

/ SVEVIDEĆE OKO

Kako je rad na daljinu tokom kovida-19
otvorio vrata za sveprisutnost
poslodavaca u životu radnika



AUTORI

Branka Anđelković, Tanja Jakobi

STRUČNI TIM/PRAVNI TIM ZA OBLAST ZAŠTITE PODATAKA O LIČNOSTI:

Tijana Žunić Marić, Advokatska kancelarija Žunić i

Danilo Krivokapić, SHARE Fondacija



SVEVIDEĆE OKO

Kako je rad na daljinu tokom kovida-19 otvorio vrata za sveprisutnost poslodavaca u životu radnika

IZDAVAČ

Centar za istraživanje javnih politika,

Beograd,

februar 2022

DIZAJN

Sonja Lundin

COPYRIGHTS

Centar za istraživanje javnih politika,

Beograd

www.publicpolicy.rs

office@publicpolicy.rs

Napomena: Objavljivanje ove studije podržao je Olaf Palme Centar u Srbiji. Stavovi izneti u ovoj studiji pripadaju isključivo CENTRU i ne predstavljaju nužno stav Olaf Palme Centra u Srbiji.



A large, stylized eye graphic in yellow and black, with a black outline and a yellow center. It is positioned on the left side of the cover, partially overlapping the title and subtitle.

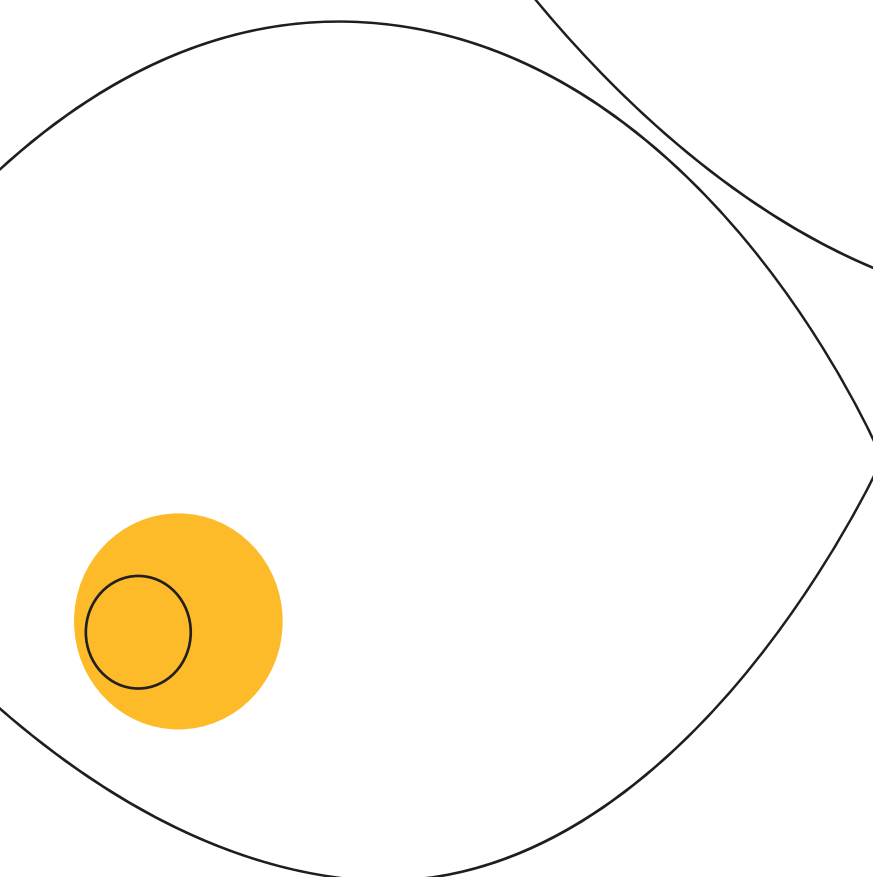
SVEVIDEĆE OKO

Istraživanje o nadzoru zaposlenih
koji rade od kuće

AUTORI

BRANKA ANĐELKOVIĆ
TANJA JAKOBI

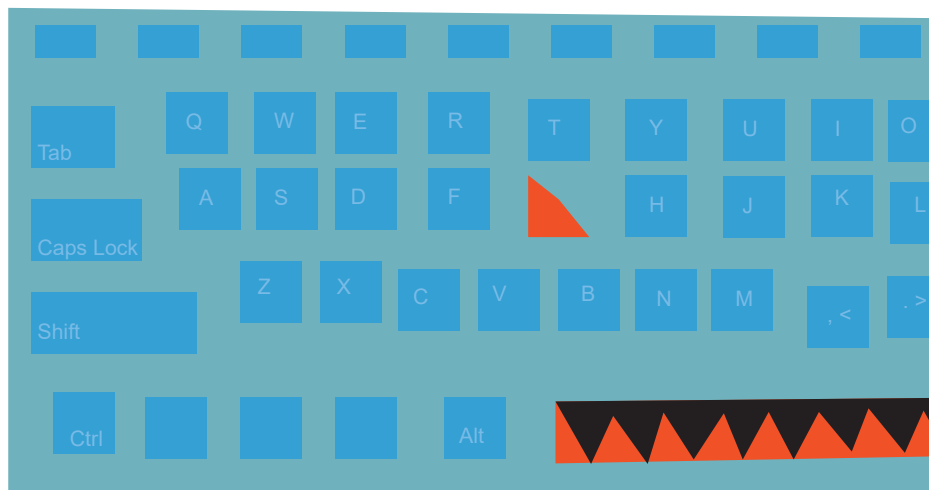
2022

A smaller, stylized eye graphic in yellow and black, with a black outline and a yellow center. It is positioned at the bottom left of the cover, partially overlapping the year.

^v SADRŽAJ

Uvod	6
Kontekst	7
Metodologija	9
Glavni nalazi	13
Osnovni preduslovi za pravno uređenje rada od kuće	13
Legitimnost prikupljanja podataka o ličnosti	15
Praćenje efikasnosti zaposlenih	17
1. Nadzor zaposlenih uopšte	17
2. Nadzor zaposlenih preko posebnih aplikacija	21
3. Procena uticaja praćenja efikasnosti zaposlenih na zaštitu podataka o ličnosti	22
IV Čuvanje podataka o ličnosti i povreda prava na privatnost	23
1. Čuvanje podataka o ličnosti	23
2. Povrede prava na privatnost	25
Zaključci	25
Predlog politika koje bi trebalo uvesti na nacionalnom nivou i nivou preduzeća	26
1. Preporuke za kreatore politika	26
2. Preporuke za poslodavce	27
3. Preporuke za sindikate	28
4. Preporuke za nevladine organizacije	29

UVOD



Pandemija kovida-19 širom je otvorila vrata radu od kuće koji je u poslednje dve godine doživeo ekspanziju. Ta promena je naročito bila vidljiva među onim zanimanjima koja intenzivno koriste informaciono-komunikacione tehnologije, počev od samog IKT sektora do raznih uslužnih delatnosti kao što su finansije i bankarstvo, marketing, e-trgovina, saobraćaj, te sektor javnih usluga kao što su obrazovanje, i zdravstvo. Rad od kuće je eskalirao tokom pandemije i ta promena u organizaciji rada je posledično dovela do porasta potražnje za softverima za praćenje zaposlenih koja je u Evropskoj uniji već u aprilu 2020. iznosila 108% u poređenju sa 2019. (European Commission, 2021). U Americi se, na primer, broj kompanija koje su koristile nadzorne aplikacije duplirao u 2021. u odnosu na prepandemijsko vreme (Blum, 2022). Praćenje rada u domovima radnika je tako brzo uzelo maha dok pravni okvir koji bi uredio pitanje mogućnosti ograničenja ovog načina nadzora nad radom zaposlenih još nije jasno uspostavljen niti dovoljno regulisan kad postoji.

Naime, rad na daljinu i rad od kuće doneli su sa sobom mnoge nepoznanice kad je u pitanju uspostavljanje jasnih granica između obezbeđivanja toka poslovnog procesa i zaštite poslodavca s jedne strane, i zaštite prava radnika i njegove privatnosti s druge strane. Zbog načina na koji se obavljanje rada zaposlenih¹ prati i podataka koji se

prikupljaju uz pomoć novih tehnologija i aplikacija tokom obavljanja rada, nadzor zaposlenih koji rade od kuće često ima intruzivni karakter i tako negativno utiče na prava i autonomiju radnika. Za kompanije koje prate rad radnika i tako u stvari u isto vreme i prikupljaju podatke o njima, pitanja regulacije takvih praksi, saglasnosti radnika i transparentnosti u ovom procesu su ključna za očuvanje dostojanstvenog rada i poverenja zaposlenih.

Otuda ova studija istražuje pravni okvir u Srbiji u kontekstu rada od kuće², načine na koje poslodavci nadziru radnike uz pomoć novih tehnologija i mogućnosti zaštite prava radnika i njihove privatnosti u takvim okolnostima. Studija osvetljava četiri važna aspekta rada od kuće. Prvo, ispituju se ključni preduslovi to jest pravni osnov koji omogućava i jasno reguliše ovaj oblik rada. Drugo, ocenjuje se opravdanost prikupljanja privatnih podataka radnika generalno i putem aplikacija. Treće, u studiji ispituju se na koje sve načine poslodavci prate efikasnost rada zaposlenih uz pomoć novih tehnologija. Četvrto, bavimo se pitanjem kako poslodavci prikupljaju i čuvaju podatke o ličnosti radnika uzev u obzir da povećani nadzor podrazumeva i veću količinu informacija koje se prikupljaju te moguću povredu prava na privatnost. Na kraju se bavimo time kako obezbediti dostojanstveni rad od kuće koji je u isto vreme pod nadzorom poslodavaca.

¹ Termin zaposleni i radnik se koriste u ovom tekstu kao sinonimi.

² U ovom tekstu rad od kuće i rad na daljinu se koriste kao sinonimi za rad van prostorija poslodavca. Prema Zakonu o radu ("Sl. glasnik RS", br. 24/2005, 61/2005, 54/2009 i 32/2013), radni odnos van prostorija poslodavca obuhvata rad na daljinu i rad kod kuće (član 42. stav 2). Međunarodna organizacija rada usvojila je 1996. godine Konvenciju br. 177 o radu kod kuće. Taj rad koji je tada prvi put definisan podrazumeva posao koji se obavlja u domu radnika ili na drugom mestu njegovog/njenog izbora, osim radnog prostora poslodavca.



Studija obuhvata uvod, odeljak o kontekstu istraživanja, metodološki deo, nalaze istraživanja, zaključke i preporuke.

KONTEKST

Pojava kovida-19 i masovni prelazak na rad od kuće aktuelizovao je pitanje nadzora radnika. Nove karakteristike posla donele su i nove metode nadzora zaposlenih kako bi se pratilo ponašanje radnika i njihovi rezultati (Maalsen & Dowling, 2020). Povećani monitoring zaposlenih stvara nove izazove ukazujući na potrebu za širim okvirom za balansiranje između ekonomskih interesa kompanija i ličnih i ekonomskih interesa radnika. Kako tehnologija proširuje obim onoga što se može uraditi pomoću alata za monitoring, zaštita na radnom mestu i prava radnika postaju pitanja čiji značaj treba više nego ikad naglašavati.

Prema definiciji koju nudi Lyon (2001) nadzor se odnosi na "svako prikupljanje i obradu ličnih podataka, u svrhu uticaja na one čiji su podaci prikupljeni".

Zapravo, nadzor zaposlenih se može smatrati uobičajenim elementom radnog procesa. Zaposleni očekuju da se njihov učinak pregleda, postave ciljevi i prikupe informacije o njihovim aktivnostima. S druge strane, poslodavci imaju pravo da nadgledaju svoje zaposlene kako bi osigurali da se resursi koriste efikasno, da zaštite komercijalnu poverljivost i rizik upravljanja, i da osiguraju da zaposleni poštuju zakon. U tom smislu, nadzor se može smatrati i dobrom praksom upravljanja.

