ARTICOLUL 29 GRUPUL DE LUCRU PENTRU PROTECȚIA DATELOR

17/RO

GL 249

Avizul nr. 2/2017 privind prelucrarea datelor la locul de muncă

Adoptat la 8 iunie 2017

Acest grup de lucru a fost constituit în temeiul articolului 29 din Directiva 95/46/CE. Acesta este un organ european privind protecția datelor și a vieții private cu rol consultativ și statut independent. Atribuțiile sale sunt descrise la articolul 30 din Directiva 95/46/CE și la articolul 15 din Directiva 2002/58/CE.

Secretariatul este asigurat de Direcția C (Drepturi fundamentale și statul de drept) din cadrul Comisiei Europene, Direcția Generală Justiție și Consumatori, B-1049 Bruxelles, Belgia, Nr. birou MO59 05/35

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

Cuprins

1 Rezumat

Prezentul aviz completează publicațiile anterioare elaborate în temeiul articolului 29 Grupul de lucru („GL 29") și intitulate *Avizul nr. 8/2001 privind prelucrarea datelor cu caracter personal în contextul ocupării unui loc de muncă* (GL 48)[1] și *Documentul de lucru privind supravegherea comunicațiilor electronice la locul de muncă* (GL 55)[2] din 2002. De la publicarea acestor documente, au fost adoptate o serie de noi tehnologii care permit prelucrarea mai sistematică a datelor cu caracter personal ale angajaților la locul de muncă, creând dificultăți semnificative în ceea ce privește protecția vieții private și a datelor.

Prezentul aviz întreprinde o nouă analiză a echilibrului dintre interesele legitime ale angajatorilor și așteptările rezonabile ale angajaților în ceea ce privește viața privată, evidențiind riscurile pe care le prezintă noile tehnologii și procedând la o evaluare a proporționalității într-o serie de scenarii în care acestea ar putea fi utilizate.

Cu toate că, în principal, vizează Directiva privind protecția datelor, avizul examinează obligațiile suplimentare impuse angajatorilor prin Regulamentul general privind protecția datelor. De asemenea, acesta reafirmă poziția și concluziile din Avizul 8/2001 și Documentul de lucru GL 55, și anume că atunci când prelucrează datele cu caracter personal ale angajaților:

- angajatorii ar trebui să țină în permanență seama de principiile fundamentale ale protecției datelor, indiferent de tehnologia utilizată;
- conținutul comunicațiilor electronice efectuate în spațiile comerciale se bucură de aceeași protecție a drepturilor fundamentale ca și comunicațiile analogice;
- procedura de aprobare este foarte puțin probabil să constituie un temei juridic pentru prelucrarea datelor la locul de muncă, cu excepția cazului în care angajații pot refuza fără consecințe nefavorabile;
- executarea unui contract și interesele legitime pot fi uneori invocate, cu condiția ca prelucrarea să fie strict necesară pentru un scop legitim și să respecte principiile proporționalității și subsidiarității;
- angajații ar trebui să primească informații eficace cu privire la monitorizarea care are loc; și
- orice transfer internațional de date privind angajații ar trebui să fie efectuat numai în cazul în care este asigurat un nivel de protecție adecvat.

2. Introducere

Adoptarea rapidă a noilor tehnologii ale informației la locul de muncă, în ceea ce privește infrastructura, aplicațiile și dispozitivele inteligente, permite prelucrarea sistematică și potențial invazivă a noi tipuri de date la locul de muncă. De exemplu:

[1] GL 29, *Avizul nr. 8/2001 privind prelucrarea datelor cu caracter personal în contextul ocupării unui loc de muncă*, GL 48, 13 septembrie 2001, url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2001/wp48_en.pdf

[2] GL 29, *Documentul de lucru privind supravegherea comunicațiilor electronice la locul de muncă*, GL 55, 29 mai 2002, url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2002/wp55_en.pdf

- tehnologiile care facilitează prelucrarea datelor la locul de muncă pot fi acum implementate la o fracțiune din costurile care au fost realizate cu mai mulți ani în urmă, în timp ce capacitatea acestor tehnologii de a prelucra date cu caracter personal a crescut exponențial;
- noile forme de prelucrare, cum ar fi cele privind datele cu caracter personal la utilizarea serviciilor online și/sau datele de localizare de pe un dispozitiv inteligent, sunt mult mai puțin vizibile pentru angajați decât alte tipuri mai tradiționale, cum ar fi camerele TVCI la vedere. Acest fapt ridică întrebări în legătură cu măsura în care angajații cunosc aceste tehnologii, întrucât angajatorii ar putea pune în aplicare în mod nelegal aceste tipuri de prelucrare, fără înștiințarea prealabilă a angajaților; și
- limitele dintre domiciliu și locul de muncă au devenit din ce în ce mai neclare. De exemplu, atunci când angajații lucrează la distanță (de exemplu, la domiciliu) sau în timp ce călătoresc în scop de afaceri, monitorizarea activităților în afara mediului fizic de lucru poate fi efectuată și ar putea include monitorizarea persoanei într-un context privat.

Prin urmare, deși utilizarea unor astfel de tehnologii poate fi utilă pentru a detecta sau a preveni pierderea proprietății intelectuale și materiale a societății, a îmbunătăți productivitatea angajaților și a proteja datele cu caracter personal pentru care operatorul de date este responsabil, acestea creează totodată provocări semnificative legate de viața privată și protecția datelor. Prin urmare, este necesară o nouă evaluare privind echilibrul dintre interesul legitim al angajatorului de a-și proteja întreprinderea și așteptarea rezonabilă privind viața privată a persoanelor vizate: angajații.

Deși prezentul aviz se va concentra asupra noilor tehnologii ale informației prin evaluarea a nouă scenarii diferite în care acestea pot apărea, acesta va analiza, de asemenea, pe scurt, metodele mai tradiționale de prelucrare a datelor la locul de muncă, în cazul cărora riscurile sunt amplificate ca urmare a schimbărilor tehnologice.

În cazurile în care se utilizează termenul „angajat” în prezentul aviz, GL 29 nu intenționează să restrângă domeniul de aplicare al acestui termen doar la persoanele cu contract de muncă recunoscut ca atare în conformitate cu legislația muncii aplicabilă. În ultimele decenii, au devenit mai frecvente noi modele de afaceri utilizate la diferite tipuri de relații de muncă și, în special, la profesiile independente. Prezentul aviz intenționează să acopere toate situațiile în care există relații de muncă, indiferent dacă această relație are la bază un contract de muncă.

Este important de precizat că angajații sunt rareori în măsură să își exprime în mod liber, să refuze sau să își revoce consimțământul, având în vedere dependența care rezultă din relația dintre angajator și angajat. În afară de cazurile excepționale, angajatorii vor trebui să se bazeze pe un alt temei juridic decât consimțământul, cum ar fi necesitatea de a prelucra datele în interesul lor legitim. Cu toate acestea, un interes legitim în sine nu este suficient pentru a prevala față de drepturile și libertățile angajaților.

Indiferent de temeiul juridic al unei astfel de prelucrări, ar trebui să fie efectuat un test al proporționalității înainte de începerea acesteia pentru a analiza dacă prelucrarea este necesară pentru atingerea unui scop legitim, precum și măsurile care trebuie luate pentru a obține certitudinea că încălcările dreptului la viață privată și la secretul comunicațiilor sunt limitate la minimum. Acesta poate face parte dintr-o evaluare a impactului asupra protecției datelor (DPIA).

3. Cadrul juridic

Deși analiza de mai jos este efectuată, în primul rând, în contextul cadrului juridic actual în temeiul Directivei 95/46/CE (Directiva privind protecția datelor sau „DPD")[3], prezentul aviz va analiza, de asemenea, obligațiile în temeiul Regulamentului 2016/679 (Regulamentul general privind protecția datelor sau „RGPD")[4], care a intrat deja în vigoare și care va deveni aplicabil de la 25 mai 2018.

În ceea ce privește propunerea de regulament asupra vieții private și comunicațiilor electronice[5], grupul de lucru face apel la organele legislative europene să creeze o excepție specifică pentru interferența cu dispozitivele emise angajaților[6]. Propunerea de regulament nu conține o excepție adecvată de la interdicția generală de interferare, iar angajatorii nu pot, de regulă, să ofere un consimțământ valabil pentru prelucrarea datelor cu caracter personal ale angajaților lor.

3,1 Directiva 95/46/CE—Directiva privind protecția datelor („DPD")

În avizul nr. 8/2001, GL 29 a subliniat anterior că angajatorii iau în considerare principiile fundamentale în materie de protecție a datelor ale DPD atunci când prelucrează date cu caracter personal în contextul ocupării unui loc de muncă. Dezvoltarea de noi tehnologii și noi metode de prelucrare în acest context nu a dus la o schimbare a acestei situații, de fapt, se poate afirma că astfel de evoluții au *crescut* importanța acestui aspect pentru angajatori. În acest context, angajatorii trebuie:

- să se asigure că datele sunt prelucrate în scopuri specificate și legitime care sunt proporționale și necesare;
- să țină seama de principiul limitării scopului, asigurându-se, în același timp, că datele sunt adecvate, relevante și neexcesive în raport cu scopul legitim;
- să aplice principiile proporționalității și subsidiarității, indiferent de temeiul juridic aplicabil;
- să exprime transparență în relația cu angajații cu privire la utilizarea și scopurile tehnologiilor de monitorizare;
- să permită exercitarea drepturilor persoanelor vizate, inclusiv a dreptului de acces și, după caz, rectificarea, ștergerea sau blocarea datelor cu caracter personal;
- să păstreze datele exacte și să nu le păstreze mai mult decât este necesar; și
- să ia toate măsurile necesare pentru a proteja datele împotriva accesului neautorizat și să se asigure de faptul că angajații sunt suficient de bine informați cu privire la obligațiile în materie de protecție a datelor.

---

[3] Directiva 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date, *JO L 281, 23.11.1995, p. 31-50*, url: http://eur-lex.europa.eu/legal-content/RO/TXT/?uri=celex%3A31995L0046.

