (Zakon 18/2018) i izmjene i dopune određenih zakona.	Ako poslodavac implementira mehanizam praćenja, poslodavac se mora konsultovati sa predstavnicima zaposlenih o obimu kontrole, načinu sprovođenja i trajanju. Ako kod poslodavca nema predstavnika zaposlenih, poslodavac postupa samostalno u skladu sa zakonskim propisima.	Poslodavac ne smije, osim iz posebnih razloga koji se odnose na specifičan karakter djelatnosti poslodavca, zadirati u privatnost zaposlenog na radnom mjestu tako što će ga pratiti, voditi evidenciju telefonskih poziva i provjeravati e-mail prepisku bez prethodnog najave.

Slovenija	Zakon o radnim odnosima, Zakon o zaštiti podataka o ličnosti, Zakon o povjereniku za informacije i Zakon o elektronskim komunikacijama.	Poslodavac mora da štiti i poštuje privatnost zaposlenih. Praćenje zaposlenih je dozvoljeno, ali poslodavac mora unapred i pismeno obavestiti zaposlene o vršenju i načinu nadzora. Potreban je pristanak zaposlenih osim ako se praćenje može opravdati objektivnim razlozima.	Video nadzor „radnih prostora" dozvoljen je samo u iznimnim slučajevima i za legitiman cilj, na primjer, zaštita ljudi ili imovine, zaštita poslovne tajne poslodavca ili kada se to ne može postići drugim sredstvima. Snimanje i slušanje telefonskih razgovora nije izričito regulisano, ali generalno nije dozvoljeno. Poslodavcu je dozvoljeno da obrađuje samo lične podatke koji su neposredno neophodni za vođenje radnog odnosa zaposlenog.
Španija	Španski zakon o digitalnim pravima (organski zakon 3/2018 o zaštiti ličnih podataka i garantovanju digitalnih prava).	Novi koncept „digitalnih prava" uveden je u špansku jurisprudenciju.	Nema podataka.
Švedska	Zakon o nadzoru kamera, Zakon o zapošljavanju (suodlučivanje na radnom mjestu) (1976:580) i Zakon o zaštiti podataka (2018:218).	Ne postoji poseban propis o praćenju i nadzoru zaposlenih na radnom mjestu.	Nadzor zaposlenih uz pomoć CCTV-a dozvoljen je samo kada za to postoje uvjerljivi razlozi (na primjer, razlozi za sumnju da zaposleni čine krivična djela). Poslodavac koji želi da postavi sistem za nadzor kamerom na radnom mjestu dužan

			je da pregovara sa predstavnicima zaposlenih. Ovo je regulisano članovima 11-14 Zakona o zapošljavanju.
Norveška	Zakon o radnom okruženju koji se odnosi na radno okruženje, radno vrijeme, zaštitu pri zapošljavanju (poglavlje 9) i Zakon o ličnim podacima (nacionalna implementacija GDPR-a). Postoji „osnovni sporazum“ između socijalnih partnera Norveške konfederacije sindikata (LO) i Konfederacije norveških kompanija (NHO), uključujući dodatne sporazume o mjerama kontrole u kompanijama.	Iako je praćenje radnog mjesta regulirano Zakonom o radnoj sredini, sam pojam nije zakonski definiran. Zakonodavni izvori, uključujući nacrte rezolucija predstavljenih parlamentu, ipak pominju specifične tehnologije, uključujući vremenske tablice, kontrolu pristupa, praćenje učinka, kontrolu kvaliteta, testiranje na droge, medicinske testove, provjere torbi ili ormarića, nadzor kamera, elektronske senzore i praćenje e-pošte.	Praćenje zaposlenih je ograničeno pravom zaposlenih na privatnost. Poslodavac mora pokazati legitimnu i stalnu potrebu imjera mora biti proporcionalna. Zaposleni moraju biti obaviješteni, a mjera mora biti razmotrena s upraviteljima trgovine.
Velika Britanija	Zakon o ljudskim pravima iz 1998., Zakon o zaštiti podataka iz 1998., Kodeks o zaštiti podataka o praksama zapošljavanja, Zakon o istražnim ovlastima iz 2000. i Propisi o telekomunikacijama iz 2000.	Kako većina oblika nadzora zaposlenih uključuje obradu ličnih podataka, takve aktivnosti praćenja moraju biti u skladu sa principima i pravilima zaštite podataka.	Prema Kodeksu o zaštiti podataka o praksi zapošljavanja, tajni nadzor je u principu zabranjen i dozvoljen samo u slučaju konkretne sumnje na kriminalnu aktivnost ili ozbiljne zloupotrebe.

Izvor: Autor završnog rada prilagođeno prema Eurofound (2020)

Prema navedenoj tabeli možemo vidjeti da zemlje u EU, kao i Norveškoj i Velikoj Britaniji su prilično dosljedne u svojim pristupima reguliranju praćenja i nadzora zaposlenih. Većina zemalja ima zakone koji balansiraju interese poslodavaca za održavanjem reda, sigurnosti i produktivnosti s pravima zaposlenih na privatnost i dostojanstvo na radnom mjestu.

Vidljivo je da postoji varijabilnost u pravnim okvirima koji regulišu praćenje i nadzor zaposlenih širom svijeta. Poslodavci su obavezni informisati zaposlene o metodama praćenja i nadzora koje koriste i svrsi tog nadzora. Praćenje mora biti opravdano i proporcionalno ciljevima poslodavca. To znači da se praćenje može koristiti samo u svrhu zaštite interesa poslodavca, kao što su sigurnost na radu ili zaštita imovine, ali ne i za neograničeno praćenje ili kontrolu zaposlenih.

U mnogim slučajevima, zakonska rješenja uključuju odredbe prema kojima se zahtijeva saglasnost zaposlenih ili bar konsultacije s njima ili njihovim predstavnicima (kao što su sindikati) prije uvođenja sistema praćenja. Navedena i analizirana zakonska rješenja, često definišu specifične aktivnosti koje su zabranjene, poput tajnog praćenja, ili postavljaju ograničenja na određene tehnologije, poput GPS praćenja izvan radnog vremena. Iako postoji određena varijacija u pristupima među zemljama, općenito se može reći da su zakoni usmjereni na zaštitu prava i privatnosti zaposlenih, dok istovremeno pružaju okvir za poslodavce da održe red i sigurnost na radnom mjestu.

3.3. Analiza ključnih presuda Evropskog suda

Standarde u vezi sa zaštitom privatnosti, uključujući iu kontekstu radnog odnosa, uspostavila su međunarodna tijela za zaštitu ljudskih prava, ponajprije Evropski sud za ljudska prava (ESLJP). Jedan od najistaknutijih slučajeva u vezi s praćenjem zaposlenika bio je Copland protiv Ujedinjenog Kraljevstva (Copland v. the United Kingdom, zahtjev br. 62617/00, presuda 3.4.2007.[4]). Radi razumijevanja cjeline ovog rada, bit će dat sažet prikaz pet slučajeva: *Copland v. the United Kingdom, zahtjev br. 62617/00, presuda 3.4.2007; Bărbulescu v. Romania, zahtjev br. 61496/08, presuda 5.9.2017; Antović and Mirković v. Montenegro, zahtjev br. 70838/13, presuda 28.11.201; López Ribalda and Others v. Spain, zahtjev br. 1874/13 i 8567/13, presuda, 17.10.2019; Florindo De Almeida Vasconcelos Gramaxo v Portugal, zahtjev br. 26968/16*

a) Copland v. the United Kingdom, zahtjev br. 62617/00, presuda 3.4.2007

U ovom slučaju, Coplandine telefonske pozive, e-mail prepisku i korištenje interneta pratio je njezin poslodavac pod sumnjom da je koristila objekte poslodavca u lične svrhe. U ovom slučaju, telefon, e-pošta i internet korištenje lične asistentice direktora zaposlene na fakultetu bili su pod nadzorom na zahtjev zamjenika direktora, koji je želio provjeriti koristi li

[4]Više informacija dostupno na: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22002-2765%22]}

asistentica sredstva fakulteta za lične svrhe. Nadzor telefona uključivao je pregled telefonskih računa koji su prikazivali brojeve, datume i vrijeme poziva, kao i njihovo trajanje i cijenu. Nadzor upotrebe interneta odnosio se na analizu posjećenih web stranica, vrijeme, datum i trajanje posjeta, dok je nadzor e-pošte uključivao pregled e-mail adresa, datuma i vremena slanja poruka (ESLJP, 2007).

U to vrijeme, na fakultetu nije postojala politika nadgledanja, a englesko pravo nije priznavalo opšte pravo na privatnost, iako su kasnije uređene regulative o presretanju komunikacija i uslovi pod kojima poslodavci mogu nadzirati komunikacije bez pristanka zaposlenika (Pivčević i Erceg Ćurić, 2022). Asistentica nije bila obaviještena o nadzoru, ali je opravdano očekivala privatnost svojih poziva, e-pošte i internet aktivnosti. Postavljeno je pitanje o negativnoj obavezi države da ne intervenira u privatni život i komunikacije podnositelja zahtjeva.

Činjenica da fakultet nije koristio prikupljene podatke protiv asistentice u disciplinskim ili drugim postupcima, niti ih je objavio trećim stranama, nije bila od značaja, jer je samo prikupljanje i čuvanje ličnih podataka bez njenog znanja predstavljalo kršenje prava na privatnost i komunikaciju prema presudi Suda (Pivčević i Erceg Ćurić, 2022).

Ovom je prilikom ESLJP utvrdio da je poslodavac prekršio pravo zaposlenika na privatni život i privatno dopisivanje prema članu 8. Evropske konvencije o ljudskim pravima. Ove presude ESLJP-a pokazuju da se zaštita koju pruža član 8. proteže i na radno mjesto te da bi zaposlenik trebao dobiti odgovarajuće i prethodne informacije o opsegu i prirodi nadzora. Istodobno, poslodavac treba opravdati mjere koje provodi i minimalizirati nadzor gdje je to moguće, na primjer, korištenjem najmanje nametljivih metoda. Važan aspekt u tom smislu je ravnoteža između legitimnog interesa poslodavca i prava na privatnost zaposlenika. To se odnosi na sve oblike praćenja i nadzora, a ne samo na praćenje lične komunikacije na radnom mjestu (Eurofond, 2020).

b) Bărbulescu v. Romania, zahtjev br. 61496/08, presuda 5.9.2017

Često citirani slučaj Bărbulescu protiv Rumunije ima važne implikacije na sudsku praksu praćenja i nadzora zaposlenika (Bărbulescu v. Romania, zahtjev br. 61496/08, presuda 5.9.2017.[5]). Slučaj se odnosio na otpuštanje zaposlenika zbog korištenja računa poslovne e-pošte u lične svrhe tokom radnog vremena, čime se krše interni propisi kompanije u kojoj su radili (ESLJP, 2017).

Podnositelj zahtjeva tvrdio je da je razlog njegovog otkaza u privatnoj kompaniji gdje je radio bio nepravedan i baziran na povredi njegove privatnosti. On je otpušten nakon što je, tokom perioda nadzora, otkriveno da je koristio službeni Yahoo Messenger za privatne

[5] Više informacija dostupno na: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-183019%22]}

razgovore s bratom i zaručnicom o ličnim temama, iako je kompanija imala pravila koja su zabranjivala privatnu upotrebu kompanijih resursa (Pivčević i Erceg Ćurić, 2022).

Sud je priznao primjenjivost člana 8. Konvencije jer je poslodavac pristupio njegovom poslovnom računu i koristio zapis o njegovoj komunikaciji u sudskom postupku. Sud je smatrao da je cilj poslodavca bio provjeriti ispunjavaju li zaposlenici svoje radne obaveze, te da je pristup računu bio u uvjerenju da se radi o poslovnoj komunikaciji. Domaći sudovi nisu razmatrali sadržaj dopisivanja ni identitet sudionika razgovora, već su se fokusirali na dokazivanje neprimjerene upotrebe kompanijih resursa za privatne svrhe tokom radnog vremena. Zato je sud prvobitno zaključio da je postignuta pravična ravnoteža između privatnih prava podnositelja i interesa poslodavaca, odbacujući povredu člana 8. Konvencije (ESLJP, 2017).

Međutim, Veliko vijeće je u junu 2016., s većinom glasova 11 prema 6, odlučilo da je ipak došlo do povrede prava podnositelja na privatnost i dopisivanje. Naglasili su da, bez obzira na očekivanja pojedinca o privatnosti, komunikacija na radnom mjestu spada pod zaštitu privatnog života i dopisivanja. Ključno pitanje bilo je je li država izvršila svoju pozitivnu obavezu zaštite prava na radnom mjestu, osiguravajući da poslodavac implementira mjere nadzora nad dopisivanjem s adekvatnim zaštitnim mjerama protiv zloupotrebe, uključujući razmjernost i proceduralna jamstva. Sud je zaključio da domaće vlasti nisu osigurale potrebnu zaštitu privatnosti i komunikacije podnositelja, zbog čega nije postignuta odgovarajuća ravnoteža između uključenih interesa, što je rezultiralo kršenjem člana 8. Konvencije (Pivčević i Erceg Ćurić, 2022).

Presudom ESLJP-a iz 2016. godine preinačene su prethodne presude i odbijen otkaz jer se smatralo da otkaz predstavlja povredu prava na privatni život i privatno dopisivanje iz člana 8. Evropske konvencije o ljudskim pravima. Član 8. općenito se koristi u svim nacionalnim jurisdikcijama za zaštitu privatnosti zaposlenika u kontekstu zapošljavanja. Presuda ESLJP-a u vezi s Bărbulescu protiv Rumunije izazvala je brojne reakcije u medijima, ali je općenito pozdravljena zbog uspostavljanja nivoa zaštite zaposlenika i postavljanja granica u kontekstu digitalizacije rada, jer ta digitalizacija općenito dovodi do sve većeg brisanja granica između posla i obiteljskog života (Eurofound, 2020).

c) Antović and Mirković v. Montenegro, zahtjev br. 70838/13, presuda 28.11.2017

Još jedan slučaj iznesen ESLJP-u bio je slučaj Antović i Mirković protiv Crne Gore (Antović and Mirković v. Montenegro, zahtjev br. 70838/13, presuda 28.11.2017.[6]). Podnositelji zahtjeva, dvojica profesora na fakultetu u Crnoj Gori, pozvali su se na član 8. Konvencije, ističući da je instalacijom videonadzora u univerzitetskim predavaonicama i ispred dekanata narušeno njihovo pravo na privatnost (ESLJP, 2018).

[6] Više informacija dostupno na: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22002-11757%22]}

Videonadzor je uveden radi zaštite osoba i imovine te praćenja izvođenja nastave, što je potaknulo profesore da se obrate Agenciji za zaštitu ličnih podataka. Agencija je utvrdila da takav videonadzor nije usklađen sa Zakonom o zaštiti ličnih podataka jer ne postoji dokazana potreba za njegovim postavljanjem niti je nadzor nastavnih aktivnosti prihvatljiv razlog. Zato je naređeno uklanjanje kamera i uništavanje prikupljenih podataka (Pivčević i Erceg Ćurić, 2022).

Podnositelji su također tražili naknadu štete za povredu privatnosti, ali je zahtjev odbijen s obzirom na to da univerzitet, kao javna ustanova, provodi aktivnosti od javnog značaja. Predavaonice su mjesta gdje profesori integriraju sa studentima, što oblikuje njihov socijalni identitet, te je prema tome Sud zaključio da su podaci dobiveni videonadzorom povezani s njihovim privatnim životom, čime je član 8. Konvencije postao primjenjiv. Sud je zaključio da videonadzor na radnom mjestu predstavlja ozbiljan zahvat u privatnost, opravdan samo iznimnim razlozima kao što su nacionalna sigurnost ili javna sigurnost. U ovom slučaju, postavljanje videonadzora nije bilo zakonski opravdano, stoga je predstavljalo povredu člana 8. Konvencije(ESLJP, 2018).

d) López Ribalda and Others v. Spain, zahtjev br. 1874/13 i 8567/13, presuda, 17.10.2019

Što se tiče videonadzora, još jedna presuda ESLJP-a odnosi se na López Ribalda i drugi protiv Španije (ESLJP, 2019), kojim je utvrđeno da tajni videonadzor zaposlenika može biti opravdan kada postoji opravdana sumnja na tešku povredu ponašanja (López Ribalda and Others v. Spain, zahtjev br. 1874/13 i 8567/13, presuda, 17.10.2019.[7]). Poslodavac je instalirao nadzorne kamere u supermarketu, gdje su radili podnositelji zahtjeva (blagajnici i prodajni pomoćnici), kako bi istražio gubitke unutar tvrtke. Iako su podnositelji bili upoznati s postojanjem vidljivih kamera, nisu bili obaviješteni o skrivenima. Nakon što su snimke otkrile krađu imovine, podnositeljima je raskinut ugovor o radu. Sudsko vijeće je ocijenilo da je dugotrajni videonadzor prekršio član 8. Konvencije jer nije ispunio zakonske uslove te domaći sudovi nisu uspjeli postići pravednu ravnotežu između privatnosti podnositelja i zaštite imovinskih prava poslodavca (Pivčević i Erceg Ćurić, 2022).

Međutim, Veliko vijeće ESLJP smatra da su, s obzirom na značajne zaštitne mjere koje pruža španski zakon i opravdanje za videonadzor koje su razmatrali domaći sudovi, nacionalne vlasti ispunile svoje obveze, te stoga nisu prekršili član 8. Sud je također naveo da supermarket kao javno mjesto i priroda snimljenih aktivnosti koje nisu intimne ili privatne sugeriraju da očekivanja podnositelja o privatnosti trebaju biti ograničena. Podnositelji su bili informirani o prisutnosti vidljivih kamera, a sud je zaključio da uplitanje u njihovu privatnost nije dostiglo visoku razinu ozbiljnosti, iako su posljedice nadzora bile znatne. Nadalje, snimke su korištene isključivo za identifikaciju odgovornih za gubitke i za poduzimanje disciplinskih mjera, a domaći sudovi su potvrdili da je videonadzor bio

[7] Više informacija dostupno na: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-197098%22]}

opravdan legitimnim ciljevima i da su mjere bile adekvatne i proporcionalne (Eurofound, 2020).

e) Florindo De Almeida Vasconcelos Gramaxo v Portugal, zahtjev br. 26968/16

U recentnom slučaju iz 2022, ESLJP donio je odluku u korist kompanije (Florindo De Almeida Vasconcelos Gramaxo v Portugal, zahtjev br. 26968/16[8]), a odnosi se otkaz na temelju podataka o kilometraži službenog vozila podnositelja zahtjeva, prikupljenih GPS uređajem koji je instalirao poslodavac podnositelja zahtjeva uz njegovo puno znanje. Godine 1994. podnositelj zahtjeva, Florindo de Almeida Vasconcelos Gramaxo, se zaposlio kao medicinski predstavnik u farmaceutskoj kompaniji. Kompanija je 2002. godine uvela proceduru za upravljanje zahtjevima za naknadu troškova službenih putovanja zaposlenika. Svi medicinski predstavnici morali su koristiti kompjutersku aplikaciju poznatu kao upravljanje odnosima sa kupcima (Customer Relationship Management, u nastavku CRM) kako bi bilježili svoje dnevne, sedmične i mjesečne aktivnosti, obavljene posjete, izostanke, troškove i raspored nadolazećih posjeta. Kompanija je 2011. ugradila GPS u službena vozila svojih medicinskih predstavnika, uključujući i vozilo podnositelja zahtjeva. Zaposlenici na koje se to odnosi obaviješteni su o instalaciji i razlozima mjere, koja je uglavnom bila osmišljena za praćenje udaljenosti koju zaposlenici prijeđu tokom svojih aktivnosti, te o posljedicama u slučaju odstupanja između GPS podataka i podataka unijeti u CRM.

Ubrzo nakon toga, podnositelj je podnio pritužbu Nacionalnoj komisiji za zaštitu podataka koja se odnosi na uvođenje geolokacijskog sistema i obradu tako prikupljenih ličnih podataka. Nacionalna komisija za zaštitu podataka je 2013. godine utvrdila da pravila o zaštiti podataka nisu prekršena te je odlučio obustaviti postupak (ESLJP, 2022).

