17/HR

WP 249

Mišljenje 2/2017 o obradi podataka na radnome mjestu

doneseno 8. lipnja 2017.

Radna skupina osnovana je u skladu s člankom 29. Direktive 95/46/EZ. Ona je neovisno europsko savjetodavno tijelo za zaštitu podataka i privatnosti. Njezine su zadaće opisane u članku 30. Direktive 95/46/EZ i članku 15. Direktive 2002/58/EZ.

Tajništvo osigurava Uprava C (Temeljna prava i vladavina prava) Europske komisije, Glavna uprava za pravosuđe i zaštitu potrošača, B-1049 Bruxelles, Belgija, Ured br. MO59 05/35

Web-mjesto: http://ec.europa.eu/justice/data-protection/index_en.htm

Sadržaj

1. Sažetak

Ovim se mišljenjem dopunjuju prethodne publikacije Radne skupine iz članka 29 *Mišljenje 8/2001 o obradi osobnih podataka u kontekstu zaposlenja* (WP48)[1] i *Radni dokument o nadzoru elektroničkih komunikacija na radnome mjestu* (WP55) iz 2002.[2] Od objave tih dokumenata uveden je niz novih tehnologija koje omogućuju sustavniju obradu osobnih podataka zaposlenika na radnome mjestu, ali i stvaraju važne izazove u pogledu zaštite privatnosti i podataka.

U ovom se Mišljenju iznosi nova ocjena ravnoteže između legitimnih interesa poslodavaca i razumnih očekivanja zaposlenika u pogledu zaštite privatnosti, i to utvrđivanjem rizika koje predstavljaju nove tehnologije i ocjenjivanjem proporcionalnosti određenog broja scenarija u kojima bi se one mogle primjenjivati.

Iako se ovo Mišljenje u prvom redu odnosi na Direktivu u zaštiti podataka, u njemu se razmatraju i dodatne obveze koje poslodavci imaju na temelju Opće uredbe o zaštiti podataka. U njemu se ponavljaju stajalište i zaključci iz Mišljenja 8/2001 i Radnog dokumenta WP55, to jest da pri obradi osobnih podataka zaposlenika:

- poslodavci trebaju uvijek imati na umu temeljna načela zaštite podataka neovisno o tehnologiji koja se upotrebljava,
- na sadržaj elektroničke komunikacije upućene iz poslovnih prostora primjenjuje se ista zaštita temeljnih prava kao i na analognu komunikaciju,
- vrlo je mala vjerojatnost da privola bude pravna osnova za obradu podataka na radnome mjestu, osim ako zaposlenici mogu odbiti dati privolu bez nepovoljnih posljedica,
- ponekad je moguće pozvati se na izvršenje ugovora i na legitimne interese, pod uvjetom da je obrada podataka izričito nužna za zakonitu svrhu i u skladu je s načelima proporcionalnosti i supsidijarnosti,
- zaposlenici bi trebali dobiti djelotvorne informacije o praćenju koje se provodi, i
- svaki međunarodni prijenos podataka o zaposlenicima trebao bi se odvijati samo ako je osigurana odgovarajuća razina zaštite.

2. Uvod

Brzo uvođenje novih informacijskih tehnologija na radnome mjestu u smislu infrastrukture, aplikacija i pametnih uređaja omogućuje nove vrste sustavne i potencijalno invazivne obrade podataka na radnome mjestu. Na primjer:

- tehnologije koje omogućuju obradu podataka na radnome mjestu mogu se sada primjenjivati uz trošak koji je tek neznatan dio troškova od prije nekoliko godina, a

[1] Radna skupina iz članka 29., *Mišljenje 08/2001 o obradi osobnih podataka u kontekstu zaposlenja*, WP 48, 13. rujna 2001., url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2001/wp48_en.pdf

[2] Radna skupina iz članka 29., *Radni dokument o nadzoru elektroničkih komunikacija na radnome mjestu*, WP 55, 29. svibnja 2002., url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2002/wp55_en.pdf

kapacitet obrade osobnih podataka s pomoću tih tehnologija eksponencijalno se povećao,

- novi oblici obrade podataka, kao što je obrada osobnih podataka o korištenju internetskim uslugama i/ili podataka o lokaciji iz pametnih uređaja, mnogo su manje vidljivi zaposlenicima nego što su to tradicionalnije vrste, primjerice lako uočljive kamere CCTV. Pitanje je u kojoj su mjeri zaposlenici svjesni tih tehnologija, s obzirom na to da poslodavci mogu nezakonito primjenjivati takve načine obrade podataka, a da o tome prethodno ne obavijeste zaposlenike, i
- granice između doma i radnog mjesta postale su sve nejasnije. Na primjer, kada zaposlenici rade na daljinu (npr. od kuće) ili dok su na poslovnom putovanju, moguće je pratiti aktivnosti izvan fizičkog radnog okruženja, što može potencijalno uključivati i praćenje pojedinca u privatnom kontekstu.

Prema tome, iako nove tehnologije mogu pomoći u otkrivanju i sprečavanju gubitka intelektualne i materijalne imovine poduzeća, poboljšanju produktivnosti zaposlenika i zaštiti osobnih podataka za koje je odgovoran voditelj obrade podataka, one postavljaju i važne izazove u pogledu zaštite privatnosti i podataka. Stoga je potrebna nova ocjena ravnoteže između legitimnog interesa poslodavca da zaštiti svoje poslovanje i razumnih očekivanja u pogledu privatnosti osoba na koje se podaci odnose, a to su zaposlenici.

Iako se u ovom Mišljenju naglasak stavlja na nove informacijske tehnologije i ocjenjuje devet različitih scenarija u kojima se one primjenjuju, u njemu se iznosi i kratak osvrt na tradicionalnije metode obrade podataka na radnome mjestu gdje se rizici povećavaju zbog promjena u tehnologiji.

Kada u ovom Mišljenju upotrebljava izraz „zaposlenik”, Radna skupina iz članka 29. nema namjeru ograničiti područje primjene tog izraza samo na osobe koje imaju ugovor o radu priznat na temelju primjenjivog radnog prava. Tijekom proteklih desetljeća sve su uobičajeniji postali novi poslovni modeli s različitim vrstama radnih odnosa, posebno zapošljavanje u svojstvu vanjskog suradnika. Ovim se Mišljenjem namjeravaju obuhvatiti sve situacije u kojima postoji radni odnos, neovisno o tome temelji li se taj odnos na ugovoru o radu.

Važno je navesti da su zaposlenici rijetko u situaciji da slobodno daju, odbiju ili povuku privolu s obzirom na ovisnost koja proizlazi iz odnosa između poslodavca i zaposlenika. Osim u iznimnim situacijama, poslodavci će se morati oslanjati na neku drugu pravnu osnovu koja nije privola, kao što je potreba za obradom podataka u svrhe njihova legitimnog interesa. Međutim, legitimni interes sam po sebi nije dovoljan da bi imao prednost pred pravima i slobodama zaposlenika.

Neovisno o pravnoj osnovi za obradu podataka, prije početka obrade trebalo bi ispitati proporcionalnost kako bi se razmotrilo je li obrada potrebna radi ostvarenja zakonite svrhe te koje se mjere moraju poduzeti kako bi se osiguralo da su kršenja prava na privatni život i tajnost komunikacija svedena na najmanju moguću mjeru. To bi mogao biti dio procjene učinka na zaštitu podataka.

3. Pravni okvir

Iako je analiza u nastavku provedena u prvom redu u odnosu na trenutačni pravni okvir na temelju Direktive 95/46/EZ (Direktiva o zaštiti podataka ili „DZP”)[3], u ovom se Mišljenju razmatraju i obveze na temelju Uredbe 2016/679 (Opća uredba o zaštiti podataka ili „OUZP”)[4], koja je već stupila na snagu i primjenjivat će se od 25. svibnja 2018.

U pogledu predložene Uredbe o e-privatnosti[5] Radna skupina poziva europske zakonodavce da predvide posebno izuzeće za zadiranje u uređaje izdane zaposlenicima[6]. Predložena uredba ne sadržava prikladno izuzeće od opće zabrane zadiranja te poslodavci obično ne mogu osigurati valjanu privolu za obradu osobnih podataka svojih zaposlenika.

3.1. Direktiva 95/46/EZ — Direktiva o zaštiti podataka („DZP”)

U Mišljenju 08/2001 Radna skupina iz članka 29. već je iznijela da pri obradi osobnih podataka u kontekstu zaposlenja poslodavci uzimaju u obzir temeljna načela zaštite podataka iz DZP-a. Razvoj novih tehnologija i novih metoda obrade podataka u tom kontekstu nije doveo do promjene situacije – može se zapravo reći da je zbog tog razvoja *još* važnije da poslodavci tako postupaju. U tom bi kontekstu poslodavci trebali:

- osigurati da se podaci obrađuju u određene i zakonite svrhe koje su proporcionalne i nužne,
- uzimati u obzir načelo ograničavanja svrhe te istodobno osiguravati da su podaci primjereni i relevantni te da nisu pretjerani u odnosu na zakonitu svrhu,
- primjenjivati načela proporcionalnosti i supsidijarnosti neovisno o primjenjivoj pravnoj osnovi,
- biti transparentni prema zaposlenicima kada je riječ o upotrebi i svrhama tehnologija praćenja,
- omogućiti ostvarivanje prava osoba čiji se podaci obrađuju, uključujući pravo pristupa i, prema potrebi, pravo na ispravljanje, brisanje ili blokiranje osobnih podataka,
- voditi računa o tome da su podaci točni i ne zadržavati ih dulje nego što je potrebno, i
- poduzimati sve potrebne mjere za zaštitu podataka od neovlaštenog pristupa te osigurati da je osoblje dovoljno upoznato s obvezama u pogledu zaštite podataka.

Ne ponavljajući prethodno dane savjete, Radna skupina iz članka 29. želi istaknuti sljedeća tri načela: pravna osnova, transparentnost i automatizirane odluke.