[4] Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor), *JO L 119, 4.5.2016, p. 1-88*, url: http://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A32016R0679.

[5] Propunere de regulament al Parlamentului European și al Consiliului privind respectarea vieții private și protecția datelor cu caracter personal în comunicațiile electronice și de abrogare a Directivei 2002/58/CE, 2017/0003 (COD), url: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=41241.

[6] A se vedea GL 29, *Avizul nr. 1/2017 privind propunerea de regulament asupra vieții private și comunicațiilor electronice*, GL 247, 4 aprilie 2017, pagina 29; url: http://ec.europa.eu/newsroom/document.cfm?doc_id=44103

Fără a repeta îndrumările oferite anterior, GL 29 dorește să sublinieze trei principii, și anume: temeiul juridic, transparența și deciziile automatizate.

3.1.1 *TEMEIUL JURIDIC (ARTICOLUL 7)*

Atunci când prelucrează date cu caracter personal în contextul ocupării unui loc de muncă, trebuie să fie îndeplinit cel puțin unul dintre criteriile prevăzute la articolul 7. În cazul în care tipurile de date cu caracter personal prelucrate implică categorii speciale (astfel cum sunt prezentate la articolul 8), prelucrarea este interzisă, cu excepția cazului în care este valabilă o excepție[7,8]. Chiar și în cazul în care angajatorul se poate baza pe una dintre aceste excepții, este nevoie totuși de un temei juridic de la articolul 7 pentru ca prelucrarea să fie legitimă.

Pe scurt, angajatorii trebuie, așadar, să rețină următoarele:

- pentru cea mai mare parte a acțiunii de prelucrare a acestor date la locul de muncă**, temeiul juridic nu poate și nu ar trebui să fie consimțământul angajaților** [articolul 7 litera (a)], având în vedere natura relației dintre angajator și angajat;
- prelucrarea poate fi necesară pentru **executarea unui contract** [(articolul 7 litera (b)] în cazul în care angajatorul trebuie să prelucreze datele cu caracter personal ale angajatului pentru a îndeplini orice astfel de obligații;
- se întâmplă destul de frecvent ca **dreptul muncii să impună obligații juridice** [articolul 7 litera (c)] **care necesită prelucrarea datelor cu caracter personal**; în astfel de cazuri, angajatul trebuie să fie informat în mod clar și pe deplin cu privire la o astfel de prelucrare (cu excepția cazului în care se aplică o excepție);
- în cazul în care un angajator caută să se bazeze pe **interes legitim** [articolul 7 litera (f)], scopul prelucrării datelor trebuie să fie legitim; metoda aleasă sau tehnologia specifică trebuie să fie necesară, proporțională și pusă în aplicare în modul cel mai puțin intruziv posibil, precum și să aibă capacitatea de a permite angajatorului să demonstreze că **au fost instituite măsurile adecvate** pentru a se asigura un echilibru cu drepturile și libertățile fundamentale ale angajaților[9];
- operațiunile de prelucrare trebuie să fie, de asemenea, în conformitate cu **cerințele de transparență** (articolele 10 și 11), iar angajații ar trebui să fie informați în mod clar și pe deplin cu privire la prelucrarea datelor lor cu caracter personal[10], inclusiv cu privire la existența oricărei acțiuni de monitorizare; și
- **ar trebui să se adopte măsuri tehnice și organizaționale adecvate** pentru a asigura securitatea prelucrării (articolul 17).

Cele mai relevante criterii prevăzute la articolul 7 sunt detaliate mai jos.

---

[7] Astfel cum este menționat în partea 8 din Avizul nr. 8/2001; spre exemplu, articolul 8 alineatul (2) litera (b) prevede o excepție în scopul respectării obligațiilor și al unor drepturi specifice ale operatorului în domeniul dreptului muncii, în măsura în care acest lucru este autorizat de dreptul Uniunii sau de dreptul intern care prevede garanții adecvate.

[8] Ar trebui remarcat faptul că, în unele țări, sunt în vigoare măsuri speciale pe care angajatorii trebuie să le respecte pentru a proteja viața privată a angajaților. Portugalia este un exemplu de astfel de țară în care există măsuri speciale, putându-se aplica măsuri similare și în alte state membre. Prin urmare, concluziile de la secțiunea 5.6, precum și exemplele prezentate în secțiunile 5.1 și 5.7.1 din prezentul aviz, nu sunt valabile în Portugalia din aceste motive.

[9] GL 29, *Avizul nr. 6/2014 privind noțiunea de interese legitime ale operatorului în conformitate cu articolul 7 din Directiva 95/46/CE*, GL 217, adoptat la data de 9 aprilie 2014, url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf.

[10] În conformitate cu articolul 11 alineatul (2) din DPD, operatorul este scutit de obligația de a furniza informații persoanei vizate în cazurile în care înregistrarea sau colectarea de date este prevăzută în mod expres prin lege.

- **Consimțământul [articolul 7 alineatul (a)]**

Conform DPD, consimțământul este definit ca fiind orice manifestare de voință, liberă, specifică și informată a dorințelor unei persoane vizate, prin care aceasta își exprimă acordul cu privire la prelucrarea datelor cu caracter personal care o privesc. Pentru a asigura valabilitatea consimțământului, acesta trebuie să fie, de asemenea, revocabil.

GL 29 a evidențiat anterior, în Avizul nr. 8/2001, că, în cazul în care un angajator trebuie să prelucreze date cu caracter personal ale angajaților săi, este o inducere în eroare să pornească de la ipoteza că prelucrarea poate fi legitimată prin consimțământul angajaților. În cazul în care un angajator declară că solicită consimțământul și există un prejudiciu real sau potențial relevant ca urmare a faptului că angajatul nu și-a exprimat consimțământul (care poate fi foarte probabil în contextul ocupării unui loc de muncă, în special când este vorba de urmărirea de către angajator a comportamentului angajatului în timp), consimțământul nu este valabil, deoarece nu este și nu poate fi exprimat în mod liber. Astfel, pentru cea mai mare parte a cazurilor de prelucrare a datelor angajaților, temeiul juridic al respectivei prelucrări nu poate și nu ar trebui să fie consimțământul angajaților, astfel încât este necesar un temei juridic diferit.

În plus, chiar și în cazurile în care consimțământul poate fi considerat a constitui un temei juridic valabil pentru o astfel de prelucrare (și anume, în cazul în care se poate concluziona, fără îndoială, că respectivul consimțământ este exprimat în mod liber), acesta trebuie să constituie o exprimare specifică și în cunoștință de cauză a dorințelor angajaților. Setările implicite pe dispozitive și/sau instalarea de software care să faciliteze prelucrarea datelor cu caracter personal în mediul electronic nu pot fi considerate drept o exprimare a consimțământului din partea angajaților, deoarece consimțământul necesită o exprimare activă a voinței. Lipsa de acțiune (și anume, nemodificarea setărilor implicite) nu poate fi, în general, considerată drept o exprimare specifică a consimțământului pentru a permite o astfel de prelucrare[11].

- **Executarea unui contract [articolul 7 alineatul (b)]**

Relațiile de muncă sunt adesea bazate pe un contract de muncă între angajator și angajat. Atunci când îndeplinesc obligații în temeiul prezentului contract, cum ar fi remunerarea angajatului, angajatorul este obligat să prelucreze anumite date cu caracter personal.

- **Obligații legale [articolul 7 litera c)]**

Se întâmplă destul de frecvent ca dreptul muncii să impună angajatorului obligații legale care să necesite prelucrarea datelor cu caracter personal (de exemplu, în scopul calculării taxelor și al administrării salariului). În mod evident, în astfel de cazuri, un astfel de act legislativ constituie temeiul juridic pentru prelucrarea datelor.

- **Interesul legitim [articolul 7 litera f)]**

În cazul în care un angajator intenționează să invoce temeiul juridic de la articolul 7 litera (f) din DPD, scopul prelucrării trebuie să fie legitim, iar metoda aleasă sau tehnologia specifică prin intermediul căreia urmează să fie desfășurată prelucrarea trebuie să fie necesară pentru

[11] A se vedea, de asemenea, GL 29, *Avizul nr. 15/2011 privind definirea consimțământului,* GL 187, 13 iulie 2011, url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf, pagina 24.

interesul legitim al angajatorului. Prelucrarea trebuie să fie, de asemenea, proporțională cu nevoile întreprinderii, adică scopul, pe care aceasta este prevăzută a le aborda. Prelucrarea datelor la locul de muncă ar trebui să fie efectuată în modul cel mai puțin intruziv posibil și să vizeze domeniul specific de risc. În plus, atunci când invocă articolul 7 litera (f), angajatul își rezervă dreptul de a contesta procesarea din motive întemeiate și legitime în conformitate cu articolul 14.

Pentru a invoca articolul 7 litera (f) ca temei juridic pentru prelucrare, este esențial să existe măsuri specifice de reducere a riscurilor pentru a asigura un echilibru corect între interesul legitim al angajatorului și drepturile și libertățile fundamentale ale angajaților[12]. Astfel de măsuri, în funcție de forma de monitorizare, ar trebui să includă limitări impuse asupra acțiunii de monitorizare pentru a garanta faptul că nu se încalcă viața privată a angajatului. Astfel de limitări ar putea fi:

- geografice (de exemplu, monitorizarea doar în locuri specifice; monitorizarea zonelor sensibile cum ar fi locurile religioase și, spre exemplu, spațiile sanitare și sălile de recreere ar trebui interzisă),
- axate pe date (de exemplu, fișierele electronice personale și comunicațiile nu ar trebui să fie monitorizate), și
- corelate cu timpul (de exemplu, eșantionarea în locul monitorizării continue).

3.1.2 *TRANSPARENȚA (ARTICOLELE 10 ȘI 11)*

Cerințele de transparență prevăzute la articolele 10 și 11 se aplică în cazul prelucrării datelor la locul de muncă; angajații trebuie să fie informați cu privire la existența oricăror acțiuni de monitorizare în scopul cărora sunt prelucrate date cu caracter personal și orice alte informații necesare pentru a asigura o prelucrare echitabilă.