Poslednjih godina nadzor se širio na različite oblasti, pre svega na polje rada. U obimnoj analizi Zajedničkog istraživačkog centra Evropske komisije (European Commission, 2021) ističe se da je povećani nadzor zaposlenih zapravo rezultat dva velika trenda na tržištu rada. Prvi je ekspanzija platformskog rada, a drugi aktuelizacija rada na daljinu i rada od kuće koji je bio uslovljen pojavom pandemije koronavirusa. Oba slučaja dovela su do povećanog nadzora radnika uz pomoć informacionih tehnologija.

Graham i Wood (2003) ukazuju na evoluciju od analognog, odnosno birokratskog načina nadziranja ka sve više zastupljenom digitalnom nadzoru koji vodi ka sve većoj efikasnosti i sveprisutnosti nadzora. U tom smislu primenom novih tehnologija omogućeno je da supervizor uvek nadzire radnika – čak i kada nije fizički prisutan.

Više nego ikada, tehnološka rešenja omogućavaju da se sve radnje i kretanja radnika mogu snimati i analizirati u realnom vremenu ili bilo kom drugom trenutku. Sa savremenim elektronskim sredstvima praćenja, radno mesto je "panoptično", odnosno pod stalnim nadzorom (Manokha, 2020).

Nadzor je tako aktuelizovao teme iz oblasti rada u vezi sa autonomijom radnika i asimetrijom moći u odnosima poslodavca i radnika. U tom kontekstu su se otvorile razne teme od toga čija je oprema za rad, koji nadzorni mehanizmi su dozvoljeni, koje aplikacije za nadzor su invazivne, a koje se smatraju prihvatljivim, koje podatke poslodavac može da skuplja i čuva, a koje ne. Na primer, pravo jedne stranke, odnosno poslodavca da vrši nadzor nad drugom stranom, tj. zaposlenim, može da ide tako daleko da menja sadržaj obaveza zaposlenog, da daje uputstva o tome kako se ispunjava radna obaveza ili pruža poslodavcu pravo da sankcioniše zaposlenog kada se određeni nalozi ne poštuju. Nove tehnologije kojima se prati rad zaposlenih mogu biti inherentno nametljivije, tako narušavajući autonomiju zaposlenih i njihova prava (Barrenechea-Mendez et al., 2016; Ludovici et al., 2021)

Do danas je većina diskusija bila usredsređena na korporativnu upotrebu nadzora i korišćenje podataka, a slabije na etička pitanja nadzora i usaglašenosti sa zakonom o radu ili stavovima zaposlenih o merama nadzora koje se sprovode. Zapravo, kako polje nadzora radnika nastavlja da raste, postojeći zakoni se proširuju i donose novi, etika i važna prava poput onog na privatnost radnika zauzimaju sve značajnije mesto u okviru regulatornih rasprava koje se tiču rada (Bodie et al., 2016).

Kada je reč o radu od kuće i potrebi za "autonomijom radnika da samostalno organizuju svoj rad", posebno se ističe upitna efikasnost "stalnih" mera nadzora (Fairweather, 1999). U nadzoru radnika treba uvažavati pravo na privatnost radnika, vodeći računa koliko je ličnost zaposlenih vidljiva menadžerima i u kojoj meri nadzor zadire u privatni život radnika (Lee & Kleiner, 2003). Što je veća sposobnost menadžmenta da direktno prati i kontroliše radni učinak zaposlenih uz pomoć novih tehnologija koje omogućavaju pojačane mehanizme kontrole nad radnicima, sve je veće nezadovoljstvo radnika poslom koji obavljaju.

U studijama koje se bave nadzorom zaposlenih posebno se ističe pitanje podataka koji se prikupljaju i načina na koji se njima upravlja. Uočeno je da je za zaposlene najvažnija transparentnost, kao i jasnost u pogledu informacija koje se prate i prikupljaju kad je u pitanju nadzor koji sprovode poslodavci (Zielinski, 2020). Identifikovana je snažna povezanost između pozitivnih stavova radnika o neophodnosti nadzora i njihovog poverenja u poslodavca - na primer zaposleni smatraju nadzor poslodavca prihvatljivim ukoliko prepoznaju da on poštuje odgovarajuće procedure (Workman, 2009).

U tom smislu, ova studija predstavlja pionirski pokušaj da se definiše praksa u odnosu poslodavaca i radnika u kontekstu rada od kuće i nadzora zaposlenih. Identifikovani nalazi treba da pomognu u razumevanju ključnih trendova i ponude preporuke za uspostavljanje efikasnog i transparentnog i na poverenju zasnovanog sistema nadzora, uz poštovanje radnih prava i akata u vezi sa praćenjem zaposlenih i prikupljanjem podataka.

METODOLOGIJA

U metodološkom smislu, u ovom istraživanju primenjen je kombinovani istraživački pristup koji je uključio kvantitativne i kvalitativne metode. Sprovedene su dve ankete, jedna sa radnicima koji su u poslednjih godina dana bar povremeno radili od kuće, a druga sa menadžerima i direktorima preduzeća koji su imali iskustva sa ovim načinom rada i pre početka izbijanja pandemije kovida-19. Istraživanje je obuhvatilo i intervjue sa ekspertima i poznaviocima oblasti radnog prava i prava o zaštiti podataka o ličnosti.

ANKETA SA RADNICIMA

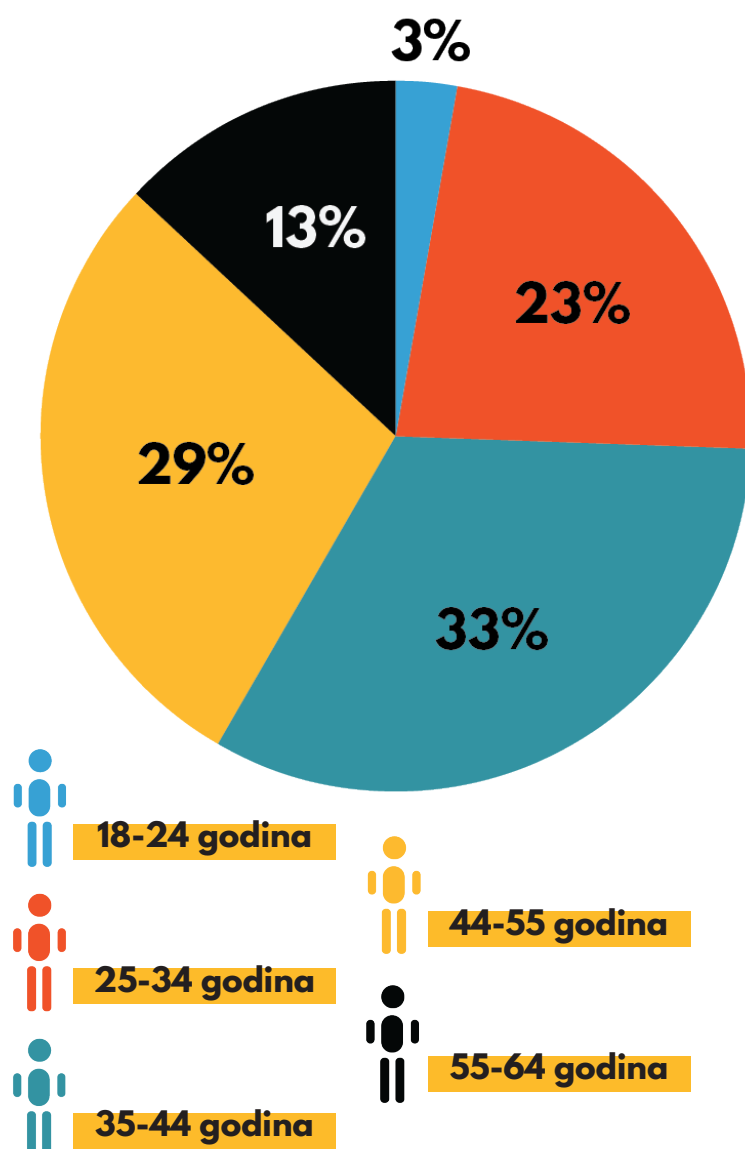
Anketa sa radnicima je rađena onlajn i bazirala se na kvantitativnom istraživanju sa strukturiranim upitnikom. Uzorak je obuhvatio ukupno 366 ispitanika, 300 radnika iz raznih ekonomskih sektora i 66 zaposlenih iz dodatnog uzorka. U ovom uzorku je anketirano 30 osoba zaposlenih u IT sektoru i 36 zaposlenih u pozivnim centrima. Anketu sa radnicima je sprovedla agencija za istraživanje tržišta Smart Plus Research iz Beograda tokom jula 2021.



Kad je rodna struktura ispitanika u pitanju, bilo je 56% žena i 44 % muškaraca. Više od polovine anketiranih je pripadalo starosnoj grupi od 25 do 44 godine starosti (51%). S druge strane, najmanji broj radnika je bio u starosnoj grupi od 18-24 godine (3 %) kao i onih u starosnoj dobi od 55-64 godina (13%).

Više od polovine naših anketiranih ima

Grafikon 1. Starosna struktura ispitanika među radnicima



visoku stručnu spremu (58%), a ostali imaju više obrazovanje (13%) i završenu srednju školu (26%).

Većina anketiranih bila je angažovana u sektorima koji su i ranije imali iskustva sa radom na daljinu kao što su finansije i bankarstvo, informisanje i komunikacije, istraživanje i razvoj, trgovina, administrativne i druge delatnosti, obrazovanje, javna uprava i druge usluge.

Uzorak je ravnomerno obuhvatio radnike i radnice iz 4 regiona u Srbiji: iz Vojvodine je bilo 25% anketiranih, iz Šumadije i zapadne Srbije 22%, iz regiona Beograda 32%, dok je iz južne i istočne Srbije bilo 20 % njih.