U 2014. podnositelj zahtjeva je otpušten. Na temelju unakrsnog povezivanja podataka prikupljenih GPS-om ugrađenim u njegovo vozilo i podataka koje je zabilježio u CRM-u, utvrđeno je da je povećao pređene udaljenosti u profesionalnom svojstvu, kako bi smanjio prividni udio putovanih privatnih putovanja vikendom i državnim praznicima i tako izbjegao nadoknadu odgovarajućih iznosa. Nadalje, prema podacima GPS-a koji se odnose na vrijeme kada je vozilo krenulo i kada se zaustavilo na kraju dana, podnositelj zahtjeva nije radio potrebnih osam sati dnevno.

Podnositelj zahtjeva osporio je svoj otkaz pred Odjelom za zapošljavanje Okružnog suda, koji je utvrdio da je otkaz bio opravdan. Žalbeni sud potvrdio je tu presudu, ali je izmijenio razloge, zabranjujući korištenje GPS-a za praćenje radnog vremena, dok je dopuštao njegovu upotrebu za praćenje prijeđenih udaljenosti za upravljanje troškovima kompanije.

[8] Više informacija dostupno na: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22002-13935%22]}

Na kraju je Evropski sud presudio da nije bilo kršenja člana 8. Konvencije (4 naprema 3), zaključivši da su portugalski sudovi zaštitili podnositeljevu privatnost na odgovarajući način unutar granica nadzora poslodavca u legitimne poslovne svrhe (ESLJP, 2022).

3.4. Pravni okvir nadzora zaposlenika u Bosni i Hercegovini

Pitanje nadzora zaposlenika u Bosni i Hercegovini nije značajnije istraženo kroz literaturu, dok sam pravni okvir za nadzor zaposlenika u Bosni i Hercegovininije regulisan sveobuhvatno kao u Evropskoj Uniji. Nadzor zaposlenika je jednim dijelom regulisan kroz regulativu na nivou Bosne i Hercegovine, i to prije svega Zakon o zaštiti ličnih podataka ("Sl. glasnik BiH", br. 49/2006, 76/2011 i 89/2011 - ispr.) i odnosi se na video nadzor. Zakonom o radu u entitetu Federacija Bosne i Hercegovine, član 30 određeno je: "Lični podaci radnika ne mogu se prikupljati, obrađivati, koristiti ili dostavljati trećim licima, osim ako je to određeno zakonom ili ako je to potrebno radi ostvarivanja prava i obaveza iz radnog odnosa". Zakonom o radu definisane su i kaznene odredbe za kršenje Člana 30 (Sl. novine FBiH).

Prema Zakonu o zaštiti ličnih podataka snimanje radnika na radnom mjestu je dozvoljeno ali samo uz poštivanje određenih uslova koje nalaže Zakon. Preciznije, prema odredbama člana 21a (Obrada ličnih podataka putem videonadzora) stav 2 navedeno je: "*da kontrolor koji vrši videonadzor dužan je da donese odluku koja će sadržavati pravila obrade s ciljem poštovanja prava na zaštitu privatnosti i ličnog života nosioca podataka, ako videonadzor nije propisan zakonom.*" Dalje, u stavu 3 navedenog člana se ističe:"*da kontrolor koji vrši videonadzor dužan je da na vidnom mjestu istakne obavještenje o vršenju videonadzora i kontakt putem kojeg se mogu dobiti pojedinosti o videonadzoru."*

Prema ovome, poslodavac je dužan sačiniti pravila ali i obavijest da se u prostorijama kompanije (poslovnog prostora) vrši snimanje, odnosno instaliran videonadzor.Ukoliko to ipak ne izvrši, poslodavac podliježe mogućoj kazni od 10.000 KM do 100.000 KM, što je propisano Zakonom u članu 49 i član 21a (Sl. novine FBiH).

Prema članu 6. navedenog zakona, poslodavac u Bosni i Hercegovini nije dužan obavijestiti radnika o snimanju, ukoliko je ispunjen jedan od sljedećih uslova:

a) ako vrši obradu ličnih podataka u skladu sa zakonom ili je obrada neophodna da bi se ispunile nadležnosti utvrđene zakonom;
b) ako je neophodno da nosilac podataka na sopstveni zahtjev pristupi pregovorima u ugovornom odnosu ili da se ispune obaveze koje su dogovorene sa kontrolorom;
c) ako je neophodno da se zaštite vitalni interesi nosioca podataka, ili se mora prekinuti obrada podataka, a prikupljeni podaci moraju se uništiti;
d) ako je obrada ličnih podataka potrebna da bi se ispunio zadatak koji se izvršava u javnom interesu;

e) ako je neophodna zaštita zakonitih prava i interesa koje ostvaruje kontrolor ili treća strana, i ako ova obrada ličnih podataka nije u suprotnosti sa pravom nosioca podataka da zaštiti sopstveni privatni ili lični život;
f) ako je neophodno da izvršavanje legitimnih aktivnosti političkih partija, pokreta, udruženja građana, sindikalnih organizacija i vjerskih zajednica, osim gdje preovladavaju interesi za osnovna prava i slobode nosioca podataka nad aktivnostima, posebno pravo na privatnost u odnosu na obradu ličnih podataka (Sl. novine FBiH).

No, prema istom zakonu, kontrolor (poslodavac) mora dobiti pisanu saglasnost od zaposlenika. Prema odredbama člana 5. navedenog Zakona kontrolor može da obrađuje lične podatke uz saglasnost nosioca podataka. Saglasnost za obradu posebne kategorije ličnih podataka mora da bude data u pisanoj formi, mora da je potpiše nosilac podataka, mora da ima tačnu naznaku podataka u vezi sa kojima se saglasnost daje, te mora da sadrži ime kontrolora, svrhu i vremenski period na koji se saglasnost daje. Saglasnost može da bude povučena u bilo kojem trenutku, osim ako se nosilac podataka i kontrolor izričito ne dogovore drugačije. Nadalje, kontrolor će morati da na zahtjev nadležnog organa, u svako vrijeme, dokaže da postoji saglasnost za period obrade ličnih podataka. U konačnici, kontrolor je dužan da čuva saglasnost za vrijeme obrade ličnih podataka za čiju obradu je data saglasnost (Sl. novine FBiH).

4. ETIČKI IZAZOVI NADZORA

Kako to ističe priznati teoretičar Caroll A.B., na početku 2000 godine "Dok prelazimo u 21. stoljeće, korisno je razmišljati o nekim od najvažnijih izazova s kojima će se poslovne i druge organizacije suočiti na početku novog milenija. Što će predstavljati "uobičajeno poslovanje" u areni poslovne etike na početku i ulasku u novo stoljeće? Moje općenito mišljenje je da ćemo pulsirati u budućnost našom sadašnjom putanjom i da novo stoljeće neće izazvati kataklizmične promjene, barem ne odmah. Umjesto toga, s problemima i izazovima s kojima se sada suočavamo suočit ćemo se i tada. Nedvojbeno će se pojaviti nova pitanja, ali ona će vjerojatnije biti produžeci sadašnjosti nego prekidi s prošlošću."

Uz navedeno, za ovaj istraživački rad su zanimljivi stavovi autora Brenkert, G.G, koji su svome radu iz 2019. godine *Mind the Gap! The Challenges and Limits of (Global) Business Ethics* navodi: "iako ovaj rad priznaje napredak postignut u poslovnoj etici u posljednjih nekoliko desetljeća, usredotočuje se na izazove i ograničenja globalne poslovne etike. Drži da su poslovni etičari dali važan doprinos u pogledu evaluacijskih, utjelovljujućih i provedbenih aspekata poslovne etike. Unatoč tome, nisu dovoljno razmotrili četvrti dio teorije moralne promjene, teoriju donošenja, prema kojoj se načela i vrijednosti koje su poslovni etičari identificirali zapravo mogu slijediti. Teorija donošenja tvrdi da pozivanje na etičko vodstvo, moralnu imaginaciju i komunikacijsko sudjelovanje nije bilo dovoljno za zadatak zatvaranja jaza između onoga što kompanije rade i onoga što bi trebale raditi. Kako bi se riješio ovaj problem, potrebno je razviti teoriju moralne promjene koja se usredotočuje

na odnose moći unutar kojih djeluju pojedinci i kompanije." Dalje on ističe: "Oslanjajući se na rad Johna Gavente, rad skicira neke smjerove u kojima bi se poslovna etika trebala nastaviti kako bi se smanjio ovaj jaz. Rezultat je da poslovna etika treba veću povezanost s ekonomskim, društvenim i političkim teorijama. Također sugerira da postoje važna ograničenja za poticanje etike globalnog poslovanja."

Uz navedeno "Odnos etike i prava bitni su za proučavanje poslovne etike. Iz navedene tvrdnje jasno slijedi da je poslovna etika zapravo primjenjena etika. Sve što je obuhvaćeno pojmom poslovanje moguće je preispitivati sa stanovišta etike u najširem smislu i njene primjenjivosti. Zato etiku, filozofsku disciplinu, koja se bavi pitanjima razlikovanja laži i istine, te dobra i zla, nije moguće odvojiti od svega što čini cjelinu poslovanja. Neki oblici poslovanja mogu biti u skladu sa zakonom, ali da u isto vrijeme budu neetični. I obrnuto. Moguće je ukazati na brojne takve slučajeve u praksi. Iako su sudovi o njima odlučili na jedan način, u javnosti su ih pratili skandali[9] i opća osuda kao neetične. Ima i slučajeva u kojima su poslovne aktivnosti u isto vrijeme nezakonite i neetične. Zato je važno istaknuti da nema poslovanja koje je moguće odvojiti od etike, niti etike koja se ne tiče i poslovanja i poslovnog prava u ukupnosti te naučne discipline." (Trifković *et al.* 2021)

"Danas je nesporno da oni koji upravljaju kompanijama imaju dužnost posebne pažnje, pažnje dobrog stručnjaka (*bonus artifex*). Odgovornost uprave treba biti uređena zakonskim aktima, normativnim aktima društva, etičkim kodeksima i menadžerskim ugovorom. Vođenje poslova društva predstavlja ne samo pravo uprave već i njenu odgovornost (Trivun, 2019.) Članovi upravnih i nadzornih odbora društva imaju obavezu da se prilikom donošenja odluka rukovode interesima društva ali i interesima svih ostalih učesnika u poslovanju." (Trifković *et al.* 2021)

4.1. Etičke dileme vezane uz savremene tehnike nadzora

Supervizija je aktivnost ispunjena etičkim dilemama vezanim uz moć koju ima supervizor, moć koju treba pažljivo izvršavati. Poslodavci mogu stvoriti složene probleme kada nadziru zaposlenike. Trebaju li poslodavci moći nadzirati svoje zaposlenike? Ako je tako, na što bi se trebali ograničiti nadzor i imaju li zaposlenici pravo znati da ih poslodavci nadziru. Svako od ovih pitanja stvara višestruki odgovor kako sa strane poslodavca, tako i sa stajališta zaposlenika. Kao što Sutter, McPherson i Geeseman primjećuju, povećana upotreba interneta među zaposlenicima stvorila je mogućnosti za nekoliko kompanija da proizvedu sofisticirani softver za praćenje, koji poslodavcima omogućuje da zavire u doslovno sve što

[9]Primjeri nedavnh etičkih i poslovnih skandala su: Volkswagen emissions scandal (2015); FIFA corruption scandal (2015); Mossack Fonseca and the Panama Papers (2016); Wells Fargo account fraud (2016); Facebook-Cambridge Analytica data scandal (2018); Boeing 737 MAX back-to-back plane crashes (2018-2019); Johnson & Johnson baby powder recall (2019); i tako dalje.

zaposlenici rade na internetu. Prema autorima, kompanija je stvorila praćenje zaposlenika jer je postojala značajna potreba da kompanije nadziru svoju radnu snagu.

Supervizor ima mnoge etičke odgovornosti kako bi osigurao učinkovit nadzor. Jedan od primarnih ciljeva supervizije je modelirati supervizanta kako provoditi etičke prakse. Etička pitanja u superviziji uključuju razmatranje prava i odgovornosti supervizora, supervizanta i klijenata. Naglašava se da supervizor ima dvije temeljne etičke odgovornosti, bez obzira na razvojnu razinu supervizanta, da podrži profesionalni razvoj supervizanta i zaštiti dobrobit klijenta kojemu služi (Bernard i Goodyear, 1998; Falender i Shafrenske, 2004). Kako bi ispunili te odgovornosti, preporučuje se da supervizori poznaju etička pravila (Aasheim, 2012) i da su odgovorni za pomoć svojim nadređenima u rješavanju etičkih dilema (Lee i Cashwell, 2002). Također, kritična je samoprocjena nadređenog o tome postupa li on ili ona etično.

Etička pitanja u procesu supervizije uključuju kompetentnost supervizora, informirani pristanak, povjerljivost i privatnost, supervizijski odnos, višestruke odnose, uzimanje u obzir dobrobiti klijenta, procjenu, multikulturalnu superviziju i korištenje tehnologije u superviziji (Bernard i Goodyear, 1998; Glosoff, Renfro-Michel i Nagarajan, 2016). O ovim problemima izvještava relevantno i američka udruga za savjetovanje (American Counseling Association) iz 2014 (ACA, 2014.) je ključni dokument koji postavlja etičke obaveze članova Američke udruge za savjetovanje (ACA) i pruža smjernice za etičku praksu profesionalnih savjetnika. Kodeks etike je relevantan jer pruža temelj za razumijevanje etičkih odgovornosti profesionalnih savjetnika, kao i za obradu upita i pritužbi vezanih za etiku među članovima Američke udruge za savjetovanje.

Lee i Cashwell (2002) navode da su empirijska istraživanja etičkih praksi u superviziji savjetovanja toliko ograničena. Erickson Cornish (2014) istaknuo je potrebu za istraživačkom etikom u stručnom usavršavanju i nadzoru. Nekoliko nacionalnih studija o superviziji bavilo se etičkim pitanjima (Aladağ i Kemer, 2016; Koçyiğit Özyiğit, 2019). U studiji (Koçyiğit Özyiğit, 2019) utvrđeno je da su upućivanje klijenta, klijentov zahtjev za susretom sa supervizorom i uzimanje zapisnika sa savjetovanja etički problemi koji su se pojavili u procesu supervizije. U drugoj studiji (Atik, 2017) vidljivo je da su se u superviziji pojavili problemi povjerljivosti, privatnosti i višedimenzionalnih odnosa.

Međutim, istraživanje se nije usredotočilo na etička pitanja s kojima se susreću nadzornici i na to kako se s njima nose. S druge strane, profesionalno rješavanje etičkih pitanja ključna je komponenta učinkovitog nadzora.

Grant, Schofield i Crawford (2012) pronašli su četiri glavne poteškoće za supervizore: etička pitanja, atribute supervizora, protutransfer supervizora i pitanja supervizorskih odnosa. Također, proces evaluacije koji razlikuje superviziju od savjetovanja može biti izvor poteškoća za supervizora (Pearson, 2000). Stoga Borders, Cashwell i Rotter (1995) tvrde da se nadređeni moraju baviti pitanjima evaluacije zbog uključivanja anksioznosti, dinamike moći i sukoba s drugim ulogama nadređenih. Osim toga, karakteristike supervizanata kao

što su niska emocionalna svijest, problemi s autonomijom, lični problemi, profesionalni identitet, poštovanje različitosti klijenata i niska motivacija (Ellis, 2006), otpor supervizanta, obrambeni stav i negativni transferi također mogu predstavljati poteškoće (Nelson *et. al.*, 2008). Sve te poteškoće mogu negativno uticati na supervizorski odnos (Ladany, 2004) i učinkovitost supervizije. Upravljanje poteškoćama u superviziji je složen proces koji zahtijeva promišljeno, usklađeno relacijsko stajalište koje uzima u obzir potrebe nadziranog, razvojnu fazu i lične karakteristike (Grant, Schofield i Crawford, 2012).

4.2. Rasprave (dileme) vezane za praćenje zaposlenika

Martin i Freeman (2003) navode da u svim sferama društva (kao što su npr. kompanijama, interesnim skupinama zaposlenika, zagovornicima privatnosti i građanskih sloboda, advokatima, profesionalnim etičarima i svim mogućim kombinacijama) postoje dileme vezano za praćenje zaposlenika. Svaki zagovornik ima svoje vlastito obrazloženje za ili protiv nadzora zaposlenika, bilo da je to ekonomsko, pravno ili etičko. Međutim, bez obzira na oblik rezoniranja, autori navode sedam ključnih rasprava (dilema) vezano za praćenje zaposlenika:

1. Rasprava o produktivnosti;
2. Rasprava o sigurnosti;
3. Rasprava o odgovornosti;
4. Raspravao privatnosti;
5. Raspravao kreativnosti;
6. Rasprava paternalizma;
7. Rasprava o društvenoj kontroli.

Za potrebe ovog završnog rada, bit će dat kratak prikaz najvažnjih analiza u vezi sa navedenim pitanjem, i to prije svega referirajući se na analize predstavljene u radu *Martin, K., & Freeman, R. E. (2003). Some problems with employee monitoring. Journal of Business Ethics.*

4.3.1. Rasprava o produktivnosti

Rasprava o produktivnosti usredotočuje se na to poboljšava li praćenje zaposlenika radnu učinkovitost. U početku kompanije opravdavaju praćenje kao sredstvo povećanja produktivnosti i kontrole troškova. Mnoge kompanije provode nadzor kako bi smanjile kompjuterske aktivnosti koje nisu povezane s poslom, poput pregledavanja interneta i lične e-pošte, što može smanjiti produktivnost. Istraživanje koje je proveo WebSense (2001) pokazalo je da je 60,7% zaposlenika priznalo da koristi internet u lične svrhe tokom radnog vremena, što sugerira da je svaka minuta potrošena na lične aktivnosti izgubljena prilika za stvaranje prihoda.

S druge strane, kritičari nadzora zaposlenika tvrde da nadzor ima štetne učinke na produktivnost. Istraživanja su pokazala korelaciju između nadzora i različitih negativnih ishoda, uključujući psihološke i fizičke zdravstvene probleme, dosadu, veliki stres, tjeskobu, depresiju, ljutnju, jak umor i mišićno-koštane probleme (Hartman, 1998.). Invazivne tehnike praćenja također su povezane s povećanim stresom i češćom pojavom stanja poput sindroma karpalnog tunela (Privacy Rights, 2001). Stresni uslovi mogu rezultirati češćim bolestima i sporijim oporavkom zaposlenika, što dovodi do više bolovanja i smanjene produktivnosti na poslu.

Kritičari tvrde da kršenje privatnosti može nepovoljno uticati na zdravlje zaposlenika i potencijalno poništiti povećanje produktivnosti kojem kompanije teže.Osim toga, neke kompanije smatraju da je praćenje ključno za upravljanje troškovima, posebno zbog troškova povezanih s telekomunikacijama. Kako bi kontrolisale potrošnju propusnosti, kompanije pomnije posmatraju upotrebu interneta. Ograničavanjem količine lične upotrebe interneta i velikih prijenosa e-pošte, kompanije mogu smanjiti potrebu za velikom propusnošću, snižavajući troškove telekomunikacija. Alati kao što je SmartFilter kompanije Secure Computing koriste se posebno za sprječavanje preuzimanja velikih datoteka s interneta, frustriraju korisnike i obeshrabruju ih od pokušaja takvih radnji u budućnosti (Martin i Freeman, 2003).

4.3.2. Rasprava o sigurnosti

Rasprava o sigurnosti usmjerena je na to povećava li nadzor zaposlenika sigurnost kompanije. Kako oslanjanje na kompjuterske sisteme raste, ta informacijska imovina postaje glavna meta potencijalnih sabotera. Kompanije koje ne uspiju pravilno osigurati svoje sisteme izlažu se rizicima poput neovlaštenog širenja, pristupa ili mijenjanja osjetljivih korporativnih informacija. Jedan haker ili virus može značajno poremetiti rad ili dovesti do velikih problema u odnosima s javnošću. U tom kontekstu, zagovornici praćenja sugeriraju da ono štiti i kompaniju i nacionalnu sigurnost (Martin i Freeman, 2003).

Poslodavci postaju sve svjesniji sigurnosnih propusta. Nelojalni zaposlenici mogu brzo i naširoko distribuirati poslovne tajne i povjerljive dokumente putem e-pošte. Opće je poznato da većina kršenja sigurnosti dolazi od dobro informiranih insajdera, a ne od vanjskih hakera (Schulman, 2001). Kroz praćenje internetske aktivnosti i sadržaja, kompanije vjeruju da mogu prepoznati i zaustaviti sigurnosne prijetnje. Dodatno, sama svijest o poboljšanom nadzoru može spriječiti potencijalnu krađu od strane zaposlenika.