3.1.1. *PRAVNA OSNOVA (ČLANAK 7.)*

Kada se osobni podaci obrađuju u kontekstu zaposlenja, mora biti ispunjen barem jedan od kriterija iz članka 7. Ako osobni podaci koji se obrađuju uključuju posebne vrste (kako je

---

[3] Direktiva 95/46/EZ Europskog parlamenta i Vijeća od 24. listopada 1995. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom protoku takvih podataka, *SL L* 281, 23.11.1995., str. 31.–50., url: http://eur-lex.europa.eu/legal-content/HR/TXT/HTML/?uri=CELEX:31995L0046&from=EN.

[4] Uredba 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka), *SL L 119, 4.5.2016., str. 1.–88.*, url: http://eur-lex.europa.eu/legal-content/HR/TXT/HTML/?uri=CELEX:32016R0679&from=EN.

[5] Prijedlog uredbe Europskog parlamenta i Vijeća o poštovanju privatnog života i zaštiti osobnih podataka u elektroničkim komunikacijama te stavljanju izvan snage Direktive 2002/58/EZ, 2017/0003 (COD), url: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=41241.

[6] Vidjeti Radnu skupinu iz članka 29., *Mišljenje 01/2017 o Prijedlogu uredbe o e-privatnosti*, WP 247, 4. travnja 2017., str. 29.; url: http://ec.europa.eu/newsroom/document.cfm?doc_id=44103

objašnjeno u članku 8.), obrada se zabranjuje osim ako se primjenjuje jedno od izuzeća[7,8]. Čak i kada se poslodavac može osloniti na jedno od tih izuzeća, ipak mora postojati pravna osnova iz članka 7. da bi obrada bila zakonita.

Ukratko, poslodavci stoga moraju primiti na znanje sljedeće:

- za većinu obrade podataka na radnome mjestu **suglasnost zaposlenika ne može i ne bi trebala biti pravna osnova** (članak 7. točka (a)) zbog prirode odnosa između poslodavca i zaposlenika,
- obrada podataka može biti nužna za **izvršavanje ugovora** (članak 7. točka (b)) u slučajevima kada poslodavac mora obraditi osobne podatke zaposlenika kako bi ispunio takve obveze,
- sasvim je uobičajeno da se **radnim pravom mogu propisati zakonske obveze** (članak 7. točka (c)) **koje zahtijevaju obradu osobnih podataka**; u takvim slučajevima zaposlenik mora biti jasno i potpuno informiran o takvoj obradi (osim ako se primjenjuje izuzeće),
- ako se poslodavac želi pozvati na **zakoniti interes** (članak 7. točka (f)), svrha obrade podataka mora biti zakonita; odabrana metoda ili posebna tehnologija mora biti nužna, proporcionalna i provedena na što nenametljiviji način te omogućivati poslodavcu da dokaže da **je uspostavio odgovarajuće mjere** kako bi se osigurala ravnoteža s temeljnim pravima i slobodama zaposlenika[9],
- postupci obrade podataka moraju biti i u skladu sa **zahtjevima u pogledu transparentnosti** (članci 10. i 11.) te zaposlenici trebaju biti jasno i potpuno informirani o obradi njihovih osobnih podataka[10], uključujući postojanje bilo kakvog praćenja, i
- trebalo bi donijeti **odgovarajuće tehničke i organizacijske mjere** kako bi se osigurala sigurnost obrade (članak 17.)

Najrelevantniji kriteriji iz članka 7. detaljno su navedeni u nastavku.

- **Suglasnost (članak 7. točka (a))**

U skladu s DZP-om svaka dobrovoljno dana, posebna i informirana izjava volje, kojom osoba čiji se podaci obrađuju daje svoju suglasnost da se obrade osobni podaci koji se na nju odnose. Da bi suglasnost bila valjana, mora postojati i mogućnost njezina povlačenja.

Radna skupina iz članka 29. u svojem je Mišljenju 8/2001 već istaknula da je u slučaju kada poslodavac mora obraditi osobne podatke svojih zaposlenika pogrešno započeti s pretpostavkom da se obradi podataka može dati legitimitet na temelju suglasnosti

[7] Kako je navedeno u dijelu 8. Mišljenja 08/2001; na primjer, člankom 8. stavkom 2. točkom (b) predviđa se izuzeće za potrebe izvršavanja obveza i nadzornika u području zakonodavstva o zapošljavanju u onoj mjeri u kojoj je to dopušteno nacionalnim zakonodavstvom koje pruža odgovarajuću zaštitu.

[8] Treba napomenuti da u nekim državama postoje posebne mjere kojih se poslodavci moraju pridržavati kako bi zaštitili privatni život zaposlenika. Takve posebne mjere postoje, primjerice, u Portugalu, a i u nekim drugim državama članicama mogle bi se primjenjivati slične mjere. Stoga za Portugal ne vrijede zaključci izu odjeljka 5.6. kao ni primjeri izneseni u odjeljcima 5.1. i 5.7.1. ovog Mišljenja.

[9] Radna skupina iz članka 29., *Mišljenje 06/2014 o pojmu zakonitih interesa nadzornika podataka u skladu s člankom 7. Direktive 95/46/EZ*, WP 217, doneseno 9. travnja 2014., url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_hr.pdf.

[10] U skladu s člankom 11. stavkom 2. DZP-a nadzornik podataka izuzima se od obveze pružanja informacija osobi čiji se podaci obrađuju u slučajevima kada je prikupljanje ili bilježenje podataka izričito propisano zakonom.

zaposlenika. U slučajevima kada poslodavac navodi da zahtijeva suglasnost zaposlenika, a nedavanje suglasnosti može prouzročiti stvarnu ili moguću štetu za zaposlenika (što je vrlo vjerojatno u kontekstu zaposlenja, posebno kad je riječ o poslodavcu koji prati ponašanje zaposlenika tijekom vremena), suglasnost nije valjana jer nije i ne može biti dana dobrovoljno. Stoga za većinu slučajeva obrade podataka o zaposlenicima pravna osnova za takvu obradu ne može i ne bi trebala biti suglasnost zaposlenika pa je potrebna neka druga pravna osnova.

Osim toga, čak i u slučajevima kada bi se moglo reći da je suglasnost valjana pravna osnova za takvu obradu (tj. kada se može nedvojbeno zaključiti da je suglasnost dana dobrovoljno), to mora biti posebna i informirana izjava volje zaposlenika. Zadane postavke na uređajima i/ili ugradnja računalnog programa koji omogućuje elektroničku obradu osobnih podataka ne mogu se smatrati suglasnošću koju je dao zaposlenik jer suglasnost zahtijeva aktivno izražavanje volje. Nepostupanje (tj. izostanak promjene zadanih postavki) općenito se ne može smatrati posebnom suglasnošću kojom se dopušta takva obrada podataka[11].

- **Izvršavanje ugovora (članak 7. točka (b))**

Radni odnosi često se temelje na ugovoru o radu zaključenom između poslodavca i zaposlenika. Da bi izvršio obveze na temelju tog ugovora, kao na primjer isplaćivanje plaće zaposleniku, poslodavac mora obraditi neke osobne podatke.

- **Zakonske obveze (članak 7. točka (c))**

Prilično je uobičajeno da se radnim pravom poslodavcima određuju zakonske obveze koje zahtijevaju obradu osobnih podataka (npr. u svrhu izračunavanja poreza ili obračuna plaća). Jasno je da je u tim slučajevima takav zakon pravna osnova za obradu podataka.

- **Zakoniti interes (članak 7. točka (f))**

Ako se poslodavac želi osloniti na pravnu osnovu iz članka 7. točke (f) DZP-a, svrha obrade podataka mora biti zakonita, a odabrana metoda ili posebna tehnologija obrade mora biti neophodna za potrebne legitimnog interesa poslodavca. Obrada podataka mora biti i proporcionalna poslovnim potrebama, tj. svrsi, zbog kojih se podaci obrađuju. Obradu podataka na radnome mjestu trebalo bi provoditi na što je moguće nenametljiviji način te bi trebala biti usmjerena na konkretno područje rizika. Osim toga, u slučaju pozivanja na članak 7. točku (f), zaposlenik zadržava pravo prigovora na obradu zbog jakih i zakonitih razloga iz članka 14.

Za pozivanje na članak 7. točku (f) kao pravnu osnovu za obradu podataka ključno je da postoje posebne ublažavajuće mjere kako bi se osigurala odgovarajuća ravnoteža između zakonitog interesa poslodavca i temeljnih prava i sloboda zaposlenika[12]. Te bi mjere, ovisno

[11] Vidjeti i Radna skupina iz članka 29., *Mišljenje 15/2011 o definiciji privole*, WP187, 13. srpnja 2011., url; http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf, STR. 24.

[12] Za primjer ravnoteže koju treba postići vidjeti predmet *Köpke protiv Njemačke*, [2010] ECHR 1725, (URL: http://www.bailii.org/eu/cases/ECHR/2010/1725.html), u kojem je zaposlenik otpušten na temelju tajnog videonadzora koji su proveli poslodavac i privatna detektivska agencija. Iako je u tom slučaju Sud zaključio da su nacionalna tijela postigla primjerenu ravnotežu između zakonitog interesa poslodavca (za zaštitu svojih prava vlasništva), prava zaposlenika na poštovanje privatnog života i javnog interesa za pravosuđe, uočeno je da bi ti različiti interesi u budućnosti mogli imati različitu težinu zbog tehnološkog razvoja.

o načinu praćenja, trebale uključivati ograničenja praćenja kako bi se zajamčilo da privatnost zaposlenika nije narušena. Ta bi se ograničenja mogla odnositi na:

- prostor (npr. praćenje samo na određenim mjestima; trebalo bi zabraniti praćenje osjetljivih područja kao što su vjerska mjesta i, primjerice, sanitarne zone i prostorije za odmor),
- podatke (npr. osobne elektroničke datoteke i komunikacija ne bi se smjele pratiti) i
- vrijeme (npr. uzorkovanje umjesto kontinuiranog praćenja).

3.1.2. *TRANSPARENTNOST (ČLANCI 10. I 11.)*

Zahtjevi u pogledu transparentnosti iz članaka 10. i 11. primjenjuju se na obradu podataka na radnome mjestu; zaposlenici moraju biti obaviješteni o postojanju praćenja, svrhama obrade osobnih podataka i o svim drugim informacijama potrebnima da bi se zajamčila pravedna obrada podataka.