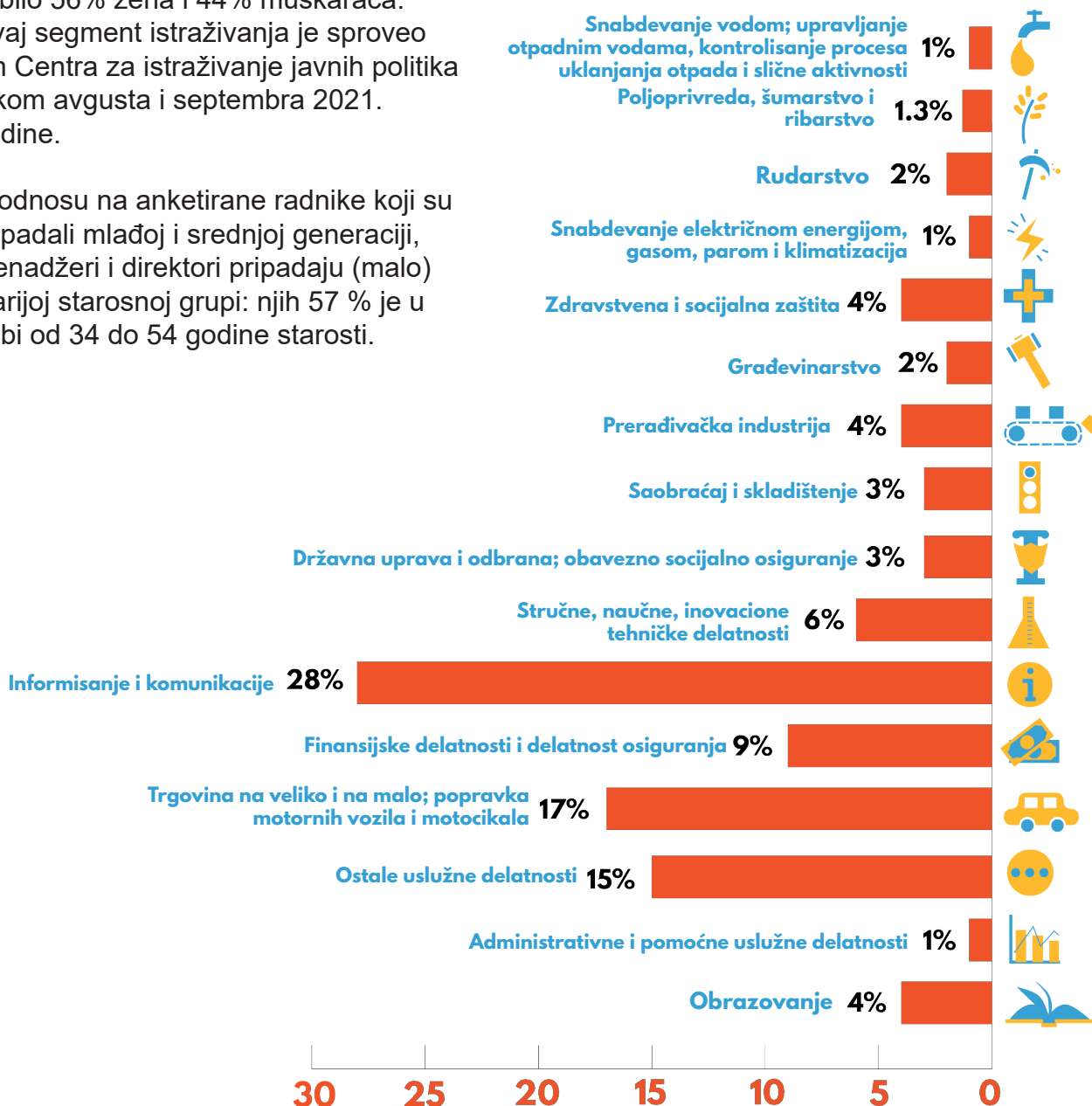
Grafikon 2. Struktura ispitanika prema privrednim delatnostima - **RADNICI**

ANKETA SA MENADŽERIMA

Anketa sa menadžerima je sprovedena telefonskim putem i bazirala se na kvalitativnom istraživanju sa strukturiranim upitnikom. Ukupno je obuhvaćeno 113 ispitanika, među kojima je bilo 56% žena i 44% muškaraca. Ovaj segment istraživanja je sproveo tim Centra za istraživanje javnih politika tokom avgusta i septembra 2021. godine.

U odnosu na anketirane radnike koji su pripadali mlađoj i srednjoj generaciji, menadžeri i direktori pripadaju (malo) starijoj starosnoj grupi: njih 57 % je u dobi od 34 do 54 godine starosti.

Kad je obrazovna struktura u pitanju, više od dve trećine naših sagovornika ima visoku stručnu spremu (76%), a potom slede onih sa višim obrazovanjem (12%). Identično kao i kad su anketirani radnici u pitanju, većina menadžera i direktora dolazi iz sektora u kojima je rad od kuće bio prisutan i pre, a još više i tokom kovida-19.



Grafikon 3. Struktura ispitanika prema privrednim delatnostima - POSLODAVCI

Za razliku od ankete sa radnicima koja je ravnomerno obuhvatila ispitanike iz 4 regiona u Srbiji, menadžeri su prvenstveno bili iz regiona Beograda (71%). Na drugom mestu su bili oni iz južne i istočne Srbije (18%) a potom iz Vojvodine (10%).

Obe ankete obuhvataju sledeće teme: uređenje rada od kuće, vrste podataka o ličnosti koji se prikupljaju, način na koji se to čini, svrhu prikupljanja podataka, poznavanje propisa i lična iskustva u vezi sa povredama prava na privatnost i dostojanstvo radnika.

INTERVJUI SA EKSPERTIMA IZ OBLASTI RADNOG PRAVA I PRAVA O ZAŠTITI PODATAKA O LIČNOSTI

Da bi se osvetlio prostor primene zakona o radu i zakona o zaštiti podataka o ličnosti koji ranije nije bio značajnije testiran u praksi, polustrukturirani intervjui su organizovani sa ekspertima iz oblasti radnog prava i oblasti zaštite podataka o ličnosti, predstavnicima nadležnih državnih institucija kao što je Ministarstvo za rad, zapošljavanje, boračka i socijalna pitanja, nezavisnih tela poput Kancelarije Poverenika za informacije od javnog značaja, predstavnika reprezentativnih sindikata u Srbiji i radnika. Ukupno je sprovedeno

11 intervjua u periodu od oktobra 2021. do februara 2022. Odgovori Inspektorata za rad pribavljeni su putem slanja zahteva za pristup podacima od javnog značaja.

Ovo, prvo eksplorativno istraživanje o nadzoru radnika koji rade od kuće u Srbiji, je sprovedeno od jula 2021. do februara 2022. Podaci su korišćeni u skladu sa etičkim principima istraživanja (Townsend & Wallace, 2016), i propisima koji regulišu zaštitu podataka ispitanika.

OGRANIČENJA ISTRAŽIVANJA

Ograničenje ovog istraživanja je da ankete sa radnicima i menadžerima nisu bile sprovedene u istim preduzećima. Drugo, ankete se razlikuju u tome što je anketa sa radnicima rađena na reprezentativnom uzorku za razliku od one sa menadžerima koja je obuhvatila prigodni uzorak. Na kraju, zbog prirode delatnosti koje su mogle da budu organizovane kroz rad od kuće u uzorku je bilo nešto više žena nego muškaraca (56% u odnosu na 44%).

GLAVNI NALAZI

Rad od kuće bio je novi izazov i za srpsko tržište rada. Prema zvaničnim podacima, usled pandemije u aprilu 2020. godine rad od kuće bio je alternativna ili jedina moguća forma rada za oko 10% aktivne radne snage u Srbiji. Najnoviji podaci za prva tri kvartala 2021. godine Republičkog zavoda za statistiku ukazuju da je slična praksa bila prisutna i tokom prošle godine. Tokom te dve godine, kako pokazuje naša studija, i radnici i poslodavci su se suočili sa brojnim izazovima kad su rad od kuće i nadzor u pitanju.

Glavni nalazi istraživanja su predstavljeni u četiri celine: 1) u prvom delu se razmatraju osnovni preduslovi za uređivanje rada od kuće, 2) u drugom se bavimo legitimnim i nezakonitim osnovama za prikupljanje podataka o ličnosti zaposlenog, a 3) u trećem delu je fokus na prikupljanju i obradi podataka zaposlenih u svrhu praćenja njihove efikasnosti tokom rada od kuće. U ovom odeljku prvo se razmatraju od ranije poznati načini nadzora zaposlenih, a potom novi načini za nadzor zaposlenih preko aplikacija. Konačno, u četvrtom delu (4) su prikazani rezultati u vezi sa čuvanjem podataka zaposlenih i njihovih prava kad je uvid u te podatke u pitanju.

OSNOVNI PREDUSLOVI ZA PRAVNO UREĐENJE RADA OD KUĆE

Rad od kuće i rad na daljinu regulisani su Zakonom o radu (2005). Temeljni dokument kojim se uređuje rad od kuće jeste ugovor o radu (kada zaposleni od prvog dana radi na ovaj način) ili aneks ugovora o radu koji je poslodavac obavezan da ponudi zaposlenom u slučaju da dolazi do promene u smislu prelaska sa rada iz prostorija poslodavca na rad od kuće (Zakon o radu, 2005). Ugovorom odnosno Aneksom moraju biti regulisane i neke od ključnih tema kao što su obaveze poslodavca u pribavljanju, održavanju i instaliranju opreme za rad, naknada na koju zaposleni ima pravo ako tokom rada koristi sopstvenu opremu, naknada drugih troškova povezanih sa radom od kuće, kao što je na primer trošak za internet, način vršenja nadzora nad radom zaposlenog, radno vreme kao i druga pitanja. Ova obaveza potvrđena je i u Vodiču za bezbedan i zdrav rad od kuće koje je Ministarstvo za rad, zapošljavanje, boračka i socijalna pitanja izdalo početkom 2021. godine.

Međutim, iako našim anketiranim direktorima i menadžerima rad od kuće nije novina, većina ovih poslodavaca (61%) nije ponudila zaposlenima aneks ugovora o radu pri prelasku na rad od kuće. Svega jedna četvrtina je navela da su to učinili (26%), dok ostali (13%) nisu odgovorili na ovo pitanje. Poslodavci koji su sa radnicama zaključili anekse ugovora o radu najčešće dolaze iz

sektora finansija i osiguranja, kao i uslužnih delatnosti.

Kad su u pitanju sredstva za rad koja obezbeđuju poslodavci, njihovi i odgovori zaposlenih bitno se razlikuju.

Oko tri petine zaposlenih izjavilo je da je koristilo svoj kompjuter/laptop, dok je svega 27% njih potvrdilo da su od poslodavca dobili ovaj vid opreme. Oko 10% njih je navelo da koristi naizmenično sopstvenu i opremu poslodavca da bi obavljali rad. Nasuprot tome 78% rukovodilaca reklo je da su svojim zaposlenima obezbedili sredstva za rad, dok je 13% njih ukazalo da su zaposleni koristili sopstveni kompjuter ili laptop.

Razlike između odgovora zaposlenih i poslodavaca delom se mogu objasniti različitim uzorcima – anketirani zaposleni i poslodavci nisu dolazili iz istih kompanija. Međutim, zbog ovolike razlike u odgovorima, bilo bi potrebno dodatno istražiti ovu temu. Iz ankete sa zaposlenima proizilazi da je u Beogradu, češće nego u drugim regionima, kao i među IT populacijom, kompjuter/laptop koji su zaposleni koristili u radu od kuće u vlasništvu kompanije.

Pitanje ko je obezbedio sredstva za rad je važno i za druga prava radnika.

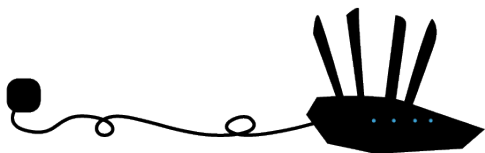
Naime, Zakon o radu jasno propisuje da su poslodavci dužni da zaposlenima koji rade od kuće isplaćuju naknadu troškova za upotrebu i korišćenje sredstava za rad koji su u vlasništvu zaposlenih, kao i da zaposlenima nadoknade druge troškove. U našoj anketi samo 15% poslodavaca je

izjavilo da isplaćuje takvu naknadu zaposlenima za korišćenje kompjutera. S druge strane, u obe ankete dobijen je sličan odgovor da zaposleni najčešće koriste sto i stolice u svom vlasništvu bez nadoknade troškova iz kompanije. Dakle, iako je iz rezultata jasno da je značajan broj zaposlenih koristio svoja sredstva za rad, mali broj poslodavaca je zaposlenima isplatio naknadu za korišćenje ovih sredstava rada.

Odredba člana 42 stav 3 tačka 4 prepoznaje da sredstva mogu pripadati i zaposlenom. Ipak, ukoliko poslodavac nije obezbedio kompjuter kao osnovno sredstvo on rizikuje na više načina. Neki od očiglednih rizika su gubitak kontrole nad poslovnim tajnama i drugim poverljivim informacijama, informaciona nebezbednost i velika šansa da dođe do povrede podataka, upotreba nelegalnog softvera u radu (ako nije ujedno obezbedio i sve licence za softvere koji se koriste), a potencijalno i prekomerni upliv u podatke o ličnosti. Takođe bi morao da plaća naknadu zaposlenom za činjenicu da zaposleni koristi svoj kompjuter. Osim toga bi morao da ima poseban pravilnik koji se odnosi na upotrebu opreme zaposlenog (Chouffani, 2021).