Štaviše, brojne korporacije, posebno u sektorima kao što su telekomunikacije, hemijska proizvodnja, nafta i gas i bankarstvo, naglašavaju zabrinutost za nacionalnu sigurnost prilikom implementacije strategija elektronskog praćenja. Uobičajeno je vidjeti lokacije za prebacivanje telekomunikacija utvrđene kao vojne ispostave, a ne kao obična komercijalna imovina. S obzirom na njihovu ovisnost o informacionoj tehnologiji za upravljanje svojim operacijama, ove korporacije su posebno podložne elektronskim napadima. Dakle,

elektronski nadzor služi kao ključni odbrambeni mehanizam za zaštitu njihovog organizacionog integriteta (Martin i Freeman, 2003).

4.3.3. Rasprava o odgovornosti

Debata o odgovornosti bavi se time da li praćenje zaposlenih smanjuje odgovornost poslodavca za radnje zaposlenih. U jednoj provedenoj anketi, više od dvije trećine ispitanika vjeruje da prijetnja tužbama uvelike utiče na njihovu odluku da provedu monitoring (Swanson, 2001). Elektronsko praćenje je posebno korisno za rješavanje seksualnog uznemiravanja i stvaranje ne-neprijateljskog radnog okruženja, jer uznemiravajući e-mailovi i posjećene pornografske stranice često pružaju kritične dokaze u pravnim slučajevima. S obzirom na to da se sedamdeset posto pornografskog saobraćaja dešava tokom radnog vremena, kako navodi SexTracker (Conry-Murray, 2001), logično je da se pristalice zalažu za praćenje internet komunikacija. Osim toga, poslodavci ne mogu priuštiti da čekaju da se pojave žalbe.

Osim seksualnog uznemiravanja, postoji i zabrinutost u vezi s ilegalnim učitavanjem ili preuzimanjem komercijalnog softvera i materijala zaštićenih autorskim pravima na korporativne sisteme tokom radnog vremena. Ključno je razumjeti da, iako pojačano praćenje korištenja interneta i e-pošte može olakšati krivično gonjenje prekršaja, to ne sprječava nedolično ponašanje. Stoga, "dilemu o odgovornosti" ne treba zamijeniti sa takozvanim argumentom "sigurnosti zaposlenika". Uznemiravanje je prethodilo digitalnoj eri i nastavit će se čak i uz sveobuhvatno praćenje. Fokus treba biti na sadržaju, a ne na načinima njegovog prenošenja (Martin i Freeman, 2003).

4.3.4. Rasprava o privatnosti

Debata o privatnosti bavi se pitanjem da li je praćenje zaposlenih u skladu sa poštovanjem privatnosti zaposlenih. Razumijevanje same privatnosti ključno je za razumijevanje cjeline rasprava u vezi sa praćenjem zaposlenika. Briga o privatnosti nije jedinstvena za praćenje zaposlenih, već se proteže kroz društvene interakcije i decenijama je predmet temeljitih rasprava. Dominiraju dvije glavne teorije: „teorija kontrole“, koja definiše privatnost na osnovu toga koliko kontrole pojedinci imaju nad svojim informacijama, i „teorija ograničenog pristupa“, koja na privatnost gleda kao na stepen do kojeg je pristup informacijama neke osobe ograničen (Martin i Freeman, 2003). Na primjer, prema teoriji ograničenog pristupa, žena zaključana u sobi bila bi u privatnom stanju kada bi samo stranac mogao da otključa vrata. Ne bi u potpunosti kontrolisala pristup, ali bi imala ograničenu izloženost, stavljajući je u stanje privatnosti. Suprotno tome, teorija kontrole bi svaku vanjsku kontrolu nad vratima smatrala kršenjem njene privatnosti, insistirajući na tome da ona mora držati jedini ključ da osigura svoju privatnost. Ova teorija podržava njeno pravo da otvori vrata i otkrije lično ponašanje uz očuvanje privatnosti (Martin i Freeman, 2003).

Pojava tehnologije podataka potaknula je preispitivanje pojmova privatnosti. S obzirom na to da je potpuno ograničenje pristupa i nepraktično i nepoželjno (uzmite u obzir jednostavnost online kupovine jednim klikom), teorija kontrole privatnosti predlaže uravnotežen pristup koji pojedincima omogućava da odluče ko će dobiti pristup njihovim informacijama bez značajnog ugrožavanja njihove privatnosti. Ovaj okvir također naglašava implikacije za praćenje zaposlenih. Kritičari monitoringa tvrde da to smanjuje kontrolu zaposlenih nad njihovim ličnim podacima omogućavanjem otvorenog pristupa. Čak i postavke koje ne nadgledaju aktivno, ali omogućavaju potencijalno praćenje u svakom trenutku, narušavaju privatnost potkopavajući ličnu kontrolu. Prema teoretičarima kontrole, zaposleni doživljavaju gubitak privatnosti samo znajući da ih poslodavac može nadzirati u bilo kojem trenutku, bez obzira da li se to aktivno radi ili ne. Ova preteća mogućnost posmatranja oduzima privatnost smanjujući ličnu autonomiju (Martin i Freeman, 2003).

4.3.5. Rasprava o kreativnosti

Debata o kreativnosti istražuje da li praćenje zaposlenih poboljšava kreativnost. Teško je zamisliti stvarnost u kojoj se svaka izgovorena riječ zapisuje za ispitivanje. Za radnike bi moglo biti zastrašujuće da razmišljaju kako provode deset sati svakog dana svjesni da se svaki pritisak na tipku i dokument provjeravaju radi produktivnosti ili psiholoških uvida. Kritičari tvrde da bi takav nadzor mogao natjerati zaposlene da stalno budu oprezni kako bi se njihovi postupci mogli trajno tumačiti. Mogu se osjećati kao da je njihov poslodavac u potrazi za greškama, spreman na kritiku. Ova vrsta nadzora mogla bi drastično inhibirati kreativno razmišljanje, uzrokujući da zaposleni modificiraju svoje postupke na osnovu prisustva nevidljivog sudije (Martin i Freeman, 2003).

Nadalje, pojava novih i nekonvencionalnih ideja mogla bi biti potisnuta ako su zaposleni zaokupljeni time kako bi ih mogli percipirati oni koji ih prate. Međutim, za napredak i razvoj korporacije zavise od svježeg i inovativnog razmišljanja. Većina kompanija nastoji stvoriti dinamično i otvoreno okruženje koje njeguje kreativnost među njihovim zaposlenima, što je ključno za generiranje inovativnih proizvoda i usluga. Ipak, postoji zabrinutost da bi kreativnost mogla biti ugrožena ako je potisnuta samo mogućnošću praćenja (Martin i Freeman, 2003).

Autori dalje, navode u svome radu, da osim navedenog, mnoge kompanije imaju eksplicitne političke, moralne i društvene agende. Oni mogu podsticati ili čak zahtijevati od zaposlenih da podrže određene dobrotvorne organizacije ili se zalažu za relevantne zakone. Uz takva eksplicitna očekivanja, kritičari sugerišu da bi prisustvo praćenja moglo uticati na zaposlene da prilagode svoje ponašanje na mreži i komunikaciju putem e-pošte kako bi bili u skladu sa izraženim preferencijama svojih poslodavaca. Ovo bi moglo dovesti do smanjenja kreativnosti jer se zaposleni prilagođavaju očekivanjima koja postavljaju njihovi monitori, umjesto da izražavaju iskrene, nezavisne misli (Martin i Freeman, 2003).

4.3.6. Rasprava paternalizma

Argument paternalizma se bavi pitanjem da li praćenje zaposlenih postavlja očekivanja slična roditeljskom autoritetu. Neki ovaj nadzor upoređuju sa "Velikim bratom", ali bolja analogija bi mogla biti ona sa strogim roditeljem. Nametanje onoga što bi trebalo da budu privatne okolnosti, zajedno sa očiglednim nepoverenjem, podstiče paternalistički odnos (Martin i Freeman, 2003). Kritičari smatraju da se ionako neravnopravan odnos između poslodavaca i zaposlenih pogoršava kada se privatnost i povjerenje daju štedljivo. Švicarski ekonomista Bruno Frey pokazao je da takvo praćenje može degradirati učinak smanjenjem morala, pri čemu se zaposleni osjećaju potcijenjenima od strane svojih poslodavaca i reagiraju ispunjavanjem tih nižih očekivanja, odražavajući tako dječje ponašanje prema figurama roditelja (Hartman, 1998).

Ova paternalistička dinamika se intenzivira sa neujednačenim praksama praćenja. Kompanije postavljaju granice privatnosti koje se razlikuju među grupama definisanim posebnim protokolima i pravilima. Zbog fragmentiranih ICT sistema, rukovodioci na visokom nivou mogu izbjeći nadzor sa kojim se njihovi zaposleni suočavaju, pod izgovorom zaštite korporativne sigurnosti i osjetljive komunikacije. Ovo je slično načinu na koji roditelji mogu postaviti određena pravila samo za svoju djecu, što dovodi do nedosljednih i nepravednih praksi praćenja među različitim nivoima osoblja (Martin i Freeman, 2003).

Štaviše, uticaj elektronskog praćenja mogao bi biti izraženiji od pukog sugerisanja paternalizma. Smanjena privatnost mogla bi potaknuti odrasle da se vrate maloljetničkom ponašanju, produbljujući tako dinamiku odnosa roditelj-dijete. Kako mladi ljudi rastu u nezavisnije odrasle osobe, oni obično uživaju više privatnosti, što odražava njihovu zrelost (Martin i Freeman, 2003). Međutim, Reiman (1995) sugerira da bi smanjenje privatnosti moglo usporiti ovaj razvoj, prisiljavajući odrasle u trajno stanje dječje podređenosti. Shodno tome, kako poslodavci smanjuju nivo privatnosti, zaposleni se mogu naći u tome da nesvjesno usvajaju uloge koje podsjećaju na djecu pod nadzorom roditelja.

4.3.7. Rasprava o društvenoj kontroli

Argument socijalne kontrole ispituje kako bi praćenje zaposlenih moglo pojačati društvenu kontrolu i promijeniti organizacionu kulturu, utičući na ponašanje zaposlenih i nadziranih i nenadgledanih, čime bi uticalo na šire društvene norme. Privatnost je istaknuta kao ključna za individualni identitet i društveno blagostanje, pri čemu Johnson (2001) naglašava njenu intrinzičnu društvenu vrijednost izvan puke korisnosti. Nadzor potencijalno preoblikuje individualna ponašanja i razmišljanja, čak i mogućnost praćenja koja vodi do promjena u načinu na koji ljudi djeluju i misle, što je fenomen ilustrovan konceptom panoptikuma Jeremyja Benthama, koji ima paralele u modernim praksama praćenja radnog mjesta.

Dok neke kompanije vide regulisanje ponašanja zaposlenih kroz praćenje kao korisno za upravljanje rizicima i troškovima, kritičari tvrde da to podriva demokratske vrijednosti

obeshrabrujući autonomiju i inovacije, ključne za društveni napredak. Ova vrsta kontrole, koju je Zuboff (1988) opisala kao "anticipatornu usklađenost", prisiljava zaposlene da prilagode svoje ponašanje na osnovu pretpostavljenih očekivanja, čak i bez direktnog posmatranja. To može dovesti do konformizma koji guši kreativnost i kritičko razmišljanje, na kraju narušavajući ličnu autonomiju i šteti društvenom razvoju. Kritičari poput Johnsona upozoravaju da pretjerana kontrola i negativne posljedice za nekonvencionalno ponašanje sprečavaju preuzimanje rizika, koče demokratski napredak i smanjuju kapacitet za društvene inovacije i obnovu.

U konačnici, Martin i Freeman (2003) zaključuju da razumijevanje složenosti koja okružuje praćenje zaposlenih je ključno jer služi kao ulazna tačka u šira pitanja kao što su društveni ugovori, identitet, moralno djelovanje i inherentne vrijednosti tehnologije. Ovaj proces počinje razumijevanjem kako privatnost i potrebno obavještavanje o praćenju oblikuju odnos poslodavac-zaposleni, naglašavajući da bez odgovarajućeg obavještavanja zaposleni ne mogu donositi informirane odluke, koje se graniče s prinudom od strane poslodavca. Štaviše, uticaj praćenja zaposlenih proteže se izvan radnog mjesta, utičući na ličnu autonomiju i mijenjajući samopercepciju i ponašanje pojedinaca.

Zahtjev za jasnim obavještenjem u situacijama kada bi privatnost mogla biti ugrožena je od suštinskog značaja za omogućavanje pojedincima da shvate i pristanu na implikacije tehnologija koje koriste. U zaključku autori ističu, širi uticaj ovih tehnologija sugeriše da one nose ugrađene vrijednosti koje utiču ne samo na dinamiku radnog mjesta već i na šire društvene norme.

Na osnovu svega izloženog, moguće je zaključiti da kompanije trebaju, a moglo bi se i reći moraju razmotriti implikacije usvajanja i širenja savremenih tehnologija u funkciji nadzora, jer svaka odluka odražava izbor da se podrže specifične vrijednosti koje su inherentne ovim sistemima. Ovo naglašava važnost promišljenog angažmana s tehnologijom, prepoznajući njen potencijal da oblikuje korporativne i društvene odgovornosti.

4.3.8. Uticaj nadzora na kvalitet rada zaposlenika

Brojni autori sugeriraju da bi nove metode nadzora, koje omogućavaju moderne digitalne tehnologije, mogle značajno naštetiti privatnosti, dostojanstvu i autonomiji radnika, posebno kada se zloupotrijebe (Moreira, 2016; Canteiro, 2017; Azevedo, 2018). Oliver (2002) tvrdi da invazivno praćenje može ugušiti kreativno razmišljanje, smanjiti samostalno razmišljanje i dovesti do bolesti povezanih sa stresom.

Španska strategija za zdravlje i sigurnost na radu 2015–2020. godine naglašava važnost razmatranja potencijalnih efekata novih tehnologija na zdravlje i sigurnost radnika (INSHT, 2015). Dokument naglašava rastuću i ekstenzivnu upotrebu ICT koja podržava implementaciju programa nadzora radnika, posebno važnih u udaljenim i fleksibilnim radnim okruženjima (Eurofond, 2020).

Studije iz 2019. godine su istraživale negativne uticaje tehnologija praćenja zaposlenih koje integrišu funkcije upravljanja poslom, gde zaposleni dobijaju povratne informacije u realnom vremenu i ocjene učinka (Mateescu i Nguyen, 2019). Takve prakse dovode do „gamifikacije“ posla, stvarajući visoko konkurentno i stresno okruženje i potencijalno smanjujući organizacijsku i pregovaračku snagu radnika, čime se obezvređuje njihov rad (Casilli, 2019). Međutim, gamifikacija[10] nije suštinski štetna; kada se pravilno implementira, može poboljšati angažman zaposlenih, inovacije i učenje na poslu (Forbes, 2017). Problemi nastaju kada se gamifikacija kombinuje sa opsežnim digitalnim nadzorom u okviru tehnologija upravljanja.

Zuboff (2019) tvrdi da samo prisustvo nadzora mijenja ponašanje onih koji se nadziru, smanjujući njihovu autonomiju i narušavajući njihovu privatnost. To nije ništa manje istina na radnom mjestu. Invazivno praćenje može ugroziti psihološki ugovor između poslodavca i zaposlenika, narušavajući povjerenje, motivaciju i organizacijsku predanost (McParland i Connolly, 2019). Ova erozija je posebno očigledna kada praksama praćenja nedostaje transparentnost o metodama i korištenju podataka. Prethodne studije pokazuju da zaposleni često posmatraju elektronsko praćenje kao nepravednu praksu koja narušava privatnost i narušava zakonom i drugim propisima zaštićena prava (Tabak i Smith, 2005; Chory, Vela i Avtgis, 2016). Posljedično, zaposleni mogu postati manje angažirani i manje spremni na ulaganje napora, što se u konačnici suprotstavlja namjeravanoj svrsi poboljšanja učinka kroz praćenje (Eurofond, 2020).

Studije slučaja kompanija koje je razvio Eurofound (2020c) u okviru svog istraživanja o radu na daljinu i mobilnom radu zasnovanom na ICT-u otkrivaju da su digitalne tehnologije proširile mogućnost kontrole i nadgledanja udaljenih radnika. Osim toga, ove studije naglašavaju vitalnu ulogu koju radnički savjeti ili drugi oblici predstavljanja zaposlenih imaju u postavljanju granica upotrebe intruzivnih tehnologija praćenja (Eurofound, 2020c).

Kvalitativno istraživanje sprovedeno sa vozačima autobusa u Londonu kroz polustrukturirane intervjue baca svijetlo na to kako mobilni radnici percipiraju i prilagođavaju se sistemima za praćenje i kontrolu (Pritchard *et al.*, 2015). Vozači autobusa koristili su ugrađeni uređaj nazvan Drivewell koji procjenjuje njihove performanse praćenjem različitih ponašanja u vožnji. Loši rezultati mogu dovesti do sankcija ili zahtjeva za prekvalifikaciju. Vozači su smatrali da je ovaj uređaj, koji su vidjeli kao alat za kontrolu

[10]Gamifikacija je implementacija principa igre u situacijama koje nisu direktno povezane s igrama, a posebice je primjetna na društvenim mrežama. Na ovaj način korisnici društvenih mreža imaju priliku osvojiti nagradu u zamjenu za aktivnosti poput lajkanja, ostavljanja komentara ili osmišljavanja kreativnih elemenata (fotografija ili kratkih tekstova). Unošenjem gamifikacije u marketinške aktivnosti kompanije potiču angažman i lojalnost kupaca, ali i rast svijesti o brendu. Također, pojam gamifikacija koristi se za označavanje tehnike ili strategije koja se koristi za motiviranje radnika i klijenata, između ostalih, u nekim njihovim zadacima u neigranim okruženjima.

upravljanja, promijenio njihovo ponašanje u vožnji i stvorio takmičarsku atmosferu (Eurofond, 2020).

Ova studija također sugerira da takvi sistemi za praćenje mogu povećati kognitivno opterećenje vozača, pojačavajući efekte drugih tehnologija nadzora i ometanja, što bi moglo povećati nivo stresa. Dok su neki vozači koristili ovaj uređaj kao pomoćno sredstvo za učenje kako bi poboljšali svoju vožnju, drugi su kritikovali njegovu tačnost, tvrdeći da je previdio faktore poput kvaliteta vozila i uslova na putu. Među vozačima je prevladavalo mišljenje da tehnologija ne odražava tačno njihove vještine ili radni učinak, već ograničava njihovu autonomiju i može negativno uticati na njihove mogućnosti za karijeru (Pritchard *et al.*, 2015).

Još jedno kvalitativno istraživanje o efektima daljinskog nadzora – korištenjem terenskih tehnologija za nadgledanje ponašanja i učinka mobilnih radnika – u 52 privatne i javne kompanije u Norveškoj otkrilo je da su predstavnici zaposlenika koji su bili oprezni zbog invazija na privatnost od terenskih tehnologija također primijetili štetne uticaje na kvalitet obavljenog posla (Bråten i Tranvik, 2017). Ova zabrinutost bila je izraženija u industrijama koje su koristile ove tehnologije za upravljanje i kontrolu rada, posebno u sektorima kao što su transport robe i instalacija elektronike i zaliha energije. Tamo gdje su se terenske tehnologije prvenstveno koristile za dokumentiranje ili inspekciju rada, negativne percepcije su bile manje uobičajene.

Glavne brige uključivale su gubitak individualne slobode, smanjenu kontrolu nad radnim rasporedom i zadacima, te povećanje stresa, radnog tempa i pritiska (Bråten i Tranvik, 2017). Štaviše, mnogi radnici nisu bili sigurni kako će prikupljene podatke koristiti njihovi poslodavci. Predstavnici zaposlenih u industrijama kao što su radovi na putevima, bezbjednost i starački domovi dijelili su slične brige, iako su prepoznate neke prednosti, kao što su poboljšana bezbjednost i mogućnost efikasnog dokumentovanja rada kako bi se suprotstavile potencijalnim pritužbama. Glavni negativan efekat uočen u većini sektora bio je porast sukoba i smanjenje povjerenja između socijalnih partnera nakon uvođenja terenskih tehnologija. Dok je povjerenje na kraju obnovljeno u nekim kompanijama, u drugim je ostalo narušeno jer je tehnologija viđena kao pokazatelj nepovjerenja prema pojedinačnim radnicima (Eurofond, 2020).