Odată cu introducerea de noi tehnologii, nevoia de transparență devine mai evidentă, deoarece acestea permit colectarea și prelucrarea ulterioară a unor cantități potențial imense de date cu caracter personal în mod disimulat.

3.1.3 *DECIZII AUTOMATIZATE (ARTICOLUL 15)*

De asemenea, articolul 15 din DPD acordă persoanelor vizate dreptul de a nu face obiectul unei decizii bazate exclusiv pe prelucrarea automată, în cazul în care decizia respectivă produce efecte juridice sau le afectează pe acestea în mod semnificativ și care se bazează exclusiv pe prelucrarea automată a datelor menite să evalueze anumite aspecte personale, cum ar fi performanța la locul de muncă, cu excepția cazului în care decizia este necesară pentru încheierea sau executarea unui contract, autorizată în temeiul dreptului Uniunii sau al statului membru sau întemeiată pe consimțământul explicit al persoanei vizate.

[12] Pentru un exemplu de echilibru care trebuie să fie asigurat, a se vedea cauza *Köpke/Germania*, [2010] CEDO 1725, (URL: http://www.bailii.org/eu/cases/ECHR/2010/1725.html), în care un angajat a fost concediat ca urmare a unei operațiuni de supraveghere video sub acoperire desfășurate de către angajator și o agenție privată de investigații. Chiar dacă, în acest caz, Curtea a concluzionat că autoritățile naționale au asigurat un echilibru echitabil între interesul legitim al angajatorului (în ceea ce privește protecția drepturilor sale de proprietate), dreptul angajatului la respectarea vieții private și interesul public în administrarea justiției, aceasta a arătat totodată că diferitelor interese vizate ar putea să li se atribuie o pondere diferită în viitor ca urmare a dezvoltării tehnologice.

3.2 Regulamentul 2016/679—Regulamentul general privind protecția datelor („RGPD”)

RGPD include și consolidează cerințele din DPD. De asemenea, acesta introduce noi obligații pentru toți operatorii de date, inclusiv angajatori.

3.2.1 *PROTECȚIA DATELOR ÎNCEPÂND CU MOMENTUL CONCEPERII*

Articolul 25 din RGPD impune operatorilor să pună în aplicare protecția datelor începând cu momentul conceperii și în mod implicit. Spre exemplu: în cazul în care un angajator eliberează dispozitive pentru angajați, ar trebui să se aleagă cele mai accesibile soluții din punctul de vedere al vieții private dacă sunt implicate tehnologii de urmărire. Trebuie să se țină cont și de reducerea la minimum a datelor.

3.2.2 *EVALUAREA IMPACTULUI ASUPRA PROTECȚIEI DATELOR*

Articolul 35 din RGPD prezintă cerințele pentru un operator de a efectua o evaluare a impactului asupra protecției datelor (DPIA) în cazul în care un tip de prelucrare, în special folosirea de tehnologii noi, și având în vedere natura, domeniul de aplicare, contextul și scopurile prelucrării în sine, este susceptibil să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice. Un exemplu este un caz de evaluare sistematică și cuprinzătoare a aspectelor personale referitoare la persoane fizice, care se bazează pe prelucrarea automată, inclusiv crearea de profiluri, și care stă la baza unor decizii care produc efecte juridice privind persoana fizică sau care o afectează în mod similar într-o măsură semnificativă.

În cazul în care RGPD indică faptul că riscurile identificate nu pot fi abordate în mod suficient de către operator, și anume că riscurile reziduale sunt în continuare ridicate, operatorul trebuie să se consulte cu autoritatea de supraveghere înainte de începerea prelucrării [articolul 36 alineatul (1)], astfel cum este clarificat în ghidul GL 29 privind evaluările DPIA[13].

3.2.2 *„PRELUCRAREA ÎN CONTEXTUL OCUPĂRII UNUI LOC DE MUNCĂ”*

Articolul 88 din RGPD prevede că, prin lege sau prin acorduri colective, statele membre pot prevedea norme mai detaliate pentru a asigura protecția drepturilor și a libertăților cu privire la prelucrarea datelor cu caracter personal ale angajaților în contextul ocupării unui loc de muncă. În mod specific, aceste norme pot fi prevăzute în următoarele scopuri:

- recrutare;
- îndeplinirea clauzelor contractului de muncă (inclusiv descărcarea de obligațiile stabilite prin lege sau prin acorduri colective);
- gestionare, planificare și organizarea muncii;
- egalitate și diversitate la locul de muncă;
- sănătate și siguranță la locul de muncă,
- protecția proprietății unui angajator sau a unui client;
- exercitarea și beneficierea (în mod individual) de drepturile și beneficiile legate de ocuparea unui loc de muncă; și

[13] GL 29, *Ghid privind evaluarea impactului asupra protecției datelor (DPIA) și stabilirea dacă prelucrarea este susceptibilă de a genera un „risc ridicat” în sensul Regulamentului 2016/679*, GL 248, 4 aprilie 2017, URL: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137, pagina 18.

- încetarea raporturilor de muncă.

În conformitate cu articolul 88 alineatul (2), orice astfel de norme ar trebui să includă măsuri corespunzătoare și specifice pentru protejarea demnității umane, a intereselor legitime și a drepturilor fundamentale ale persoanei vizate, în special în ceea ce privește:

- transparența prelucrării;
- transferul de date cu caracter personal în cadrul unui grup de întreprinderi sau al unui grup de întreprinderi implicate într-o activitate economică comună; și
- sistemele de monitorizare la locul de muncă.

În prezentul aviz, grupul de lucru a furnizat orientări pentru utilizarea legitimă a noilor tehnologii într-o serie de situații specifice, detaliind măsuri corespunzătoare și specifice pentru garantarea demnității umane, a interesului legitim și a drepturilor fundamentale ale angajaților.

4. Riscuri

Tehnologiile moderne permit angajaților să fie urmăriți în timp, de la un loc de muncă la altul și în locuințele lor prin intermediul a numeroase dispozitive diferite cum ar fi telefoanele inteligente, calculatoarele de birou, tabletele, vehiculele și dispozitivele destinate purtării. În cazul în care nu există limite cu privire la prelucrare, și, în cazul în care aceasta nu este transparentă, există un risc ridicat ca interesul legitim al angajatorilor în îmbunătățirea eficienței și protecția activelor societăților să se transforme într-o acțiune de monitorizare nejustificată și intruzivă.

Tehnologiile care monitorizează comunicațiile pot avea, de asemenea, un efect descurajant asupra drepturilor fundamentale ale angajaților de a organiza și a desfășura întruniri cu lucrătorii și de a comunica în mod confidențial (inclusiv dreptul de a solicita informații). Monitorizarea comunicațiilor și a comportamentului va exercita o presiune asupra comportamentului angajaților de a se conforma pentru a evita depistarea a ceea ce ar putea fi perceput drept anomalii, într-un mod comparabil cu modul în care utilizarea intensivă a TVCI a influențat comportamentul cetățenilor în spații publice. În plus, datorită capacităților unor astfel de tehnologii, este posibil ca angajații să nu știe ce date cu caracter personal sunt prelucrate și în ce scopuri, în același timp fiind posibil, de asemenea, ca aceștia să nu știe nici măcar de existența însăși a tehnologiei de monitorizare.

De asemenea, utilizarea TI de monitorizare diferă de alte instrumente de observare și monitorizare mai vizibile precum TVCI prin faptul că aceasta poate avea loc în mod disimulat. În absența unei politici de monitorizare la locul de muncă ușor de înțeles și ușor accesibilă, este posibil ca angajații să nu știe de existența și consecințele monitorizării care are loc, și, prin urmare, nu pot să își exercite drepturile. Un alt risc apare ca urmare a „colectării excesive” a datelor în astfel de sisteme, de exemplu cele care colectează date de localizare WiFi.

Creșterea volumului de date generate în mediul de lucru, în combinație cu tehnici noi de analiză a datelor și verificări încrucișate, poate genera, de asemenea, riscuri de prelucrare ulterioară incompatibilă. Printre exemplele de prelucrare ulterioară nelegitimă se numără folosirea unor sisteme care sunt instalate în mod legitim pentru protejarea proprietăților

pentru a monitoriza apoi disponibilitatea, performanța și capacitatea angajaților de a fi deschiși cu clienții. Printre altele se numără utilizarea datelor colectate prin sistemul TVCI pentru a monitoriza în mod regulat comportamentul și performanța angajaților sau utilizarea datelor unui sistem de geolocalizare (cum ar fi, de exemplu, urmărirea prin WiFi sau Bluetooth) pentru a verifica în mod constant deplasările și comportamentul unui angajat.

Prin urmare, astfel de acțiuni de urmărire ar putea încălca drepturile angajaților privind viața privată, indiferent dacă monitorizarea are loc în mod sistematic sau ocazional. Riscul nu se limitează la analiza conținutului comunicațiilor. Astfel, analiza metadatelor despre o persoană ar putea permite o monitorizare detaliată și la fel de invazivă din punctul de vedere al vieții private a vieții și a modelelor comportamentale ale unei persoane.

Utilizarea pe scară largă a tehnologiilor de monitorizare ar putea, de asemenea, să limiteze disponibilitatea angajaților, precum și a canalelor prin care aceștia pot să informeze angajatorii cu privire la nereguli sau acțiunile ilegale ale superiorilor lor și/sau ale altor angajați care amenință să dăuneze activității (în special datelor privind clienții) sau locului de muncă. Anonimatul este adesea necesar pentru ca un angajat îngrijorat să ia măsuri și să raporteze astfel de situații. Monitorizarea care încalcă dreptul la viața privată al angajaților poate compromite comunicările necesare către responsabilii potriviți. Într-o astfel de situație, mijloace stabilite pentru denunțătorii interni ar putea deveni ineficace[14].