U slučaju kada poslodavac ne zaključi aneks ugovora o radu sa zaposlenim prilikom prelaska na obavljanje rada od kuće, on može snositi prekršajnu odgovornost, što povlači i novčanu kaznu za poslodavca i odgovorno lice kod poslodavca u iznosu od 800.000 do 2.000.000 dinara.³

U slučaju da smatraju da im je



povređeno pravo iz radnog odnosa zaposleni imaju pravo da se obrate Inspektoratu za rad, ili da pokrenu sudski postupak radi utvrđivanja povrede nekog od njihovih prava. Prema odgovoru Inspektorata za rad Ministarstva za rad, zapošljavanje, boračka i socijalna pitanja od marta 2020. do danas nije bilo prijava o potencijalnom kršenju prava zaposlenih koji rade od kuće.⁴ Imajući u vidu da u velikom broju slučajeva zaposleni nisu dobili aneks ugovora o radu, može se pretpostaviti da se zaposleni nisu obraćali Inspektoratu iz drugih razloga, uključujući neobaveštenost i/ili strah da ne izgube posao.

Da zaključimo, veliki broj zaposlenih obavljao je rad od kuće bez odgovarajućeg aneksa o radu, što znači da njihova prava nisu bila regulisana u skladu sa Zakonom o radu. Imajući u vidu da je ovo istraživanje sprovedeno u vreme kada je pored Zakona postojao i Vodič za bezbedan i zdrav rad od kuće može se zaključiti da su poslodavci imali dovoljno informacija o tome na koji način treba da urede rad od kuće.

Bez aneksa ugovora o radu i znanja ili volje da se obrate za zaštitu svojih prava Inspektoratu rada, zaposleni su se dodatno izložili riziku nedozvoljenog nadzora nad njihovim radom o čemu govorimo u sledećim odeljcima.

LEGITIMNOST PRIKUPLJANJA PODATAKA O LIČNOSTI

Prikupljanje i obrada podataka o ličnosti zaposlenog regulisani su Zakonom o zaštiti podataka o ličnosti (ZZPL; 2018) i Zakonom o radu (2005), ali ova dva zakona nisu međusobno usaglašena. Naime, obaveza propisana Zakonom o zaštiti podataka o ličnosti da se svi drugi zakonski dokumenti usaglase sa njim do kraja 2020. nije ispoštovana u slučaju Zakona o radu,⁵ što otvara „sivo polje“ u nadzoru radnika u prostorijama poslodavca uključujući rad od kuće. Ovo se kosi sa praksom Evropske unije gde je usvajanje Opšte uredbe o zaštiti podataka (GDPR)⁶ transponovano u oblasti radnih odnosa, i takođe podrazumeva visoke kazne za kršenje privatnosti pojedinca uopšte i u oblasti radnih odnosa.⁷ U Srbiji, kaznene odredbe propisane Zakonom o zaštiti podataka o ličnosti odnose se na sve slučajeve prikupljanja i obrade podataka o ličnosti suprotno odredbama ovog zakona, bez obzira o kojim licima se radi, te bi se ove odredbe svakako imale primenjivati i na poslodavce koji bi suprotno odredbama zakona postupali u pogledu podataka o ličnosti zaposlenih. U samom Zakonu o radu nije posvećena adekvatna pažnja zaštiti podataka o ličnosti zaposlenih niti je to pitanje na adekvatan način definisano u odnosu na zaposlene. Drugim rečima, nisu uzete u obzir specifičnosti podređenog položaja zaposlenih prema poslodavcima, te se na njih primenjuju samo opšte kaznene odredbe iz Zakona o zaštiti podataka o

3 U slučaju kada ne poštuje druge odredbe zakona (uključujući ovde prava zaposlenih koja proizilaze iz člana 42. ugovora koji reguliše rad od kuće) propisana je kazna od 600.000 do 1.500.000 dinara.

4 Odgovor pribavljen po osnovu Zahteva za pristup informacijama od javnog značaja 11. februara 2022. godine.

5 Intervju, Povernik za informacije od javnog značaja i zaštite podataka o ličnosti, 18. februar 2022.

6 General Data Protection Regulation tojest GDPR je akronim za Opštu uredbu o zaštiti podataka. Reč je o evropskoj regulativi koja je u primeni od maja 2018. godine kako bi se poboljšala kontrola građana EU nad ličnim podacima koje kompanije mogu legalno da poseduju.

7 Intervju, Povernik za informacije od javnog značaja i zaštite podataka o ličnosti, 18. februar 2022.

ličnosti.

Uobičajeno je da poslodavci, bez obzira na mesto rada, podatke o ličnosti prikupljaju prilikom zaključivanja ugovora o radu.⁸ Pored toga, poslodavci u našoj anketi navode i druge razloge za ovakvu aktivnost, poput čuvanja poslovne tajne (34%), praćenja prisutnosti i efikasnosti zaposlenih (po 24%), praćenja i planiranja politike zapošljavanja (19%), zaštite intelektualne svojine (17%), sprečavanja zloupotrebe službenih vozila i opreme (14%), itd. U manjoj meri je navođeno prikupljanje podataka za potrebe arhiviranja u javnom interesu, u svrhu istraživanja i za potrebe statistike. Oko 4% poslodavaca je navelo da ne prikuplja lične podatke zaposlenih, što je malo verovatno i pre govori o nerazumevanju šta su lični podaci zaposlenih nego o aktuelnoj politici preduzeća budući da svaki poslodavac koji zaključuje bilo koju vrstu ugovora u cilju radnog angažovanja lica, prikuplja i lične podatke angažovanih lica.

Potpuna transparentnost u obradi podataka koju sprovode rukovaoci (u ovom slučaju poslodavci), odnosno pravo na informisanje, predstavlja jedno od osnovnih prava koje zaposleni imaju po Zakonu o zaštiti podataka o ličnosti (ZZPL) iz 2018. godine. Naime, u skladu sa ZZPL poslodavci su dužni da obaveste zaposlene o prikupljanju i obradi njihovih podataka o ličnosti. Takvo obaveštenje, između ostalog, mora sadržati informacije o podacima o ličnosti koji su predmet obrade, svrsi obrade, osnovu obrade, roku čuvanja, eventualnom međunarodnom transferu podataka, a pored toga mora i sadržati

obaveštenje o pravima zaposlenih u vezi sa predmetnom obradom njihovih podataka o ličnosti.

Međutim, kako naše istraživanje pokazuje, samo oko polovine poslodavaca u skladu sa zakonom dostavlja zaposlenima obaveštenje o obradi podataka o ličnosti. Drugim rečima, polovina poslodavaca u našem uzorku vrši obradu podataka o ličnosti zaposlenih na nezakonit način.

Dalje, poslodavci su dužni da na detaljan način odrede svrhu obrade ovih podataka, što se po pravilu čini internim aktima poslodavca. Međutim, imajući u vidu da je samo 41% poslodavaca internim aktima uredilo obradu podataka o ličnosti, može se zaključiti da većina poslodavaca nije ispunila ovu obavezu.

Među aktivnostima koje su sproveli u cilju informisanja zaposlenih o prikupljanju i obradi njihovih podataka o ličnosti, poslodavci navode razno⁹: da su pribavili saglasnost zaposlenih¹⁰(32%), da su ih o prikupljanju podataka obavestili na sastancima (27%) ili da su sastavili pisanu informaciju (15%). Međutim, sva tri opisana slučaja su sporna sa stanovišta zakona. U slučaju usmenog obaveštavanja, zaposleni nemaju pisanu i lako dostupnu formu obaveštenja o podacima koji se prikupljaju, svrsi obrade ovih podataka i načinu skladištenja, kao i o svojim pravima. Za poslodavce koji su naveli da su obavestili zaposlene u pisanoj formi ostaje otvoreno pitanje da li su to uradili sasvim u skladu sa ZZPL, odnosno na razumljiv i lako dostupan način, te da

⁸ Zakonom o radu propisno je da se tom prilikom mogu prikupiti sledeći podaci: ime i prezime, adresa prebivališta/boravišta, vrsta i stepen stručne spreme, kao i podaci koji se odnose na radno mesto zaposlenog (naziv i opis poslova, mesto rada, vrsta radnog odnosa, trajanje ugovora, dan početka rada, radno vreme, iznos zarade).

⁹ Mogućnost višestrukih odgovora.

¹⁰ Ovde je važno ukazati na činjenicu da je pristanak, tj. saglasnost zaposlenih samo jedan od zakonskih osnova za prikupljanje podataka o ličnosti zaposlenih, dok se većina podataka o ličnosti zaposlenih prikuplja po drugim osnovima propisanim ZZLP-om o čemu se zaposleni obaveštavaju, što može ukazivati da poslodavci ne prave razliku između različitih osnova zakonite obrade podataka o ličnosti, kao i između obaveštavanja i davanja pristanka na obradu podataka o ličnosti.

li su pružili sve informacije propisane Zakonom.

Kako nalazi istraživanja pokazuju, poslodavci često koriste pribavljanje pristanka od zaposlenih kao pravni osnov za obradu podataka o ličnosti u radnim odnosima. Naša anketa, kao što je gore navedeno, ukazuje da je 32% rukovodilaca navelo da su zaposleni potpisali saglasnost u ove svrhe dok je isto navelo i 33% zaposlenih. Međutim, pribavljanje pristanka **nije jedini pravni osnov** za prikupljanje i obradu podataka o ličnosti u slučajevima obrade podataka ovih podataka u radnim odnosima i drugim odnosima koji se tiču radnog angažovanja lica. Pored pristanka, ZZPL predviđa i druge pravne osnove za obradu podataka o ličnosti, poput onog koji propisuje da je obrada zakonita ukoliko je neophodna za izvršenje ugovora zaključenog sa licem na koje se podaci odnose ili za preduzimanje radnji na zahtev lica na koje se podaci odnose, pre zaključenja ugovora (što je upravo slučaj pri zaključivanju ugovora sa radno angažovanim licima), u cilju poštovanja pravnih obaveza rukovaoca (koje poslodavac takođe ima u slučaju radnog angažovanja lica), i druge.¹¹

Dakle, ograničene su situacije u kojima bi se prikupljanje i obrada podataka o ličnosti zaposlenih morala zasnivati na pristanku ovih lica. Pored toga, treba imati na umu da pristanak mora biti slobodno dat bez ikakvih uslovljavanja, što je delikatno pitanje u odnosima zaposlenih i poslodavaca koji se odlikuju pravnom podređenošću zaposlenog. Takođe, pristanak se u svakom trenutku može opozvati, čime svaka dalja obrada

zasnovana na tom pristanku postaje nezakonita.