S novim tehnologijama sve je očitija potreba za transparentnošću jer te tehnologije omogućuju prikriveno prikupljanje i daljnju obradu potencijalno velike količine osobnih podataka.

3.1.3. *AUTOMATSKE ODLUKE (ČLANAK 15.)*

Člankom 15. DZP-a osobi čiji se podaci obrađuju daje se pravo da se o njoj ne donese odluka koja proizvodi pravne učinke u vezi nje ili na nju značajno utječe i koja je isključivo osnovana na automatskoj obradi podataka s namjerom procjene određenih osobnih vidova, kao što je njezin uspjeh na poslu, osim ako je odluka potrebna za sklapanje ili izvršenje ugovora, ako je dopuštena pravom Unije ili države članice ili ako se temelji na izričitoj suglasnosti ispitanika.

3.2. Uredba 2016/679/EZ – Opća uredba o zaštiti podataka („OUZP”)

OUZP obuhvaća i proširuje zahtjeve utvrđene DZP-om. Njome se uvode i nove obveze za sve voditelje obrade podataka, uključujući i poslodavce.

3.2.1. *INTEGRIRANA ZAŠTITA PODATAKA*

Člankom 25. OUZP-a od voditelja obrade podataka zahtijeva se da provode tehničku i integriranu zaštitu podataka. Na primjer: kada poslodavac zaposlenicima ustupi neki uređaj, potrebno je odabrati rješenja kojima se u najvećoj mjeri pogoduje zaštiti privatnosti ako su uključene tehnologije praćenja. Mora se uzeti u obzir i smanjenje količine podataka.

3.2.2. *PROCJENE UČINKA NA ZAŠTITU PODATAKA*

Člankom 35. OUZP-a od voditelja obrade podataka zahtijeva se provedba procjene učinka na zaštitu podataka ako je vjerojatno da će neka vrsta obrade, osobito putem novih tehnologija i uzimajući u obzir prirodu, opseg, kontekst i svrhe obrade, prouzročiti visok rizik za prava i slobode pojedinaca. Primjer je za to sustavna i opsežna evaluacija osobnih aspekata u vezi s pojedincima koja se temelji na automatiziranoj obradi, uključujući izradu profila, i na temelju koje se donose odluke koje proizvode pravne učinke koji se odnose na pojedinca ili na sličan način znatno utječu na pojedinca.

Ako procjena učinka na zaštitu podataka pokaže da utvrđene rizike ne može u dovoljnoj mjeri riješiti voditelj obrade, tj. da je preostali rizik i dalje visok, voditelj obrade mora se savjetovati s nadzornim tijelom prije početka obrade (članak 36. stavak 1.), kako je pojašnjeno u smjernicama o procjeni učinka na zaštitu podataka koje je izdala Radna skupina iz članka 29.[13]

3.2.2. „*OBRADA U KONTEKSTU ZAPOSLENJA*"

U članku 88. OUZP-a navodi se da države članice mogu zakonom ili kolektivnim ugovorima predvidjeti preciznija pravila radi osiguravanja zaštite prava i sloboda u vezi s obradom osobnih podataka zaposlenika u kontekstu zaposlenja. Ta se pravila konkretno mogu predvidjeti za potrebe:

- zapošljavanja,
- izvršavanja ugovora o radu (što uključuje ispunjavanje zakonski propisanih obveza ili obveza propisanih kolektivnim ugovorima),
- upravljanja, planiranja i organizacije rada,
- jednakosti i različitosti na radnome mjestu,
- zdravlja i sigurnosti na radu,
- zaštite imovine poslodavca ili klijenta,
- ostvarenja ili uživanja prava i koristi iz radnog odnosa (na individualnoj osnovi), i
- prestanka radnog odnosa.

U skladu s člankom 88. stavkom 2., sva ta pravila trebala bi uključivati prikladne i posebne mjere za zaštitu ljudskog dostojanstva ispitanika, njegovih legitimnih interesa i temeljnih prava, posebno u odnosu na:

- transparentnost obrade,
- prijenos osobnih podataka unutar grupe poduzetnika ili grupe poduzeća koja se bave zajedničkom gospodarskom djelatnošću, i
- sustave praćenja na radnome mjestu.

U ovom je Mišljenju Radna skupina dala smjernice za zakonitu upotrebu nove tehnologije u nizu konkretnih situacija te je podrobno opisala prikladne i posebne mjere za zaštitu ljudskog dostojanstva zaposlenika te njihovih legitimnih interesa i temeljnih prava.

4. Rizici

Suvremene tehnologije omogućuju praćenje zaposlenika tijekom vremena, na različitim radnim mjestima i u njihovim domovima, s pomoću brojnih različitih uređaja kao što su pametni telefoni, stolna računala, tableti, vozila i nosivi elektronički uređaji. Ako ne postoje ograničenja u pogledu obrade podataka te ako obrada nije transparentna, postoji visok rizik da se legitimni interes poslodavaca za poboljšanje učinkovitosti i zaštitu imovine poduzeća pretvori u neopravdano i nametljivo praćenje.

[13] Radna skupina iz članka 29., *Smjernice o procjeni učinka na zaštitu podataka i određivanju vjerojatnosti da će obrada dovesti do „visokog rizika" za potrebe Uredbe 2016/679*, WP 248, 4. travnja 2017., url: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137, str. 18.

Tehnologije za praćenje komunikacija mogu isto tako imati odvraćajući učinak u pogledu temeljnih prava zaposlenika na organiziranje, održavanje skupova radnika te povjerljivo komuniciranje (što uključuje i pravo na traženje informacija). Praćenjem komunikacije i ponašanja izvršit će se pritisak na zaposlenike da se ponašaju u skladu s pravilima kako bi spriječili otkrivanje nečega što bi se moglo smatrati nepravilnošću, na način koji je usporediv s načinom na koji je intenzivna upotreba CCTV-a utjecala na ponašanje ljudi na javnim mjestima. Osim toga, zbog mogućnosti koje pružaju takve tehnologije, zaposlenici možda nisu ni svjesni koji se osobni podaci obrađuju i u koje svrhe, a moguće je i da nisu svjesni ni postojanja same tehnologije praćenja.

Praćenje upotrebe informacijske tehnologije razlikuje se od drugih vidljivijih alata za promatranje i praćenje, kao što je CCTV, po tome što se može provoditi na prikriven način. Ako ne postoji lako razumljiva i dostupna politika praćenja na radnome mjestu, zaposlenici možda neće biti svjesni postojanja i posljedica praćenja te stoga nisu u mogućnosti ostvariti svoja prava. Dodatni rizik predstavlja pretjerano prikupljanje podatka u takvim sustavima, npr. onima koji prikupljaju podatke o lokaciji putem WiFi-ja.

Povećanje količine podataka stvorenih u okruženju radnog mjesta, u kombinaciji s novim tehnikama za analizu i unakrsno provjeravanje podataka, isto tako može stvoriti rizike od daljnje obrade u nesukladne svrhe. Na primjer, nezakonita daljnja obrada može biti upotreba sustava koji je zakonito ugrađen radi zaštite imovine za praćenje dostupnosti i učinkovitosti zaposlenika i njihove ljubaznosti prema klijentima. Drugi su primjeri upotreba podataka prikupljenih putem sustava CCTV-a za redovito praćenje ponašanja i učinkovitosti zaposlenika ili upotreba podataka iz sustava za geolociranje (kao što su, na primjer,praćenje putem WiFi-ja ili Bluetootha) za stalno provjeravanje kretanja i ponašanja zaposlenika.

Takvo praćenje može stoga narušavati prava zaposlenika na privatnost, neovisno o tome je li riječ o sustavnom ili povremenom praćenju. Rizik nije ograničen na analizu sadržaja komunikacija. Analiza metapodataka o nekoj osobi mogla bi omogućiti detaljno praćenje života i obrazaca ponašanja pojedinca na način koji u jednakoj mjeri zadire u privatnost.

Intenzivna upotreba tehnologija praćenja može isto tako ograničiti spremnost zaposlenika da obavijeste (i kanale putem kojih bi mogli obavijestiti) poslodavce o nepravilnostima ili nezakonitim radnjama nadređenih i/ili drugih zaposlenika koje bi mogle naštetiti poslovanju (posebno podacima o klijentima) ili radnome mjestu. Često je potrebna anonimnost da bi zabrinuti zaposlenik djelovao i prijavio takve situacije. Praćenje kojim se narušavaju prava na privatnost zaposlenika može kočiti potrebnu komunikaciju prema odgovarajućim službenicima. U takvom slučaju ustaljena sredstva kojima se mogu služiti interni zviždači mogu postati neučinkovita[14].

5. Scenariji

[14] Vidjeti, na primjer, Radna skupina iz članka 29., *Mišljenje 1/2006 o primjeni pravila EU-a o zaštiti podataka u internim sustavima za prijavu nepravilnosti u području računovodstva, unutarnjih računovodstvenih kontrola, revizije, borbe protiv podmićivanja te bankovnog i financijskog kriminala*, WP 117, 1. veljače 2006., url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2006/wp117_en.pdf.

U ovom se odjeljku iznosi niz scenarija obrade podataka na radnome mjestu u kojima nove tehnologije i/ili razvoj postojećih tehnologija mogu ili bi mogle prouzročiti visoke rizike za privatnost zaposlenika. U svim takvim slučajevima poslodavci trebaju razmotriti:

- je li obrada nužna te, ako je, koja se pravna osnova primjenjuje,
- je li predložena obrada osobnih podataka poštena prema zaposlenicima,
- je li aktivnost obrade proporcionalna utvrđenim nedostacima, i
- je li aktivnost obrade transparentna.

5.1. Obrada podataka tijekom postupka zapošljavanja

Upotreba društvenih medija raširena je među pojedincima te je relativno uobičajeno da javnost može vidjeti profile korisnika ovisno o postavkama koje je odabrao vlasnik računa. Poslodavci stoga mogu vjerovati da je opravdano tijekom postupka zapošljavanja pregledavati profile potencijalnih kandidata na društvenim medijima. To može biti slučaj i s drugim javno dostupnim informacijama o potencijalnim zaposlenicima.