5. INTERAKCIJA PRAVA I ETIKE U KONTEKSTU NADZORA

Praćenje nadzora, koje obuhvata aktivnosti od vladinog špijuniranja do nadzora poslodavaca i prikupljanja podataka od strane kompanija, postoji na složenom raskrižju zakona i etike. Pravni okviri koji reguliraju nadzor su različiti i uvelike ovise o nadležnosti, dok etička razmatranja često nadilaze zakonske granice, postavljajući pitanja o privatnosti, pristanku, povjerenju i dinamici moći (Abraha, 2022).

Kako to navodi Kagan R.A (2007) "nema sumnje da je globalizacija uticala na autonomiju nacionalnih vlada, gurajući pravne sisteme ekonomski naprednih demokracija prema konvergenciji na značajan način. Sve integriranije, konkurentnije međunarodno poslovanje i demografske promjene suočavaju sve bogate demokracije sa sličnim društvenim, ekonomskim, političkim i ekološkim problemima. Prijedlozi zakonskih rješenja kruže globalnom komunikacijskom mrežom. Europska unija i međunarodni ugovori zahtijevaju međunacionalno usklađivanje domaćih zakona o važnim aspektima kontrole onečišćenja, sigurnosti banaka, ljudskih prava, javnog zdravlja, intelektualnog vlasništva i još mnogo toga." (Kagan, R.A. 2007). To je očekivano, prema Beth Simmons (2004.), jer u svijetu koji je sve više međuovisan, kada moćne države kao što su SAD i Europska unija (ili važne izborne jedinice unutar njih) trpe značajne troškove ili nedostatke zbog različitih nacionalnih zakona i praksi, vjerojatno će koristiti međunarodne ili nadnacionalne institucije, kao i vlastitu ekonomsku i političku moć, kako bi potaknuli druge nacije da prihvate pravne standarde moćne države Simmons B (2004).

Iako je predmet ovog rada prije svega analiza pravnog okvira i rješenja na nivou Evropske unije u vezi sa pitanjima nadzora zaposlenika, razumijevanje te cjeline nije moguće bez uzimanja u obzir najvažnijih rješenja u Sjedinjenim Američkim Državama. Dugi niz godina i u mnogočemu, pravni sistemi SAD i zapadnoevropskih zemalja više su slični nego različiti. Pravne ideje neprekidno prelaze Atlantik u oba smjera. Iste temeljne individualne i političke slobode i koncepti jednakog tretmana ugrađeni su u zakone i pravna rješenja obaju kontinenata.

Iz pravne perspektive, zemlje provode različite propise za nadzor. U SAD-u, na primjer, četvrti amandman Ustava štiti građane od neopravdanih pretraga i zapljena, utičući na to kako se provodi nadzor. Međutim, zakoni kao što je PATRIOT Act[11] proširili su mogućnosti vladinog nadzora, što je često opravdano zabrinutošću za nacionalnu sigurnost (Solove, 2011). EU, prema GDPR, nudi kontrastni pristup, naglašavajući individualna prava na privatnost i zahtijevajući privolu za prikupljanje podataka (Abraha, 2022). Ovi pravni instrumenti odražavaju različita stajališta o tome kako bi nadzor trebao biti uravnotežen s pravima pojedinca.

Etički gledano, nadzor izaziva duboku zabrinutost oko ravnoteže između kolektivnih dobrobiti i individualnih sloboda. Filozofi i etičari poput Nissenbauma (2009) tvrde da je privatnost kontekstualna i da kršenje kontekstualnih normi protoka informacija može biti etički štetno, bez obzira na zakonitost. Nadzor, osobito kada je opsežan i bez jasnih ograničenja, može narušiti povjerenje između pojedinaca i institucija, povjerenje koje je temelj društvene stabilnosti i međusobnog poštovanja (Rudiyanto et al., 2023).

[11]Više informacija dostupno na: https://www.justice.gov/archive/ll/what_is_the_patriot_act.pdf

Uloga tehnologije dodatno komplikuje interakciju zakona i etike u nadzoru. Napredne tehnologije kao što su umjetna inteligencija i mašinsko učenje omogućavaju prodorniji i manje nametljiv nadzor, često nadmašujući zakonske propise. Ovaj tehnološki napredak stvara prazninu u kojoj aktivnosti mogu biti tehnički legalne, ali etički upitne (Hintz, Dencik i Wahl-Jorgensen, 2018). Etički okviri poput Just Surveillance, koji je predložio Macnish (2014), zalažu se za prakse nadzora koje su ne samo pravno usklađene već i moralno opravdane osiguravajući da su neophodne, proporcionalne i transparentne.

Izazov je, dakle, razvoj koherentnog pristupa koji poštuje i zakonska prava ali i etičke principe. Autori poput Lyon (2015) zagovaraju sintezu pravnog nadzora i etičke pažnje kako bi se upravljalo praksama nadzora, osiguravajući da služe javnom interesu bez nepravednog kršenja prava pojedinca. Ovo zahtijeva stalni dijalog između tehnologa, pravnih stručnjaka, etičara i javnosti kako bi se kretali kroz razvojni krajolik nadzora na način koji poštuje i vladavinu zakona i moralni integritet.

5.1. Slučajevi sukoba prava i etike

"Etika je širi društveni podsistem nego što je pravo, koje pokriva samo ona područja za koje država ima naročiti interes. I pored činjenice da pravne norme nužno ne ovise o etičkim razlozima, zakoni često uključuju etičke norme. Takve etičke norme postaju pravne norme a da ne gube svoj etički karakter."(Trifković *et al*. 2021) Etički podsistem pokriva šire područje društvenih odnosa nego što je slučaj s pravom, te ima dublje društvene korijene. Legitimitet moralnih normi mora biti dokazan historijski, uz sociološku i filozofsku argumentaciju. S druge strane, legitimitet prava ovisi gotovo isključivo o državi koja monopolom fizičke prinude usmjerava ponašnja pojedinaca u društveno željenom pravcu nastojeći ostvariti osnovne vrijednosti u pravu - mira i pravne sigurnosti, te osigurati jednakost svih pred zakonom i na taj način djelovati etički (Trifković *et al*. 2021). Biti etičan idealno znači činiti dobro i suzdržavati se od nanošenja štete u cjelini pravnog poretka. Pitanje etike uvelike ovisi i o percepcijama pojedinca i društva, odnosno kultura. Zakonom je definisano što se smije, a što se ne smije činiti; to je pravilo koje je izričito propisano i njegovo je kršenje kažnjivo (Chaloner, 2007). Ali, uz to mnoge profesije i društva donijeli su službene kodekse ponašanja koji definišu vrijednosti relevantnih skupina i kako bi se članovi trebali ponašati.

Neki autori zastupaju stajalište da bi se moglo općenito reći da "zakon oslikava etiku koju je postavilo društvo" (Chaloner, 2007). Ipak, pravo i etika mogu biti u sukobu; na primjer, radnja može biti legalna, ali neetična. Do sukoba može doći tamo gdje je nešto nezakonito, ali etički potvrđeno, poput racionalizacije za eutanaziju (Ogata, 2005). Dileme se obično vrte oko kvalitete života nasuprot kvantitete, pro-life protiv pro-izbora, slobode protiv moći, istine protiv laži i empirijskog znanja protiv individualnih uvjerenja među ostalim pitanjima. Kako bi se ispunili zahtjevi dobre prakse, "potrebna je dobro obrazložena procjena (...) zajedno s uvažavanjem zašto, kao i kako bi to trebalo učiniti" (Chaloner, 2007).

Upotreba e-pošte od strane zaposlenika stvara druge probleme privatnosti na radnom mjestu. Kao što je objasnio McEvoy (2002), iako je e-pošta sveprisutna i čini zaposlenike učinkovitijima, ona se nalazi na tvrdim diskovima radnih stanica i mrežnih poslužitelja – ostavljajući za sobom dokaze o svim komunikacijama zaposlenika. McEvoy dalje navodi kako bi poslodavci trebali savjetovati zaposlenike da ozbiljno razmisle prije nego što kliknu dugme za slanje s radnog e-maila. Jedna gadna šala o nadređenom, nepristojna šala ili slika mogu stvoriti probleme na radnom mjestu. Čak i ako zaposlenik misli da je on ili ona izbrisao poruku e-pošte, neko bi je mogao kasnije dohvatiti budući da kompanije gotovo svu e-poštu spremaju na mrežni poslužitelj. Prema objavi kompanijeTangent Inc iz 2008., kompanija obavlja otprilike 90% dnevne poslovne komunikacije putem e-pošte ili nezaštićenih direktnih poruka (Alexi, 2008). Komunikacije, uključujući nestrukturirane podatke, mogu začepiti propusnost mreže kompanije i zauzeti velike količine prostora za pohranu. Količina e-mailova i sličnih obrazaca za podatke u većini kompanija udvostruči se svakih 12 do 18 mjeseci (Chaloner, 2007).

5.2. Analiza pravnih rješenja u svjetlu etičkih standarda u SAD

Za razumijevanje cjeline pitanja nadzora u pravu Evropske unije, nužno je dati prikaz etičkih standarda i pravnih rješenja u Sjedinjenim Američkim Državama. Trebaju li kompanije nadzirati zaposlenike dok su na poslu? Koje radnje bi kompanije trebala pratiti? Koje su vrste praćenja prihvatljive? Izvješće Ureda za procjenu tehnologije SAD-a definiše kompjuterizirano praćenje učinka kao "kompjuterizirano prikupljanje, pohranjivanje, analiza i izvješćivanje informacija o produktivnim aktivnostima zaposlenika" (Peters, 1999). Praksa praćenja radnika kontroverzna je praksa koja je nedvojbeno u porastu (AMA, 2008). Kada je riječ o temi praćenja zaposlenika postoji siva zona; važeći zakoni nalažu da je praćenje zakonito, no postavljaju se pitanja učinkovitosti i etike. Kompanije moraju nadzirati zaposlenike kako bi zaštitile i kompanijei zaposlenike, ali također moraju marljivo paziti na etičko postupanje sa zaposlenicima (Bezek i Britton, 2001). Bhatt (2001) opisuje praćenje zaposlenika i upravljanje znanjem ističući da mnoge kompanije “vjeruju da mogu upravljati znanjem ako se fokusiraju isključivo na ljude, tehnologije ili tehnike”. Takva strategija neće omogućiti kompaniji da zadrži konkurentsku prednost. Kompanije moraju stvoriti okruženje odgovornosti i transparentnosti kako bi učinkovito poslovale (Bhatt, 2001).

Elektronička pošta i internet sastavni su dijelovi svakodnevne rutine tipičnog radnika. Zbog svoje brzine i ukupne pogodnosti, e-pošta je zamijenila memorandum između kancelarija kao preferirani način komunikacije. Stoga mnogi zaposlenici koriste e-poštu i internet samo za posao. Međutim, problemi nastaju kada zaposlenici koriste poslovne resurse za neposlovne zadatke. Stoga kompanije odgovaraju na pravne rizike proaktivnom borbom protiv problema korištenja interneta od strane zaposlenika izvan posla. Proaktivni korak koji kompanije poduzimaju jest praćenje aktivnosti svojih zaposlenika, tačnije praćenje elektronskih aktivnosti zaposlenika (Bezek i Britton, 2001). Kao što su izvijestili Court i Warmington (2004), brojni poslodavci širom zemlje koriste neki oblik praćenja zaposlenika.

Sud navodi statistiku zloupotrebe interneta i e-pošte od strane radnika, te potencijalne zamke odgovornosti, kao glavne razloge za praćenje zaposlenika. Praćenje zaposlenika u mnogim je slučajevima tu da zaštiti poslovanje od pravne odgovornosti, kao i da proizvede učinkovitijeg zaposlenika.

Praćenje postupaka zaposlenika stvara raspravu o tome treba li zaposlenik imati pravo na privatnost. Međutim, praćenje zaposlenika postavlja i etička pitanja. Woodbury (2003) objašnjava da neka od etičkih pitanja uključuju zaposlenike koji preuzimaju pornografiju, stavljaju lične web stranice na mašine u vlasništvu kompanija ili prikazuju uvredljive slike na računarskim monitorima. Zaposlenici su provodili sate svog radnog dana igrajući igre na svojim računarima, šaljući ličnu e-poštu ili kockajući. Dva velika problema su dnevno trgovanje i online kupovina (Woodbury, 2003.). Etička pitanja kojima se poslodavac bavi mogu se razlikovati od onoga što zaposlenik smatra etičkim. Sve se vraća na tačku gledišta o tome što je dopušteno, a što ispravno ili pogrešno. Woodbury nastavlja da sa stajališta zaposlenika, kompanijemogu djelovati neetično dok nadziru pritiske tipki, gledaju privatnu e-poštu ili daju neadekvatnu opremu koja dovodi do oštećenja vida, vrata, šake, zgloba ili ruke. Praćenje pritiskanja tipki posebno je invazivno, jer svaki put kad se zaposlenik odmara, možda proteže radi zdravlja ili vodi kratki razgovor radi zdravog razuma, osoba nema zadatak (Woodbury, 2003). Takav strogi nadzor može stvoriti odluke ili odluke na radnom mjestu koje bi mogle disciplinirati zaposlenika zbog jednostavnog uzimanja legitimne pauze. Programi za praćenje ne mogu znati kada zaposlenik ima želučane tegobe i mora biti udaljen od svog stola - oni samo osjećaju da zaposlenik trenutno ne radi. Poslodavci dobivaju, u neku ruku, pristrane i nepotpune podatke.

Osim toga, programi za praćenje kao što su *key logeri* mogu biti izuzetno invazivni. Rosen (2000) opisuje sofisticirani program za praćenje nazvan Assentor koji provjerava svaki dolazni i odlazni e-mail u potrazi za dokazima rasizma, seksizma ili određenih dijelova tijela. Assentor svakoj e-pošti dodjeljuje ocjenu uvredljivosti i prosljeđuje poruke s visokim ocjenama nadređenom na pregled.Program u ovom slučaju nije druga osoba, ali može izračunati formulu za slanje e-pošte ljudskom nadzorniku da pročita e-poštu.

Rosen u svome radu dalje piše da su sudovi presudili da vladini poslodavci mogu slobodno pretraživati kancelarije svojih zaposlenika u potrazi za nedoličnim ponašanjem na poslu (kada imaju jasnu sumnju na nedjelo), jer ljudi očekuju manje privatnosti na radnom mjestu koje dijele s drugim zaposlenicima. Neki bi to mogli smatrati neetičkim. Četvrti amandman Ustava Sjedinjenih Američkih Država garantuje pravo pojedinaca na zaštitu od neopravdanih pretraga i zapljena. Prema ovom amandmanu, pretrage i zapljene mogu se vršiti samo uz nalog koji je izdan na osnovu vjerovatnog uzroka, što znači da postoji opravdana sumnja da će se pronaći dokazi ili predmeti povezani s krivičnim djelom. Osim toga, nalog mora precizno opisati mjesto koje se pretražuje i predmete ili osobe koje se zapljenuju, čime se ograničava moć državnih organa da intervenišu u privatni život građana bez opravdanih razloga.

U Sjedinjenim Američkim Državama, iako državni službenici često smatraju da ih četvrti amandman štiti od neopravdanih pretraga, nadređeni može pretraživati radnikovu e-poštu, internetsku historiju ili bilo što drugo što odluče da treba istražiti. Međutim, takve pretrage moraju biti u skladu s ustavnim zahtjevima četvrtog amandmana kako bi se zaštitila prava pojedinaca od nezakonitih intervencija države u njihovu privatnost (United States Congress. (n.d.). Fourth Amendment). Gledajući na praćenje zaposlenika s etičkog stajališta, praksa bi trebala biti podložna regulaciji. Ipak, trenutni zakoni i standardi daju nekoliko smjernica za reguliranje nadzora zaposlenika. Postoji nekoliko stotina programa sličnih ovom o kojem se govori. Noviji programi su robusniji, dostupniji, lakši za korištenje i mogu biti potpuno nevidljivi krajnjem korisniku.

5.3. Mišljenja, smjernice i dobre prakse u praćenju zaposlenika u EU

Eurofound 2020 Employee Monitoring and Surveillance: The challenges of digitalisation, Publications Office of the European Union, Luxemburg (Eurofound (2020)) u svome izvještaju navodi da nacionalna tijela za zaštitu podataka u državama članicama EU ključna su u tumačenju relevantnih zakona i izdala su različita mišljenja, smjernice i najbolje prakse u vezi s praćenjem zaposlenih, kako općenito tako i za specifične vrste nadzora na radnim mjestima. Eurofound (2020) navodi primjere nekoliko zemalja koje su predstavljene u nastavku.

U Francuskoj, nacionalno tijelo za zaštitu podataka objavilo je više smjernica i mišljenja prilagođenih radnom okruženju, nudeći direktive o različitim praksama praćenja. To uključuje video nadzor, snimanje i slušanje telefonskih razgovora, kontrolu pristupa na radnim lokacijama, praćenje radnog vremena, GPS praćenje i korištenje ICT alata za zapošljavanje i upravljanje zaposlenicima, kao i nadzor korištenja kompjutera zaposlenika. S obzirom na potencijalno invazivnu prirodu video nadzora, često se daju smjernice koje objašnjavaju zakonske uslove pod kojima je ovo praćenje dozvoljeno. Na primjer, u Mađarskoj je nacionalni zakon nejasan u pogledu specifičnosti video nadzora; stoga je mađarsko nacionalno tijelo za zaštitu podataka i slobodu informacija utvrdilo detaljne zahtjeve i ograničenja za njegovu primjenu.

Na Kipru, smjernice koje je izdao Povjerenik za zaštitu ličnih podataka posebno se odnose na korištenje biometrijskih sistema u praćenju zaposlenih, što je oblast koja nije obuhvaćena zakonima. Generalno, na Kipru je uobičajeno da socijalni partneri svoje nesuglasice rješavaju kroz kolektivno pregovaranje. Ako to ne uspije, sindikati ili pojedini zaposleni često podnose žalbe Povjereniku. Nedavne žalbe i upiti u vezi sa praćenjem korištenja računara zaposlenih naveli su Povjerenika da izda smernice u kojima se navodi da poslodavci mogu da prate određene računarske aktivnosti pod određenim uslovima i u okviru određenih zakonskih ograničenja, ali nije dozvoljen potpuni nadzor nad svim radnjama kompjutera ili privatnom e-poštom.

U Grčkoj, Hellenic Data Protection Authority je izradio različite smjernice za definiranje uslova pod kojima se poslodavac može uključiti u određene vrste nadzora na radnom mjestu, kao što su provjera e-pošte zaposlenih i korištenje interneta, video nadzor, GPS praćenje i korištenje biometrijskih tehnologija.

Tamo gdje nedostaje poseban zakon, kao na Malti, Ured povjerenika za informacije i zaštitu podataka je također objavio smjernice koje savjetuju poslodavce o zakonom dozvoljenim metodama praćenja i nadzora. Isto tako, holandsko tijelo za zaštitu podataka nudi smjernice o različitim vrstama praćenja, jasno praveći razliku između nadzora (toezicht) i nadzora (kontrole), eksplicitno povezujući ove prakse sa privatnošću zaposlenih.

Norveško tijelo za zaštitu podataka izdalo je više izjava u vezi s praćenjem i nadzorom na radnom mjestu, naglašavajući smanjenje povjerenja u odnose na radnom mjestu zbog nadzora zaposlenih. Napominje da iako postojeći zakoni dovoljno pokrivaju prava radnika na privatnost i informacije o prikupljanju podataka, poslodavci ih ne poštuju uvijek. Šef norveškog tijela za zaštitu podataka je sugerirao da ovo pitanje često proizlazi iz stavova poslodavaca i nedostatka znanja (Thon, 2015). Studija iz 2019. godine među 140 norveških poslodavaca otkrila je da značajan broj ne poštuje propise o nadzoru na radnom mjestu – 36% je priznalo da im nedostaju ikakve smjernice o praćenju i nadzoru (Deloitte, 2019), a gotovo 60% je napomenulo da se o praksi praćenja nije razgovaralo sa zaposlenima.

U Velikoj Britaniji, nacionalno tijelo za zaštitu podataka objavljuje Kodeks prakse zapošljavanja, koji se posebno bavi praćenjem radnog mjesta. Iako kodeks nije pravno provediv, može se pozvati u pravnim postupcima vezanim za kršenje Zakona o zaštiti podataka Ujedinjenog Kraljevstva. Kodeks naglašava da praćenje na radnom mjestu mora biti saopšteno zaposlenima, biti proporcionalno i uzeti u obzir privatnost zaposlenih. Da li se takvo praćenje smatra razumnim i proporcionalnim zavisi od faktora kao što su svrha praćenja, njegovi potencijalni negativni efekti, da li bi alternative mogle da postignu iste rezultate, i opšta opravdanost prakse praćenja. Kodeks također ukazuje na probleme sa pojmom pristanka u okviru radnog odnosa.