5. Scenarii

Această secțiune abordează o serie de scenarii de prelucrare a datelor, la locul de muncă, în care noile tehnologii și/sau evoluțiile tehnologiilor existente au sau ar putea avea potențialul de a determina creșterea riscurilor pentru viața privată a angajaților. În toate aceste cazuri, angajatorii ar trebui să aibă în vedere dacă:

- activitatea de prelucrare este necesară și, în caz afirmativ, temeiul juridic valabil;
- prelucrarea propusă a datelor cu caracter personal este echitabilă pentru angajați;
- activitatea de prelucrare este proporțională cu problemele semnalate; și
- activitatea de prelucrare este transparentă.

5.1 Operațiunile de prelucrare în timpul procesului de recrutare

Utilizarea platformelor de comunicare socială de către persoane este larg răspândită, iar posibilitatea de vizualizare publică a profilurilor de utilizator în funcție de setările alese de către titularul de cont este o situație relativ frecventă. Prin urmare, angajatorii ar putea crede că verificarea profilurilor sociale ale unor candidați în perspectivă poate fi justificată în cadrul proceselor lor de recrutare. Acest lucru poate fi valabil și în cazul altor informații publice despre un potențial angajat.

Însă angajatorii nu ar trebui să presupună că, doar datorită faptului că profilul unei persoane de pe platformele de comunicare socială este public, aceștia sunt autorizați să prelucreze

[14] A se vedea, de exemplu, GL 29, *Avizul nr. 1/2006 cu privire la aplicarea normelor UE referitoare la protecția datelor în sistemele interne de denunțare în domeniul contabilității, al controalelor contabile interne, al chestiunilor de audit, al luptei împotriva corupției, precum și al infracțiunilor financiare și bancare*, GL 117, 1 februarie 2006, url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2006/wp117_en.pdf.

respectivele date în scopuri proprii. Este nevoie de un temei juridic pentru o astfel de prelucrare, cum ar fi interesul legitim. În acest context, înainte de verificarea unui profil de pe platformele de comunicare socială, angajatorul trebuie să aibă în vedere dacă profilul candidatului de pe respectivele platforme este legat de un context profesional sau personal, deoarece acest lucru poate fi un element important care indică admisibilitatea juridică a inspecției datelor. În plus, angajatorii sunt autorizate să colecteze și să prelucreze datele cu caracter personal referitoare la candidații la un post doar în măsura în care colectarea acestor date este necesar și relevantă pentru îndeplinirea atribuțiilor postului pentru care aceștia s-au înscris.

Datele colectate în timpul procesului de recrutare ar trebui să fie, în general, șterse de îndată ce devine evident faptul că nu va fi înaintată o ofertă de muncă sau că aceasta nu este acceptată de către persoana în cauză[15]. De asemenea, persoana trebuie să fie corect informată cu privire la orice astfel de prelucrare înainte de a se angaja în procesul de recrutare.

Nu există niciun temei juridic pentru ca un angajator să solicite unui potențial angajat să „devină prieten" cu potențialul angajator, sau să obțină accesul în alte moduri la conținutul profilului acestuia.

Exemplu

La recrutarea unor noi angajați, un angajator verifică profilurile candidaților pe diverse rețele de socializare și include informații de pe aceste rețele (și orice alte informații disponibile pe internet) în procesul de verificare.

Doar dacă este necesar pentru locul de muncă să se verifice pe platformele de comunicare socială informații privind un candidat, de exemplu, pentru a putea evalua riscurile specifice în ceea ce privește candidații la o anumită funcție, iar candidații sunt informați în mod corect (de exemplu, în anunțul pentru postul vacant), angajatorul poate avea un temei juridic în conformitate cu articolul 7 litera (f) pentru a verifica informații publice despre candidați.

[15] A se vedea, de asemenea, Consiliul Europei, *Recomandarea CM/Rec(2015)5 a Comitetului de Miniștri către statele membre privind prelucrarea datelor cu caracter personal în contextul ocupării unui loc de muncă*, punctul 13.2 (1 aprilie 2015, url: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c3f7a). În cazurile în care angajatorul dorește să păstreze datele în vederea unei oportunități de angajare viitoare, persoana vizată ar trebui să fie informată în consecință și să aibă posibilitatea de a se opune prelucrării ulterioare, iar în acest caz datele respective ar trebui să fie șterse (Id.).

5.2 Operațiuni de prelucrare care rezultă din verificarea după angajare

Dat fiind faptul că există profiluri pe platformele de comunicare socială și că au fost dezvoltate noi tehnologii analitice, angajatorii au (sau pot obține) capacitatea tehnică de a verifica permanent angajații, colectând informații referitoare la prietenii, opiniile, convingerile, interesele, obiceiurile, locația, atitudinile și comportamentele acestora și captând așadar date, inclusiv date sensibile, legate de viața privată și de familie a angajatului.

Verificarea după angajare a profilurilor angajaților pe platformele de comunicare socială nu ar trebui să fie generalizată.

Mai mult, angajatorii ar trebui să se abțină de la a solicita unui angajat sau candidat la un post accesul la informații pe care acesta le partajează cu alte persoane prin socializarea în rețea.

Exemplu
Un angajator monitorizează profilurile LinkedIn ale foștilor angajați care sunt implicați pe durata clauzelor de neconcurență. Scopul acestei monitorizări este de a monitoriza conformitatea cu astfel de clauze. Monitorizarea este limitată la acești foști angajați.

În măsura în care angajatorul poate dovedi că o astfel de monitorizare este necesară pentru protejarea intereselor sale legitime, că nu există alte mijloace mai puțin invazive și că foștii angajați au fost informați în mod corespunzător cu privire la amploarea observării regulate a comunicărilor lor publice, angajatorul poate să invoce temeiul juridic al articolului 7 litera (f) din DPD.

În plus, nu ar trebui să li se impună angajaților să utilizeze un profil pe platformele de comunicare socială pus la dispoziție de către angajatorul lor. Chiar și atunci când acest lucru este prevăzut în mod specific în contextul sarcinilor acestora (de exemplu, purtător de cuvânt al unei organizații), aceștia trebuie să își rezerve opțiunea de a-și crea un profil care nu este public, „în afara serviciului”, pe care să îl poată folosi în locul profilului „oficial” asociat angajatorului, iar acest lucru ar trebui specificat în termenii și condițiile contractului de muncă.

5.3 Operațiuni de prelucrare ca urmare a monitorizării utilizării TIC la locul de muncă

În mod tradițional, monitorizarea comunicărilor electronice la locul de muncă (de exemplu, telefonul, navigarea pe internet, poșta electronică, mesageria instantanee, telefonia VOIP etc.) a fost considerată a fi principala amenințare la adresa vieții private ale angajaților. În *Documentul de lucru privind supravegherea comunicațiilor electronice la locul de muncă* din 2001, GL 29 a formulat o serie de concluzii în ceea ce privește monitorizarea poștei electronice și a utilizării internetului. Deși aceste concluzii rămân valabile, este necesar să se țină seama de evoluțiile tehnologice care au permis introducerea unor modalități mai noi, posibil mai invazive și prevalente de monitorizare. Astfel de evoluții includ, printre altele:

- instrumente de prevenire a pierderilor de date (DLP), care monitorizează comunicările emise în scopul depistării unor posibile încălcări ale securității datelor;
- sisteme de tip firewall de generație următoare (NGFW) și de gestionare unificată a amenințărilor (UTM), care pot oferi o varietate de tehnologii de monitorizare, inclusiv inspecția detaliată a pachetelor, interceptarea TLS, filtrarea site-urilor, filtrarea

conținutului, raportarea despre aplicații, informarea despre identitatea utilizatorului și, conform descrierii de mai sus, prevenirea pierderii de date. Astfel de tehnologii pot fi utilizate și individual, în funcție de angajator;

- aplicațiile și măsurile de securitate care implică păstrarea evidenței accesului angajaților la sistemele angajatorului;
- tehnologia eDiscovery, care se referă la orice proces prin care se caută date electronice cu scopul de a fi utilizate drept elemente de probă;
- urmărirea utilizării aplicațiilor și a dispozitivelor prin utilizarea de software disimulat, fie pe desktop, fie în cloud;
- utilizarea la locul de muncă a aplicațiilor de birou furnizate ca serviciu de tip cloud, care permit teoretic păstrarea unei evidențe foarte detaliate a activităților angajaților;
- monitorizarea dispozitivelor personale (de exemplu, calculatoare personale, telefoane mobile, tablete) pe care angajații le utilizează pentru activitatea lor în conformitate cu o politică de utilizare specifică, cum ar fi Bring-Your-Own-Device (BYOD), precum și tehnologia Mobile Device Management (MDM) care permite distribuirea aplicațiilor, a datelor și a setărilor de configurare, precum și codurile de tip patch pentru dispozitivele mobile; și
- utilizarea unor dispozitive portabile (de exemplu, dispozitive pentru sănătate și condiția fizică).

Este posibil ca un angajator să implementeze o soluție de monitorizare de tip integrat („all-in-one”), cum ar fi o serie de pachete de securitate care le permit să monitorizeze toate utilizările TIC la locul de muncă, spre deosebire de simpla monitorizare a poștei electronice și/sau a site-urilor, astfel cum se proceda odată. Concluziile adoptate în cadrul GL 55 ar fi valabile pentru orice sistem care permite efectuarea unei astfel de monitorizări[16].

Exemplu

Un angajator intenționează să utilizeze o aplicație de inspectare TLS pentru a decripta și a verifica traficul securizat cu scopul de a detecta orice acțiune rău-intenționată. De asemenea, aplicația poate să înregistreze și să analizeze întreaga activitate online a unui angajat din rețeaua organizației.

Se recurge din ce în ce mai mult la protocoale de comunicații criptate pentru a proteja fluxurile de date online care implică date cu caracter personal împotriva interceptării. Cu toate acestea, această modalitate poate prezenta, de asemenea, probleme, deoarece criptarea face imposibilă monitorizarea datelor primite și a celor transmise. Echipamentul de inspectare TLS decriptează fluxul de date, analizează conținutul în scopuri de securitate și, ulterior, criptează din nou fluxul.