Međutim, poslodavci ne bi smjeli pretpostaviti da im je dopušteno obrađivati te podatke za vlastite potrebe samo zato što je nečiji profil javno dostupan na društvenim medijima. Za tu obradu mora postojati pravna osnova, kao što je legitimni interes. U tom bi kontekstu poslodavac, prije pregledavanja profila na društvenim medijima, trebao voditi računa o tome ima li profil kandidata na društvenom mediju poslovnu ili privatnu svrhu,jer to može biti važan pokazatelj pravne prihvatljivosti pregledavanja podataka. Osim toga, poslodavcima je dopušteno jedino prikupljanje i obrađivanje osobnih podataka koji se odnose na kandidate za zaposlenje u mjeri u kojoj je prikupljanje tih podataka nužno i relevantno za obavljanje posla za koji se kandidat prijavljuje.

Podatke prikupljene tijekom postupka zapošljavanja u načelu bi trebalo izbrisati čim postane jasno da se pojedincu neće ponuditi posao ili da ga on neće prihvatiti[15]. Pojedinac isto tako mora biti točno informiran o svakoj takvoj obradi podataka prije postupka zapošljavanja.

Ne postoji pravna osnova na temelju koje poslodavac može zahtijevati od potencijalnog zaposlenika da ga prihvati kao „prijatelja" ili da mu na neki drugi način omogući pristup sadržaju svojeg profila.

Primjer

Pri zapošljavanju novog osoblja poslodavac provjerava profile kandidata na različitim društvenim mrežama te uključuje podatke s tih mreža (i sve druge podatke dostupne na internetu) u postupak provjere.

Jedino kada je zbog prirode posla nužno da se informacije o kandidatu provjeravaju na društvenim medijima, na primjer kako bi se procijenili posebni rizici povezani s kandidatima za određenu funkciju, te ako su kandidati pravilno o tome obaviješteni (na primjer u tekstu oglasa za posao), poslodavac može imati pravnu osnovu na temelju članka 7. točke (f) za pregledavanje javno dostupnih informacija o kandidatima.

[15] Vidjeti i Vijeće Europe, *Preporuka CM/Rec(2015)5 Odbora ministara državama članicama o obradi osobnih podataka u kontekstu zaposlenja*, stavak 13.2. (1. travnja 2015., url: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c3f7a). Ako poslodavac želi zadržati podatke radi kasnije mogućnosti zapošljavanja, osobu na koju se podaci odnose trebalo bi o tome obavijestiti i dati joj mogućnost prigovora na daljnju obradu te bi, u slučaju prigovora, podatke trebalo izbrisati (Id.).

5.2. Obrada podataka tijekom provjere postojećih zaposlenika

Zahvaljujući postojanju profila na društvenim medijima i razvoju novih analitičkih tehnologija poslodavci imaju (ili mogu dobiti) tehničke mogućnosti za stalnu provjeru zaposlenika prikupljanjem informacija o njihovim prijateljima, mišljenjima, vjerovanjima, interesima, navikama, kretanjima, stavovima i ponašanjima te na taj način mogu doći do podataka, pa i onih osjetljivih, o privatnom i obiteljskom životu zaposlenika.

Pregledavanje profila postojećih zaposlenika na društvenim medijima ne bi se smjelo općenito provoditi.

Osim toga, poslodavci bi se trebali suzdržati od toga da od zaposlenika ili kandidata za posao zahtijevaju da im omogući pristup informacijama koje dijeli s drugim osobama na društvenim mrežama.

Primjer
Za vrijeme trajanja klauzula o zabrani tržišnog natjecanja poslodavac prati profile bivših zaposlenika obuhvaćenih tim klauzulama na društvenoj mreži LinkedIn. Svrha je tog praćenja utvrditi poštovanje tih klauzula. Praćenje je ograničeno na te bivše zaposlenike.

Sve dok poslodavac može dokazati da je takvo praćenje nužno radi zaštite njegovih legitimnih interesa, da nema drugih, manje invazivnih načina te da su ti bivši zaposlenici na odgovarajući način obaviješteni o opsegu redovitog promatranja njihovih javnih komunikacija, poslodavac se može pozivati na pravnu osnovu iz članka 7. točke (f) DZP-a.

Nadalje, od zaposlenika se ne bi smjelo zahtijevati da se koriste profilom na društvenom mediju koji je osigurao njihov poslodavac. Čak i kad je izričito predviđeno s obzirom na njihove zadaće (npr. glasnogovornik organizacije), moraju imati mogućnost koristiti se „neposlovnim" profilom koji nije javan umjesto „službenog" profila povezanog s poslodavcem te bi to trebalo biti navedeno u uvjetima ugovora o radu.

5.3. Obrada podataka koja proizlazi iz upotrebe informacijskih i komunikacijskih tehnologija (IKT) na radnome mjestu

Tradicionalno se smatralo da je praćenje elektroničkih komunikacija na radnome mjestu (npr. telefoniranja, pretraživanja interneta, elektroničke pošte, slanja trenutačnih poruka, VOIP itd.) glavna prijetnja privatnosti zaposlenika. U *Radnom dokumentu o nadzoru elektroničkih komunikacija na radnome mjestu* iz 2001. Radna skupina iz članka 29. iznijela je niz zaključaka u pogledu praćenja elektroničke pošte i korištenja internetom. Iako ti zaključci i dalje vrijede, potrebno je uzeti u obzir tehnološka dostignuća koja omogućuju novije, potencijalno nametljivije i prodornije načine praćenja. Ta dostignuća uključuju, među ostalim, i sljedeće:

- alate za sprečavanje gubitka podataka (eng. *Data Loss Prevention* – DLP) kojima se prate izlazne komunikacije radi otkrivanja mogućih povreda podataka,
- vatrozidove nove generacije (eng. *Next-Generation Firewalls* – NGFW-i) i sustave za cjelovito upravljanje prijetnjama (eng. *Unified Threat Management* – UTM), koji sadržavaju brojne tehnologije praćenja, među ostalim i dubinsku analizu paketa, presretanje komunikacija zaštićenih protokolom TLS, filtriranje *web*-mjesta, filtriranje sadržaja, davanje informacija o sigurnosti mreže u stvarnom vremenu (eng.

on-appliance reporting), davanje informacija o identitetu korisnika i (kako je prethodno opisano) sprečavanje gubitka podataka. Te se tehnologije mogu primjenjivati i pojedinačno, ovisno o poslodavcu,

- sigurnosne aplikacije i mjere koje uključuju evidentiranje pristupa zaposlenika sustavima poslodavca,
- tehnologiju eDiscovery, koja se odnosi na svaki postupak u kojem se pretražuju elektronički podaci radi njihove upotrebe kao dokaza,
- praćenje upotrebe aplikacija i uređaja s pomoću nevidljivog računalnog programa na računalu ili u oblaku,
- upotrebu uredskih aplikacija koje se nude kao usluga u oblaku na radnome mjestu, što teoretski omogućuje vrlo detaljnu evidenciju aktivnosti zaposlenika,
- praćenje osobnih uređaja (npr. osobnih računala, mobitela, tableta) koje zaposlenici upotrebljavaju za obavljanje posla u skladu s određenom politikom upotrebe uređaja, kao što je politika „donesi vlastiti uređaj" (eng. *Bring-Your-Own-Device* – BYOD), kao i tehnologija upravljanja mobilnim uređajima (eng. *Mobile Device Management* – MDM) koja omogućuje dijeljenje aplikacija, podataka, konfiguracijskih postavki i programskih popravaka za mobilne uređaje, i
- upotrebu nosivih uređaja (npr. uređaja za praćenje zdravlja i tjelovježbu).

Postoji mogućnost da će poslodavac provoditi praćenje koristeći se sveobuhvatnim rješenjem, kao što je niz povezanih sigurnosnih paketa koji mu omogućuju praćenje cjelokupnog korištenja IKT-om na radnome mjestu, za razliku od praćenja samo elektroničke pošte i/ili *web*-mjesta kao što je nekada bio slučaj. Zaključci izneseni u dokumentu WP55 mogli bi se primijeniti za svaki sustav koji omogućuje takvo praćenje[16].

Primjer

Poslodavac se namjerava koristiti uređajem za kontrolu prometa kriptiranog protokolom TLS kako bi dekriptirao i kontrolirao siguran promet radi otkrivanja svih zlonamjernih aktivnosti. Uređaj može bilježiti i analizirati sve internetske aktivnosti koje zaposlenik provodi na mreži poduzeća.

Sve se više upotrebljavaju kriptirani komunikacijski protokoli kako bi se mrežni protok podataka, koji uključuju i privatne podatke, zaštitio od presretanja. Međutim, to može predstavljati i probleme jer enkripcija onemogućuje praćenje ulaznih i izlaznih podataka. Opremom za kontrolu prometa kriptiranog protokolom TLS podatkovni se tok prvo dekriptira, potom se sadržaj analizira u sigurnosne svrhe te se nakon toga tok ponovno kriptira.

U ovom se primjeru poslodavac oslanja na legitimni interes, a to je potreba da se mreža te osobni podaci zaposlenika i klijenata sadržanih unutar mreže zaštite od neovlaštenog pristupa ili od curenja podataka. Međutim, praćenje svake internetske aktivnosti zaposlenika predstavlja neproporcionalnu reakciju i zadiranje u pravo na tajnost komunikacije.

[16] Vidjeti i predmet *Copland protiv Ujedinjene Kraljevine*, (2007) 45 EHRR 37, 25 BHRC 216, 2 ALR Int'l 785, [2007] ECHR 253 (url: http://www.bailii.org/eu/cases/ECHR/2007/253.html), u kojem je Sud naveo da bi elektronička pošta poslana iz poslovnih prostorija te informacije dobivene praćenjem upotrebe interneta mogli biti dio privatnog života i korespondencije zaposlenika te da bi prikupljanje i pohranjivanje tih informacija bez znanja zaposlenika moglo predstavljati zadiranje u prava zaposlenika, iako Sud nije odlučio da takvo praćenje nikada ne bi bilo potrebno u demokratskom društvu.

Poslodavac bi prvo trebao istražiti druga, manje invazivna sredstva zaštite tajnosti podataka o klijentima i sigurnosti mreže.