6. STUDIJA SLUČAJA –„ADRIATIC METALS“

6.1. Općenito o Adriatic Metals

Adriatic Metals je prva kompanija ovog tipa u rudarskoj industriji Bosni i Hercegovini, fokusiran na istraživanje i razvoj polimetalnih projekata. Sjedište kompanije je u Londonu, također kompanija je izlistana na Londonskoj berzi, čime demonstrira svoj globalni doseg i poslovni model. Ova studija slučaja namijenjena je da dublje istraži kako Adriatic Metals upravlja pravnim i etičkim izazovima u kontekstu nadzora zaposlenika.

Adriatic Metals se bavi istraživanjem i razvojem bogatih nalazišta metala, s posebnim fokusom na Vareš Projekt u Bosna i Hercegovina. Kompanija je brzo napredovala od otkrića

do razvojne faze, pokazujući značajan potencijal za proizvodnju strateških metala u Evropi. Njihov portfolio uključuje vrijedne metale poput srebra, cinka, i olova, koji su ključni za industrijski razvoj i energetsku tranziciju.

Bosna i Hercegovina, kao domaćin operacija Adriatic Metals, je habitat za poslovno i rudarsko okruženje, glavni problemi su njesni pravni okviri u rudastvu a posebno za rudarske kompanije koje su u privatnom vlasništvu. Kompanija je uključena u aktivno istraživanje i razvoj, koristeći napredne tehnologije i pristupe za minimalizaciju ekološkog utjecaja i promicanje održivog rudarenja.Kompanija je donijela mnoge novitete na tržište Bosne i Hercegovine u poslovanju.

Ilustracija 2. Vizija i vrijednost kompanije Adriatic Metals

Izvor: Eastern Mining web stranica

6.2. Cilj i svrha istraživanja: Razumijevanje dinamike nadzora unutar Adriatic Metals

Cilj ovog istraživanja je pružiti dubinsko razumijevanje dinamike nadzora zaposlenika unutar Adriatic Metals, rudarske kompanije u Bosni i Hercegovini s globalnim dosegom. Svrha je izgraditi sveobuhvatan uvid u sljedeće aspekte:

Stavovi zaposlenika: Kako zaposlenici percipiraju nadzor na radnom mjestu? Koje su njihove glavne brige, percepcije i stavovi prema različitim formama nadzora koje implementira Adriatic Metals?

Uticaj na produktivnost i moral: Kako nadzor utiče na produktivnost i moral zaposlenika? Postoji li korelacija između stupnja i načina nadzora s produktivnošću, angažiranošću i zadovoljstvom zaposlenika?

Prava zaposlenika: Kako nadzor utiče na pravna prava zaposlenika? U kojoj mjeri su pravni okviri i etički standardi integrirani u prakse nadzora kompanije?

6.3. Metodologija istraživanja

Za postizanje ciljeva istraživanja, biti će korištena kvantativna metoda. To je omogućilo sveobuhvatnu analizu stavova zaposlenika, uticaja nadzora na radno ponašanje i pravne aspekte nadzora.

U kontekstu kvantitativnog istraživanja, implementirana je anketa putem Culture Amp platforme za anonimno prikupljanje podataka o stavovima zaposlenika, nadzoru i zadovoljstvu. Anonimnost osigurava iskrene odgovore i pouzdane podatke. Ciljna populacija su bili svi zaposlenici Adriatic Metals, njih ukupno 267.

Alati za prikupljanje podataka bili su anketni upitnik, razvijen i distribuiran putem Culture Ampa, s prilagođenim pitanjima za mjerenje različitih aspekata radne kulture i nadzora.Anketa je jedinstvena tehnika koja se koristi za prikupljanje podataka i uvida o stavovima i razmišljanjima ljudi. Općenito, to uključuje prikupljanje podataka putem ispitivanja. Važno je napomenuti da su u znanstvenom kontekstu ankete više od pukog postavljanja pitanja ispitanicima. Prvenstveno, anketa podrazumijeva postavljanje specifičnih pitanja pomno odabranoj skupini pojedinaca na strateški strukturiran način, s ciljem izazivanja najiskrenijih mogućih odgovora kako bi se dobile značajne informacije o temi istraživanja (Vujević, 1983).

Etika danas predstavlja temeljni segment ljudskog djelovanja i zbog toga je dobro biti upoznat s temeljnim načelima etičkog ponašanja. Kako bi se osigurala kako bi se etičnost u ovom naučnom istraživanju dobivena je saglasnost učesnika u anketi o podjeli podataka, gdje su učesnici ankete informisani o svrsi i prirodi istraživanja.

Prikupljanje podataka je izvršeno u periodu od novembra 2023. do decembra 2023. godine. Anketa je poslana u dva vala. Nakon prvog slanja ankete 28.11.2023. godine, drugi val, odnosno napomena za popunjavanje ankete je poslana 05.12.2023. godine. U konačnici, ukupno je prikupljeno 225 odgovora, što je predstavljao 84% od ukupne populacije. Nakon prikupljanja podataka se pristupilo analizi istih. Za potrebe analize kvantitativni podataka korištena je jednostavna statistička analiza, odnosno deskriptivna statistika. Za analizu kvalitativnih podataka dobivenih iz intervjua i fokus grupa korištena je tematska analiza.

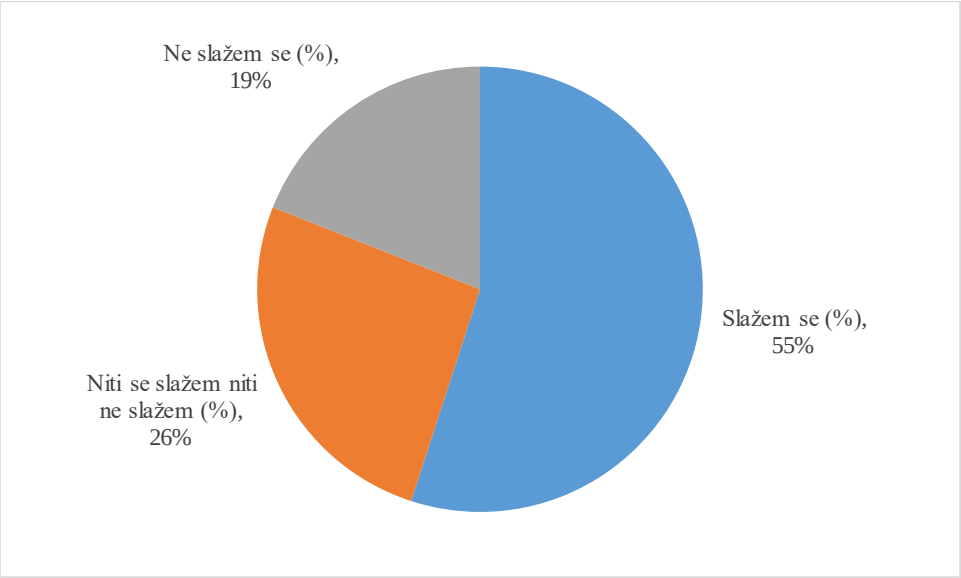
Anketa distribuirana ispitanicima sastojala se od nekoliko cjelina i napravljen je kombinacijom prethodno validiranih upitnika kao što su od Tran (2017), Baek i Morimoto (2012) i Segijn, Opree i van Ooijen (2022). Prva cjelina se odnosi na opću percepciju nadzora, nakon čega se ispituju specifične metode nadzora koje se odnose na korištenje videonadzora u vozilima i zabrinutosti zbog praćena internet komunikacija. Naredna dva pitanja se odnose na uticaj na privatnost i autonomiju, odnosno koliko su zaposlenici zabrinuti da nadzorne prakse narušavaju njihovu privatnost i autonomiju. Sljedeća dva pitanja se odnose na percepciju korisnosti i sigunosti te nakon toga anketa se osvrće na uticaj nadzora na moral i produktivnost zaposlenika (dva pitanja). Posljednje dvije sekcije odnose se na pravna i etička pitanja odnosno transparentnost i politike (po dva pitanja). Kompletna anketa se nalazi u prilogu 1.

6.4. Istraživanje i analiza nadzora zaposlenika u Adriatic Metals

Istraživanje je provedeno među zaposlenicima Adriatic Metals, njih 267, s ciljem procjene njihovih stavova i reakcija na različite oblike nadzora, uključujući videonadzor, GPS u vozilima, dash kamere u vozilima, monitoring internetske komunikacije i nadzor mobilnih i drugih uređaja. Korištenjem Culture Amp platforme za anonimne ankete i seriju strukturiranih intervjua, prikupljeni su kvantitativni podaci. Da bi jednostavnije objasnili podatke grupirali smo odgovore za opciju 5 (u potpunosti se slažem) i opciju 4 (slažem se), kao i za opcije 1 (u potpunosti se ne slažem) i 2 (ne slažem se) kako bi dobili kumulativne procene koji odražavaju visok nivo slaganja ili zadovoljstva.

Prvi dio odnosi se na opću percepciju nadora. Prema grafikonu 1, više od polovine ispitanika (55%) je odgovorilo da se slaže da je nadzor na radnom mjestu opravdan i potreban, dok skoro dva od 10 ispitanika (19%) se ne slaže sa navedenom tvrdnjom.

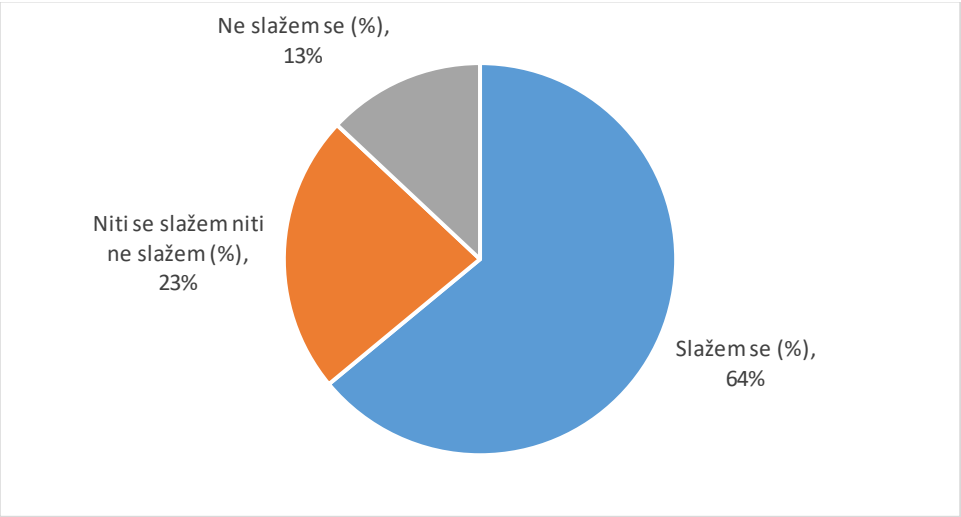
Grafikon 1. U kojoj mjeri se slažete da je nadzor na radnom mjestu opravdan i potreban?



Izvor: Autor završnog rada

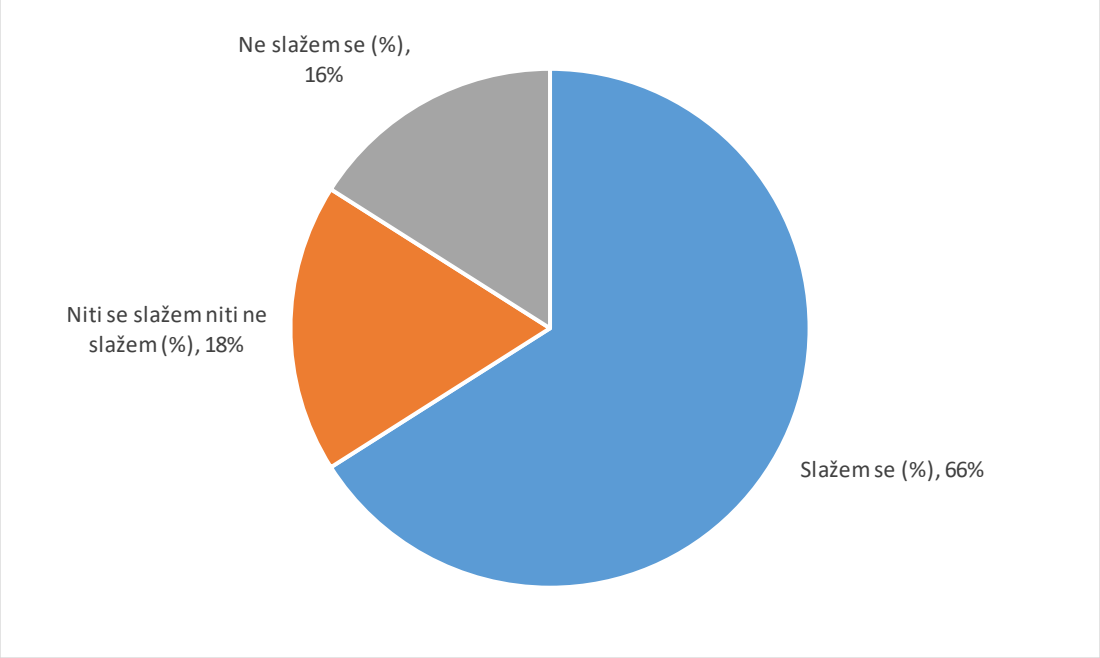
Sljedeći set pitanja odnosi se na specifične mjere nadzora zaposlenika, odnosno na zabrinutnost zaposlenika vezano za korištenje videonadzora u vozilima i praćenja internetskih komunikacija. Prema anketi, skoro dvije trećine ispitanika (64%) je zabrinuto zbog korištenja videonadzora u vozilima (Grafikon 2), kao i zbog praćenja internetskih komunikacija zaposlenika (66%) (Grafikon 3) .

Grafikon 2. U kojoj mjeri se slažete da vas zabrinjava korištenje videonadzora u vozilima?



Izvor: Autor završnog rada

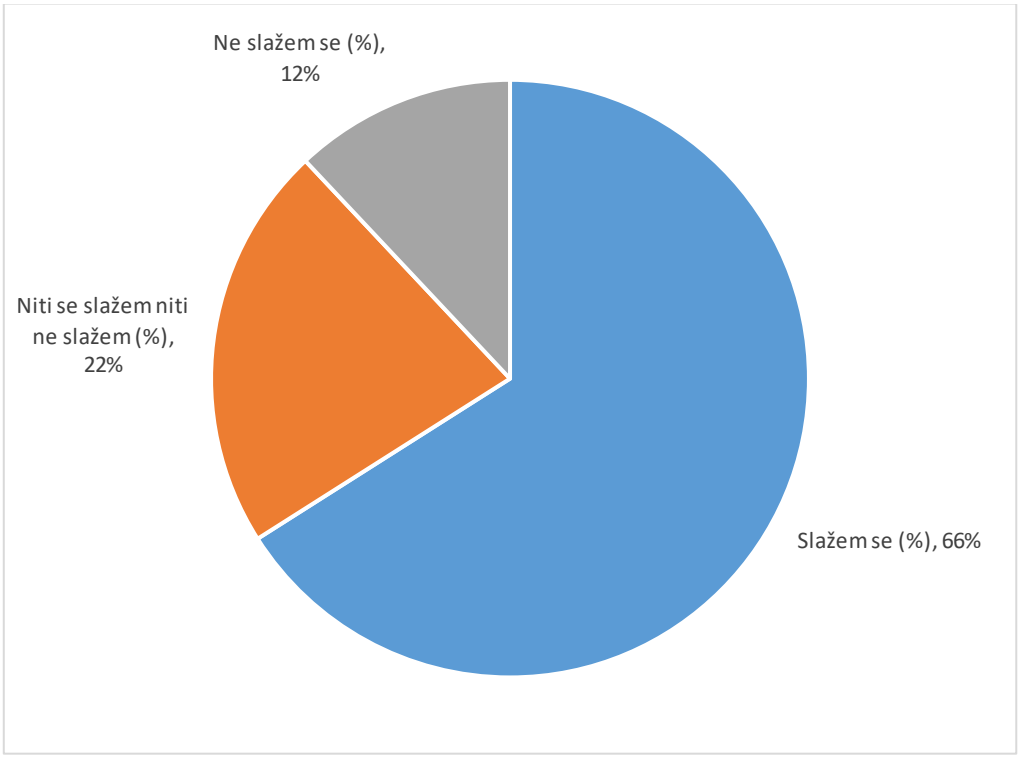
Grafikon 3. U kojoj mjeri se slažete da ste zabrinuti zbog praćenja internetskih komunikacija?



Izvor: Autor završnog rada

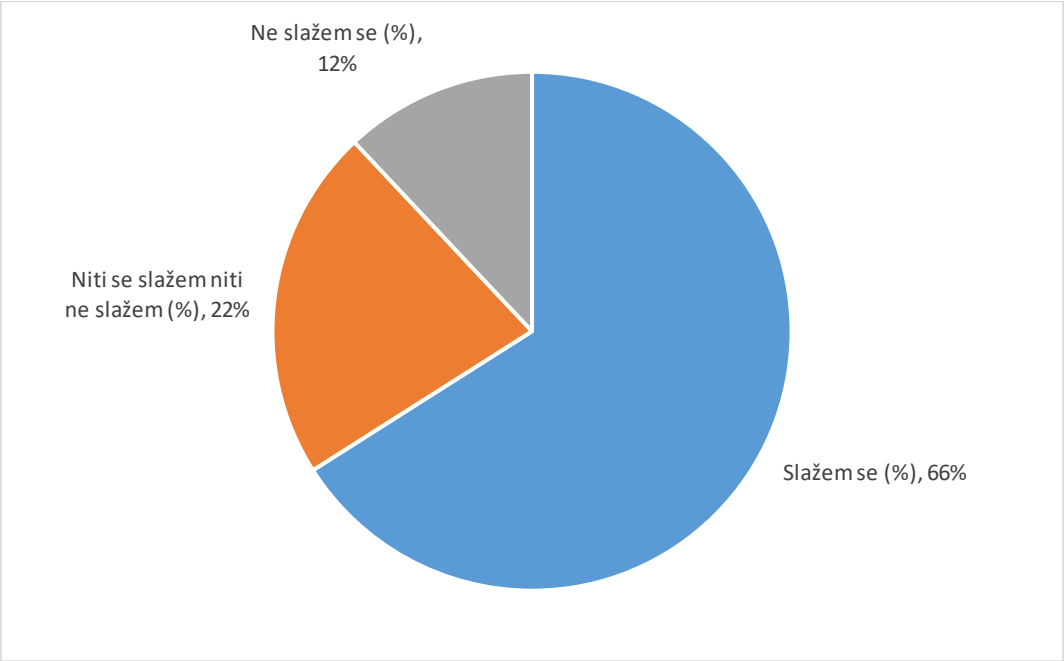
Što se tiče uticaja nadzora na privatnost i autonomiju, dvije trećine ispitanika su zabrinuti da nadzorne prakse narušavaju privatnost i autonomiju zaposlenika (66% u oba slučaja).

Grafikon 4. Koliko se slažete da ste zabrinuti da nadzorne prakse narušavaju vašu privatnost?