În acest exemplu, angajatorul se bazează pe interesele legitime, necesitatea de a proteja rețeaua și datele cu caracter personal ale angajaților și ale clienților, care sunt deținute în rețeaua respectivă, împotriva accesului neautorizat sau a scurgerii de date. Însă monitorizarea fiecărei activități online a angajaților constituie o reacție disproporționată și o atingere adusă

[16] A se vedea, de asemenea, *Copland/Regatul Unit*, (2007) 45 EHRR 37, 25 BHRC 216, 2 ALR Int'l 785, [2007] CEDO 253 (url: http://www.bailii.org/eu/cases/ECHR/2007/253.html), în care Curtea a precizat că mesajele electronice trimise de la sediul societății și informațiile obținute ca urmare a monitorizării utilizării internetului ar putea face parte din viața și corespondența privată a angajatului și că acțiunea de colectare și stocare a informațiilor respective fără știrea angajatului ar reprezenta o ingerință în drepturile angajatului, deși Curtea nu a statuat niciodată că o astfel de acțiune de monitorizare nu ar fi necesară niciodată într-o societate democratică.

dreptului la secretul comunicațiilor. Angajatorul ar trebui ca, în primul rând, să investigheze alte mijloace mai puțin invazive de protejare a confidențialității datelor referitoare la clienți și a securității rețelei.

În măsura în care o oarecare interceptare a traficului TLS poate fi calificată ca fiind strict necesară, aparatul trebuie configurat în așa fel încât să prevină păstrarea permanentă a evidenței activității angajaților, de exemplu prin blocarea traficului suspect care intră sau care iese și redirecționarea utilizatorului spre un portal de informare unde i se poate solicita acestuia să modifice o astfel de decizie automatizată. În cazul în care păstrarea unei evidențe generale ar fi totuși considerată ca fiind strict necesară, aparatul poate fi configurat, de asemenea, să nu stocheze datele înregistrate decât dacă aparatul semnalează apariția unui incident, cu reducerea la minimum a informațiilor colectate.

Ca exemplu de bună practică, angajatorul ar putea să ofere angajaților un mod de acces alternativ nemonitorizat. Acest lucru ar putea fi realizat prin oferirea de WiFi gratuit sau de dispozitive sau terminale autonome (cu garanții adecvate pentru asigurarea confidențialității comunicațiilor), prin care angajații își pot exercita dreptul legitim de a utiliza în interes personal locul de muncă[17]. Mai mult, angajatorii ar trebui să ia în considerare anumite tipuri de trafic a căror interceptare pune în pericol echilibrul adecvat dintre interesele lor legitime și viața privată a angajatului, cum ar fi utilizarea interfeței web pentru poșta electronică, vizitele online pe site-urile de servicii bancare online și sănătate, pentru a configura în mod adecvat aparatul astfel încât să nu se intercepteze comunicații în condiții care nu sunt conforme cu principiul proporționalității. Angajaților ar trebui să li se prezinte informații cu privire la tipul de comunicații pe care le monitorizează aparatul.

Ar trebui să se elaboreze o politică privind scopurile, momentul și persoanele care pot avea acces la datele suspecte din evidență, care să fie ușor și permanent accesibilă tuturor angajaților, de asemenea, pentru a-i îndruma pe aceștia cu privire la utilizarea acceptabilă și inacceptabilă a rețelei și a echipamentelor. Aceasta permite angajaților să își adapteze comportamentul pentru a evita monitorizarea atunci când utilizează în mod legitim echipamentele informatice de lucru pentru uz personal. Ca și exemplu de bună practică, o astfel de politică ar trebui să fie evaluată cel puțin o dată pe an pentru a analiza dacă soluția de monitorizare aleasă asigură rezultatele prevăzute și dacă există alte instrumente sau mijloace mai puțin invazive disponibile pentru a îndeplini același scop.

Indiferent de tehnologia vizată sau de capacitățile pe care le deține, temeiul juridic al articolului 7 litera (f) este disponibil doar dacă prelucrarea îndeplinește anumite condiții. În primul rând, angajatorii care utilizează aceste produse și aplicații trebuie să țină cont de proporționalitatea măsurilor pe care le pun în aplicare, și de problema dacă se pot lua măsuri suplimentare pentru a atenua sau a reduce amploarea și impactul prelucrării datelor. Ca și exemplu de bună practică, această analiză ar putea fi efectuată prin intermediul unei evaluări DPIA înainte de introducerea unor tehnologii de monitorizare. În al doilea rând, angajatorii trebuie să pună în aplicare și să comunice politici acceptabile de utilizare, pe lângă politici

[17] A se vedea, *Halford/Regatul Unit*, [1997] CEDO 32, (url: http://www.bailii.org/eu/cases/ECHR/1997/32.html), în care Curtea statuează că „apelurile telefonice efectuate din sediul societății, precum și de la domiciliu, pot fi acoperite de noțiunile de „viață privată" și „corespondență" în sensul articolului 8 alineatul 1 [din convenție]"; și *Barbulescu/România*, [2016] CEDO 61, (url: http://www.bailii.org/eu/cases/ECHR/2016/61.html), cu privire la utilizarea unui cont de mesagerie instantanee profesională pentru corespondență cu caracter personal, în care Curtea a afirmat că monitorizarea contului de către angajator a fost limitată și proporțională; opinia contrară a judecătorului Pinto de Alberquerque, care a susținut că trebuie să se asigure un echilibru atent.

privind viața privată, evidențiind condițiile de utilizare admisă a rețelei și echipamentelor organizației și prezentând în detaliu în mod strict procesul de desfășurare a acțiunii de prelucrare.

În unele țări, elaborarea unei astfel de politici ar presupune în mod legal aprobarea din partea unui consiliu al lucrătorilor sau a unei autorități similare care reprezintă angajații. În practică, astfel de politici sunt adesea redactate de către personalul de întreținere TI. Întrucât va fi vizată, în principal, securitatea, nu așteptarea legitimă de respectare a vieții private a angajaților, GL 29 recomandă ca, în toate cazurile, să fie implicat un eșantion reprezentativ de angajați în evaluarea necesității de monitorizare, precum și a logicii și a accesibilității politicii.

Exemplu

Un angajator utilizează un instrument de prevenire a pierderilor de date pentru a monitoriza în mod automat mesajele din poșta electronică trimise, cu scopul de a preveni transmiterea neautorizată a datelor care fac obiectul unui drept de proprietate (de exemplu, datele cu caracter personal ale clientului), indiferent dacă o astfel de acțiune este neintenționată sau nu. Dacă se consideră că un mesaj din poșta electronică este o posibilă sursă a unei încălcări a securității datelor, se efectuează investigații suplimentare.

Repetăm, angajatorul invocă necesitatea pentru interesul său legitim de a proteja datele cu caracter personal ale clienților și activele sale împotriva accesului neautorizat sau a scurgerii de date. Însă un astfel de instrument DLP poate implica prelucrarea inutilă a datelor cu caracter personal – de exemplu, o alertă „fals pozitivă” ar putea determina accesul neautorizat la mesaje legitime din poșta electronică, trimise de către angajați (care ar putea fi, de exemplu, mesaje personale din poșta electronică).

Prin urmare, necesitatea instrumentului DLP și utilizarea acestuia sa ar trebui să fie justificate pe deplin pentru a se obține echilibrul corect între interesele sale legitime și dreptul fundamental la protecția datelor cu caracter personal ale angajaților. Pentru a se invoca interesele legitime ale angajatorului, ar trebui să fie luate anumite măsuri în vederea atenuării riscurilor. De exemplu, regulile pe care le aplică sistemul pentru a caracteriza un mesaj electronic drept o posibilă încălcare a securității datelor ar trebui să fie pe deplin transparente pentru utilizatori și, în cazurile în care instrumentul recunoaște un mesaj din poșta electronică ce urmează să fie trimis ca o posibilă încălcare a securității datelor, ar trebui să existe un mesaj de avertizare care să informeze expeditorul mesajului din poșta electronică înainte de transmiterea acestuia pentru a se oferi expeditorului opțiunea de a anula această transmitere.

În unele cazuri, este posibilă monitorizarea angajaților nu atât din cauza faptului că se utilizează anumite tehnologii, ci pur și simplu pentru că se așteaptă din partea angajaților să utilizeze aplicații online puse la dispoziție de către angajatorul care prelucrează date cu caracter personal. Utilizarea aplicațiilor de birou bazate pe tehnologia de tip cloud (de exemplu, programe de editare a documentelor, calendare, socializare în rețea) este un exemplu în acest sens. Ar trebui să se asigure faptul că angajații pot desemna anumite spații private la care angajatorul nu poate avea acces decât în situații excepționale. Acest lucru este relevant, de exemplu, în cazul calendarelor, care sunt deseori utilizate și pentru întâlniri personale. În cazul în care angajatul încadrează o întâlnire în categoria „Personale” sau

notează acest lucru în conținutul întâlnirii, angajatorii (și alți angajați) nu ar trebui să aibă permisiunea de a examina conținutul întâlnirii.

Cerința subsidiarității, în acest context, înseamnă uneori că nu poate avea loc nicio acțiune de monitorizare. De exemplu, acest lucru este valabil atunci când utilizarea interzisă a serviciilor de comunicații poate fi evitată prin blocarea anumitor site-uri. Dacă este posibilă blocarea site-urilor, în locul monitorizării permanente a tuturor comunicațiilor, ar trebui să se aleagă blocarea pentru a asigura conformitatea cu această cerință a subsidiarității.

La un nivel mai general, ar trebui să se acorde mai multă importanță prevenirii decât detectării, interesele angajatorului fiind mai bine servite dacă se previne utilizarea necorespunzătoare a internetului prin mijloace tehnice, decât dacă se risipesc resurse pentru detectarea utilizării necorespunzătoare.

5.4 Operațiuni de prelucrare ca urmare a monitorizării utilizării TIC în afara locului de muncă

Utilizarea TIC în afara locului de muncă a devenit mai frecventă odată cu creșterea frecvenței muncii la domiciliu, a muncii la distanță și a politicilor de tipul „adu-ți propriul dispozitiv”. Capacitățile unor astfel de tehnologii pot prezenta un risc pentru viața privată a angajaților, întrucât, în multe cazuri, sistemele de monitorizare existente la locul de muncă sunt extinse în mod eficace pentru a intra în mediul domestic al angajaților atunci când utilizează astfel de echipamente. .

