Nadzor zaposlenih na delovnem mestu

Avtorici: Maja Brajnik, dipl. prav., in Eva Langeršek, mag. prava

VZPOSTAVITEV NADZORA NAD DELOVNIMI SREDSTVI

Delodajalec mora varovati in spoštovati delavčevo osebnost ter upoštevati in ščititi delavčevo zasebnost.[a] Zaradi spoštovanja teh dveh pravic delavcev pogosto prihaja do njunega prepletanja v delovnih razmerjih, saj razmerje tvorita dve stranki z različnimi interesi.

Na eni strani je legitimen interes delodajalca, da delavec dela učinkovito ter uporablja delovna sredstva skladno s politikami in navodili delodajalca. Na drugi strani pa je interes delavca, ki upravičeno pričakuje določen krog zasebnosti na delovnem mestu.[b]

Zaradi kolizije dveh pravic oziroma interesov je pri vzpostavitvi nadzora nad delovnimi sredstvi smotrno upoštevati izhodišča, ki jih je pripravil Informacijski pooblaščenec RS:[c]

- nobena od dveh pravic ni absolutna, zato je v vsakem konkretnem primeru treba iskati primerno in čim manj invazivno rešitev glede na dane okoliščine;
- delodajalec je dolžan cilj, ki ga zasleduje (čim bolj racionalno izrabo delovnega časa in delovnih sredstev za doseganje poslovnih rezultatov), podpreti s čim manj invazivnimi in represivnimi ukrepi;
- vsaka oblika nadzora, ki pomeni poseg v pravico do zasebnosti, mora biti vnaprej utemeljena in transparentno predstavljena zaposlenim v internih aktih podjetja (v katerih primerih, na kakšen način in kdo ga lahko izvaja), mora imeti zakonsko podlago ter biti skladna z ustavnimi določili glede varstva zasebnosti;
- **ključni element sodne prakse Evropskega sodišča za človekove pravice je standard utemeljenosti pričakovanja zasebnosti delavcev na delovnem mestu.**[d] Pri tem je pomembno, ali lahko zaposleni subjektivno in objektivno v določenih okoliščinah predvidi oblike nadzora (ali je bil vnaprej natančno seznanjen s tem, kaj, kdaj in v kakšnem obsegu je lahko predmet nadzora);
- delodajalec mora delavcu predstaviti meje pričakovane zasebnosti pri uporabi delovnih sredstev, pri čemer mora upoštevati, da je absolutna prepoved uporabe službenih sredstev v zasebne namene nerealna in zato nesprejemljiva rešitev;
- opredeljenost nadzora v internih aktih še ne pomeni, da je vsak tak nadzor tudi dopusten – predhodna obveščenost zaposlenih je tako potreben, ne pa nujno tudi zadosten pogoj za zakonitost nadzora uporabe delovnih sredstev, ki vključuje obdelavo osebnih ali komunikacijskih podatkov.

PODROČJA NADZORA NAD DELOVNIMI SREDSTVI

Delodajalci se najpogosteje poslužujejo nadzora **nad delovnimi sredstvi, kot so službeni telefon, e-pošta, avtomobili (GPS sledenje) in delovnimi prostori (videonadzor, biometrija).**

Ukrepe, s katerimi bi delodajalec omejeval pravico do zasebnosti, je dopustno vpeljati v delovni proces le pod posebej določenimi pogoji, ki so za nekatere posamezne vrste nadzora zakonsko natančno opredeljeni. Ob odsotnosti konkretne zakonske ureditve uporabe tehnologij, s katerimi se uvaja nadzor nad zaposlenimi, je v prvi vrsti treba oceniti, ali je določena obdelava osebnih podatkov skladna z načelom sorazmernosti, ter nato ugotoviti, pod katerimi pogoji je tudi zakonita.[e]

Sistemom, s katerimi se posega v ustavno varovano pravico delavcev (pravico do zasebnosti), je skupno to, da jih je v delovni proces dopustno uvesti šele, ko delodajalec opravi test sorazmernosti določenega posega v zasebnost. Presoditi je potrebno minimalno tri vidike takšnega posega, in sicer ali je poseg:

- nujen (potreben),
- ali je ocenjevani poseg primeren za dosego zasledovanega cilja ter
- ali je teža posledic ocenjevanega posega v prizadeto človekovo pravico proporcionalna vrednosti zasledovanega cilja oziroma koristim, ki bodo zaradi posega nastale (načelo sorazmernosti v ožjem pomenu oziroma načelo proporcionalnosti).
- Šele če poseg prestane vse tri vidike testa, je ustavno

a 46. člen ZDR-1.

b Povzeto po: Sonja Bien Karlovšek ... [et al.], Zasebnost delavcev in interesi delodajalcev – kje so meje?, Uradni list Republike Slovenije, Ljubljana, 2008, stran 53.

c Izhodišča so povzeta po: Smernice o OP v delovnih razmerjih, 2016, stran 21.

d Standard utemeljenosti pričakovanja zasebnosti delavcev na delovnem mestu je bil pojasnjen v zadevi Halford v. Združeno kraljestvo, št. zadeve: 00020605/92.

e Za presojo drugih kriterijev (zakonitost, transparentnost, ipd.), ki pogojujejo dovoljeno uporabo GPS sledilnih naprav z vidika varstva osebnih podatkov.

dopusten.[f] V določenih situacijah bo namreč uporaba posamezne tehnologije povsem utemeljena, upravičena in sorazmerna, v drugih pa bo tehtanje sorazmernosti pokazalo, da je mogoče iste cilje doseči na milejše načine.

V kolikor delodajalec ugotovi, da je uvedba posamezne tehnologije, s katero se posega v zasebnost delavca, sorazmerna zasledovanemu ciljem, mora delodajalec kot upravljavec osebnih podatkov zagotoviti, da je nadzorni sistem zavarovan pred dostopom nepooblaščenih oseb in drugimi zlorabami.

1. GPS NADZOR

Pred uvedbo GPS nadzora zaposlenih je potrebno izvesti presojo vplivov na zasebnost po temeljnih načelih varstva osebnih podatkov. Presoja vplivov na zasebnost po temeljnih načelih varstva osebnih podatkov je vnaprejšnjo presoja, ali oziroma pod katerimi pogoji bi bila uporaba GPS naprav sorazmerna, zakonita, transparentna, varna itd. Zelo pomembno je izhajati iz težav, ki naj bi jih delodajalci reševali z uvedbo GPS tehnologije, pri čemer je potrebno narediti realno oceno, ali bodo s temi podatki dejansko doseženi zasledovani cilji. Če je glavni povod za uvedbo GPS tehnologije ugotavljanje oziroma dokazovanje, ali je bilo delo dejansko opravljeno ali ne, potem GPS naprave same po sebi ne morejo ponuditi rešitve. Prav tako sama ekonomičnost uporabe GPS naprav ne sme biti edini kriterij, ki narekuje njihovo uporabo.[g]

Za ustrezno presojo sorazmernosti morajo biti na voljo predvsem naslednje informacije:[h]

- o predvidenem načinu delovanja naprave,
- kdo bo obdeloval podatke,
- kateri so zasledovani nameni uporabe naprave,
- o obsegu zbranih podatkov,
- o osebah, katerih podatki bodo obdelovani (ali gre za voznike, prenašalce paketov, taksiste, otroke, kupce izdelkov ipd.),
- o tem, kje bodo naprave nameščene (na vozilih, mobilnih napravah ipd.),
- o tem, kako (konkretno) naj bi bili s pomočjo uporabe doseženi zasledovani cilji,
- o tem, ali obstajajo milejši ukrepi, ki bi omogočili doseganje ciljev,
- druge pomembne okoliščine, ki imajo lahko vpliv na oceno sorazmernosti (npr. varovanje posebno vrednega premoženja, predvidene varovalke za zmanjšanje posegov v zasebnost posameznika).

f Ibidem.

g Povzeto po: Smernice Informacijskega pooblaščenca, Uporaba GPS sledilnih naprav in varstvo osebnih podatkov, (v nadaljevanju: Smernice o GPS sledilnih napravah), stran 7 in 8, dostopne na povezavi: https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/GPS_smernice_net.pdf.

h Povzeto po: Smernice o GPS sledilnih napravah, strani 7 in 8.