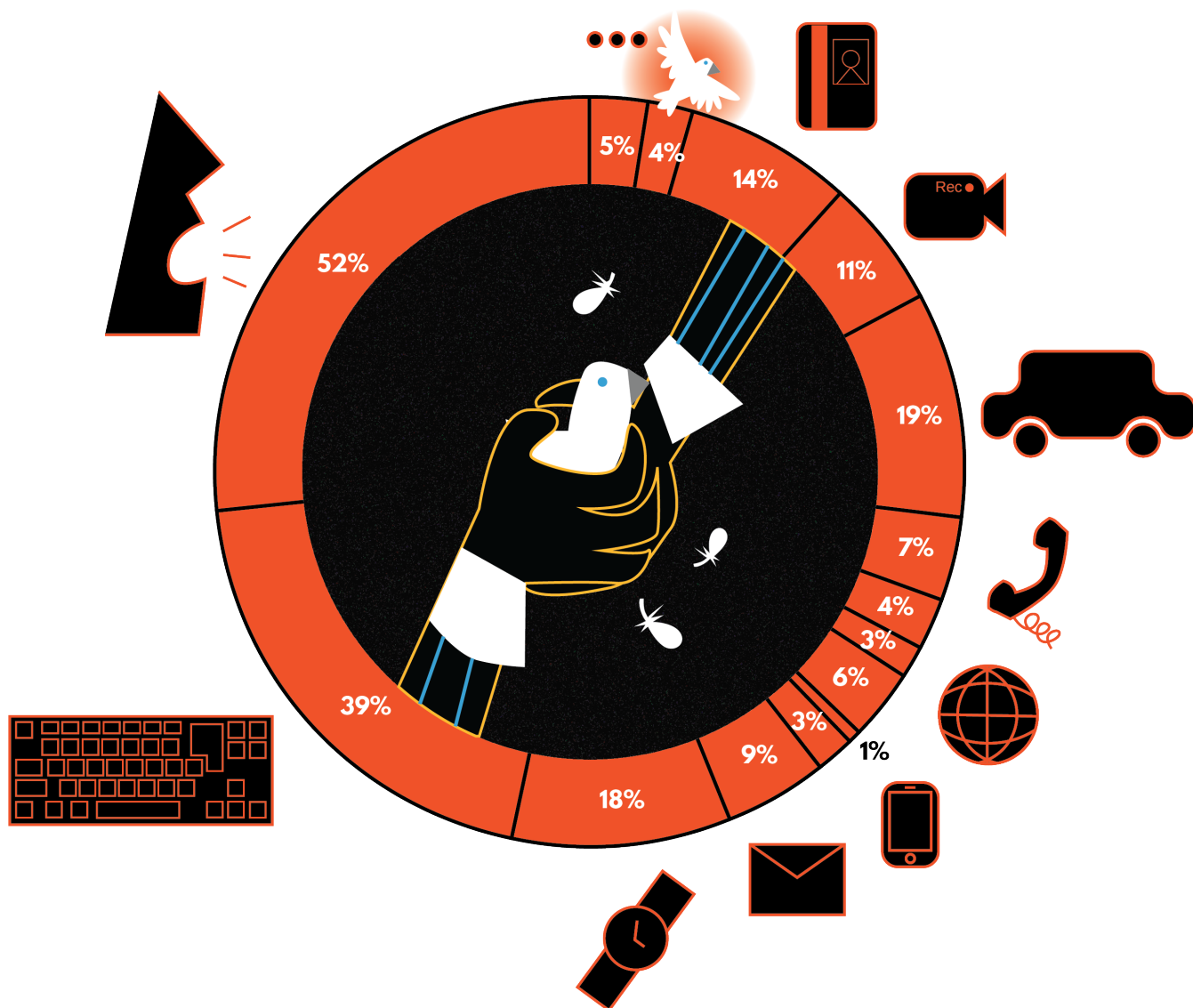
Da zaključimo, brojni poslodavci nisu upoznati ili namerno krše svoje zakonske obaveze. Nepoštovanje ZZPL je dobrim delom u sprezi i sa blagim kaznenim odredbama. Ovakva politika dodatno otvara prostor za zloupotrebe u nadzoru zaposlenih.

PRAĆENJE EFIKASNOSTI ZAPOSLENIH

1. NADZOR ZAPOSLENIH UOPŠTE

Uopšteno gledajući, većina poslodavaca prati rad zaposlenih koji rade od kuće, na isti način na koji je to činila i dok su ovi radili u prostorijama poslodavaca. Kako navode i zaposleni i poslodavci pri radu od kuće korišćeni su metodi nadzora koji su ranije ustanovljeni. Kao što prikazuje grafik 4. najveći broj poslodavaca rad zaposlenih prati putem usmenih i pismenih izveštaja koje zaposleni dostavljaju poslodavcu ili unošenjem vremena koje je zaposleni potrošio radom na određenom projektu koje unosi sam zaposleni. Takođe, poslodavci nagledaju e-mail korespondenciju zaposlenih, prate korišćenje službenih vozila i telefona, koriste aplikacije za praćenje efikasnosti rada, video nadzor, a deo njih prati i aktivnost zaposlenih na internetu i društvenim mrežama.

11 Kako bi obrada podataka o ličnosti bila zakonita, ona mora biti zasnovana na jednom od zakonom propisanih osnova, odnosno mora ispuniti jedan od sledećih uslova koji su propisani Zakon o zaštiti podataka o ličnosti: (i) lice na koje se podaci o ličnosti odnose je pristalo na obradu svojih podataka o ličnosti za jednu ili više posebno određenih svrha; (ii) obrada je neophodna za izvršenje ugovora zaključenog sa licem na koje se podaci odnose ili za preduzimanje radnji, na zahtev lica na koje se podaci odnose, pre zaključenja ugovora; (iii) obrada je neophodna u cilju poštovanja pravnih obaveza rukovaoca; (iv) obrada je neophodna u cilju zaštite životno važnih interesa lica na koje se podaci odnose ili drugog fizičkog lica (v) obrada je neophodna u cilju obavljanja poslova u javnom interesu ili izvršenja zakonom propisanih ovlašćenja rukovaoca; (vi) obrada je neophodna u cilju ostvarivanja legitimnih interesa rukovaoca ili treće strane, osim ako su nad tim interesima pretežniji interesi ili osnovna prava i slobode lica na koje se podaci odnose koji zahtevaju zaštitu podataka o ličnosti, a posebno ako je lice na koje se podaci odnose maloletno lice.



Grafikon 4. Šta se od sledećeg primenjuje u Vašoj kompaniji od kada je rad organizovan od kuće? ODGOVORI POSLODAVACA

*Napomena. Moguće više odgovora

5% **Nisu odgovorili**

4% **Drugo**

14% **Nije bilo nikakvog nadzora**

11% **Video nadzor**

19% **U službenim vozilima se prati kilometraža i putanje**

7% **Praćanje razgovora između radnika i klijente**

4% **Praćenje službenog telefona**

3% **Prati se aktivnost na socijalnim mrežama**

6% **Prati se aktivnost na internetu**

1% **Koristi se program kojim se meri prelazak između aplikacija (npr. Teramind)**

3% **Aplikacija ili aplikacije mere vreme provedeno u toj aplikaciji (npr. Habstaf i sl.)**

9% **Nadgleda se e-mail komunikacija**

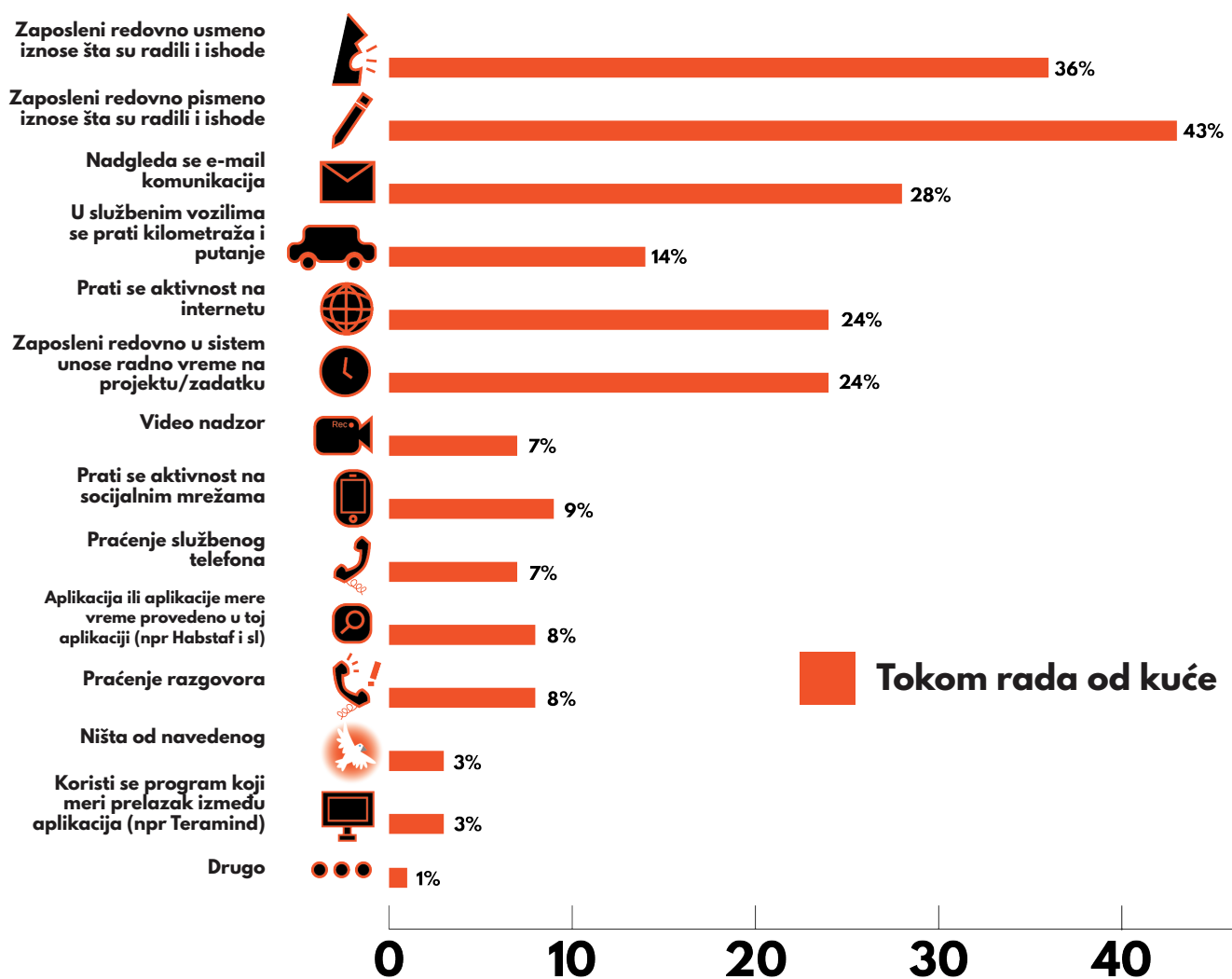
18% **Zaposleni redovno u sistem unose radno vreme**

39% **Zaposleni redovno pismeno iznose šta su radili i ishode**

52% **Zaposleni redovno usmeno znose šta su radili i ishode**

Zaposleni takođe najčešće kao oblik nadzora navode usmeno i pismeno izveštavanje o obavljenom poslu, zatim nadgledanje e-mail komunikacije, praćenje kilometraže u službenim

vozilima, praćenje aktivnosti na internetu, redovno unošenje podataka o radnom vremenu u sistem i video nadzor. Grafik 5. prikazuje detaljnije dobijene odgovore:



Grafikon 5. Šta se od sledećeg primenjuje u Vašoj kompaniji od kada je rad organizovan od kuće? ODGOVORI RADNIKA

*Napomena. Moguće više odgovora

Da bi mogli da prikupljaju ovakve podatke zaposlenih, poslodavci moraju da imaju pravni osnov. Po pravilu, osnov obrade podataka o ličnosti zaposlenih, koji se prikupljaju prilikom video nadzora zaposlenih, jeste legitiman interes poslodavca. Kako bi se utvrdila opravdanost sprovođenja ovakvog načina nadzora, potrebno je da poslodavac sprovede procenu legitimnog interesa kao osnova obrade podataka o ličnosti, kojom prilikom se mora utvrditi da li se svrha usled koje dolazi do obrade podataka o ličnosti može ostvariti primenom drugih oblika nadzora kojima se manje zadire u privatnost lica. Procena legitimnog interesa poslodavca bi trebalo da bude izričito dokumentovana.