5.4.1 *MONITORIZAREA MUNCII LA DOMICILIU ȘI A MUNCII LA DISTANȚĂ*

A devenit din ce în ce mai frecvent cazul în care angajatorii oferă angajaților posibilitatea de a lucra la distanță, de exemplu, de la domiciliu și/sau atunci când sunt în tranzit. Într-adevăr, acesta este un factor esențial care stă la baza distincției reduse dintre locul de muncă și domiciliu. În general, acest lucru presupune asigurarea de către angajator a unor echipamente sau software TIC pentru angajați, care, odată ce au fost instalate la domiciliul lor/pe dispozitivele proprii, le permit acestora să beneficieze de același nivel de acces la rețeaua, sistemele și resursele angajatorului pe care aceștia l-ar avea dacă ar fi la locul de muncă, în funcție de punerea în aplicare.

În timp ce munca la distanță poate fi o evoluție pozitivă, aceasta prezintă totodată un domeniu de risc suplimentar pentru un angajator. De exemplu, angajații care au acces la distanță la infrastructura angajatorului nu sunt obligați prin măsurile de securitate fizică care pot fi instituite la sediul angajatorului. Mai simplu: fără aplicarea de măsuri tehnice corespunzătoare, crește riscul de acces neautorizat, putând duce la pierderea sau distrugerea informațiilor, inclusiv a datelor cu caracter personal ale angajaților sau clienților, pe care angajatorul le-ar putea deține angajatorul.

Pentru a atenua acest domeniu de risc, angajatorii ar putea crede că există o justificare pentru utilizarea pachetelor de software (fie la locul de muncă, fie în cloud) care dispun, spre exemplu, de capacități de înregistrare a apăsărilor de taste și a mișcărilor mouse-ului, de capturare a ecranului (fie aleatoriu, fie la intervale fixe), de înregistrare a aplicațiilor utilizate (și a perioadei pentru care acestea au fost utilizate) și, pe dispozitive compatibile, care permit filmarea cu camere web și colectarea înregistrărilor acestora. Astfel de tehnologii sunt disponibile pe scară largă, inclusiv de la părți terțe cum ar fi furnizorii de servicii cloud.

Cu toate acestea, prelucrarea implicată în astfel de tehnologii este disproporționată și este foarte puțin probabil ca angajatorul să aibă un temei juridic într-un interes legitim, de exemplu, pentru înregistrarea apăsărilor de taste și a mișcărilor mouse-ului efectuate de către un angajat.

Este esențial ca riscul reprezentat de munca la domiciliu și de munca la distanță să fie abordat în mod proporțional și neexcesiv, indiferent de opțiunea oferită și oricare ar fi tehnologia propusă, în special în cazul în care linia de demarcație dintre utilizarea în scopuri profesionale și în folosul personal este vagă.

5.4.2 *PRINCIPIUL „ADU-ȚI PROPRIUL DISPOZITIV" (BYOD)*

Ca urmare a creșterii popularității, caracteristicilor și capacității dispozitivelor electronice de larg consum, angajatorii se pot confrunta cu cereri din partea angajaților de a utiliza propriile dispozitive la locul de muncă pentru îndeplinirea sarcinilor lor de serviciu. Acest fenomen este cunoscut sub numele de „adu-ți propriul dispozitiv" sau BYOD.

Aplicarea principiului BYOD în mod eficace poate genera o serie de beneficii pentru angajați, inclusiv creșterea satisfacției angajaților la locul de muncă, creșterea generală a moralului, eficientizarea muncii și o mai mare flexibilitate. Cu toate acestea, prin definiție, într-o anumită măsură, utilizarea de către angajat a unui dispozitiv va fi de natură personală, acest lucru fiind mai probabil să se întâmple în anumite momente ale zilei (de exemplu, seara și la sfârșit de săptămână). Prin urmare, există posibilitatea distinctă ca utilizarea de către angajați a propriilor dispozitive să conducă la prelucrarea de către angajatori a informațiilor fără caracter profesional referitoare la respectivii angajați și, eventual, la orice membri ai familiei care utilizează, de asemenea, dispozitivele în cauză.

În contextul ocupării unui loc de muncă, riscurile la adresa vieții private pe care le prezintă BYOD sunt adesea asociate unor tehnologii de monitorizare care colectează identificatori precum adrese MAC sau cazurilor în care un angajator accesează dispozitivul unui angajat cu justificarea că efectuează o scanare de securitate, și anume pentru malware. În ceea ce privește acesta din urmă, există o serie de soluții comerciale care permit scanarea dispozitivelor private, însă prin utilizarea acestora s-ar putea accesa toate datele de pe dispozitivul respectiv și, prin urmare, acestea trebuie să fie gestionate cu atenție. De exemplu, aceste secțiuni de pe un dispozitiv care se presupune că sunt utilizate exclusiv în scopuri personale (de exemplu, dosarul care stochează fotografii făcute cu dispozitivul) nu pot fi, în principiu, accesate.

Monitorizarea locației și a traficului de pe astfel de dispozitive poate fi considerată ca servind un interes legitim de protejare a datele cu caracter personal pentru care angajatorul este responsabil în calitate de operator; însă acest lucru poate fi ilegal în cazul dispozitivului personal al unui angajat în cazul în care o astfel de monitorizare capturează, de asemenea, date referitoare la viața privată și de familie a angajatului. Pentru a preveni monitorizarea informațiilor cu caracter personal, trebuie luate măsuri corespunzătoare pentru a face distincția între utilizarea în scopuri profesionale și utilizarea personală a dispozitivului.

De asemenea, angajatorii ar trebui să aplice metode prin care datele acestora care există pe dispozitiv să fie transferate în condiții de securitate între dispozitivul respectiv și rețeaua lor. Așadar, este posibil ca dispozitivul să fie configurat pentru a depista toate tipurile de trafic printr-o rețea VPN înapoi în rețeaua întreprinderii, astfel încât să se ofere un anumit nivel de securitate; însă în cazul în care este utilizată o astfel de măsură, angajatorul ar trebui să aibă

în vedere, de asemenea, faptul că software-ul instalat în scopuri de monitorizare prezintă un risc asupra vieții private în perioadele de utilizare personală de către angajat. Ar putea fi utilizate dispozitive care oferă măsuri de protecție suplimentare cum ar fi reținerea datelor sub forma „sandboxing" (păstrarea datelor conținute într-o anumită aplicație).

Pe de altă parte, angajatorul trebuie să aibă în vedere, de asemenea, interzicerea utilizării anumitor dispozitive de lucru în scopuri personale dacă nu există nicio modalitate de prevenire a unei astfel de utilizări, de exemplu dacă dispozitivul oferă accesul de la distanță la datele cu caracter personal al căror operator este angajatorul.

5.4.3 *GESTIONAREA DISPOZITIVELOR MOBILE (MDM)*

Gestionarea dispozitivelor mobile permite angajatorilor să localizeze dispozitive de la distanță, să utilizeze anumite configurații și/sau aplicații, precum și să șteargă date, la cerere. Un operator ar putea activa el însuși această funcționalitate sau să utilizeze un terț pentru aceasta. De asemenea, serviciile MDM le permit angajatorilor să înregistreze sau să urmărească dispozitivul în timp real, chiar dacă acesta nu a fost declarat furat.

Ar trebui să fie efectuată o evaluare DPIA înainte de utilizarea oricărei astfel de tehnologii atunci când aceasta este nouă sau nouă pentru operator. În cazul în care rezultatul DPIA este acela că tehnologia MDM este necesară în anumite situații, ar trebui să fie efectuată totuși o evaluare cu privire la problema dacă prelucrarea datelor care rezultă este conformă cu principiile proporționalității și subsidiarității. Angajatorii trebuie să se asigure că datele colectate în cadrul acestei capacități de localizare la distanță sunt prelucrate pentru un anumit scop și nu fac, și nu ar putea face, parte dintr-un program mai amplu care permite monitorizarea continuă a angajaților. Chiar și în scopuri specifice, caracteristicile de urmărire ar trebui să fie atenuate. Ar putea fi concepute sisteme de urmărire pentru a înregistra datele de localizare fără a le prezenta angajatorului, iar în astfel de situații, datele de localizare ar trebui să devină disponibile doar în cazurile în care dispozitivul ar fi declarat pierdut sau pierdut.

Angajații ale căror dispozitive sunt înscrise în servicii MDM trebuie să fie, de asemenea, pe deplin informați cu privire la urmărirea care are loc și la consecințele acesteia pentru aceștia.

5.4.4 *DISPOZITIVE PORTABILE*

Angajatorii sunt din ce în ce mai tentați să ofere angajaților lor dispozitive portabile pentru a urmări și a monitoriza starea lor de sănătate și activitatea acestora la locul de muncă și uneori în afara acestuia. Însă acest tip de prelucrare a datelor presupune prelucrarea datelor privind sănătatea și, prin urmare, este interzisă în temeiul articolului 8 din DPD.

Având în vedere raporturile inegale dintre angajatori și angajați, și anume faptul că angajatul depinde financiar de angajator, și caracterul sensibil al datelor privind sănătatea, este foarte puțin probabil să se poată acorda consimțământul valabil din punct de vedere legal pentru urmărirea sau monitorizarea unor astfel de date, întrucât angajații nu sunt practic „liberi" să dea un astfel de consimțământ de la bun început. Chiar dacă angajatorul utilizează un terț pentru a colecta date privind sănătatea, care să ofere angajatorului doar informații agregate cu privire la evoluția generală a sănătății, prelucrarea ar fi ilicită.

De asemenea, astfel cum este descris în *Avizul nr. 5/2014 privind tehnicile de anonimizare*[18], din punct de vedere tehnic este foarte dificil să se asigure anonimizarea completă a datelor. Chiar și într-un mediu cu peste o mie de angajați, având în vedere disponibilitatea altor date despre angajați, angajatorul ar putea totuși să identifice individual angajații cu anumite indicații privind sănătatea, cum ar fi hipertensiunea arterială sau obezitatea.