Izvor: Autor završnog rada

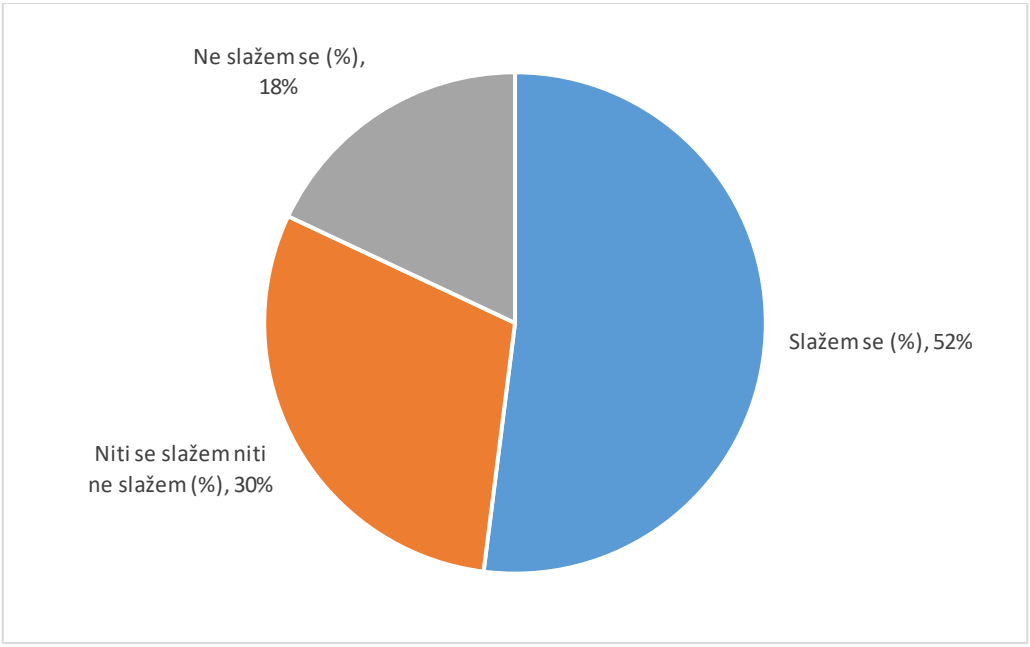
Grafikon 5. Koliko se slažete da ste zabrinuti da nadzorne prakse narušavaju vašu autonomiju?



Izvor: Autor završnog rada

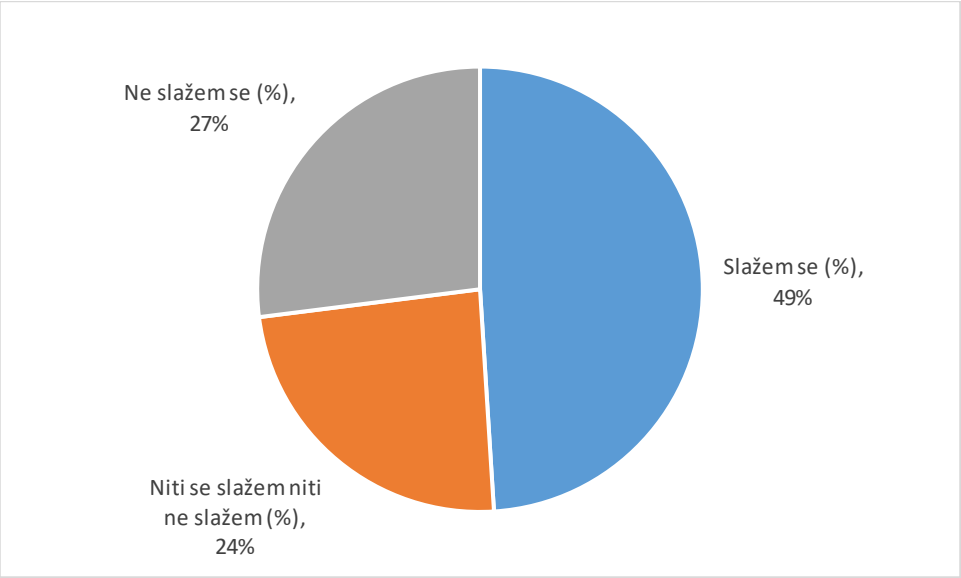
Što se tiče koristi od nadzora zaposlenika, više od pola ispitanika (52%) slaže se da prepoznaje koristi od nadzora za vlastitu sigurnost (Grafikon 5), dok nešto manje ispitanika se slaže da prepoznaje koristi nadzora za efikasnost operacija (49%) (Grafikon 6).

Grafikon 6. U kojoj mjeri se slažete da prepoznajete koristi od nadzora za vašu sigurnost?



Izvor: Autor završnog rada

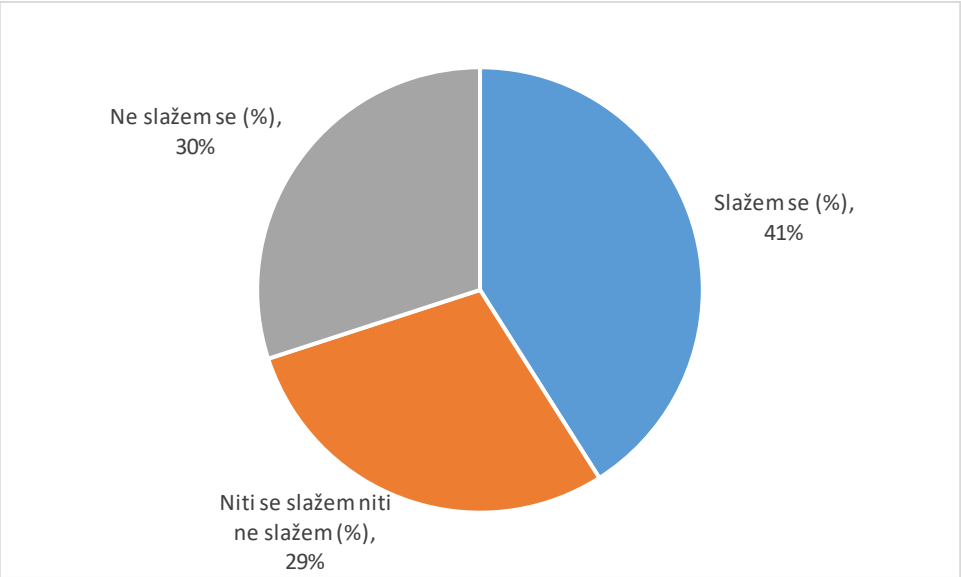
Grafikon 7. U kojoj mjeri se slažete da prepoznajete koristi od nadzora za efikasnost operacija?



Izvor: Autor završnog rada

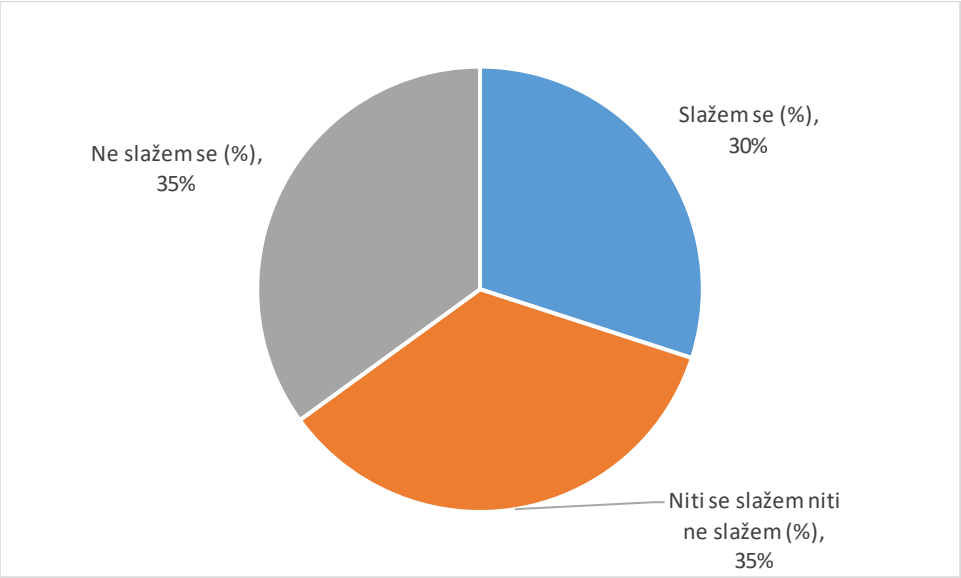
Što se tiče uticaja nadzora na moral i produktivnost, oko četiri od 10 ispitanika (41%) smatra da nadzor povećava njihovu anksioznost na radu (Grafikon 7), dok jedna trećina ispitanika (30%) smatra da nadzor utiče na njihovu produktivnost (Grafikon 8).

Grafikon 8. Koliko se slažete da nadzor povećava vašu anksioznost na radu?



Izvor: Autor završnog rada

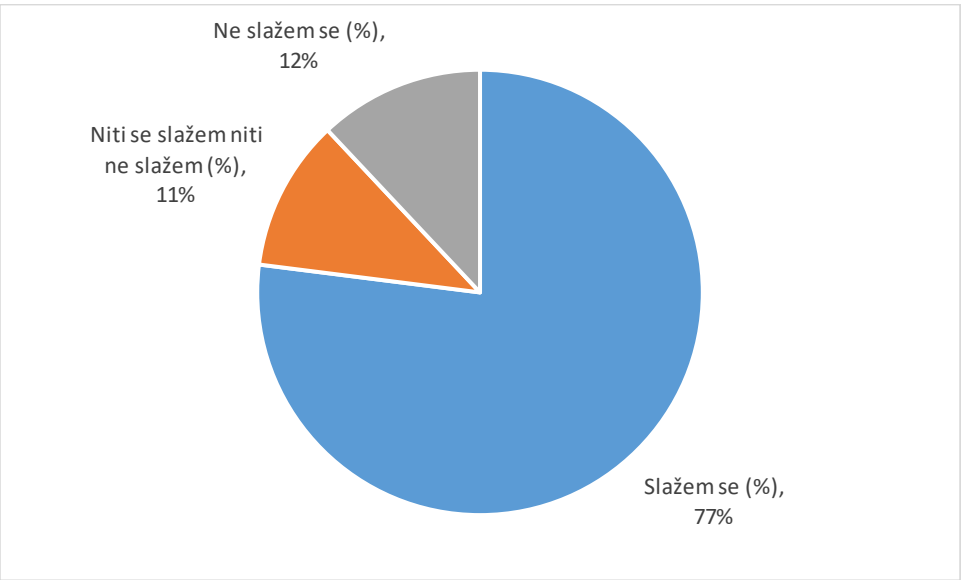
Grafikon 9. Koliko se slažete da nadzor utiče na vašu produktivnost?



Izvor: Autor završnog rada

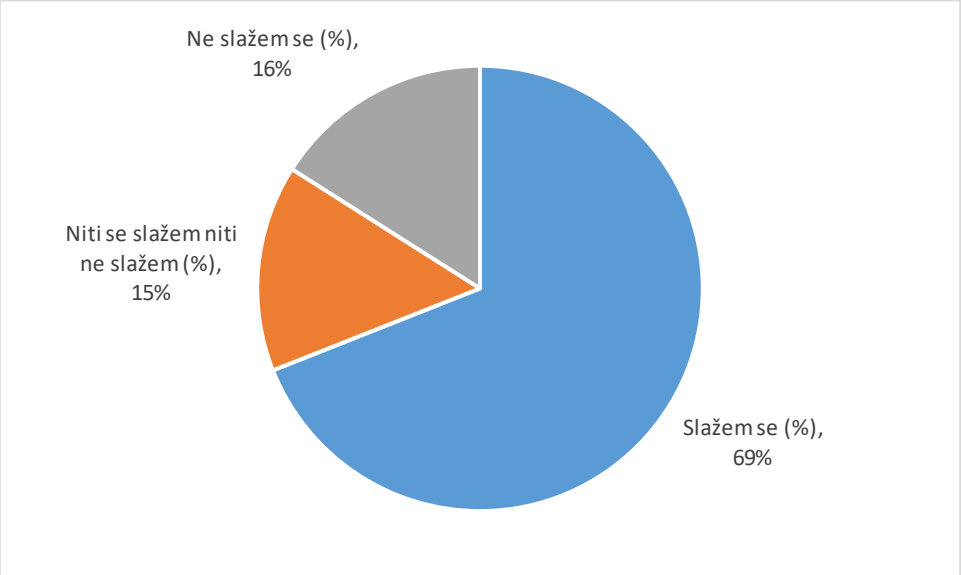
Velika većina ispitanika, odnosno skoro osam od 10 ispitanika (77%) je upoznato sa njihovim pravima u kontekstu nadzora na radu, dok više od dvije trećine ispitanika (69%) smatra da kompanija transparentno provodi nadzor.

Grafikon 10. U kojoj mjeri se slažete da ste upoznati s vašim pravima u kontekstu nadzora na radu?



Izvor: Autor završnog rada

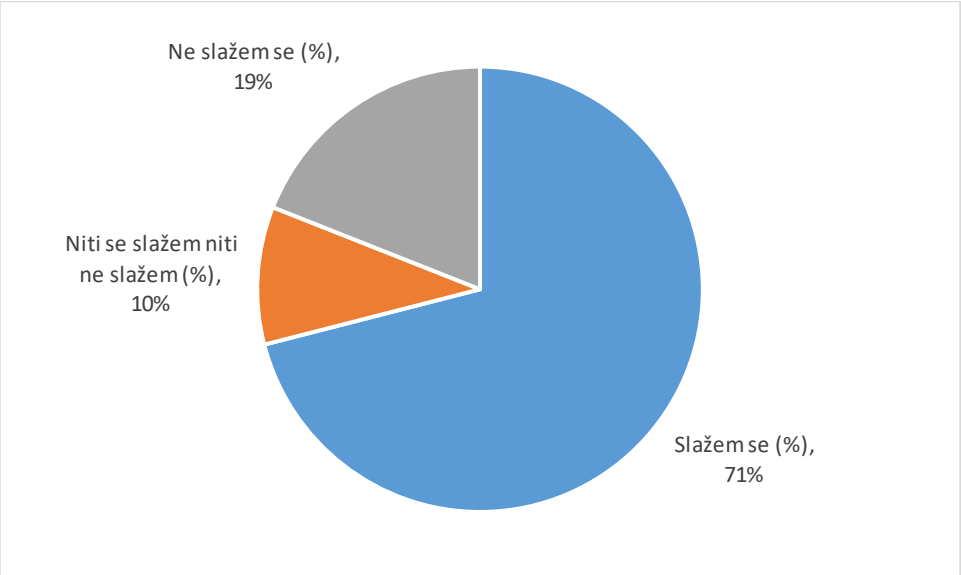
Grafikon 11. U kojoj mjeri se slažete da kompanija transparentno provodi nadzor?



Izvor: Autor završnog rada

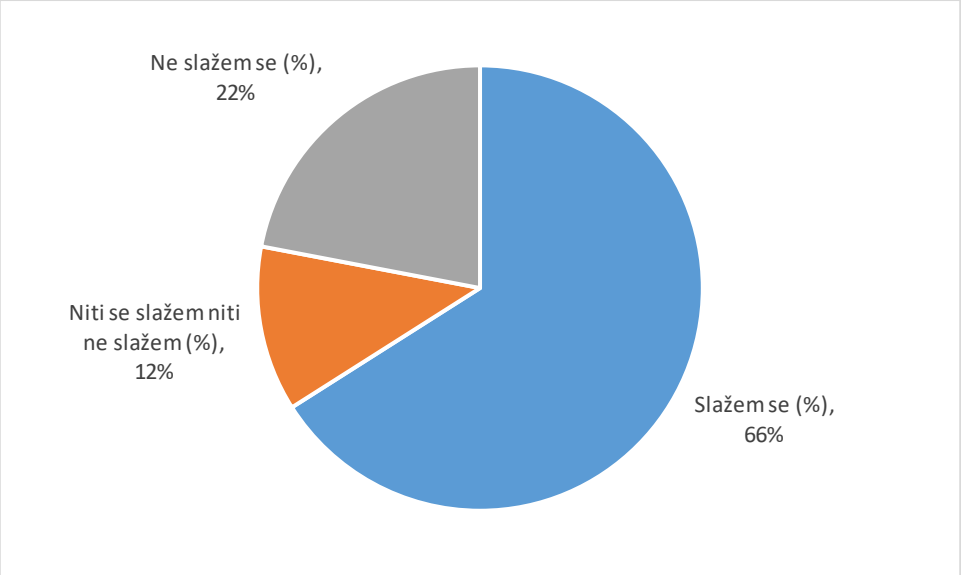
Iako su ispitanici zabrinuti praksama nadzora (Grafikon 2 i 3) većina (71%) njih se slaže da treba povećati transparentnost nadzornih praksi (Grafikon 11), a dvije trećine (66%) ispitanika se slaže da su trenutne politike nadzora kompanije Adriatic Metals adekvatne i jasne (Grafikon 12).

Grafikon 12. Koliko se slažete da kompanija treba povećati transparentnost nadzornih praksi?



Izvor: Autor završnog rada

Grafikon 13. Koliko se slažete da su trenutne politike nadzora adekvatne i jasne?



Izvor: Autor završnog rada

U konačnici, nadzor zaposlenika u Adriatic Metals možemo prikazati kroz sljedeće grupe odgovora:

Zabrinutost zbog invazivnosti:

Dvije trećine (66%)ispitanika izrazilo je zabrinutost zbog invazivnosti nadzora, posebno u kontekstu internetskih komunikacija i videonadzora u vozilima. Ova zabrinutost temelji se na strahu za privatnost i autonomiju, gdje zaposlenici osjećaju da njihov privatni prostor i sloboda postaju predmet neopravdanog nadzora. Posebno je istaknuta nelagoda s videonadzorom u vozilima, gdje su neki zaposlenici smatrali da to prelazi granice potrebne za sigurnost i ulazi u domenu ličnog prostora. Samo uvođenje videonadzora u vozila bio je jako osjetljiv projekat kompanija je napravila plan promjene i ipak uspjela radnicima objasniti korisnosti i dobiti njihov pristanak za obradu podataka, ali unatoč tome i dalje postoji velika usprotivljenost ovakvom obliku nadzora.

Priznavanje koristi:

Iako postoji izražena zabrinutost, više od pola (52%)ispitanika prepoznalo je koristi određenih oblika nadzora. Navedeno je da tehnologije poput videonadzora mogu povećati sigurnost na radnom mjestu i pridonijeti efikasnosti operacija. Ove odgovore je indicirala izvješta IT odjela koliko se u kompaniji internet prometa potroši na društvene mreže i ostale sadžaje ovog tipa, oko 50%. Međutim, postoji nuansa u prihvaćanju ovih koristi, s komentarima koji ukazuju na to da videonadzor u vozilima možda nije potreban ili je pretjeran.

Povećana anksioznost:

Oko 41% zaposlenika izvijestilo je o povećanoj anksioznosti i smanjenju morala, što se izravno povezuje s pojačanim nadzorom. Anksioznost i smanjenje morala mogu biti rezultat osjećaja da su stalno promatrani i procjenjivani, što dovodi do psihološke nelagode i potencijalno smanjuje otvorenost i kreativnost u radu.

Prilagodba na nadzor:

S druge strane, 55% ispitanika adaptiralo se na nadzorne prakse, ne osjećajući značajan utjecaj na svoju produktivnost ili zadovoljstvo poslom. Ovaj podatak sugerira da postoji segment zaposlenika koji može prihvatiti nadzor kao dio radnog okruženja, posebice ako vjeruju da doprinosi njihovoj sigurnosti ili je adekvatno obrazložen. Ovaj podatak također treba uzeti u obzir da pedest posto radne snage su novouposleni, koji se još nisu priviknuli na ovakav sistem nadzora.

Svijest o pravima:

Skoro 8 od 10 ispitanika (77%) svjesno je potrebe za jasnim pravnim i etičkim smjernicama koje reguliraju nadzorne prakse. Ova visoka razina svijesti ukazuje na to da zaposlenici očekuju da će njihova prava biti zaštićena i da postoji sistem koji regulira kako i kada se nadzor može provoditi. Pravo na privatnost istaknuto je kao primarno područje zabrinutosti.

Potreba za transparentnošću:

Više od dvije trećine ispitanika (69%) izrazilo je potrebu za većom transparentnošću u implementaciji nadzornih tehnologija. Transparentnost se vidi kao ključ za smanjenje anksioznosti i povećanje prihvaćanja nadzora. Zaposlenici žele jasne politike koje objašnjavaju svrhu, opseg i ograničenja nadzora, kao i informacije o tome kako se njihovi podaci koriste i štite. Iako je kompanija poduzela i napravila planove promjene svaku put kada je uvodila neki vid nadzora, ipak vidimo potrebu za jakom transparentnosti ovih oblika nadzora.

Preporuke koje su rezultat istraživanja odnose se na:

- Povećanje transparentnosti:
    - Jasne politike: Adriatic Metals treba formulirati jasne politike koje detaljno objašnjavaju svrhu, opseg i ograničenja svih oblika nadzora, kao i informacije o tome kako i gdje se podaci koriste i čuvaju.
    - Komunikacija s zaposlenicima: Redovito i otvoreno komunicirati s zaposlenicima o svim pitanjima vezanim uz nadzor, uključujući uvođenje novih tehnologija, kako bi se smanjila anksioznost i izgradilo povjerenje.Impementirati određeni izvještaj koji će se slati na svakih 60 dana kako radnici bili informirani.