Nadzor koji nije neophodan, već je moguće ostvariti svrhu i putem manje invazivnog načina kontrole (u ovom slučaju **merenje efikasnosti zaposlenih**), mora se prekinuti. Ovo važi kako za rad od kuće tako i za rad u prostorijama poslodavca. Na primer, poslodavac koji koristi video nadzor na ulazu u zgradu ili u pojedinim hodnicima iz bezbednosnih razloga bi trebalo da osim Pravilnika o video nadzoru izvrši procenu legitimnog interesa u skladu sa tripartitnim testom i takvu procenu dokumentuje u skladu sa modelom koji je Poverenik objavio.¹²

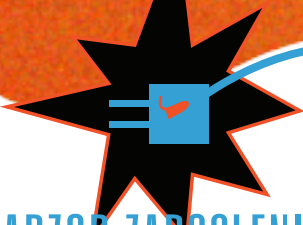
Određene vrste monitoringa, kao što je **nadgledanje email korespodencije, video nadzor i snimanje telefonskih razgovora je prema stanovištu Poverenika dozvoljeno samo u izuzetnim slučajevima**, i to u jasno određenu svrhu koja se ne može postići na drugi način.

Praćenje aktivnosti zaposlenih na socijalnim mrežama predstavlja problematičan način nadzora zaposlenih. U određenim situacijama ovakvo postupanje poslodavca bi moglo biti legitimno, na primer ako je njihovo korišćenje deo radne obaveze zaposlenih ili iz određenih razloga postoji izričita zabrana korišćenja određenih društvenih mreža i sajtova.

Ovakvo postupanje bi bilo dozvoljeno samo uz punu transparentnost, odnosno jasno i potpuno obaveštavanje zaposlenih o ovakvom praćenju. Ipak u najvećem broju slučajeva ovako postupanje ne bi bilo dozvoljeno čak ni uz punu transparentnost i to ukoliko ne bi postojala jasna i dozvoljena svrha za takvo postupanje, pa bi tako nasumično nadgledanje korišćenja društvenih mreža zaposlenih bilo nedozvoljeno (ZZPL, 2018).

Kako pokazuje istraživanje, i pre prelaska na rad od kuće poslodavci su vršili nadzor nad zaposlenima na načine koji su zakonom nedozvoljeni ili su dozvoljeni samo pod posebnim okolnostima. Tokom rada od kuće ovi pristupi u nadzoru zaposlenih uopšte i nadzoru efikasnosti zaposlenih su zadržani, a kako ćemo videti iz sledećeg poglavlja i prošireni uvođenjem aplikacija za praćenje rada zaposlenih od kojih je korišćenje nekih od njih nedozvoljeno budući da ovakav način prikupljanja podataka o ličnosti nije opravdan svrhom koja se ovakvim postupanjem ostvaruje na strani poslodavaca.

¹² O poštovanju ovog principa biće reči nešto kasnije u tekstu ispod.



2. NADZOR ZAPOSLENIH PREKO POSEBNIH APLIKACIJA

Kako rezultati istraživanja pokazuju, obim nadzora zaposlenih preko posebnih aplikacija je relativno mali. Softver za praćenje efikasnosti se retko koristio (2%), ali je bio češći u IT industriji (13%) i za zaposlene iz pozivnih centara (8%). Svega 8% zaposlenih i 4% poslodavaca navelo je da koristi aplikacije za praćenje efikasnosti novije generacije kao što su *Clockify*¹³ i *Time Doctor*¹⁴ (Hamers, 2019; Christian, 2020) od kojih je prva zasnovana na poverenju između poslodavca i zaposlenog da su uneta vremena rada na tačno određenim projektima ili zadacima tačna, a druga se smatra intruzivnom i može biti instalirana bez znanja zaposlenog.

Intervjui sa ekspertima u oblasti zaštite prava ličnosti¹⁵ i sindikatima¹⁶ pokazuju da su poslodavci razmatrali uvođenje različitih aplikacija, ali su odustali posle konsultacija sa advokatom ili posle intervencije sindikata.

Važno je znati da se i aplikacije koje nisu namenjene nadzoru rada zaposlenih od kuće mogu koristiti za nedozvoljeni nadzor. To je na primer slučaj sa korišćenjem aplikacije Zoom i sličnih koje se koristi za održavanje sastanaka. Tako naši intervju pokazuju da je od zaposlenih traženo da tokom radnog vremena drže upaljenu kameru

na svom kompjuteru da bi poslodavac mogao da ih nadgleda¹⁷, što predstavlja povredu prava radnika na privatnost i način prikupljanja podataka o ličnosti koji ne može biti opravdan legitimnim interesom poslodavca.¹⁸ Još jedna vrsta zloupotrebe vezana je za korišćenje inače neinvazivne aplikacije Slack gde je poslodavac tražio da zaposleni u veoma kratkim periodima vremena unose svoje aktivnosti čime je omogućio stalni nadzor njihovih aktivnosti u realnom vremenu.¹⁹

Iako korišćenje aplikacija za praćenje produktivnosti i efikasnosti kod nas nije previše često, primeri iz drugih zemalja ukazuju da se ono brzo širi. Zato smo posebnu pažnju posvetili pretpostavkama za instaliranje ovih aplikacija na opremi koji zaposleni koriste u radu.

Videli smo da se u praksi u Srbiji u radu od kuće koriste kako kompjuteri u vlasništvu kompanije tako i oni u privatnom vlasništvu. Iz pitanja vlasništva proizilazi i pravo pristupa kompjuteru zaposlenog. U našem istraživanju oko 40% zaposlenih izjavljuje da poslodavci imaju pristup njihovim računarima na daljinu, a to je naročito slučaj kada je reč o zaposlenima u pozivnim centrima (64%). Imajući u vidu da su u anketi i intervjuima radnici u pozivnim centrima²⁰ izjavili da se u praćenju efikasnosti njihovog rada ništa nije promenilo, ovako visok procenat ne treba tumačiti kao povećanje već postojeće intruzivnosti u privatnost zaposlenih

13 Clockify je uređaj za praćenje vremena zasnovan na poverenju, što znači da se pojedinci ohrabruju da verno i odgovorno unose informacije u aplikaciju

14 Time Doctor je jedan od najpopularnijih proizvoda za praćenje efikasnosti zaposlenih koja se može koristiti za nadgledanje web lokacija i aplikacija kako bi se izlečile „navike gubljenja vremena“. Kompanija svoj proizvod predstavlja kao „alat za produktivnost“, a ne kao „alat za nadzor“ ali se on može koristiti za praćenje nekoga bez njihovog znanja.

15 Intervju sa ekspertom za oblast zaštite podataka o ličnosti, 21. januar, 2022.

16 Intervju sa predstavnicima sindikata, 19. januar, 2022.

17 Ibid

18 Intervju sa ekspertom za oblast zaštite podataka o ličnosti, 21. januar, 2022.

19 Ibid

20 Intervju sa zaposlenima u pozivnim centrima 29. septembar, 2021, 30. septembar, 2021.

koja postoji u ovoj industriji (Jakobi & Radonjić, 2019). Trećina zaposlenih navodi da poslodavac može da pristupi njihovom kompjuteru uz njihov pristanak, trećina ne odobrava pristup svom kompjuteru već poslodavac može bilo kada da pristupi njihovom računaru, a ostali su rekli da poslodavac ni pod kakvim uslovima ne može da pristupi njihovom kompjuteru. Ovaj poslednji odgovor treba sagledati u svetlu dodatnih podataka, odnosno da su među aplikacijama koje su zaposleni najčešće instalirali upravo one koje daju mogućnost IT podršci kompanije (AnyDesk, TeamViewer, na primer) da pristupi kompjuteru zaposlenog bilo da otkloni neku grešku u radu kompjutera ili instalira novi softver.

Ako podatke o pristupu kompjuteru sagledamo iz ugla vlasništva, vidimo da je od 37% ispitanika koji su naveli da koriste računar u vlasništvu kompanije, više od polovine njih (60%) izjavilo da poslodavac ima mogućnost pristupa njihovom računaru, bilo sa ili bez prethodnog odobrenja od strane samog zaposlenog.

Mogućnost pristupa računarima i podacima na daljinu sama po sebi ne predstavlja povredu prava na privatnost. Ipak, on je dozvoljen samo ukoliko je ovo neophodno, ukoliko za to postoji opravdana i zakonita svrha i ukoliko je pristup u potpunosti transparentan. U tom kontekstu **pristup na daljinu bez dozvole zaposlenog** (čega je svesno svega 13% zaposlenih) nije u skladu sa načelima obrade propisanim ZZPL - om kao ni zagaranovanim pravom na dostojanstvo ličnosti propisanim

Zakonom o radu.

Da zaključimo, imajući u vidu da je kompjuter/laptop pre svega sredstvo za rad koje je poslodavac u obavezi da nabavi, instalira i održava **postoje legitimni zahtevi poslodavca da ima određeni pristup ovom kompjuteru kao delu sopstvene tehničke infrastrukture**. Sa druge strane pristup privatnom kompjuteru na kome se nalaze lični podaci zaposlenog bi u velikom procentu slučajeva mogao predstavljati kršenje prava na privatnost zaposlenih. U tom smislu, jedino jasno rešenje je da se za obavljanje posla isključivo koristi kompjuter u vlasništvu kompanije, dok bi se privatni računari ili drugi uređaji (mobilni telefoni) mogli sporadično koristiti u izuzetnim situacijama, na primer za proveru e-mail komunikacije i slično, ali tada poslodavac nema pristup ličnom uređaju zaposlenog. Ukratko, na ovaj način se rešava i čitav niz daljih pitanja, s obzirom da je mogućnost instaliranja i ograničenja aplikacija od strane poslodavca, ograničenog pristupa računaru i održavanja računara mnogo lakše ostvarivo u skladu sa pravilima ZZPL - a ukoliko je u pitanju kompjuter kompanije na kome zaposleni ne skladišti i druge svoje lične podatke koje nemaju veze sa obavljanjem posla, dok su rizici povrede prava privatnosti zaposlenih u slučaju kada je kompjuter u vlasništvu zaposlenog mnogo veći.

3. PROCENA UTICAJA PRAĆENJA EFIKASNOSTI ZAPOSLENIH NA ZAŠTITU PODATAKA O LIČNOSTI

Videli smo da je mali procenat poslodavaca instalirao aplikacije za praćenje efikasnosti zaposlenih. Većina onih koji su to uradili (77%) obavestila je zaposlene pismenim putem da će koristiti ove aplikacije pre njihovog instaliranja, dok su ostali poslodavci ovo obaveštenje podelili sa zaposlenima usmenim putem pre početka korišćenja aplikacije (7.7 %) ili usmenim putem pošto je korišćenje ovih aplikacija već počelo (7.7%) . Preostali poslodavci nisu svoje zaposlene obavestili o tome.

Za samo korišćenje gore pomenutih aplikacija ne može se bez ulaska u detalje reći da li predstavljaju kršenje prava na privatnost zaposlenih ili opravdan, legitiman i dozvoljen način za vođenje poslovnih procesa. To zavisi od više faktora kao što su svrha ovakvog praćenja, sektor u kome se posluje, srazmernost ovakvog praćenja, transparentnost i drugo.

Ako je verovatno da će neka vrsta obrade prouzrokovati visok rizik za prava i slobode fizičkih lica – u ovom slučaju zaposlenih, rukovalac, tj. poslodavac će biti u obavezi da izvrši **procenu uticaja obrade na zaštitu podataka o ličnosti** pre započinjanja obrade. U našoj anketi sa poslodavcima od već veoma malog broja onih koji

koriste ovakve aplikacije polovina je sproveda procenu uticaja na zaštitu podataka o ličnosti. Ako procena uticaja na zaštitu podataka o ličnosti, koja je izvršena, ukazuje da će nameravane radnje obrade proizvesti visok rizik ako se ne preduzmu mere za umanjeње rizika, rukovalac je dužan da zatraži **mišljenje Poverenika** pre započinjanja radnje obrade.