Exemplu:

O organizație oferă angajaților săi dispozitive de monitorizare a condiției fizice drept cadou cu titlu general. Dispozitivele contorizează numărul de pași făcuți de către angajați și înregistrează bătăile inimii acestora, precum și tiparele de somn în timp.

Datele rezultante privind sănătatea ar trebui să fie accesibile doar angajatului, nu și angajatorului. Orice date transferate între angajat (în calitate de persoană vizată) și dispozitiv/prestatorul de servicii (operator) reprezintă o chestiune care ține de părțile respective.

Întrucât datele privind sănătatea ar putea să fie prelucrate și de către partea comercială care a realizat dispozitivele sau care oferă un serviciu angajatorilor, atunci când alege dispozitivul sau serviciul angajatorul ar trebui să evalueze politica producătorului și/sau a prestatorului de servicii cu privire la viața privată pentru a se asigura că aceasta nu conduce la prelucrarea ilegală a datelor privind sănătatea angajaților.

5.5 Operațiunile de prelucrare legate de timp și de prezență

Sistemele care permit angajatorilor să controleze cine poate intra în sediile lor și/sau în anumite zone din sediile lor pot permite, de asemenea, urmărirea activităților angajaților. Deși astfel de sisteme există de mai mulți ani, noile tehnologii destinate monitorizării timpului și prezenței angajaților sunt utilizate din ce în ce mai mult, inclusiv cele care prelucrează date biometrice, și altele precum cele de urmărire a dispozitivelor mobile.

Chiar dacă astfel de sisteme pot constitui o componentă importantă a pistei de audit a unui angajator, ele prezintă totodată riscul de a asigura un nivel invaziv de cunoștințe și de control în ceea ce privește activitățile angajatului atunci când se află la locul de muncă.

Exemplu:

Un angajator păstrează o sală a serverelor, unde sunt stocate în format digital datele comerciale sensibile, datele cu caracter personal ale angajaților și datele cu caracter personal ale clienților. Pentru a respecta obligațiile legale de securizare a datelor împotriva accesului neautorizat, angajatorul a instalat un sistem de control al accesului care înregistrează intrarea și ieșirea angajaților care au permis corespunzător pentru a intra în sală. În cazul în care dispare un echipament sau dacă există date accesate neautorizat, pierdute sau furate, evidențele păstrate de către angajator îi permite acestuia să stabilească cine a avut acces la sală la momentul respectiv.

[18] GL 29, *Avizul nr. 5/2014 privind tehnicile de anonimizare*, GL 216, 10 aprilie 2014, url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

Dat fiind faptul că prelucrarea este necesară și că nu depășește importanța dreptului la viața privată a angajaților, aceasta poate fi realizată în interesul legitim în temeiul articolului 7 litera (f) în cazul în care angajații au fost informați în mod adecvat cu privire la operațiunea de prelucrare. Cu toate acestea, monitorizarea continuă a frecvenței și a momentelor exacte de intrare și ieșire a angajaților nu poate fi justificată dacă aceste date sunt utilizate și în alte scopuri, cum ar fi evaluarea performanței angajaților.

5.6 Operațiuni de prelucrare în care se utilizează sisteme de monitorizare video

Monitorizarea și supravegherea video continuă să prezinte probleme similare pentru viața privată a angajatului, la fel ca înainte: capacitatea de a înregistra în permanență comportamentul lucrătorului[19]. Cele mai relevante schimbări legate de aplicarea acestei tehnologii în contextul ocupării unui loc de muncă sunt capacitatea de a accesa cu ușurință datele colectate de la distanță (de exemplu, prin intermediul unui smartphone); reducerea dimensiunilor camerelor (împreună cu o creștere a capacităților lor, de exemplu calitatea de înaltă definiție); și prelucrarea care pot fi efectuată prin sisteme noi de analiză video.

Prin capacitățile conferite de sistemele de analiză video, un angajator poate să monitorizeze expresiile faciale ale lucrătorului prin mijloace automate, să identifice abaterile de la tiparele de mișcare predefinite (de exemplu, în contextul unei fabrici) și mai multe. Acest lucru ar fi disproporționat în raport cu drepturile și libertățile fundamentale ale angajaților și, prin urmare, în general ilegal. De asemenea, este probabil ca prelucrarea să implice crearea de profiluri și, eventual, luarea unor decizii automatizate. Prin urmare, angajatorii trebuie să se abțină de la utilizarea tehnologiilor de recunoaștere facială. Pot exista unele excepții marginale de la această regulă, însă astfel de scenarii nu pot fi folosite pentru a invoca o legitimare generală a utilizării acestor tehnologii[20].

5.7 Operațiuni de prelucrare care implică vehicule utilizate de către angajați

Se adoptă pe o scară din ce în ce mai largă tehnologii care permit angajatorilor să își monitorizeze vehiculele, în special în rândul organizațiilor ale căror activități implică transportul sau care dețin parcuri de vehicule semnificative.

Orice angajator care utilizează telematica vehiculelor va colecta date atât despre vehicul, cât și despre fiecare angajat care utilizează vehiculul respectiv. Aceste date pot include nu doar date despre localizarea vehiculului (și, prin urmare, a angajatului), care sunt colectate de sistemele de urmărire prin GPS, ci, în funcție de tehnologie, o multitudine de alte informații, inclusiv comportamentul la volan. Anumite tehnologii pot permite, de asemenea, monitorizarea permanentă atât a vehiculului, cât și a conducătorului auto (de exemplu, înregistratorul de date despre evenimente).

Un angajator ar putea fi obligat să instaleze o tehnologie de urmărire la bordul vehiculelor pentru a demonstra conformitatea cu alte obligații legale, de exemplu, pentru a asigura siguranța angajaților care conduc aceste vehicule. De asemenea, angajatorul poate avea un interes legitim pentru a putea localiza vehiculele în orice moment. Chiar dacă angajatorii ar

[19] A se vedea mai sus trimiterea la cauza *Köpke/Germania*; în plus, ar trebui remarcat, de asemenea, că, în unele jurisdicții, instalarea de sisteme precum TVCI cu scopul de a dovedi un comportament ilegal a fost declarată admisibilă; a se vedea cauza *Bershka* la Curtea Constituțională a Spaniei.

[20] În plus, în temeiul RGPD, prelucrarea datelor biometrice în scopuri de identificare ar trebui să fie bazată pe o excepție prevăzută la articolul 9 alineatul (2).

avea un interes legitim pentru a atinge aceste obiective, ar trebui ca mai întâi să se evalueze dacă prelucrarea în aceste scopuri este necesară și dacă aplicarea efectivă respectă principiile proporționalității și subsidiarității. În cazul în care se permite utilizarea în scopuri personale a unui vehicul de serviciu, cea mai importantă măsură pe care o poate lua un angajator pentru a asigura respectarea acestor principii este să ofere o clauză de neparticipare: angajatul ar trebui să aibă, în principiu, opțiunea de a dezactiva temporar funcția de urmărire a locației în cazul în care există circumstanțe speciale care justifică acest lucru, cum ar fi o vizită la un medic. Astfel, angajatul își poate proteja, din proprie inițiativă, anumite date de localizare ca fiind date cu caracter personal. Angajatorul trebuie să se asigure că datele colectate nu sunt utilizate pentru o prelucrare ulterioară nelegitimă, cum ar fi urmărirea și evaluarea angajaților.

De asemenea, angajatorul trebuie să informeze în mod clar angajații cu privire la faptul că, într-un vehicul al societății pe care aceștia îl conduc, a fost instalat un dispozitiv de monitorizare și că deplasările acestora sunt înregistrate pe toată durata utilizării vehiculului respectiv (și că, în funcție de tehnologia utilizată, este posibil ca și comportamentul lor la volan să fie înregistrat). De preferință, astfel de informații ar trebui să fie afișate în mod vizibil în fiecare mașină, la vederea conducătorului auto.

Este posibil ca angajații să utilizeze vehiculele societății în afara orelor de program, de exemplu, în folosul personal, în funcție de politicile specifice care guvernează utilizarea acestor vehicule. Având în vedere gradul de sensibilitate a datelor de localizare, este puțin probabil să existe un temei juridic pentru monitorizarea locațiilor vehiculelor angajaților în afara orelor de program convenite. Cu toate acestea, în cazul în care există o astfel de necesitate, ar trebui să se aibă în vedere o aplicare proporțională cu riscurile. De exemplu, acest lucru ar putea însemna că, pentru a preveni furtul de mașini, locația vehiculului nu este înregistrată în afara orelor de program, cu excepția cazului în care vehiculul părăsește o arie larg definită (o regiune sau chiar țara). În plus, locația ar fi indicată doar în mod excepțional, angajatorul activând doar „vizibilitatea" locației, având acces la datele deja stocate în sistem, atunci când vehiculul părăsește o regiune prestabilită.

Astfel cum se menționează în *Avizul nr. 13/2011 privind serviciile de geolocalizare pe dispozitivele mobile inteligente*[21] al GL 29:

> „Dispozitivele de urmărire a vehiculelor nu sunt dispozitive care urmăresc angajații. Funcția acestora este de a urmări sau a monitoriza locația vehiculelor în care acestea sunt instalate. Angajatorii nu ar trebui să le considere pe acestea drept dispozitive pentru urmărirea sau monitorizarea comportamentului sau a locației în care se află conducătorii auto sau alți angajați, de exemplu, prin trimiterea de alerte în ceea ce privește viteza vehiculului."