- Podizanje svijesti o pravima:
    - Edukacija zaposlenika: Organizirati redovne edukativne sesije o pravima zaposlenika i obvezama poslodavca vezanim za nadzor, kako bi se povećala svijest i razumijevanje također uključit ovaj tip edukacije kao dio probnog perioda svakog zaposlenika.

- Sudjelovanje zaposlenika: Uključiti zaposlenike u proces donošenja odluka o nadzornim praksama, možda kroz ankete ili fokus grupe, kako bi se osiguralo da njihovi glasovi budu čuti. Ovo treba uraditi kroz instutu vijeća uposlenika jer kompanija ima uspostavljeno vijeće uposlenika.

- Pravni pregled i usklađivanje:
    - Usklađivanje s pravnom regulativom: Redovito pregledavati i ažurirati nadzorne prakse kako bi bile u skladu s lokalnim, nacionalnim i međunarodnim zakonima o privatnosti i radnim pravima.Zbog specifičnosti kompanije koja posluje u međunarodnom okruženju a osobito zbog razloga da dijeli podatke van granica Evrope.

7. ZAKLJUČAK

Održavanje sigurnog i učinkovitog radnog mjesta zahtijeva od kompanija da budno prate aktivnosti zaposlenika, koje bi mogle naštetiti drugima ili stvoriti odgovornost za kompanije. Jedan od načina da kompanija održi učinkovitost i smanji odgovornost je da poslodavac nadzire svoje zaposlenike. Praćenje je, međutim, samo prvi korak. Zaposlenici moraju biti educirani o praćenju kako bi razumjeli nedostatak privatnosti koji trenutno postoji na poslu.

Zaposlenici moraju biti educirani da razumiju kako tehnologija funkcionira, da razumiju mogućnosti i ograničenja. Poslodavci koji nadziru moraju biti odgovorni i razumni. Poslodavci moraju objasniti radnicima što nadziru. Mora postojati disciplinski plan za kažnjavanje zaposlenika za kršenje pravila korištenja računara. Dok zakon polako sustiže tehnologiju, mnoga pitanja ostaju. Zagovornici privatnosti vjerojatno će nastaviti snažno insistirati na nužnimi očekivanim reformama koje bi ponudile veću zaštitu zaposlenika. Ako je historija sudac, ovi napori vjerojatno neće uspjeti. Opravdano je očekivati da će pravni okvir biti takav da će kompanijama, pa čak i vladi, dati dodatnu dozvolu za praćenje više aspekata svakodnevnog života svakog građanina, unutar i izvan radnog mjesta. Kompanije će morati aktivno obučavati zaposlenike da isprave probleme i pogrešne percepcije koje trenutno postoje s korištenjem računara zaposlenika. Većina teoretičara i praktičara iz područja prava, ali i iz područja menadžmenta, saglasna je sa stavom da akokompanija mora nadzirati aktivnosti svojih zaposlenika kako bi stvorila sigurno radno okruženje, neka tako i bude.

Iako neki ljudi i kompanije vjeruju da je praćenje zaposlenika pogrešno ili neetično, postoji jasna potreba za takvom praksom. Praćenje zaposlenika je tu da ostane. Status nadzora zaposlenika može se promijeniti ako se promijene i pravna rješenja u skladu sa izazovima i zahtjevimakoje nameće razvoj tehnologije, akoji je u stalnom mijenjanju - ali i bez obzira na navedene promjene, moguće je zaključiti - na osnovi provedenih analiza dostupnih akademskih članaka i studija - da nadzor zaposlenika neće nestati.

U radu je detaljno analiziran pravni okvir nadzora zaposlenika u Evropskoj uniji i Bosni i Hercegovini. Uz navedeno, sistematično suprikazani relevantni pravni dokumentikoji su zastupljeni u svim pojedinačnim zemljama Evropske unije (uzimajući u obzir i Norvešku i Veliku Britaniju), same specifičnosti svake o zemalja Evropske unije, te ograničenja korištenja nadzora zaposlenika. Na osnovu navedenoga potvđena je glavna hipoteza ovog završnog rada, odnosno da pravni okvir u Evropskoj uniji koji regulira pitanja nadzora zaposlenika, adekvatno štiti prava zaposlenika. Pored navedenoga, u funkciji postavljene izvedene i pomoćne hipoteze, u radu su analizirani i proučavani pravni okvir nadzora zaposlenika u Bosni i Hercegovini, te odredbe Zakona o zaštiti ličnih podataka Bosne i Hercegovine, kojima su jasno određeni načini i mogućnosti nadzora zaposlenika u Bosni i Hercegovini.

Nadalje, potvrđena je i izvedena hipoteza ovog završnog rada, odnosno da su tehnološka rješenja često u koliziji sa važećim pozitivno-pravnim propisima i praksama, pa je u skladu s tim u savremenim uvjetima poslovanja nužno naći pravu ravnotežu između prava zaposlenika, na jednoj i prava nadzora od strane poslodavca, na drugoj strani, uz nužno uvažavanje etičkih principa. Obzirom da nisu ograničena birokratskim procedurama, tehnološka rješenja su u većini slučajeva uvijek "ispred" pozitivno-pravnih propisa koji moraju da „prate“ tehnološki razvoj kako bi uspjeli da reguliraju sve aspekte neophodne za svakodnevni nesmetani rad zaposlenika. Naravno, pri tome se mora u obzir uzeti etika, odnosno uvažavati etički principi, naročito u poslovanju.

U konačnici, pomoćna hipoteza je potvrđena jer se analizom u radu potvrdilo da su odnosi u pravu Evropske unije prema pitanju prava zaposlenika, na jednoj i pravu nadzora od strane poslodavca, na drugoj strani na višoj razini razvoja nego u Bosni i Hercegovini. U Bosni i Hercegovini nadzor zaposlenika reguliran je Zakonom o zaštiti ličnih podataka. Imajući u vidu da je u Evropskoj uniji segment nadzora zaposlenika dosta detaljnijeg obuhvata, a uvažavajući činjenicu da je Bosna i Hercegovina zemlja kandidat za pristupanje Evropskoj uniji, nužna su sveobuhvatna usklađivanja postojećeg zakonodavstva u skladu sa najboljim praksama Evrospke unije. U Izvještaju o Bosni i Hercegovini za 2023. uz dokument Saopštenje Komisije Evropskom parlamentu, Vijeću, Evropskom ekonomskom i socijalnom odboru i Odboru regija (Brisel, 8.11.2023. SWD (2023) 691 final) navodi se da: "Zakoni o radu, koji su na snazi na entitetskom nivou i u Brčko distriktu, primjenjuju se na sve zaposlene osim na državne službenike, i garantuju minimalni nivo zaštite prava zaposlenih. Da bi se u potpunosti ispunili standardi EU, trebalo bi dodatno poboljšati pravni okvir, naročito u pogledu zaštite radnika od diskriminacije. (...) Zakoni o radu i dalje se ne provode

na odgovarajući način, naročito kada su u pitanju socijalni dijalog, zaštita radnika i inspekcije rada. Nedostaci u zakonima o radu koji se odnose na upravljanje krizama, postali su očigledni tokom pandemije COVID-19. Na primjer, radnom zakonodavstvu generalno nedostaju odredbe za rad na daljinu i odredbe za organizaciju rada u vanrednim situacijama."[12] Opravdano je zaključiti da ni područje nadzora zaposlenika i prava zaposlenika i prava poslodavaca, nije izuzetak.

Najvažniji regulativni okvir za zaštitu podataka u Evropskoj unije je GDPR koji postavlja stroge zahtjeve za obradu ličnih podataka zaposlenika, uključujući potrebu za jasnim pravnim osnovama za obradu, obavezu informiranja zaposlenika o nadzoru, te prava zaposlenika da pristupe svojim podacima i traže njihovo brisanje. Također, GDPR i nacionalni zakoni članica EU detaljno regulišu nadzor na radnom mjestu, uključujući video nadzor, praćenje e-mailova, internet aktivnosti i drugih oblika digitalnog nadzora. Pravila su stroga, a poslodavci moraju dokazati nužnost i proporcionalnost svake vrste nadzora, dok postojeća pravna regulativa u Bosni i Hercegovini nije detaljna i sveobuhvatna, što kao nužnost proizilazi iz analize pravnih rješenja i praksi na nivou zemalja članica Evropske unije.

Rezultati istraživanja jasno ukazuju na to da zaposlenici Adriatic Metals imaju miješane osjećaje o nadzornim praksama unutar kompanije. Dok postoji priznanje potencijalnih koristi od nadzora u smislu sigurnosti i efikasnosti, zabrinutost za invazivnost, posebno u vezi s praćenjem internetskih komunikacija i videonadzora u vozilima, ostaje visoka. Anksioznost i smanjenje morala kod značajnog dijela zaposlenika ukazuju na negativne posljedice koje nadzor može imati na radnu atmosferu. Istovremeno, postoji visok stepen svijesti o pravima i potrebi za transparentnim i etičkim nadzornim praksama.

[12] Izvještaj o Bosni i Hercegovini za 2023. uz dokument Saopštenje Komisije Evropskom parlamentu, Vijeću, Evropskom ekonomskom i socijalnom odboru i Odboru regija (Brisel, 8.11.2023. SWD(2023) 691final)(str.102)
https://www.eeas.europa.eu/sites/default/files/documents/2023/Izvje%C5%A1taj%20o%20Bosni%20i%20Hercegovini%20za%202023.%20%20-%20BHS%20prijevod%20%28002%29.pdf

REFERENCE

1. Aasheim, L. L. (2012). *Practical clinical supervision for counselors: An experiential guide*. New York: Springer Pub.
2. Abraha, H.H., (2022). A pragmatic compromise? The role of Article 88 GDPR in upholding privacy in the workplace. *International Data Privacy Law, 12*(4), pp.276-296
3. Aitkenhead, M., (2023) Workplace Survei l lance Policy *Workplace surveillance-1.0 Policy Statement*.
4. Aladağ, M., & Kemer, G. (2016). Clinical supervision: An emerging counseling specialty in Turkey. *The Clinical Supervisor*, 35(2), 175-191.
5. Alder, G. S. (1998). Ethical issues in electronic performance monitoring: A consideration of deontological and teleological perspectives. *Journal of Business Ethics*, 17(7), 729-743.
6. Alexi, E. (2008). T*he Law Requires Email Archiving*. IT Solutions, Tangent Inc
7. Aloisi, A. &Gramano, E., (2019). Artificial intelligence is watching you at work: Digital surveillance, employee monitoring, and regulatory issues in the EU context. *Comp. Lab. L. &Pol'y J*., 41, p.95.
8. American Counseling Association (2014). *The ACA Code of Ethics*. Retrieved from https://www.counseling.org/resources/aca-code-of-ethics.pdf
9. American Management Association (2008). *2007 Electronic Monitoring & Surveillance Survey*, Retrieved Feb 28, 2008, from http://press.amanet.org/press-releases/177/2007-electronicmonitoring-surveillance-survey/
10. American Psychological Association. (2015). Guidelines for clinical supervision in health service psychology. *American Psychologist*, 70(1), 33-46.
11. Anteby, M., & Chan, C.K. (2018). A Self-Fulfilling Cycle of Coercive Surveillance: Workers' Invisibility Practices and Managerial Justification. *Organization Science*, 29(2): 247-263.
12. Antović and Mirković v. Montenegro, *zahtjev br. 70838/13, presuda 28.11.2017* (dostupno na: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22002-11757%22]}) (Pristupljeno: 16.12.2023)
13. Atik, Z. (2017). Evaluations of psychological counselor candidates on individual counseling and supervision. Hacettepe University, Ankara.
14. Attewell, P. (1987). The deskilling controversy. *Work and occupations*, 14(3), 323-346.
15. Azevedo, F. M. (2018), 'GPS – meio de vigilância à distância e a suarepercussão no direito à reserva da intimidade da vidaprivada do trabalhador', *RevistaJulgar Online*, March.
16. Baase, S. (2012). *A gift of fire*. Pearson Education Limited.
17. Baek, T. H., & Morimoto, M. (2012). Stay away from me. *Journal of Advertising*, 41(1), 59–76. https://doi.org/10.2753/JOA0091-3367410105

18. Ball, K. (2010). Workplace surveillance: An overview. *Labor History*, 51(1), 87-106.
19. Ball, K. (2021), *Electronic Monitoring and Surveillance in the Workplace*, Publications Office of the European Union, Luxembourg, ISBN 978-92-76-43340-8, doi:10.2760/5137, JRC125716.
20. Bărbulescu v. Romania, *zahtjev br. 61496/08, presuda 5.9.2017* (dostupno na: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-183019%22]}) (Pristupljeno: 16.12.2023)
21. Beniger, J. (1989). *The Control Revolution: Technological and Economic Origins of the Information Society*. Cambridge, MA: Harvard University Press.
22. Bernard, J. M., & Goodyear, R. K. (1998). *Fundamentals of clinical supervision* (2nd ed.). Allyn & Bacon.
23. Bernstein, E.S. (2012). The Transparency Paradox: A Role for Privacy in Organizational Learning and Operational Control. *Administrative Science Quarterly*, 57(2), 181-216.
24. Bezek, P.J., & Britton, S.M. (2001). Employer Monitoring Of Employee Internet Use And EMail: MEALEY'S *Cyber Tech Litigation Report*, 2, Retrieved April 7, 2009, from http://www.foleybezek.com/art.InternetFile.pdf

147. Bezek, P.J., & Britton, S.M. (2001). Employer Monitoring Of Employee Internet Use And EMail: MEALEY'S *Cyber Tech Litigation Report*, 2, dostupno na: http://www.foleybezek.com/art.InternetFile.pdf(Pristupljeno: 12.12.2023).

25. Bhatt, G. D. (2000). Organizing knowledge in the knowledge development cycle. *Journal of Knowledge Management*, 4, 15-26.
26. Bhatt, G. D. (2001). Organizing knowledge in the knowledge development cycle. *Journal of Knowledge Management*, 4, 15-26.
27. Borders, L. D., Cashwell, C. S., & Rotter, J. P. (1995). Supervision of Counselor Licensure Applicants: A Comparative Study. Journal of Chemical Information and Modeling, (35), 54–69.
28. Bråten, M. and Tranvik, T. (2017), 'The visible employee – Technological governance and control of the mobile workforce', *Socio-Economic Studies*, Vol. 28, No. 3, pp. 319–337.
29. Braverman, H. (1998). *Labor and Monopoly Capital: The Degradation of Work in the Twentieth Century*. New York, NY: NYU Press.
30. Bronowicka, J., Ivanova, M., Klicki, W., King, S., Kocher, E., Kubisa, J. and Zielińska, J., (2020) 'Game that you can't win'? *Workplace Surveillance in Germany and Poland*.
31. Business Insider (2020), "*Companies are using webcams to monitor employees working from home"*, 23 March.
32. Bygrave, L. A. (2002). Data Protection Law: Approaching Its Rationale, *Logic and Limits*. Information Law Series.
33. Camerini, X., (2021). The topic of video surveillance and its countless repercussions. *European Journal of Privacy Law & Technologies*.

34. Campbell, J. M. (2000). *Becoming an effective supervisor: A workbook for counselor and psychotherapist*. USA: Routledge
35. Canteiro, P. (2017), 'As redes sociais e a des(proteção) da privacidade do trabalhador', conference paper, O Direito do Trabalho e as Empresas: Novosdesafios, Novas Soluções?, *Atas do IX Congresso Internacional de CiênciasJurídico-Empresariais,* 10 October 2017, Escola Superior de Tecnologia e Gestão de Leiria, Portugal.
36. Carayon, P. (1993). Effects of electronic performance monitoring on job design and worker stress: Review of the literature and conceptual model. *Human Factors*, 35 pp. 385–395.
37. Casilli, A. A. (2019), *En attendant les robots: Enquête sur le travail du clic*, Seuil, Paris.
38. Cate, F. H., & Mayer-Schönberger, V. (2013). Notice and consent in a world of Big Data. *International Data Privacy Law*, 3(2), 67-73.
39. Chaloner, C. (2007). An introduction to ethics in nursing. Nursing standard, 21(32).
40. Chory, R. M., Vela, L. E. and Avtgis, T. A. (2016), 'Organizational surveillance of computer-mediated workplace communication: Employee privacy concerns and responses', *Employee Responsibilities and Rights Journal*, Vol. 28, pp. 23–43.
41. Chrysochou, C. and Iglezakis, I., (2019) Employees' Protection: Workplace Surveillance 3.0. In *Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications* (pp. 1329-1348). IGI Global.
42. Conry-Murray, A. (2001). 'Special Report – The Pros and Cons of Employee Surveillance' (2001), *Network Magazine*. February 5, 2001, http://www.networkmagazine.com/article/NMG20010125S0011.
43. Copland v. the United Kingdom, *zahtjev br. 62617/00, presuda 3.4.2007* (dostupno na: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22002-2765%22]}) (Pristupljeno: 16.12.2023)
44. Council Directive 2000/78/EC of 27 November 2000 establishing a general framework for equal treatment in employment and occupation *OJ L 303, 2.12.2000, p. 16–22* (dostupno na: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32000L0078) (Pristupljeno: 15.12.2023)
45. Council Directive 2003/88/EC of the European Parliament and of the Council of 4 November 2003 concerning certain aspects of the organisation of working time *OJ L 299, 18.11.2003, p. 9–19* (dostupno na: https://eur-lex.europa.eu/eli/dir/2003/88/oj) (Pristupljeno: 15.12.2023)
46. Council Directive 2006/54/EC of the European Parliament and of the Council of 5 July 2006 on the implementation of the principle of equal opportunities and equal treatment of men and women in matters of employment and occupation (recast) *OJ L 204, 26.7.2006, p. 23–36* (dostupno na: https://eur-lex.europa.eu/eli/dir/2006/54/oj) (Pristupljeno: 15.12.2023)
47. Council Directive 89/391/EEC of 12 June 1989 on the introduction of measures to encourage improvements in the safety and health of workers at work *OJ L 183,*

29.6.1989, p. 1–8 (dostupno na: https://eur-lex.europa.eu/eli/dir/1989/391/oj) (Pristupljeno: 15.12.2023)
48. Council Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data *OJ L 281, 23.11.1995, p. 31–50* (dostupno na: https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:31995L0046 (Pristupljeno: 14.12.2023)
49. Council of Europe. (1950). ETS 5 - *Convention for the Protection of Human Rights and Fundamental Freedoms* (distupno na: https://rm.coe.int/1680063765 (Pristupljeno: 13.12.2023)
50. Court, L., & Warmington, C. (2004). The workplace privacy myth: why electronic monitoring is here to stay. *Employment and Labor Law*, 1(1), 1-20.
51. Dash, A. (2014). "What is Public?" *Medium*, July 24, 2014. https://medium.com/message/f33b16d780f9
52. De Stefano, V. and Wouters, M., (2022). AI and digital tools in workplace management and evaluation: An assessment of the EU's legal framework. *Osgoode Legal Studies Research Paper Forthcoming*.
53. Dean, R. G., & Rhodes, M. L. (1992). Ethical-clinical tensions in clinical practice. *Social Work*, 37(2), 128-132.
54. Deloitte (2019), Undersøkelse om overvåking: Tyderpåmanglenderetningslinjerinorskevirksomheter – *Elektroniskovervåkninginorskevirksomheten*, web page, accessed 30 September 2020.
55. DRI (European Digital Rights Initiative). (2020). *Annual Report on Digital Rights and Surveillance*.
56. Ebert, I., Wildhaber, I. and Adams-Prassl, J., (2021). Big Data in the workplace: Privacy Due Diligence as a human rights-based approach to employee privacy protection. *Big Data & Society*, *8*(1), p.20539517211013051.
57. Ellis, M. V. (2006). Critical incidents in clinical supervision and in supervisor supervision: Assessing supervisory issues. *Training and Education in Professional Psychology*, S, 122–132.
58. Erdemir, E. (2008). New Dimension of Labor Relations in the Information Society: Commercial and Condition Monitoring Activities in Turkey and Employee-oriented, *1st National Labor Relations Congress*, 6-8 November 2008, Sakarya University, Proceedings
59. Erickson Cornish, J. A. (2014). Ethical issues in education and training. *Training and Education in Professional Psychology*, 8(4), 197-200.
60. Eurofound (2020*), Employee monitoring and surveillance: The challenges of digitalisation*, Publications Office of the European Union, Luxembourg.
61. Eurofound (2020b), Regulations to address work–life balance in digital flexible working arrangements, *New forms of employment series*, Publications Office of the European Union, Luxembourg.