2. VIDEONADZOR NA DELOVNEM MESTU

Videonadzor delovnih prostorov je urejen v 77. členu ZVOP-1, kjer je določeno, kdaj in pod katerimi pogoji se videonadzor delovnih prostorov lahko uvede. Predvsem mora obstajati nujnost uvedbe videonadzora za:

- varnost ljudi ali premoženja;
- varovanje tajnih podatkov;
- varovanje poslovne skrivnosti,
- tega pa ni mogoče doseči z milejšimi sredstvi.

Tudi kadar so pogoji za njegovo uvedbo izpolnjeni, mora biti videonadzor usmerjen na izvor nevarnosti – nikoli na zaposlene. Videonadzora pa nikakor ni dopustno izvajati v garderobah, dvigalih in sanitarnih prostorih. Zaposleni morajo biti pred začetkom izvajanja videonadzora vnaprej pisno obveščeni o njegovem izvajanju, delodajalec pa se mora pred uvedbo videonadzora posvetovati z reprezentativnim sindikatom pri delodajalcu.[i]

Takšno obvestilo mora obvezno vsebovati naslednje informacije:

- da se izvaja videonadzor,
- naziv osebe javnega ali zasebnega sektorja, ki ga izvaja,
- telefonsko številko za pridobitev informacije, kje in koliko časa se shranjujejo posnetki iz videonadzornega sistema.

3. NADZOR E-POŠTE

V okviru elektronske pošte predstavlja zbirko osebnih podatkov zgolj zbirka t. i. prometnih podatkov (elektronski naslovi, datum in čas pošiljanja in prejema sporočila, zadeva sporočila in drugi tehnični podatki v povezavi s sporočilom – priponka, velikost itd.). Predpisi s področja varstva osebnih podatkov varujejo le prometne podatke, medtem ko je sama vsebina elektronske pošte varovana v okviru določb o kršitvi tajnosti občil iz 139. člena Kazenskega zakonika oziroma določb o zahtevi za prenehanje kršitve osebnostnih pravic iz 134. člena Obligacijskega zakonika.[j]

»Delodajalec mora vnaprej opredeliti in pisno obvestiti zaposlene, v katerih izrednih primerih in pod katerimi strogimi pogoji ter po kakšnem postopku lahko izjemoma vpogleda v prometne podatke. Splošno delodajalec načeloma torej nima pravne podlage za vpogled v vsebino elektronske pošte zaposlenega niti za vpogled v t. i. prometne podatke. Seveda morajo biti takšni razlogi taksativni in izjemni, zato bi bilo v takšnih primerih potrebno presojati vsak primer posebej. Predhodna obveščenost zaposlenih delavcev sama po sebi še ne pomeni, da je nadzor nad službenimi sredstvi dopusten in je tako potrebni, ne pa nujno tudi zadostni pogoj za zakonitost nadzora uporabe delovnih sredstev, ki vključuje obdelavo osebnih in/ali komunikacijskih podatkov. Bistveno je tudi, da je nadzor oziroma vpogled v elektronski predal dopusten le izjemoma v primeru, ko se

i Informacijski pooblaščenec RS, mnenje št: 0712-1/2017/75, z dne 16.01.2017.

j Informacijski pooblaščenec RS, Smernice Informacijskega pooblaščenca, Varstvo osebnih podatkov v delovnih razmerjih, stran 22.

namenov, zaradi katerih se pregled opravi, ne more doseči na drug, milejši način, torej z manjšim posegov v delavčevo zasebnost.«[k]

4. UVEDBA BIOMETRIJSKIH UKREPOV

Biometrija je veda o načinih prepoznave ljudi na podlagi njihovih telesnih, fizioloških ter vedenjskih značilnosti, ki jih imajo vsi posamezniki, ki so hkrati edinstvene in stalne za vsakega posameznika posebej in je možno z njimi določiti posameznika, zlasti z uporabo prstnega odtisa, posnetka papilarnih linij s prsta, šarenice, očesne mrežnice, obraza, ušesa, DNK ter značilne drže.[l]

Z obdelavo biometričnih značilnosti se ugotavljajo ali primerjajo lastnosti posameznika, tako da se lahko izvrši njegova identifikacija oziroma preveri njegova identiteta, zato je obdelava dovoljena le pod posebnimi pogoji, ki jih določa zakon.[m] Delodajalec **sme izvajati biometrijske ukrepe šele po prejemu odločbe Informacijskega pooblaščenca RS,** s katero je izvajanje biometrijskih ukrepov dovoljeno.[n]

Informacijski pooblaščenec RS preveri, ali je so nameravani biometrijski ukrepi nujno potrebno za opravljanje dejavnosti, za varnost ljudi ali premoženja ali za varovanje tajnih podatkov ali poslovnih skrivnosti.