U mjeri u kojoj se presretanje prometa kriptiranog protokolom TLS može smatrati nužnim, uređaj bi trebalo konfigurirati tako da sprečava stalno evidentiranje aktivnosti zaposlenika, na primjer blokiranjem sumnjivog ulaznog ili izlaznog prometa i preusmjeravanjem korisnika na informacijski portal gdje može zatražiti preispitivanje takve automatske odluke. Ako bi se neko opće evidentiranje ipak smatralo izričito nužnim, uređaj se može konfigurirati i tako da zabilježene podatke pohranjuje samo ako ukaže na pojavu incidenta, uz smanjenu količinu prikupljenih informacija.

Dobra bi praksa bila kad bi poslodavac mogao zaposlenicima ponuditi alternativni pristup koji se ne prati. Mogao bi im, primjerice, ponuditi besplatan WiFi ili samostalne uređaje ili terminale (s odgovarajućim zaštitnim mjerama za osiguravanje povjerljivosti komunikacije) s pomoću kojih se zaposlenici mogu koristiti svojim legitimnim pravom na upotrebu radnih prostora u neke privatne svrhe[17]. Osim toga, poslodavci bi trebali razmotriti određene vrste prometa čije presretanje ugrožava odgovarajuću ravnotežu između njihovih legitimnih interesa i privatnosti zaposlenika – kao što je upotreba privatne internetske pošte, posjećivanje *web*-mjesta za internetsko bankarstvo ili *web*-mjesta o zdravlju – radi pravilnog konfiguriranja uređaja tako da ne presreće komunikaciju u okolnostima koje nisu u skladu s načelom proporcionalnosti. Zaposlenicima bi trebalo pružiti informacije o vrsti komunikacije koja se prati uređajem.

Trebalo bi izraditi politiku u pogledu svrha u koje se može pristupiti sumnjivim evidentiranim podacima, kada im se može pristupiti i tko im može pristupiti, te bi ta politika trebala biti lako i stalno dostupna svim zaposlenicima kako bi im služila kao smjernica o tome koja je upotreba mreže i opreme prihvatljiva, a koja neprihvatljiva. Time se zaposlenicima omogućuje da svoje ponašanje prilagode kako ne bi bili praćeni kada se legitimno koriste informacijskom tehnologijom na radnome mjestu u privatne svrhe. Dobra bi praksa bila da se takva politika ocjenjuje najmanje jednom godišnje kako bi se procijenilo postižu li se izabranim rješenjem za praćenje očekivani rezultati te može li se ista svrha postići drugim, manje invazivnim alatima ili sredstvima.

Bez obzira na to o kojoj je tehnologiji riječ ili koje kapacitete posjeduje, pravna osnova iz članka 7. točke (f) postoji samo ako obrada podataka ispunjuje određene uvjete. Prvo, poslodavci koji se koriste tim proizvodima i aplikacijama moraju razmotriti jesu li mjere koje provode proporcionalne te mogu li se poduzeti neke dodatne radnje kako bi se ublažio ili smanjio opseg i utjecaj obrade podataka. Dobra bi praksa bila, primjerice, da se u tu svrhu provede procjena učinka na zaštitu podataka prije uvođenja bilo koje tehnologije praćenja. Drugo, poslodavci moraju provesti politike prihvatljive upotrebe i izvijestiti o njima zajedno s politikama privatnosti, te utvrditi dopuštenu upotrebu mreže i opreme poduzeća i detaljno opisati kakva se obrada podataka provodi.

[17] Vidjeti predmet *Halford protiv Ujedinjene Kraljevine*, [1997] ECHR 32, (url: http://www.bailii.org/eu/cases/ECHR/1997/32.html), u kojem je Sud utvrdio da „telefonski pozivi upućeni iz poslovnih prostora kao i oni upućeni od kuće mogu biti obuhvaćeni pojmom „privatnog života" i „korespondencije" u smislu članka 8. stavka 1. [Konvencije]"; i predmet *Barbulescu protiv Rumunjske*, [2016] ECHR 61, (url: http://www.bailii.org/eu/cases/ECHR/2016/61.html), koji se odnosi na upotrebu poslovnog računa za slanje trenutačnih poruka za privatno dopisivanje i u kojem je Sud utvrdio da je praćenje računa koje je provodio poslodavac bilo ograničeno i proporcionalno; uz izdvojeno mišljenje suca Pinta de Alberquerquea koji se založio za pažljivo uspostavljanje ravnoteže.

U nekim je zemljama zakonom propisano da je za izradu takve politike potrebno odobrenje radničkog vijeća ili sličnog predstavničkog tijela zaposlenika. Takve politike u praksi obično izrađuje osoblje zaduženo za održavanje IT-a. S obzirom na to da će oni uglavnom biti usredotočeni na sigurnost, a ne na legitimna očekivanja zaposlenika u pogledu zaštite privatnosti, Radna skupina iz članka 29. preporučuje da se u procjenu potrebe za praćenjem te logike i dostupnosti politike u svim slučajevima uključi reprezentativni uzorak zaposlenika.

Primjer

Poslodavac se koristi alatom za sprečavanje gubitka podataka (DLP) kako bi automatski pratio izlaznu elektroničku poštu u svrhu sprečavanja neovlaštenog slanja vlasničkih podataka (npr. osobnih podataka klijenata), neovisno o tome je li to slanje namjerno ili nenamjerno. Nakon što se utvrdi da bi neka poruka poslana elektroničkom poštom mogla biti potencijalni izvor povrede podataka, provodi se daljnja istraga.

I ovdje se poslodavac oslanja na legitimni interes, odnosno na potrebu da se osobni podaci klijenata i njegova imovina zaštite od neovlaštenog pristupa ili od curenja podataka. Međutim, takav alat za DLP može uključivati nepotrebnu obradu osobnih podataka – na primjer, „lažno pozitivna" uzbuna može dovesti do neovlaštenog pristupa legitimnoj elektroničkoj pošti koju su zaposlenici poslali (na primjer, može biti riječ o osobnim porukama e-pošte).

Stoga je potrebno u cijelosti opravdati potrebu za alatom za DLP i njegovu upotrebu kako bi se postigla odgovarajuća ravnoteža između legitimnih interesa poslodavca i temeljnog prava na zaštitu osobnih podataka zaposlenika. Da bi se poslodavac mogao pozvati na svoje legitimne interese, potrebno je poduzeti određene mjere za ublažavanje rizika. Na primjer, pravila u skladu s kojima sustav karakterizira neku elektroničku poštu kao potencijalnu povredu podataka trebala bi biti u cijelosti transparentna korisnicima, a u slučajevima kada alat prepoznaje da bi elektronička pošta koju se namjerava poslati mogla predstavljati povredu podataka, upozoravajuća poruka trebala bi obavijestiti pošiljatelja elektroničke pošte prije njezina slanja kako bi mu se dala mogućnost odustajanja od slanja.

U nekim je slučajevima praćenje zaposlenika moguće ne toliko zbog upotrebe posebnih tehnologija nego jednostavno zbog toga što se od zaposlenika očekuje upotreba internetskih aplikacija koje im je poslodavac dao na upotrebu, a koje obrađuju osobne podatke. Primjer je toga upotreba uredskih aplikacija u oblaku (npr. uređivači dokumenata, kalendari, društveno umrežavanje). Trebalo bi osigurati da zaposlenici mogu odrediti određene privatne prostore kojima poslodavci ne mogu dobiti pristup, osim u iznimnim okolnostima. To je, primjerice, relevantno za kalendare koji se često upotrebljavaju i za bilježenje privatnih sastanaka. Ako zaposlenik obilježi neki sastanak oznakom „Privatno" ili to navede u samoj bilješci o sastanku, poslodavcima (ili ostalim zaposlenicima) ne bi smjelo biti dopušteno pregledavati sadržaj sastanka.

U tom kontekstu zahtjev supsidijarnosti ponekad znači da se praćenje ne smije uopće provoditi. To je, na primjer, slučaj kada se zabranjena upotreba komunikacijskih usluga može spriječiti blokiranjem određenih *web*-mjesta. Ako je umjesto kontinuiranog praćenja svih komunikacija moguće blokirati *web*-mjesta, trebalo bi izabrati blokiranje kako bi se ispunio zahtjev supsidijarnosti.

Sprečavanju bi općenito trebalo dati veću važnost nego otkrivanju – interesi poslodavca bolje se ostvaruju ako se umjesto povećavanja resursa za otkrivanje zlouporabe interneta takva zlouporaba sprečava tehničkim sredstvima.

5.4. Obrada podataka koja proizlazi iz praćenja upotrebe IKT-a izvan radnog mjesta

Porastom rada od kuće, rada na daljinu i politike „donesi vlastiti uređaj" upotreba IKT-a izvan radnog mjesta postala je sve uobičajenija. Mogućnosti koje pružaju takve tehnologije

mogu predstavljati rizik za privatni život zaposlenika s obzirom na to da se u brojnim slučajevima sustavi praćenja koji postoje na radnome mjestu učinkovito proširuju na privatno područje zaposlenika kada upotrebljavaju takvu opremu. .

5.4.1. *PRAĆENJE RADA OD KUĆE I RADA NA DALJINU*

Sve je češća praksa da poslodavci nude zaposlenicima mogućnost rada na daljinu, npr. od kuće i/ili dok putuju. To je jedan od glavnih čimbenika zbog kojeg je razlika između radnog mjesta i doma sve manja. Ta se praksa općenito sastoji od toga da poslodavac daje zaposlenicima na upotrebu opremu ili računalni program za IKT koji im omogućuju, nakon što je instaliraju kod kuće/na svoje vlastite uređaje, istu razinu pristupa mreži, sustavima i resursima poslodavca kao što bi imali da su na radnome mjestu, ovisno o provedbi.

Iako rad na daljinu može biti pozitivno postignuće, on je i područje dodatnog rizika za poslodavca. Primjerice, zaposlenici koji imaju daljinski pristup infrastrukturi poslodavca nisu obvezni pridržavati se fizičkih sigurnosnih mjera koje se možda primjenjuju u poslovnim prostorima poslodavca. Jednostavno rečeno: bez provedbe odgovarajućih tehničkih mjera povećava se opasnost od neovlaštenog pristupa, što može dovesti do gubitka ili uništenja podataka koje posjeduje poslodavac, među ostalim i osobnih podataka zaposlenika.