62. Eurofound (2020c), Telework and ICT-based mobile work: Flexible working in the digital age, *New forms of employment series*, Publications Office of the European Union, Luxembourg.
63. European Commission. (2017). Article 29 17/EN WP 249 - *Opinion 2/2017 on data processing at work* (dostupno na: https://ec.europa.eu/newsroom/article29/redirection/document/45631 (Pristupljeno:13.12.2023).
64. European Parliament (2019), *Health and safety in the workplace of the future, Directorate*-General for Internal Policies of the Union, Brussels.
65. European Parliament. (2016). Regulation 2016/679 - *Protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Direct*ive 95/46/EC (General Data Protection Regulation, dostupno na: https://www.eumonitor.eu/9353000/1/j9vvik7m1c3gyxp/vk3sygzz13zi(Pristupljeno : 12.12.2023).
66. Falender, C. A., & Shafranske, E. P. (2004). *Clinical supervision.* John Wiley & Sons, Inc
67. Fernandez, V and Gallardo-Gallardo, E (2020) Tackling the HR digitalization challenge: key factors and barriers to HR analytics adoption C*ompetitiveness Review* 10.1108/CR-12-2019-0163
68. Findlay, P., & McKinlay, A. (2003). Surveillance, electronic communications technologies and regulation. *Industrial Relations Journal*, 34(4), 305-318.
69. Florindo De Almeida Vasconcelos Gramaxo v Portugal, *zahtjev br. 26968/16* (dostupno na: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22002-13935%22]}) (Pristupljeno: 16.12.2023)
70. Forbes (2017), '*How to drive employee engagement with workplace gamification'*, 28 November.
71. Fowler, G.A. (2019). *The spy in your wallet: Credit cards have a privacy problem*. The Washington Post, August 26. Retrieved from https://beta.washingtonpost.com/technology/2019/08/26/spyyour-wallet-credit-cards-haveprivacy-problem/
72. Glosoff, H. L., Renfro-Michel, E., & Nagarajan, S. (2016). Ethical issues related to the use of technology in clinical supervision. In T. Rousmaniere & E. RenfroMichel (Eds.), *Using technology to enhance clinical supervision*, (pp. 31–46). Alexandria, VA: American Counseling Association.
73. Grant, J., Schofield, M. J., & Crawford, S. (2012). Managing difficulties in supervision: Supervisors' perspectives. *Journal of counseling psychology*, 59(4), 528.
74. Gumzej, N. and Dragicevic, D., 2019. Video Surveillance in the Workplace Under the Croatian Act on Implementation of the General Data Protection Regulation. *Zbornik PFZ, 69*

75. Harmon, A. (2019). *As Cameras Track Detroit's Residents, a Debate Ensues Over Racial Bias.* The New York Times, July 8. Retrieved from https://www.nytimes.com/2019/07/08/us/detroit-facial-recognition-cameras.html
76. Harris, D., O'Boyle, M., Warbrick C.: Law of the European Convention on Human Rights, Third edition, Oxford, University Press, 2014.
77. Hart, G., Borders, L. D., Nance, D., & Paradise, L. (1995). Ethical guidelines for counseling supervisors. *Counselor Education and Supervision*, 34(3), 270-276.
78. Hartman, Laura Pincus: 1998, 'The Rights and Wrongs of Workplace Snooping', *Journal of Business Strategy* 19(3) (May–June), 16(4).
79. Hintz, A., Dencik, L., & Wahl-Jorgensen, K. (2018). *Digital citizenship in a datafied society.* John Wiley & Sons.
80. Hofstede, G. (2001). *Culture's consequences: Comparing values, behaviors, institutions, and organizations across nations*. Sage publications
81. Holland, P. and Tham, T.L., (2020) Total surveillance: electronic monitoring and surveillance in the 21st century. In *Contemporary Work and the Future of Employment in Developed Countries* (pp. 135-150). Routledge.
82. Igo, S. (2018). *The Known Citizen: A History of Privacy in Modern America.* Cambridge MA: Harvard University Press.
83. INSHT (Instituto Nacional de Seguridad e Higiene en el Trabajo) (2015), *Estrategia Española de Seguridad y Salud en el Trabajo* 2015–2020, Madrid.
84. *Izvještaj o Bosni i Hercegovini za 2023.* uz dokument Saopštenje Komisije Evropskom parlamentu, Vijeću, Evropskom ekonomskom i socijalnom odboru i Odboru regija (Brisel, 8.11.2023. SWD(2023) 691final)
85. *Izvještaj o Bosni i Hercegovini za 2023*. uz dokument Saopštenje Komisije Evropskom parlamentu, Vijeću, Evropskom ekonomskom i socijalnom odboru i Odboru regija (Brisel, 8.11.2023. SWD(2023) 691final)
86. Johnson, D. (2001). *Computer Ethics* (Prentice- Hall, Inc., New Jersey).
87. Johnson, R. (2010). *Employee Perspectives on Electronic Monitoring: Benefits and Challenges.* DEF Publishers
88. Koçyiğit M.. (2022). Challenges and Ethical Issues in Counseling Supervision from Faculty Supervisors' Perspective. *Participatory Educational Research.* 9. 305-329. 10.17275.
89. Koçyiğit Özyiğit, M. (2019). *An investigation of group supervision process of individual Counseling Practice course: A Case Study*. Ege University, Turkey
90. Kuner, C., Cate, F. H., Millard, C., & Svantesson, D. J. B. (2013). PRISM and privacy: will this change everything?. *International Data Privacy Law*, 3(4), 217-219.
91. Kwet, M. (2019). In Stores, *Secret Surveillance Tracks Your Every Move*. The New York Times, 14 June. https://www.nytimes.com/interactive/2019/06/14/opinion/bluetooth-wirelesstracking-privacy.html

92. Ladany, N. (2002). P*sychotherapy supervision: How dressed is the emperor*? Psychotherapy Bulletin, 37, 14–18.
93. Lee, R. W., & Cashwell, C. S. (2002). Ethical issues in counseling supervision: A comparison of university and site supervisors. *The Clinical Supervisor*, 20(2), 91-100
94. Lei n.º 58/2019, de 8 de agosto (dostupno na: https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?artigo_id=3118A0002&nid=3118&tabela=leis&pagina=1&ficha=1&so_miolo=&nversao=) (Pristupljeno: 15.12.2023)
95. Lei n.º 7/2009, de 12 de fevereiro (dostupno na: https://diariodarepublica.pt/dr/detalhe/lei/7-2009-602073) (Pristupljeno: 15.12.2023)
96. Levy, K., & Barocas, S. (2018). Privacy at the Margins| refractive surveillance: Monitoring customers to manage workers. *International Journal of Communication*, 12, 23.
97. Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles (dostupno na: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037085952) (Pristupljeno: 15.12.2023)
98. López Ribalda and Others v. Spain, *zahtjev br. 1874/13 i 8567/13, presuda, 17.10.2019* (dostupno na: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-197098%22]}) (Pristupljeno: 16.12.2023)
99. Lyon, D. (2015). Surveillance, Snowden, and *Big Data: Capacities, consequences, critique*. Big Data & Society.
100. Macnish, K. (2014). *Just surveillance? Towards a normative theory of surveillance*. Surveillance & Society, 12(1), 142-153.
101. Mantello, P., Ho, M.T., Nguyen, M.H. and Vuong, Q.H., (2023). Bosses without a heart: socio-demographic and cross-cultural determinants of attitude toward Emotional AI in the workplace. *AI & society*, *38*(1), pp.97-119.
102. Martin, K., & Freeman, R. E. (2003). Some problems with employee monitoring. *Journal of Business Ethics*, 43, 353-361.
103. Mateescu, A. and Nguyen, A. (2019), *Workplace monitoring and surveillance*, Data and Society Research Institute, New York.
104. McCahill, M., & Norris, C. (2003). *Estimating the Extent, Sophistication and Legality of CCTV in London.* In M. Gill (Ed.), CCTV. Leicester, UK: Perpetuity Press.
105. McEvoy, S. (2002). E-mail and Internet Monitoring and the Workplace: Do Employees have a Right to Privacy? , *Communications and the Law*, 24(2), 69-84.
106. McParland, C. and Connolly, R. (2019), 'Employee monitoring in the digital era: Managing the impact of innovation', conference paper, *ENTRENOVA – Enterprise Research Innovation Conference*, 12–14 September, Rovinj, Croatia.
107. Meade, M., ed., (2001). I've Got My Eye on You: Workplace Privacy in the Electronic Age, in Practicing Law Institute Patents, *Copyrights, Trademarks, and*

Literary Property Course Handbook Series (pp. 1 - 10). Practicing Law Institute - Thomson/West

108. Middel, L., (2019.) *Workplace surveillance in the light of employee data protection.*

109. Molè, M., (2022,) May. The Quest For Effective Fundamental Labour Rights in The European Post-Pandemic Scenario: Introducing Principles of Explainability and Understanding For Surveillance Through AI Algorithms and IoT Devices. In *19th International Conference in Commemoration of Marco Biagi" Work Beyond the Pandemic. Towards a Human-Centred Recovery*.

110. Moor, J. H. (2005). Why we need better ethics for emerging technologies. *Ethics and Information Technology*

111. Moreira, T. (2016), 'The electronic control of the employer in Portugal', *Labour and Law Issues*, Vol. 2, No. 1.

112. Mozur, P. (2019). *One Month*, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority. The New York Times, April 14. Retrieved from https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligenceracial-profiling.html

113. Nelson, M. L., Barnes, K. L., Evans, A. L., &Triggiano, P. J. (2008). Working with conflict in clinical supervision: Wise supervisors' perspectives. *Journal of Counseling Psychology*, 55(2), 172-184.

114. Nissenbaum, H. (2009). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press

115. OECD (Organisation for Economic Co-operation and Development). (2019), *Recommendation of the Council on responsible innovation in neurotechnology*, Paris.

116. Ogata, S. S. (2005). *Legal, Ethical, and Political Issues in Nursing* 2nd Edition.

117. Oliver, H. (2002), 'Email and internet monitoring in the workplace: information privacy and contracting-out', *Industrial Law Journal*, Vol. 31, pp. 321–352.

118. Pearson, Q. M. (2000). Opportunities and challenges in the supervisory relationship: Implications for counselor supervision. *Journal of Mental Health Counseling*, 22(4). 283-394.

119. Peters, T. A. (1999). *Computerized Monitoring and Online Privacy.* Jefferson, North Carolina: McFarland & Company.

120. Pivčević, D., & Erceg Ćurić, I. (2022). Nadzor u radnome okruženju i povreda privatnosti radnika u sudskoj praksi. *Sigurnost: časopis za sigurnost u radnoj i životnoj okolini*, 64(2), 121-133.

121. Pritchard, G., Briggs, P., Vines, J. and Oliver, P. (2015), 'How to drive a London bus: measuring performance in a mobile and remote workplace', conference paper, 33rd *Annual ACM Conference on Human Factors in Computing Systems.* Seoul, 18–23 April 2015.

122. Privacy Rights Clearinghouse. (2001). "*Employee Monitoring: Is there privacy in the workplace: 2001*, http://www.privacyrights.org/FS/fs7-work.htm (San Diego).
123. Reiman, J. H.: 1995, 'Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future', *Computer and High Technology Law Journal* 11.
124. Roemmich, K., Schaub, F. and Andalibi, N., 2023, April. Emotion AI at Work: Implications for Workplace Surveillance, Emotional Labor, and Emotional Privacy. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems* (pp. 1-20).
125. Rosen, J. (2000). *The Unwanted Gaze*, the Destruction of Privacy in America. New York: Random House.
126. Rosenblat, A., & Stark, L. (2016). Algorithmic labor and information asymmetries: A case study of Uber's drivers. *International journal of communication*, 10, 27.
127. Rosenblat, A., Kneese, T., & Boyd, D. (2014). Workplace surveillance. Open Society Foundations' *Future of Work Commissioned Research Papers*.
128. Rudiyanto, T., Kunda, H., Dunn, A., Shenderovskiy, S., & Gibson, R. (2023). *Ethical and Legal Concerns of Artificial Intelligence in the Workplace: Examining Current Legislations in the United States*. Lex Publica, 10(1), 84-100.
129. Rule, J. B. (1973). *Private Lives and Public Surveillance*. London: Allen Lane.
130. Saval, N. (2014). *Cubed: A Secret History of the Workplace*. New York, NY: Doubleday.
131. Schulman, A. (2001). *'The Extent of Systematic Monitoring of Employee E-mail and Internet Use'*, Privacy Foundation. July 9, 2001, http://www.privacyfoundation.com.
132. Segijn, C. M., van Ooijen, I., & Opree, S. J. (2022). Privacy cynicism and its role in privacy decision-making. *Communication Research*. Advance online publication. https://doi.org/10.1177/00936502211060984
133. Sewell, G. (2005). "Nice Work? Rethinking Managerial Control in an Era of Knowledge Work." *Organization*, 12(5), 685–704.
134. Sitzia, A., 2019. The Role of the Proportionality Test in the Workplace Surveillance Field. *Judicial Power in a Globalized World: Liber Amicorum Vincent De Gaetano*, pp.579-595
135. Smith, A. (2008). *History and Evolution of Workplace Surveillance*. ABC University Press
136. Solon, O. (2017). *Big Brother isn't just watching: workplace surveillance can track your every move.* The Guardian, 6.
137. Solove, D. J. (2011). *Nothing to Hide: The False Tradeoff between Privacy and Security.* Yale University Press.

138. Solove, D. J., & Schwartz, P. M. (2021). *ALI data privacy: overview and black letter text*. UCLA L. Rev., 68, 1252.
139. Sostero, M., Milasi, S., Hurley, J., Fernandez-Macias, E. and Bisello, M. (2020), Teleworkability and the COVID-19 crisis: A new digital divide?, *JRC Working Papers Series on Labour, Education and Technology 2020/05*, European Commission, Seville.
140. Stark, L., Stanhaus, A., & Anthony, D. L. (2020). "i don't want someone to watch me while i'm working": Gendered views of facial recognition technology in workplace surveillance. *Journal of the Association for Information Science and Technology*, 71(9), 1074-1088.
141. Stein, MK; Wagner, EL; Tierney, P; Newell, S and Galliers, RD (2019) Datification and the Pursuit of Meaningfulness in Work *Journal of Management Studies* 56 (3) pp. 685 – 717.
142. Stoney A., (1998), *Ethical Issues in Electronic Performance Monitoring: A Consideration of Deontological and Teleological Perspectives*
143. Suder, S. and Siibak, A., 2022. Proportionate response to the COVID-19 threat? Use of apps and other technologies for monitoring employees under the European Union's data protection framework. *International Labour Review*, *161*(2), pp.315-335.
144. Sutter, E., McPherson, R. H., & Geeseman, R. (2002). Contracting for supervision. Professional Psychology: *Research and Practice*, 33(5), 495-498.
145. Tabak, F. and Smith, W. (2005), 'Privacy and electronic monitoring in the workplace: A model of managerial cognition and relational trust development', *Employee Responsibilities and Rights Journal*, Vol. 17, No. 3, pp. 173–189.
146. The Washington Post (2020), *"Managers turn to surveillance software, always-on webcams to ensure employees are (really) working from home"*, 30 April.
147. Thon, B. E. (2015), *Op-ed in Fri Fagbevegelse*, 20 January.
148. Tran, T. P. (2017). Personalized ads on Facebook: An effective marketing tool for online marketers. *Journal of Retailing and Consumer Services*, 39, 230–242. https://doi.org/10.1016/j.jretconser.2017.06.010
149. Trifković, M, Simić, M, Trivun, V, Silajdžić, V, Mahmutćehajić, F (2021) *Poslovno pravo: uvod u pravo, osnoviobligacija, privrednadruštvaiposlovnaetika*, Sarajevo: Ekonomski fakultet
150. Trifković, Miloš (2016) Can Moral Behaviour of Public Enterprises in Bosnia and Herzegovina be Improved by Legislated Model Code of Ethics?, Montenegrin Academy of Sciences and Arts, Scientific Meetings, Volume 138, *Proceedings International Conference Technology+Society→?Future*, 19-20 May, 2016, Podgorica, Montenegro, str. 115-144.
151. Trivun, V. (2019) *Odgovornost privrednih društava*, Sarajevo: Ekonomski fakultet

152. Tursunbayeva, A., Di Lauro, S., & Pagliari, C. (2018). People analytics—A scoping review of conceptual boundaries and value propositions. I*nternational journal of information management,* 43, 224-247.

153. Ullmann-Margalit, E. (2008). The case of the camera in the kitchen: Surveillance, privacy, sanctions, and governance. *Regulation & Governance*, 2(4), 425-444.

86. *Uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism* (USA patriot act) act of 2001, dostupno na: PLAW-107publ56.pdf (govinfo.gov) (Pristupljeno: 12.12.2023).

154. Vatcha, A., (2020.) Workplace Surveillance Outside the Workplace: An Analysis of E-Monitoring Remote Employees. *iSChannel*, *15*(1).

155. Vujević, M. *Uvođenje u znanstveni rad u području društvenih znanosti,* Informator, Zagreb, 1983.

156. Watson, N. (2001). The private workplace and the proposed "notice of electronic monitoring act": is "notice" enough? *Federal Communications Law Journal*, 54(1), 79-104.

157. WebSense: 2001, by NetPartner: http://www.websense.com/products/why/stats.cfm

158. Woodbury, M. (2003). *Computer and information ethics. Champaign*, IL: Stipes Publishing LLC.

159. Yerby, J. (2013). Legal and ethical issues of employee monitoring. Online *Journal of Applied Knowledge Management* (OJAKM), 1(2), 44-55.

160. Zakon o zaštiti ličnih podataka BiH („Sl. glasnik BiH“, br. 49/2006, 76/2011 i 89/2011 - ispr.) (dostupno na: https://www.paragraf.ba/propisi/bih/zakon-o-zastiti-licnih-podataka.html) (Pristupljeno: 17.12.2023)

161. Zickuhr, K., (2021). Workplace surveillance is becoming the new normal for US workers. *Washington Center for Equitable Growth*. https://equitablegrowth. org/research-paper/workplace-surveillance-is-becomingthe-new-normal-for-us-workers/. Institute for Research on Labor and Employment University of California, Berkeley, 2521, pp.94720-5555.

162. Zuboff, S. (1988). *In the Age of the Smart Machine: The Future of Work and Power*. New York: Basic Books

163. Zuboff, S. (2019). *The Age of Surveillance Capitalism*. New York: PublicAffairs/Hachette.

164. Zureik, E. (2003). “Theorizing Surveillance: the Case of the Workplace.” In David Lyon (Ed.). *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination.* New York and London: Routledge.

PRILOZI

PRILOG 1.

ANEKTA ZAPOSLENIKA ADRIATIC METALS

Lista pitanja za anketu (Likertova skala od 1 (u potpunosti se ne slažem) – 5 (u potpunosti se slažem):

- Opća percepcija nadzora:
  - "U kojoj mjeri se slažete da je nadzor na radnom mjestu opravdan i potreban?" (1-5)
- Specifične metode nadzora:
  - "U kojoj mjeri se slažete da vas zabrinjava korištenje videonadzora u vozilima?" (1-5)
  - "U kojoj mjeri se slažete da ste zabrinuti zbog praćenja internetskih komunikacija?" (1-5)
- Uticaj na privatnost i autonomiju:
  - "Koliko se slažete da ste zabrinuti da nadzorne prakse narušavaju vašu privatnost" (1-5)
  - "U kojoj mjeri se slažete da prepoznajete koristi od nadzora za vašu sigurnost?" (1-5)
- Percepcija koristi i sigurnosti:
  - "U kojoj mjeri se slažete da prepoznajete koristi od nadzora za vašu sigurnost?" (1-5)
  - "U kojoj mjeri se slažete da prepoznajete koristi od nadzora za efikasnost operacija?" (1-5)
- Uticaj na moral i produktivnost:
  - "Koliko se slažete da nadzor povećava vašu anksioznost na radu?" (1-5)
  - "Koliko se slažete da nadzor utječe na vašu produktivnost?" (1-5)
- Pravna i etička pitanja:
  - "U kojoj mjeri se slažete da ste upoznati s vašim pravima u kontekstu nadzora na radu?" (1-5)
  - "U kojoj mjeri se slažete da kompanija transparentno provodi nadzor?" (1-5)
- Transparentnost i politike:
  - "Koliko se slažete da kompanija treba povećati transparentnost nadzornih praksi?" (1-5)
  - "Koliko se slažete da su trenutne politike nadzora adekvatne i jasne?" (1-5)