Smiselno je, da delodajalec pred uvedbo biometrijskih ukrepov odgovori na naslednja vprašanja:[o]

- Ali že imamo vzpostavljen sistem za evidentiranje prisotnosti zaposlenih na delu in/ali sistem za kontrolo vstopov v prostore?
- Zakaj ga želimo zamenjati?
- Kakšne so poglavitne slabosti tega sistema?
- Ali so slabosti posledica nepopolnega izvajanja ali so neločljivo povezane z naravo samega sistema?
- Ali smo preverili več različnih tipov sistemov, ki bi prišli v poštev za naše potrebe?
- Ali bi sistemi, ki ne vključujejo biometrijskih ukrepov, zadovoljivo izpolnili naše potrebe?
- Ali potrebujemo sistem, ki vključuje biometrijske ukrepe?
- Če ga potrebujemo, katere vrste sistem potrebujemo?
- Ali potrebujemo sistem, ki temelji na ugotavljanju identitete, ali sistem, ki temelji na preverjanju identitete (avtentikacija)?
- Ali potrebujemo centralno zbirko biometričnih podatkov?
- Ali bi lahko sistem temeljil tudi na decentraliziranem shranjevanju biometričnih podatkov?

- Katere namene pravzaprav želimo doseči z biometrijskimi ukrepi?
- Ali ga potrebujemo za evidentiranje prisotnosti zaposlenih na delu ali/in za kontrolo vstopa v prostore (fizične in informacijske)?
- Kako natančno želim zajeti biometrične podatke?
- Kakšni so postopki za zagotavljanje točnosti in ažurnosti biometričnih podatkov?
- Ali je biometrične podatke, ki jih bomo shranjevali, potrebno ažurirati?
- Kakšni so postopki in načini za zavarovanje biometričnih podatkov?
- Kdo bo imel dostop do biometričnih podatkov?
- Zakaj, kdaj in pod katerimi pogoji bo do teh podatkov mogoč dostop?
- Kaj se bo štelo za zlorabo sistema s strani zaposlenih?
- Kateri bodo postopki ugotavljanja, ali je šlo za zlorabo ali le za napako?
- Ali bo sistem poleg biometrijskih ukrepov temeljil še na katerem dodatnem načinu ugotavljanju oz. preverjanju identitete (osebna gesla, brezkontaktne kartice ipd.)?
- Če bo, ali bi ti dodatni načini ugotavljanja oz. preverjanja identitete zadovoljivo izpolnili namene, ki jih zasledujemo tudi brez biometrijskih ukrepov?
- Kako bomo obvestili vse zaposlene o uvedbi biometrijskih ukrepov?
- Katere informacije bomo posredovali zaposlenim?[p]

V kolikor je večina odgovorov kaže na to, da je uvedba biometrije smiselna in sorazmerna glede na cilj, ki ga zasleduje, je smiselno, da se za biometrični nadzor pridobi dovoljenje Informacijskega pooblaščenca RS. V drugih primerih, kjer je že na podlagi odgovorov na vprašanja razvidno, da je mogoče enak cilj doseči z milejšim posegom v zasebnost delavcev, je smiselna uvedba ukrepov, ki v manjši meri posegajo v zasebnost delavcev. ■

k Informacijski pooblaščenec RS, mnenje št: 0712-1/2019/112, z dne 22. 01. 2019.

l Definicija povzeta po: Smernice informacijskega pooblaščenca, Smernice glede uvedbe biometrijskih ukrepov, 2008, stran 5, dostopne na povezavi: https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Biometrija_-_smernice.pdf.

m 79.–81. člen ZVOP-1.

n Četrti odstavek 80. člena ZVOP-1.

o Povzeto po irskem organu pristojnem za varstvo osebnih podatkov.

p Informacijski pooblaščenec RS, mnenje št: 0600-16/2006/2, z dne 22. 11. 2006.