Kako bi umanjili tu opasnost, poslodavci mogu smatrati da postoji opravdanje za upotrebu softverskih paketa (na licu mjesta ili u oblaku) koji imaju mogućnost, na primjer, evidentirati pritiske na tipke ili pokrete miša, snimati zaslone (nasumice ili u zadanim vremenskim razmacima), evidentirati upotrebu aplikacija (i koliko su dugo upotrebljavane), te, na kompatibilnim uređajima, pokretati *web*-kamere i prikupljati snimljeni materijal. Takve su tehnologije široko dostupne, uključujući i od trećih osoba kao što su pružatelji usluga u oblaku.

Međutim, obrada podataka koju te tehnologije uključuju neproporcionalna je i poslodavac vrlo vjerojatno neće imati pravnu osnovu na temelju legitimnog interesa, npr. za evidentiranje zaposlenikovih pritisaka na tipke ili kretanja miša.

Od ključne je važnosti da se rizik koji predstavljaju rad od kuće i rad na daljinu riješi na razmjeran način koji nije prekomjeran, bez obzira na koji je način mogućnost ponuđena i koja se tehnologija upotrebljava, posebno ako su granice između poslovne i privatne upotrebe nejasne.

5.4.2. *DONESI VLASTITI UREĐAJ (ENG.* **BRING YOUR OWN DEVICE** *– BYOD)*

Zbog sve veće popularnosti te boljih značajki i mogućnosti potrošačkih elektroničkih uređaja poslodavci se mogu suočiti sa zahtjevom zaposlenika da se za obavljanje posla koriste vlastitim uređajima na radnome mjestu. Ta je praksa poznata pod nazivom „donesi vlastiti uređaj” (eng. „*bring your own device*” ili BYOD).

Učinkovito provođenje prakse BYOD može dovesti do brojnih koristi za zaposlenike, uključujući zaposlenikovo veće zadovoljstvo poslom, veću sveukupnu motiviranost, veću učinkovitost na poslu te veću fleksibilnost. Međutim, po definiciji, određena upotreba zaposlenikova uređaja po prirodi je privatna te je veća vjerojatnost da će ona biti takva u određenim dijelovima dana (npr. navečer ili tijekom vikenda). Stoga postoji velika vjerojatnost da će u slučaju kada se zaposlenici koriste vlastitim uređajima poslodavci

obrađivati informacije koje nisu poslovne prirode, a odnose se na zaposlenike i možda na sve članove obitelji koji se isto tako koriste predmetnim uređajima.

U kontekstu zaposlenja, rizici za privatnost koje za sobom povlači praksa BYOD-a uglavnom su povezani s tehnologijama praćenja kojima se prikupljaju identifikatori kao što su MAC adrese, ili u slučajevima kada poslodavac pristupa uređaju zaposlenika uz opravdanje da provodi sigurnosni pregled radi otkrivanja zlonamjernih programa. U pogledu potonjeg postoji niz komercijalnih rješenja koja omogućuju pregledavanje privatnih uređaja, ali njihova bi upotreba mogla dovesti do pristupa svim podacima na predmetnom uređaju te se stoga moraju pažljivo primjenjivati. Na primjer, u načelu se ne bi smjelo pristupati onim dijelovima uređaja za koje se pretpostavlja da se upotrebljavaju samo u privatne svrhe (npr. datoteka s fotografijama snimljenima uređajem).

Može se smatrati da je praćenje lokacije i prometa na tim uređajima u legitimnom interesu zaštite osobnih podataka za koje je poslodavac odgovoran kao voditelj obrade podataka; međutim, kada je riječ o osobnom uređaju zaposlenika, to može biti nezakonito ako se takvim praćenjem prikupljaju i podaci koji se odnose na zaposlenikov privatni i obiteljski život. Kako bi se spriječilo praćenje privatnih informacija, moraju se provoditi odgovarajuće mjere kako bi se razlikovala privatna i poslovna upotreba uređaja.

Poslodavci bi trebali primjenjivati i metode s pomoću kojih se njihovi vlastiti podaci na uređaju sigurno prenose između uređaja i njihove mreže. Postoji mogućnost da uređaj stoga bude konfiguriran tako da sav promet usmjerava preko virtualne privatne mreže (VPN) natrag u mrežu poduzeća kako bi se osigurala određena razina sigurnosti; međutim, ako se primjenjuje takva mjera, poslodavac bi trebao uzeti u obzir i to da računalni program ugrađen radi praćenja predstavlja rizik za privatnost u razdobljima kada se zaposlenik koristi uređajem u privatne svrhe. Mogli bi se upotrebljavati uređaji koji nude dodatnu zaštitu, kao što je izoliranje podataka u kontroliranom okruženju (zadržavanje podatka unutar određene aplikacije – eng. *sandboxing*).

S druge strane, poslodavac mora isto tako razmotriti zabranu upotrebe posebnih radnih uređaja u privatne svrhe ako ne postoji način da se spriječi praćenje privatne upotrebe – primjerice ako uređaj omogućuje daljinski pristup osobnim podacima za koje je poslodavac voditelj obrade podataka.

5.4.3. *UPRAVLJANJE MOBILNIM UREĐAJIMA (ENG.* MOBILE DEVICE MANAGEMENT – *MDM)*

Tehnologija upravljanja mobilnim uređajima omogućuje poslodavcima da daljinski lociraju uređaj, upotrebljavaju posebne konfiguracije i/ili aplikacije te da na zahtjev brišu podatke. Poslodavac može sam upotrebljavati ovu funkciju ili može za to angažirati treću osobu. Usluge upravljanja mobilnim uređajima omogućuju poslodavcima i da evidentiraju ili prate uređaj u stvarnom vremenu čak i ako nije prijavljeno da je ukraden.

Prije primjene bilo koje takve tehnologije koja je nova, ili je nova za voditelja obrade podataka, trebalo bi provesti procjenu učinka na zaštitu podataka. Ako se procjenom učinka na zaštitu podataka pokaže da je tehnologija upravljanja mobilnim uređajima nužna u posebnim okolnostima, trebalo bi provesti i procjenu o tome je li obrada podataka koja iz nje proizlazi u skladu s načelima proporcionalnosti i supsidijarnosti. Poslodavci moraju osigurati da se podaci koji su prikupljeni u okviru daljinskog lociranja obrađuju u točno određene svrhe te da nisu i ne mogu biti dio šireg programa koji omogućuje stalno praćenje

zaposlenika. Čak i kad je riječ o točno određenim svrhama, trebalo bi ublažiti značajke koje omogućuju praćenje. Sustavi praćenja mogu biti osmišljeni tako da bilježe podatke o lokaciji bez njihova dostavljanja poslodavcu – u takvim bi im okolnostima podaci o lokaciji trebali biti dostupni jedino ako se uređaj prijavi ili izgubi.

Zaposlenici čiji su uređaji obuhvaćeni uslugama upravljanja mobilnim uređajima moraju biti u cijelosti informirani o tome što se prati i koje su posljedice tog praćenja za njih.

5.4.4. *NOSIVI UREĐAJI*

Sve je češća praksa da poslodavci daju svojim zaposlenicima nosive uređaje kako bi pratili i nadzirali njihovo zdravlje i aktivnosti na radnome mjestu, a ponekad čak i izvan radnog mjesta. Međutim, takva obrada podataka uključuje i obradu podataka o zdravlju te je stoga zabranjena na temelju članka 8. DZP-a.

S obzirom na nejednak odnos između poslodavca i zaposlenika – tj. zaposlenik financijski ovisi o poslodavcu – te osjetljivu prirodu podataka o zdravlju, vrlo je mala vjerojatnost da će biti dana pravno valjana izričita privola za praćenje i nadziranje takvih podataka jer, kao prvo, zaposlenici u biti nisu „slobodni" dati takvu privolu. Čak i ako poslodavac angažira treću osobu da skuplja podatke o zdravlju, koja bi poslodavcu davala samo zbirne podatke o općim zdravstvenim kretanjima, obrada podataka i dalje bi bila nezakonita.

Isto tako, kako je opisano u *Mišljenju 5/2014 o tehnikama anonimizacije*[18], tehnički je vrlo teško osigurati potpunu anonimizaciju podataka. Čak i u okruženju s više od tisuću zaposlenika poslodavac bi, s obzirom na dostupnost drugih podataka o zaposlenicima, mogao izdvojiti pojedine zaposlenike s posebnim zdravstvenim indikacijama kao što je visoki krvni tlak ili pretilost.

Primjer:

poduzeće daje na dar svojim zaposlenicima uređaje za praćenje tjelesne spremnosti. Uređaj broji korake koje zaposlenik napravi te bilježi njegove otkucaje srca i obrasce spavanja tijekom vremena.

Tako dobiveni podaci o zdravlju trebali bi biti dostupni samo zaposleniku, a ne poslodavcu. Svi podaci koji se razmijene između zaposlenika (kao ispitanika) i uređaja/pružatelja usluge (kao voditelja obrade podataka) stvar su tih stranaka.

S obzirom na to da bi podatke o zdravlju mogla obrađivati komercijalna stranka koja je proizvela uređaj ili koja nudi uslugu poslodavcima, poslodavac bi pri odabiru uređaja ili usluge trebao ocijeniti politiku zaštite privatnosti proizvođača i/ili pružatelja usluge kako bi osigurao da ne dođe do nezakonite obrade podataka o zdravlju zaposlenika.

5.5. Obrada podataka o radnom vremenu i prisutnosti na poslu

Sustavi koji poslodavcima omogućuju da kontroliraju tko može ulaziti u njihove prostorije i/ili u određene prostore unutar njihovih prostorija mogu omogućiti i praćenje aktivnosti zaposlenika. Iako takvi sustavi postoje već niz godina, sve se više primjenjuju nove

[18] Radna skupina iz članka 29., *Mišljenje 5/2014 o tehnikama anonimizacije*, WP 216, 10. travnja 2014., url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_hr.pdf

tehnologije praćenja radnog vremena i prisutnosti zaposlenika, uključujući i one kojima se obrađuju biometrijski podaci, kao i ostale tehnologije, na primjer praćenje mobilnih uređaja.