Iako vidimo da u praksi poslodavaca postoje primeri kršenja Zakona o zaštiti podataka o ličnosti, Poverenik u posmatranom periodu nije primio nijednu žalbu niti je u svom redovnom nadzoru naišao na primer nedozvoljenog korišćenja aplikacija za praćenje efikasnosti zaposlenih.²¹

Ukratko, čini se da relativno nizak nivo korišćenja intruzivnih aplikacija za praćenje efikasnosti zaposlenih nije rezultat strogog poštovanja pravila propisanih zakonom već ga treba tražiti u drugim uzrocima među kojima su niži nivo tehnološke pismenosti, kao i različiti faktori odvrćanja kao što su saveti stručnih lica i aktivno delovanje sindikata.

21 Intervju, Poverenik za informacije od javnog značaja i zaštite podataka o ličnosti, 18. februar 2022.

ČUVANJE PODATAKA O LIČNOSTI I POVREDA PRAVA NA PRIVATNOST

1. ČUVANJE PODATAKA O LIČNOSTI

Obaveštenje zaposlenom o prikupljanju i obradi njegovih podataka sadrži i informaciju o načinu čuvanja tih podataka, osobama koje imaju pristup tim podacima i mogućnostima zaposlenog da ima uvid u te podatke i prava da ih izmeni ili zahteva brisanje u slučajevima predviđenim ZZPL - om.

Među zaposlenima je svega njih 38% reklo da je svesno postojanja dokumenta koji uređuje čuvanje podataka. Svega 40% anketiranih zna gde se taj dokument može jednostavno pronaći (ili je dostavljen ili je na oglasnoj tabli).

Zaposleni su pokazali nešto bolje znanje o tome kako se čuvaju njihovi podaci i ko ima pristup tim podacima. Većina (70%) je navela da preduzeće u kojem rade, čuva njihove lične podatke u elektronskom i u papirnom obliku, dok jedna trećina nije bila upoznata sa tim gde se čuvaju njihovi podaci.

Najveći broj ispitanika rekao je da njihovim podacima može da pristupi kadrovska služba (61%) ili njihov neposredni nadređeni (57%) ili finansijska služba (31%). Jedna petina

zaposlenih (20%) prijavila je da njihovim podacima može da pristupi veliki broj kolega (svi nadređeni ili čak svi radnici). Slični podaci dobijeni su i u anketi sa poslodavcima koji su takođe rekli da pristup podacima imaju kadrovska služba (46%), nadređeni (16%) i finansijska služba (10%). Zabrinjava ipak što 46% poslodavca nije odgovorilo na ovo pitanje, a još 10% je izabralo odgovor da svi nadređeni ili čak svi radnici imaju pristup ovim podacima. Ako govorimo samo o čuvanju podataka o produktivnosti i pristupu tim podacima vidimo da je 88% zaposlenih reklo da ne znaju gde se čuvaju informacije o produktivnosti, 75% nema informacije o posledicama praćenja njihovog rada, a 43% zaposlenih ne zna koliko se često proveravaju informacije o produktivnosti i prisutnosti. Istovremeno, više od 50% zaposlenih navelo je da nemaju pristup sopstvenim unosima o produktivnosti. To ne mora samo po sebi biti povreda prava, ali oni moraju biti obavešteni o tome da imaju pravo da zahtevaju i pristupe ovim podacima (ZZPL, 2018).

Da zaključimo, iz odgovora zaposlenih i poslodavaca može se uočiti da mnogi poslodavci podatke o ličnosti zaposlenih skladište tako da svi zaposleni imaju pristup o njima, što nije dozvoljeno. Podaci o ličnosti moraju se čuvati na takav način da samo ovlašćena lica smeju imati pristup kroz odgovarajući sistem autorizacija pristupa (ZZPL, 2018).

U skladu sa ZZPL - om, lični podaci koji se odnose na zaposlenog ne mogu da budu dostupni trećem licu, osim u slučajevima i pod uslovima utvrđenim

zakonom ili ako je to potrebno radi dokazivanja prava i obaveza iz radnog odnosa ili u vezi sa radom. Ukoliko dođe do povrede gore navedenih prava, zaposleni ima pravo da traži, po pravilima obligacionog prava, naknadu štete, i to zbog povrede prava ličnosti.

Zaposleni su retko znali da imaju pravo uvida u dokumente koji sadrže lične podatke koji se čuvaju kod poslodavca i pravo da zahtevaju brisanje podataka koji nisu od neposrednog značaja za poslove koje obavljaju iako je to propisano zakonom. Zakon garantuje svakome **pravo na uvid** (ZZPL, 2018), odnosno da u Zakonom propisanoj proceduri ostvari **pravo na pristup** podacima koji se odnose na njega. Pravo na uvid povezano je sa pravom da se traži ispravka ili brisanje u zakonom predviđenim slučajevima. Ovakav stepen neobaveštenosti među zaposlenima dovodi u pitanje sposobnost poslodavaca da na adekvatan način informišu svoje zaposlene o njihovim pravima.

Kad je obaveštenost poslodavaca u vezi sa čuvanjem ličnih podataka o zaposlenima u pitanju, već pomenuti podatak da je svega 41% poslodavaca svojim internim aktima regulisalo oblast prikupljanja i skladištenja podataka o ličnosti, govori da poslodavci nedovoljno dobro poznaju ovu materiju. Ovo potvrđuju i intervjui sa ekspertima koji primećuju veoma mali pomak u primeni ZZPL - a na kompanijskom nivou.²²

2. POVREDE PRAVA NA PRIVATNOST

Sagledavanje razmera poznavanja, odnosno nepoznavanja propisa o zaštiti podataka o ličnosti na radnom mestu omogućava nam da bolje razumemo i prikupljene podatke o povredama prava na privatnost.

Zaposleni i rukovodioci u niskom procentu prepoznaju povrede prava na privatnost u svojim kompanijama. Zaposleni su naveli da su oni retko - (7%), ali i njihove kolege (8%) bili u situacijama koje se mogu svrstati kao povreda prava na privatnost. Kao glavni oblik povrede znali su da prepoznaju "neovlašćeni pristup podacima zaposlenih". Istovremeno, 82% poslodavaca reklo je da nisu bili u situaciji da sumnjaju da su povredili privatnost svojih zaposlenih. Ostalih 18% imali su nedoumica o poštovanju privatnosti u slučaju zahteva za obaveznom vakcinacijom zaposlenih, ili uvida u podatke o vakcinaciji zaposlenih ili u slučaju skeniranja lica tokom ulaska i izlaska radnika iz firme.

Na pitanje da li veruju da je praksa povrede prava na privatnost zaposlenih rasprostranjena u Srbiji, zaposleni pokazuju da imaju poverenje u (svoje) poslodavce. Tako više od 80% ispitanika, u potpunosti ili uglavnom veruje da se njihovi lični podaci u preduzeću skupljaju i koriste na zakonit način, a većina veruje su slučajevi neovlašćenog prikupljanja podataka

22 Intervju sa ekspertom za oblast zaštite podataka o ličnosti, 12. januar, 2022.

zaposlenih slabo rasprostranjeni u Srbiji. Poslodavci s druge strane manje veruju svojim kolegama: 69% njih smatra da su slučajevi neovlašćenog prikupljanja podataka zaposlenih relativno ili veoma rasprostranjeni u Srbiji.

V ZAKLJUČCI

Rezultati istraživanja pokazuju da kako na strani zaposlenih, tako i na strani poslodavaca ne postoji razumevanje njihovih prava i obaveza kada je u pitanju rad od kuće i zaštita podataka o ličnosti.

Nerazumevanje i nepoznavanje prava i obaveza je znatno izraženije u pogledu prikupljanja i obrade podataka o ličnosti. Iako je ZZPL stupio na snagu pre više od dve godine, njegova primena u praksi je i dalje ograničena, te poslodavci ne razumeju na koji način da obezbede zakonitost prikupljanja i obrade podataka o ličnosti zaposlenih.

U trenutku izbijanja pandemije, Srbija nije raspolagala odgovarajućim mehanizmima za zaštitu prava na privatnost radnika koji rade od kuće ili na daljinu, uprkos tome što su ova prava prepoznata u Zakonu o radu. Delom je razlog to što je visina zaprečenih kazni relativno niska i što se primena ovih odredbi u praksi dodatno slabo primenjuje. Takođe, propuštanje da se odredbe Zakona o radu usklade

sa ZZPL-om u propisanim rokovima, stvorilo je prostor da poslodavci potencijalno pređu granicu legitimnog prava na nadzor radnika. Takođe, Zakon o radu, rad od kuće definiše u samo dva člana, te bi bilo neophodno da se ovo pitanje detaljnije reguliše.

PREDLOG POLITIKA KOJE BI TREBALO UVESTI NA NACIONALNOM NIVOU I NIVOU PREDUZEĆA

1. PREPORUKE ZA KREATORE POLITIKA

S obzirom da je **Zakon o zaštiti podataka o ličnosti** donet po uzoru na Opštu Uredbu o zaštiti podataka EU, on sadrži niz opštih odredbi i pravnih standarda što predstavlja izazov za primenu čak i onim poslodavcima koji sasvim žele da se usklade sa ovim Zakonom. U tom kontekstu potreban je niz **normativnih intervencija** kako bi se olakšala primena i obezbedila pravna sigurnost u ovoj oblasti:

▶ Raditi na **izmenama i dopunama ZZPL - a** kako bi se rešile nedoumice koje zadaju probleme u primeni zakona. Naročito treba obratiti pažnju na odredbe koje se tiču radnog prava, s

obzirom da trenutno samo član 91 na izuzetno opšti način reguliše ovu oblast. Izrada Strategije Zaštite podataka o ličnosti, u kojoj su među članovima radne grupe i predstavnici Ministarstva za rad, zapošljavanje, boračka i socijalna pitanja predstavlja odličnu priliku da se utvrde strateški pravci rada u oblasti obrade podataka o ličnosti zaposlenih.

▶ Uskladiti **radno zakonodavstvo** sa Zakonom o zaštiti podataka o ličnosti. Obaveza usklađivanja svih zakona je propisana članom 100 ZZPL - a i ovo usklađivanje je trebalo da se završi do kraja 2020-te godine.

▶ Insistirati na donošenju **Zakona koji bi regulisao video nadzor** s obzirom da je ova oblast sasvim neregulisana. Posebnu pažnju treba posvetiti regulisanju video nadzora zaposlenih koji rade van prostorija poslodavca.

▶ Raditi na usklađivanju prakse kroz objavljivanje **stavova i mišljenja Poverenika** u oblasti radno pravnih odnosa, sa posebnim osvrtom na pitanja nadzora zaposlenih i primene novih tehnologija.

▶ Raditi na izradi **kodeksa postupanja** koji bi regulisao ovu oblast. Ovaj institut je predviđen članom 59 ZZPL - a ali nije zaživeo u praksi. Ovakav kodeks bi mogao biti donet na nivou različitih udruženja kao što su Unija poslodavaca, Privredna komora ili drugih užih entiteta. Ovakvi kodeksi se izrađuju u cilju efikasnije primene zakona, odobravaju se od strane Poverenika i mogu regulisati sva sporna pitanja u ovoj

oblasti.

▶ **Pokrenuti inicijativu za usvajanje Konvencije o radu kod kuće br. 177 iz 1996. godine Međunarodne organizacije rada**, koja utvrđuje norme opšte primene u pogledu uslova rada koji se mogu primeniti na radnike koji rade od kuće, a koja će uzeti u obzir posebne karakteristike rada kod kuće.