Premda takvi sustavi mogu biti važna sastavnica revizijskog traga poslodavca, oni predstavljaju i rizik od nametljive razine znanja i kontrole u pogledu aktivnosti zaposlenika dok je na radnome mjestu.

Primjer:

poslodavac ima posebnu serversku prostoriju u kojoj se poslovno osjetljivi podaci, osobni podaci koji se odnose na zaposlenike i osobni podaci koji se odnose na klijente čuvaju u digitalnom obliku. Kako bi ispunio zakonsku obvezu osiguravanja podataka od neovlaštenog pristupa, poslodavac je ugradio sustav za kontrolu pristupa kojim se bilježe ulasci i izlasci zaposlenika koji imaju odgovarajuće dopuštenje za ulazak u prostoriju. U slučaju da nestane bilo koji dio opreme ili da se podacima neovlašteno pristupi, da se izgube ili ukradu, evidencije koje vodi poslodavac omogućuju mu da utvrdi tko je imao pristup prostoriji u tom trenutku.

S obzirom na to da je obrada podataka nužna te da ne nadilazi zaposlenikovo pravo na privatni život, ona može biti u legitimnom interesu na temelju članka 7. točke (f), pod uvjetom da su zaposlenici na odgovarajući način obaviješteni o predmetnom postupku obrade podataka. Međutim, stalno praćenje učestalosti i točnog vremena ulaska i izlaska zaposlenika ne može biti opravdano ako se ti podaci upotrebljavaju i u druge svrhe, kao što je ocjenjivanje uspješnosti zaposlenika u obavljanju posla.

5.6. Postupci obrade podataka s pomoću sustava za videonadzor

Videonadzor i dalje sa sobom povlači slične probleme za privatnost zaposlenika kao i do sada, a odnose se na mogućnost stalnog praćenja ponašanja radnika[19]. Najrelevantnije promjene koje se odnose na primjenu te tehnologije u kontekstu zaposlenja jesu sljedeće: mogućnost jednostavnog daljinskog pristupa prikupljenim podacima (npr. putem pametnog telefona), smanjenje veličine kamera (uz povećanje njihovih mogućnosti, npr. visoku rezoluciju) te obrada podataka koja se može provesti s pomoću nove videoanalitike.

Zahvaljujući mogućnostima koje pruža videoanalitika poslodavac može s pomoću automatiziranih sredstava pratiti izraze lica zaposlenika, prepoznati odstupanja od unaprijed definiranih obrazaca kretanja (npr. u tvorničkom kontekstu) i drugo. To je neproporcionalno pravima i slobodama zaposlenika te je stoga općenito nezakonito. Obrada podataka vjerojatno će uključivati i izradu profila, a možda i automatizirano donošenje odluka. Stoga bi se poslodavci trebali suzdržavati od upotrebe tehnologija prepoznavanja lica. Mogu postojati neke marginalne iznimke od tog pravila, ali takvi scenariji ne mogu poslužiti kao opravdanje za opću zakonitost upotrebe takve tehnologije[20].

5.7. Postupci obrade podataka koji uključuju vozila kojima se koriste zaposlenici

[19] Vidjeti prethodno navedeni predmet *Köpke protiv Njemačke*; osim toga, treba napomenuti da u je nekim jurisdikcijama ugradnja sustava kao što je CCTV u svrhu dokazivanja nezakonitog ponašanja dopustiva; vidjeti predmet *Bershka* na Ustavnom sudu Španjolske.

[20] Osim toga, u skladu s OUZP-om, obrada biometrijskih podataka u svrhe utvrđivanja identiteta mora se temeljiti na nekom od izuzeća predviđenih u članku 9. stavku 2.

Sve više poduzeća, posebno onih koja se bave prijevoznom djelatnošću ili imaju veliki vozni park, uvode tehnologije koje poslodavcima omogućuju praćenje svojih vozila.

Svaki poslodavac koji upotrebljava telematske sustave za vozila prikupljat će podatke i o vozilu i o zaposleniku koji se koristi tim vozilom. Ti podaci mogu uključivati ne samo podatke o lokaciji vozila (a time i o lokaciji zaposlenika) prikupljene s pomoću osnovnog sustava za praćenje GPS-om, nego, ovisno o tehnologiji, i cijeli niz drugih informacija, među ostalim i onih o ponašanju vozača tijekom vožnje. Neke tehnologije mogu omogućiti i stalno praćenje vozila i vozača (npr. uređaji za bilježenje podataka o događajima).

Poslodavac će možda biti obvezan ugraditi u vozila tehnologiju praćenja kako bi dokazao da ispunjuje ostale pravne obveze, npr. za osiguravanje sigurnosti zaposlenika koji voze predmetna vozila. Poslodavac može imati i legitimni interes da bude u mogućnosti locirati vozilo u svakom trenutku. Čak i da poslodavac ima legitimni interes da ostvari te svrhe, trebalo bi prvo procijeniti je li obrada podataka u te svrhe nužna te je li stvarna provedba u skladu s načelima proporcionalnosti i supsidijarnosti. Ako je dopuštena upotreba službenih vozila u privatne svrhe, najvažnija mjera koju poslodavac može poduzeti da bi osigurao poštovanje tih načela jest ponuditi mogućnost odstupanja: zaposlenik bi u načelu trebao imati mogućnost privremeno isključiti funkciju praćenja lokacije ako je takvo isključivanje opravdano posebnim okolnostima, kao što je posjet liječniku. Na taj način zaposlenik može na vlastitu inicijativu zaštititi određene podatke o lokaciji kao privatne podatke. Poslodavac mora osigurati da se prikupljeni podaci ne upotrebljavaju za nezakonitu daljnju obradu, kao što je praćenje i ocjenjivanje zaposlenika.

Poslodavac mora isto tako jasno informirati zaposlenike da je u službeno vozilo koje voze ugrađen uređaj za praćenje te da se tijekom njihova korištenja tim vozilom bilježe njihova kretanja (te da se, ovisno o tehnologiji koja se primjenjuje, mogu bilježiti i podaci o njihovu ponašanju tijekom vožnje). Poželjno je da te informacije budu prikazane na vidljivom mjestu u svakom vozilu, u vidnom polju vozača.

Postoji mogućnost da se zaposlenici smiju koristiti vozilom poduzeća izvan radnog vremena, npr. u privatne svrhe, ovisno o posebnim politikama kojima je uređena upotreba tih vozila. S obzirom na osjetljivost podataka o lokaciji, vjerojatno neće postojati pravna osnova za praćenje lokacija vozila zaposlenika izvan dogovorenog radnog vremena. Međutim, u slučaju da takva potreba postoji, trebalo bi razmisliti o provedbi koja bi bila proporcionalna rizicima. Na primjer, to bi moglo značiti da se, radi sprečavanja krađe automobila, lokacija automobila ne bilježi izvan radnog vremena, osim ako vozilo napušta neko šire određeno područje (regiju ili čak zemlju). Osim toga, lokacija bi bila prikazana samo u hitnim slučajevima – poslodavac bi aktivirao „vidljivost" lokacije, procjenjujući podatke koje je sustav već pohranio, ako vozilo napusti unaprijed definirano područje.

Kao što je Radna skupina iz članka 29. navela u *Mišljenju 13/2011 o geolokacijskim uslugama na pametnim mobilnim uređajima*[21]:

„Uređaji za praćenje vozila nisu uređaji za praćenje osoblja. Njihova je funkcija praćenje ili nadziranje lokacije vozila u koja su ugrađeni. Poslodavci ih ne smiju smatrati uređajima koji

[21] Radna skupina iz članka 29., *Mišljenje 13/2011 o geolokacijskim uslugama na pametnim mobilnim uređajima,* WP 185, 16. svibnja 2011., url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp185_en.pdf

služe za praćenje ili nadziranje ponašanja ili lokacije vozača ili drugih članova osoblja, na primjer slanjem upozorenja o brzini vozila."

Nadalje, kao što je Radna skupina iz članka 29. navela u *Mišljenju 5/2005 o upotrebi podataka o lokaciji u cilju obavljanja usluga s dodanom vrijednošću*[22]:

„Obrada podataka o lokaciji može biti opravdana ako se provodi kao dio praćenja prijevoza ljudi ili robe ili poboljšanja raspodjele resursa za usluge na raspršenim lokacijama (npr. planiranje operacija u stvarnom vremenu) ili ako se želi ostvariti sigurnosni cilj u pogledu samog zaposlenika ili robe ili vozila za koje je odgovoran. S druge strane, Radna skupina smatra da je obrada podataka pretjerana ako zaposlenici sami organiziraju svoje putovanje u skladu s vlastitim željama ili ako se provodi isključivo u svrhu praćenja rada zaposlenika, ako se njegov rad može pratiti na druge načine."

5.7.1. UREĐAJI ZA BILJEŽENJE PODATAKA O DOGAĐAJIMA

Uređaji za bilježenje podataka o događajima pružaju poslodavcu tehničku mogućnost obrade velike količine osobnih podataka o zaposlenicima koji voze vozila poduzeća. Takvi se uređaji sve više ugrađuju u vozila radi snimanja videozapisa, uz eventualni tonski zapis, u slučaju nesreće. Ti sustavi mogu bilježiti u određenim trenucima, npr. u slučaju naglog kočenja, iznenadne promjene smjera ili nesreće, pri čemu se spremaju podaci o trenucima netom prije događaja, ali mogu biti namješteni i tako da neprestano prate. Ti se podaci mogu kasnije upotrijebiti za promatranje i preispitivanje ponašanja pojedinca tijekom vožnje radi njegova poboljšanja. Osim toga, mnogi od tih sustava sadržavaju GPS za praćenje lokacije vozila u stvarnom vremenu, a i druge pojedinosti povezane s vožnjom (kao što je brzina vozila) mogu biti pohranjene za daljnju obradu.

Te uređaje posebno često upotrebljavaju poduzeća koja se bave prijevoznom djelatnošću ili imaju veliki vozni park. Međutim, upotreba uređaja za bilježenje podataka o događajima može biti zakonita jedino ako postoji potreba za obradom osobnih podataka o zaposleniku u zakonitu svrhu te ako je ta obrada u skladu s načelima proporcionalnosti i supsidijarnosti.