2. PREPORUKE ZA POSLODAVCE

Poslodavci bi u svom radu trebalo da primene sledeće mere kako bi ispoštovali obaveze propisane Zakonom o zaštiti podataka o ličnosti i Zakonom o radu:

▶ Ukoliko to nije već učinjeno, **sprovesti detaljan projekat usklađivanja sa Zakonom o zaštiti podataka o ličnosti** koji, između ostalog, podrazumeva mapiranje svih podataka o ličnosti, određivanje njihove konkretne svrhe i pravnog osnova za obradu, određivanje rokova čuvanja, donošenje procedura i pravilnika koji regulišu način postupanja sa tim podacima, revizija i osnaživanje tehničkih i organizacionih mera, obezbeđivanje adekvatnog međunarodnog transfera (ako postoji).

▶ Organizovati **obuke** o obavezama i pravima u ovoj oblasti kako za menadžment tako i za ostale zaposlene. Obuke bi trebalo organizovati na godišnjem nivou.

Poštovati obavezu zaključivanja aneksa ugovora o radu u slučaju prelaska na rad na daljinu ili rad od

kuće koji bi regulisao način vršenja nadzora nad zaposlenim i korišćenje i upotrebu sredstava za rad, kao i naknadu za korišćenje sredstava zaposlenog, te naknadu drugih troškova. Ukoliko se radni odnos od samog početka obavlja van prostorija poslodavca, takav ugovor o radu mora da sadrži sve neophodne elemente propisane Zakonom o radu.

▶ Težiti praksi da se svim zaposlenima, kada je to neophodno ili moguće, **obezbedi kompjuter** od strane poslodavca kao osnovno sredstvo za rad. Kompjuter koji se isključivo koristi za radne obaveze zaposlenih znatno olakšava primenu propisa od strane poslodavca te čuva privatnost zaposlenih.

▶ Ne koristiti **pristanak kao pravni osnov za obradu podataka o ličnosti** zaposlenih preširoko tj. samo izuzetno: s obzirom da ovo nije jedini pravni osnov za prikupljanje i obradu podataka o ličnosti, poslodavci moraju izbeći trenutnu praksu da ove aktivnosti zasnivaju na pristanku zaposlenih čak i kada ovo nije adekvatan pravni osnov, već zasnovati prikupljanje i obradu podataka o ličnosti na adekvatnim pravnim osnovama propisanim ZZPL-om (kao što su izvršenje nekog ugovora, poštovanja pravnih obaveza i drugi).

▶ **Obaveštenje o obradi podataka o ličnosti** zaposlenih izraditi u skladu sa zakonom što znači da mora sadržati sve propisane informacije, ali i biti sastavljeno na sažet, transparentan i razumljiv način, te treba zaposlenima biti uvek i lako dostupno.

▶ Poštovati obavezu **izrade Procene uticaja radnji obrade na zaštitu podataka o ličnosti** u situacijama koje mogu proizvesti visok rizik po prava i slobode zaposlenih (što može biti slučaj prilikom korišćenja određenih aplikacija za nadzor nad obavljanjem rada zaposlenih, ali i u drugim slučajevima). S obzirom na kompleksnost ove obaveze, bilo bi poželjno da se izrade smernice za izradu ovakve procene od strane Poverenika ili esnafskih udruženja.

▶ Osim opštih dokumenata koji se odnose na obradu podataka o ličnosti, a koji su neophodni prema Zakonu o zaštiti podataka o ličnosti, kompanije bi morale da izrade i **interne dokumente o obradi podataka o ličnosti** koji se bave specifičnim pitanjima kao što su korišćenje aplikacija za nadzor zaposlenih, video nadzor, pristup računarima na daljinu. Izradu ovih dokumenata bi morale da prate stroge i transparentne procedure kako ne bi došlo do povrede podataka o ličnosti zaposlenih i drugih radno angažovanih lica. I u ovom slučaju izrada smernica za sastavljanje ovakvih dokumenata od strane Poverenika ili esnafskih udruženja bila bi dobrodošla.

3. PREPORUKE ZA SINDIKATE

Sindikati bi u svom radu trebalo da pojačaju mere informisanja svojih članova i zaposlenih uopšte o obavezama propisanih Zakonom o zaštiti podataka o ličnosti i Zakonom o radu.

- ▶ Samostalno ili u saradnji sa udruženjima poslodavaca organizovati **obuke** o obavezama i pravima koji proizilaze iz ove oblasti.
- ▶ Obučiti sindikalne predstavnike u preduzećima da u **slučaju sklapanja kolektivnih ugovora o radu insistiraju na ugrađivanju obaveza i prava poslodavaca i zaposlenih u vezi sa nadzorom na radu i kod kuće** u ove dokumente.
- ▶ U saradnji sa Inspektoratom za rad i poslodavcima izraditi smernice za **preventivni nadzor poslodavaca čiji zaposleni rade od kuće**.
- ▶ Samostalno, ili u saradnji sa poslodavcima i/ili nevladinim organizacijama koje se bave zastupanjem prava radnika organizovati kampanje za **informisanje radnika o njihovim pravima tokom rada od kuće**.
- ▶ U saradnji sa inostranim sindikatima i samostalno pratiti pojavu novih aplikacija za nadzor zaposlenih od kuće i **informisati zaposlene i široku javnost o prednostima i manama ovih aplikacija**.
- ▶ U saradnji sa stručnjacima iz oblasti zaštite podataka o ličnosti, eksperata u oblasti visokih tehnologija, predstavnikom Poverenika za zaštitu podataka o ličnosti i drugim zainteresovanim stranama **organizovati okrugle stolove o uticaju visokih tehnologija na razvoj novih tehnika za nadzor zaposlenih**.

4. PREPORUKE ZA NEVLADINE ORGANIZACIJE

Nevladine organizacije na različite načine mogu da podrže aktivnosti:

- ▶ Kroz rad u različitim telima koje se bave monitoringom harmonizacije propisa između EU i Srbije, u vezi sa Poglavljem 19 Socijalna politika i zapošljavanje staviti **fokus na uređivanje oblasti nadzora na radu i posebno nadzora zaposlenih prilikom obavljanja rada od kuće**.
- ▶ U saradnji sa stručnjacima iz oblasti zaštite podataka o ličnosti, ekspertima u oblasti visokih tehnologija, predstavnikom Poverenika za zaštitu podataka o ličnosti i drugim zainteresovanim stranama **voditi kampanje za jačanje svesti radnika, posebno onim u novim formama rada, o rizicima nadzora na radu na daljinu i od kuće**.

LITERATURA

Ball, K. (2021), *Electronic Monitoring and Surveillance in the Workplace*, Publications Office of the European Union, Luxembourg. Retrieved from <https://publications.jrc.ec.europa.eu/repository/handle/JRC125716>

Barrenechea-mendez, M., Ortin-Angel, P., Rodes, E.C. 2016. *Autonomy and Monitoring*, *Journal of Economic and Management Strategy*, 25 (4): 911 – 935

Blum, S. (2022). *Employee surveillance is exploding with remote work—And could be the new norm*. Morning Brew. [web log]. Retrieved from <https://www.morningbrew.com/series/the-years-ahead/stories/2022/01/19/employee-surveillance-is-exploding-with-remote-work-and-could-be-the-new-norm>

Bodie, M. T., Cherry, M. A., McCormick, M. L., & Tang, J. 2016. *The law and policy of people analytics*. *University of Colorado Law Review*, 88(4): 961–1042.

Chouffani, R. (2021). *What is BYOD? Bring Your Own Device Definition*. WhatIs.Com. [web log]. Retrieved from <https://whatistechtarget.com/definition/BYOD-bring-your-own-device>

Christian, A. (2020). *Corporate snitches are using screen monitoring to find and fire slackers* [web log]. Retrieved from <https://www.wired.co.uk/article/productivity-tracking-office-surveillance>

European Commission. (2021). *Electronic monitoring and surveillance in the workplace: Literature review and policy recommendations*. Publications Office. Brussels: European Commission. Retrieved from <https://data.europa.eu/doi/10.2760/5137>

Fairweather, N. B. (1999). *Surveillance in Employment: The Case of Teleworking*. *Journal of Business Ethics*, 22(1), 39–49. <https://doi.org/10.1023/A:1006104017646>

Graham, S., & Wood, D. (2003). *Digitizing Surveillance: Categorization, Space, Inequality*. *Critical Social Policy*, 23(2), 227–248. <https://doi.org/10.1177/0261018303023002006>

Hamers, K. (2019). *The Best Windows Time Trackers for more productivity in 2020* [web log]. Retrieved from <https://www.projecttimer.com/best-windows-time-trackers-2020/>

Jakobi, T. & Radonjić, Lj. (2020). *Da li da ostanem ili da odem? Da li su kontakt centri i zajednički uslužni centri dobar karijerni izbor za stručnu radnu snagu u Srbiji*. Beograd: Centar za istraživanje javnih politika. <https://publicpolicy.rs/publikacije/2547b25a2c8eeb14cbadeeebe674b1a458e850ac.pdf>

Lee, S., & Kleiner, B. H. (2003). *Electronic surveillance in the workplace*. *Management Research News*, 26(2/3/4), 72–81. <https://doi.org/10.1108/01409170310784014>

Lyon, D. (2001). *Surveillance Society: Monitoring Everyday Life*. London: McGraw-Hill Education.

Maalsen, S., & Dowling, R. (2020). *Covid-19 and the accelerating smart home*. *Big Data & Society* 7(2). <https://doi.org/10.1177/2053951720938073>

Manokha, I. (2020). *The Implications of Digital Employee Monitoring and People Analytics for Power Relations in the Workplace*. *Surveillance & Society*, 18(4), 540–554. <https://doi.org/10.24908/ss.v18i4.13776>

Ministarstvo za rad, zapošljavanje, boračka i socijalna pitanja (2021). *Vodič za bezbedan i zdrav rad od kuće*. Posećeno 3. novembra 2021. <https://www.minrzs.gov.rs/sites/default/files/2021-01/%D0%92%D0%BE%D0%B4%D0%B8%D1%87%20%D0%B1%D0%B5%D0%B7%D0%B1%D0%B5%D0%B4%D0%B0%D0%BD%20%D1%80%D0%B0%D0%B4%20%D0%BE%D0%B4%20>

%D0%BA%D1%83%D1%9B%D0%B5.pdf

Republički zavod za statistiku. (2020). Bilten - anketa o radnoj snazi u Republici Srbiji. Beograd: Republički zavod za statistiku. <https://publikacije.stat.gov.rs/G2021/Pdf/G20215671.pdf>

Republički zavod za statistiku. (2022). Podaci pribavljeni po osnovu prava na pristup informacijama od javnog značaja. Odgovor na zahtev, 41983. 28. februar 2022.

Samek Lodovici, M, et al. (2021). The impact of teleworking and digital work on workers and society, Publication for the committee on Employmen and Social Affairs, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg [https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662904/IPOL_STU\(2021\)662904_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662904/IPOL_STU(2021)662904_EN.pdf)

Townsend , L., & Wallace, C. (2016). Social Media Research: A Guide to Ethics. Aberdeen: The University of Aberdeen.

Workman, M. (2009). A field study of corporate employee monitoring: Attitudes, absenteeism, and the moderating influences of procedural justice perceptions. *Information and Organization*, 19, 218–232. <https://doi.org/10.1016/j.infoandorg.2009.06.001>

Zakon o radu, Službeni glasnik RS, br. 24/2005 br. 24/2005, 61/2005, 54/2009, 32/2013, 75/2014, 13/2017 - odluka US, 113/2017 i 95/2018.

Zakon o zaštiti podataka o ličnosti, Službeni glasnik RS, br. 87/2018.

Zielinski, D. (2020). Monitoring Remote Workers [web log]. Retrieved from <https://www.shrm.org/hr-today/news/all-things-work/pages/monitoring-remote-workers.aspx>