Primjer

Prijevozničko poduzeće oprema sva svoja vozila videokamerom u kabini koja snima zvučne i videozapise. Svrha je obrade tih podataka poboljšati vozačke vještine zaposlenika. Kamere su konfigurirane tako da zadrže snimljene zapise kad god se dogode incidenti kao što su naglo kočenje ili iznenadna promjena smjera. Poduzeće pretpostavlja da ima pravnu osnovu za obradu podataka u svojem legitimnom interesu na temelju članka 7. točke (f) Direktive radi zaštite sigurnosti svojih zaposlenika i sigurnosti drugih vozača.

Međutim, legitiman interes poduzeća da prati vozače nema prednost pred pravima tih vozača na zaštitu vlastitih osobnih podataka. Stalno praćenje zaposlenika s pomoću takvih kamera ozbiljno je zadiranje u njihovo pravo na privatnost. Postoje druge metode (npr. ugradnja opreme kojom se sprečava upotreba mobilnih telefona) i drugi sigurnosni sustavi, kao što je napredni sustav za kočenje u slučaju nužde ili sustav za upozoravanje na napuštanje prometne trake, koji se mogu upotrijebiti za sprečavanje automobilskih nesreća i koji su možda

[22] Radna skupina iz članka 29., *Mišljenje 5/2005 o upotrebi podataka o lokaciji u cilju obavljanja usluga s dodanom vrijednošću,* WP 115, 25. studenoga 2005., url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2005/wp115_en.pdf

primjereniji. Nadalje, kod takvih videozapisa postoji velika vjerojatnost da će doći do obrade osobnih podatka trećih osoba (kao što su pješaci) te za takvu obradu legitiman interes poduzeća nije dovoljno opravdanje.

5.8. Postupci obrade podataka u kojima se podaci o zaposlenicima otkrivaju trećim osobama

Poduzeća sve češće dostavljaju svojim klijentima podatke o zaposlenicima kako bi osigurala pouzdano pružanje usluga. Ti podaci mogu biti prilično pretjerani ovisno o opsegu usluga koje se pružaju (npr. mogu uključivati i fotografiju zaposlenika). Međutim, zbog neravnoteže moći zaposlenici nisu u mogućnosti dobrovoljno dati privolu na obradu svojih osobnih podataka koju provodi poslodavac, a ako obrada podataka nije proporcionalna, poslodavac nema pravnu osnovu za nju.

Primjer:

poduzeće za dostavu šalje klijentima poruku e-pošte s poveznicom na ime i lokaciju dostavljača (zaposlenika). Poduzeće je namjeravalo poslati i službenu fotografiju dostavljača. Poduzeće je pretpostavljalo da ima pravnu osnovu za obradu podataka u svojem legitimnom interesu (članak 7. točka (f) Direktive), a to je omogućiti klijentu da provjeri je li dostavljač prava osoba.

Međutim, nije nužno klijentima dati ime i fotografiju dostavljača. S obzirom na to da ne postoji druga legitimna osnova za obradu podataka, poduzeću za dostavu nije dopušteno davati te osobne podatke klijentima.

5.9. Postupci obrade podataka koji uključuju međunarodne prijenose podataka o ljudskim resursima i drugih podataka o zaposlenicima

Poslodavci sve više upotrebljavaju aplikacije i usluge u oblaku, na primjer one namijenjene postupanju s podacima o ljudskim resursima, kao i internetske uredske aplikacije. Pri upotrebi većine tih aplikacija dolazi do međunarodnog prijenosa podataka od zaposlenika i o zaposlenicima. Kao što je već navedeno u Mišljenju 08/2001, u članku 25. Direktive navodi se da se prijenos osobnih podataka trećoj zemlji izvan EU-a može izvršiti jedino ako ta zemlja osigurava odgovarajuću razinu zaštite. Koja god bila osnova za prijenos, on treba biti u skladu s odredbama Direktive.

Stoga treba osigurati ispunjavanje tih odredaba koje se odnose na međunarodni prijenos podataka. Radna skupina iz članka 29. ponavlja svoje već izrečeno stajalište da je poželjnije oslanjati se na primjerenu zaštitu nego na iznimke navedene u članku 26. DZP-a; ako se poziva na privolu, ona mora biti posebna, nedvosmislena i dobrovoljna. Međutim, trebalo bi isto tako osigurati da podaci koji se dijele izvan EU-a/EGP-a te kasniji pristup drugih subjekata unutar skupine, budu ograničeni na minimum nužan za predviđene svrhe.

6. Zaključci i preporuke

6.1. Temeljna prava

Na sadržaj prethodno opisanih oblika komunikacije, kao i na podatke o prometu koji se odnose na tu komunikaciju, primjenjuje se ista zaštita temeljnih prava kao i na analognu komunikaciju.

Elektronička komunikacija upućena iz poslovnih prostora može biti obuhvaćena pojmom „privatnog života" i „korespondencije" u smislu članka 8. stavka 1. Europske konvencije. Na temelju trenutačne Direktive o zaštiti podataka poslodavci mogu prikupljati podatke samo u zakonite svrhe, obrađivati ih u skladu s odgovarajućim uvjetima (npr. u mjeri koja je proporcionalna i nužna, za stvarni i sadašnji interes, na zakonit, jasan i transparentan način) te imati pravnu osnovu za obradu osobnih podataka prikupljenih ili generiranih putem elektroničke komunikacije.

Činjenica da je poslodavac vlasnik elektroničkih sredstava ne isključuje pravo zaposlenika na tajnost komunikacije, povezanih podataka o lokaciji i korespondencije. Praćenje lokacije zaposlenika putem njihovih vlastitih uređaja ili uređaja koje im je ustupilo poduzeće trebalo bi biti ograničeno samo na slučajeve u kojima je to nužno potrebno za određenu zakonitu svrhu. U slučaju kad se primjenjuje praksa „donesi vlastiti uređaj", važno je da je zaposlenicima dana mogućnost da zaštite svoju privatnu komunikaciju od svakog praćenja povezanog s poslom.

6.2. Privola; legitimni interes

Zaposlenici gotovo nikada nisu u situaciji da slobodno daju, odbiju ili povuku privolu s obzirom na ovisnost koja proizlazi iz odnosa poslodavac-zaposlenik. Zbog neravnoteže moći, zaposlenici mogu dobrovoljno dati privolu jedino u iznimnim okolnostima, kada prihvaćanje ili odbijanje ponude ne povlači za sobom nikakve posljedice.

Ponekad je moguće pozvati se na legitimni interes poslodavca kao pravnu osnovu, ali samo ako je obrada podataka nužna za zakonitu svrhu i u skladu je s načelima proporcionalnosti i supsidijarnosti. Prije upotrebe bilo kojeg alata za praćenje trebalo bi ispitati proporcionalnost kako bi se razmotrilo jesu li svi podaci potrebni, nadilazi li obrada podataka opća prava na privatnost koja zaposlenici imaju na radnome mjestu te koje se mjere moraju poduzeti kako bi se osiguralo da su kršenja prava na privatni život i prava na tajnost komunikacija ograničena na potreban minimum.

6.3. Transparentnost

Zaposlenici bi trebali biti na učinkovit način obaviješteni o svakom praćenju koje se provodi, svrhama u koje se provodi i okolnostima, kao i o mogućnostima koje zaposlenici imaju za sprečavanje prikupljanja njihovih podataka tehnologijama praćenja. Politike i pravila koji se odnose na zakonito praćenje moraju biti jasni i lako dostupni. Radna skupina preporučuje da se u izradu i evaluaciju tih pravila i politika uključi reprezentativan uzorak zaposlenika jer većina praćenja može potencijalno zadirati u privatni život zaposlenika.

6.4. Proporcionalnost i smanjenje količine podataka

Obrada podataka na radnome mjestu mora biti proporcionalan odgovor na rizike s kojima se suočava poslodavac. Na primjer, zlouporaba interneta može se otkriti i bez potrebe za analizom sadržaja *web*-mjesta. Ako se zlouporaba može spriječiti (npr. s pomoću filtara za *web*-mjesta), poslodavac nema opće pravo na praćenje.

Nadalje, opća zabrana komunikacije u privatne svrhe nepraktična je i njezina provedba može zahtijevati neproporcionalnu razinu praćenja. Sprečavanju bi trebalo dati puno veću važnost nego otkrivanju – interesima poslodavca bolje se služi ako se zlouporaba interneta sprečava tehničkim sredstvima umjesto povećavanja resursa za otkrivanje zlouporabe.

Informacije koje se bilježe stalnim praćenjem, kao i informacije koje se prikazuju poslodavcu, trebalo bi svesti na sto manju mjeru. Zaposlenici bi trebali biti u mogućnosti privremeni isključiti funkciju praćenja lokacije, ako to opravdavaju okolnosti. Rješenja za, primjerice, praćenje vozila mogu biti tako osmišljena da bilježe podatke o položaju bez njihova prikazivanja poslodavcu.

Kada odlučuju o uvođenju novih tehnologija, poslodavci moraju uzeti u obzir načelo smanjenja količine podataka. Informacije bi trebalo pohraniti na minimalno potrebno vrijeme, s točno određenim vremenom njihova čuvanja. Čim informacije više nisu potrebne, trebali bi ih izbrisati.

6.5. Usluge u oblaku, internetske aplikacije i međunarodni prijenosi

Ako se od zaposlenika očekuje da se koriste internetskim aplikacijama koje obrađuju osobne podatke (kao što su internetske uredske aplikacije), poslodavci bi trebali razmisliti o tome da zaposlenicima omoguće određivanje određenih privatnih prostora u koje poslodavac ne može dobiti pristup ni u kojim okolnostima, kao što su datoteke s privatnom poštom ili privatnim dokumentima.

Pri upotrebi većine aplikacija u oblaku dolazi do međunarodnog prijenosa podataka o zaposlenicima. Trebalo bi osigurati da se prijenos osobnih podataka u treću zemlju izvan EU-a odvija jedino ako je osigurana primjerena razina zaštite te da podaci koji se dijele izvan EU-a/EGP-a, i kasniji pristup drugih subjekata unutar skupine, budu ograničeni na minimum nužan za predviđene svrhe.

* * *

Sastavljeno u Bruxellesu 8. lipnja 2017.

Za Radnu skupinu
Predsjednica
Isabelle FALQUE-PIERROTIN