În plus, astfel cum se menționează în *Avizul nr. 5/2005 privind utilizarea datelor de localizare în vederea furnizării de servicii cu valoare adăugată*[22] al GL 29:

[21] GL 29, *Avizul nr. 13/2011 privind serviciile de geolocalizare pe dispozitivele mobile inteligente*, GL 185, 16 mai 2011, url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp185_en.pdf

[22] GL 29, *Avizul nr. 5/2005 privind utilizarea datelor de localizare în vederea furnizării de servicii cu valoare adăugată,* GL 115, 25 noiembrie 2005, url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2005/wp115_en.pdf

„Prelucrarea datelor de localizare poate fi justificată în cazul în care aceasta este efectuată în cadrul monitorizării transportului de persoane sau de bunuri sau al procesului de îmbunătățire a distribuției de resurse pentru servicii în locațiile disparate (de exemplu, planificarea unor operațiuni în timp real), sau în cazul în care se urmărește un obiectiv de securitate în legătură cu angajatul însuși sau cu mărfurile sau vehiculele aflate în răspunderea sa. Pe de altă parte, Grupul de lucru consideră că prelucrarea datelor este excesivă în cazul în care angajații sunt liberi să își organizeze detaliile de călătorie după cum doresc sau în cazul în care aceasta este efectuată în scopul exclusiv de a monitoriza activitatea unui angajat atunci când aceasta poate fi monitorizată prin alte mijloace."

5.7.1 ÎNREGISTRATOARE DE DATE DESPRE EVENIMENTE

Înregistratoarele de date despre evenimente oferă unui angajator capacitatea tehnică de a prelucra o cantitate semnificativă de date cu caracter personal cu privire la angajații care conduc vehiculele societății. Astfel de dispozitive sunt din ce în ce mai des instalate în vehicule cu scopul de a înregistra date în format video și, posibil, audio în caz de accident. Aceste sisteme pot să înregistreze în anumite momente, de exemplu, în urma frânării bruște, a unor schimbări bruște de direcție sau a accidentelor, în aceste cazuri fiind stocate momentele care precedă imediat incidentul, însă acestea pot fi programate, de asemenea, să monitorizeze în continuu. Aceste informații pot fi utilizate ulterior pentru a observa și a analiza comportamentul la volan al unei persoane, cu scopul de a-l îmbunătăți. Mai mult, multe dintre aceste sisteme includ GPS pentru a urmări locația vehiculului în timp real, putându-se stoca și alte detalii legate de condus (cum ar fi viteza vehiculului) în vederea prelucrării ulterioare.

Aceste dispozitive au devenit deosebit de răspândite în rândul organizațiilor ale căror activități implică transportul sau care dețin parcuri de vehicule semnificative. Cu toate acestea, utilizarea înregistratoarelor de date despre evenimente poate fi legală doar dacă există o necesitate de a prelucra datele cu caracter personal obținute cu privire la angajat într-un scop legitim și dacă prelucrarea respectă principiile proporționalității și subsidiarității.

Exemplu

O companie de transport își dotează toate vehiculele cu o cameră video în interiorul cabinei, care efectuează înregistrări audio și video. Scopul prelucrării acestor date este de a îmbunătăți competențele de conducere ale angajaților. Camerele sunt configurate pentru a păstra înregistrările ori de câte ori se produc incidente cum ar fi frânarea bruscă sau schimbările bruște de direcție. Compania pretinde că are un temei juridic pentru prelucrare în interesul său legitim, în temeiul articolului 7 litera (f) din directivă, de a proteja siguranța angajaților săi și a altor conducători auto.

Însă interesul legitim al societății de a monitoriza conducătorii auto nu prevalează asupra drepturilor respectivilor conducători auto la protecția datelor lor cu caracter personal. Monitorizarea continuă a angajaților cu astfel de camere constituie o atingere gravă adusă dreptului lor la viață privată. Există și alte metode (de exemplu, instalarea de echipamente care împiedică utilizarea de telefoane mobile), precum și alte sisteme de siguranță, cum ar fi un sistem avansat de frânare de urgență sau un sistem de avertizare la trecerea involuntară peste liniile de separare a benzilor de circulație, care pot fi utilizate pentru prevenirea accidentelor rutiere și care pot fi mai adecvate. În plus, în cazul unui astfel de material video este foarte probabil să se ajungă la prelucrarea datelor cu caracter personal ale unor terți (cum

ar fi pietoni) și, pentru o astfel de prelucrare, interesul legitim al societății nu este suficient pentru a justifica prelucrarea.

5.8 Operațiuni de prelucrare care implică divulgarea de date privind angajații către terți

A devenit din ce în ce mai răspândită practica societăților de a transmite datele angajaților lor clienților lor în scopul de a asigura o furnizare fiabilă a serviciilor. Aceste date pot fi destul de excesive, în funcție de domeniul de aplicare al serviciilor prestate (de exemplu, ar putea fi inclusă fotografia unui angajat). Însă, având în vedere dezechilibrul de putere, angajații nu sunt în măsură să își dea consimțământul liber la prelucrarea datelor sale cu caracter personal de către angajatorul lor, iar dacă prelucrarea datelor nu este proporțională, angajatorul nu are un temei juridic.

Exemplu:

O societate de livrări trimite clienților săi un mesaj electronic printr-un link către numele și locația furnizorului (angajatului). De asemenea, societatea a intenționat să furnizeze o fotografie de tip pașaport a furnizorului. Societatea a presupus că are un temei juridic pentru prelucrare în interesele sale legitime [articolul 7 litera (f) din directivă], permițând clientului să verifice dacă furnizorul este, într-adevăr, persoana corectă.

Însă nu este necesar să se ofere clienților numele și fotografia furnizorului. Întrucât nu există niciun alt motiv legitim pentru această prelucrare, societății de livrări nu i se permite să ofere clienților aceste date cu caracter personal.

5.9 Operațiuni de prelucrare care implică transferuri internaționale de date privind resursele umane și alte date despre angajați

Angajatorii utilizează din ce în ce mai mult de aplicații și servicii bazate pe tehnologia de tip cloud, cum ar fi cele concepute pentru gestionarea datelor despre resurse umane, precum și aplicații de birou online. Utilizarea celor mai multe dintre aceste aplicații va conduce la transferul internațional de date de la și referitoare la angajați. Astfel cum s-a subliniat anterior în Avizul nr. 8/2001, articolul 25 din directivă prevede că transferurile de date cu caracter personal într-o țară terță din afara UE pot fi efectuate doar în cazul în care țara respectivă asigură un nivel de protecție adecvat. Indiferent de temei, transferul trebuie să respecte dispozițiile directivei.

Astfel, ar trebui să se asigure respectarea acestor dispoziții privind transferul internațional de date. GL 29 își reafirmă poziția anterioară conform căreia este de preferat să se invoce o protecție adecvată, nu derogările enumerate la articolul 26 din DPD; în cazul în care este invocat consimțământul, acesta trebuie să fie specific, lipsit de ambiguitate și exprimat în mod liber. Însă ar trebui să se asigure, de asemenea, faptul că datele partajate în afara UE/SEE, precum și accesul ulterior al altor entități din cadrul grupului, rămân limitate la minimul necesar pentru scopurile prevăzute.

6. Concluzii și recomandări

6.1 Drepturi fundamentale

Conținutul comunicațiilor de mai sus, precum și datele privind traficul legate de aceste comunicații se bucură de aceleași protecții ale drepturilor fundamentale ca și comunicațiile „analoge”.

Comunicațiile electronice efectuate din incinta sediilor pot fi acoperite de noțiunile de „viață privată” și de„corespondență” în sensul articolului 8 alineatul (1) din Convenția europeană. În temeiul actualei Directive privind protecția datelor, angajatorii pot colecta date numai în scopuri legitime, iar prelucrarea trebuie să aibă loc în condiții adecvate (de exemplu, să fie proporțională și necesară, să fie efectuată pentru un interes real și existent și în mod legal, specificat și transparent) și trebuie să existe un temei juridic pentru prelucrarea datelor cu caracter personal colectate din comunicațiile electronice sau generate prin intermediul acestora.

Faptul că un angajator deține proprietatea asupra mijloacelor electronice nu exclude dreptul angajaților la confidențialitatea comunicațiilor lor, a datelor de localizare aferente și a corespondenței lor. Monitorizarea localizării angajaților prin intermediul dispozitivelor proprii sau al celor puse la dispoziție de către societate ar trebui să fie limitată la cazurile în care acest lucru este strict necesar pentru un scop legitim. Cu siguranță, în cazul în care sunt utilizate dispozitive personale în scopuri profesionale, este important ca angajaților să li se ofere posibilitatea de a-și proteja comunicațiile cu caracter personal de orice monitorizare efectuată în interes de serviciu.

6.2 Consimțământul: interesul legitim

Angajații nu sunt aproape niciodată în măsură să își exprime, să refuze sau să își revoce în mod liber consimțământul, având în vedere dependența care rezultă din relația dintre angajator și angajat. Având în vedere dezechilibrul de puteri, angajații își pot da consimțământul liber numai în situații excepționale, atunci când nu există deloc consecințe legate de acceptarea sau respingerea unei oferte.

Interesul legitim al angajatorilor poate fi uneori invocat ca temei juridic, însă numai dacă prelucrarea este strict necesară într-un scop legitim și aceasta respectă principiile proporționalității și subsidiarității. Înainte de utilizarea oricărui instrument de monitorizare, ar trebui să se efectueze un test al proporționalității pentru a analiza dacă sunt necesare toate datele, dacă această prelucrare are o importanță mai mare decât drepturile generale privind viața privată pe care angajații le dețin, de asemenea, la locul de muncă și ce măsuri trebuie luate pentru a asigura faptul că atingerile aduse dreptului la viața privată și dreptului la confidențialitatea comunicațiilor sunt limitate la minimul necesar.

6.3 Transparență

Ar trebui să se comunice angajaților în mod eficace orice monitorizare care are loc, scopurile și circumstanțele acestei monitorizări, precum și posibilitățile angajaților de a preveni înregistrarea datelor lor prin tehnologiile de monitorizare. Politicile și normele privind monitorizarea legitimă trebuie să fie clare și ușor accesibile. Grupul de lucru recomandă implicarea unui eșantion reprezentativ de angajați în elaborarea și evaluarea acestor norme și

politici, deoarece cea mai mare parte a monitorizării are potențialul de a aduce atingere vieții personale a angajaților.

6.4 Proporționalitate și reducerea la minimum a datelor

Prelucrarea datelor la locul de muncă trebuie să constituie o reacție proporțională la riscurile cu care se confruntă un angajator. De exemplu, poate fi depistată utilizarea greșită a internetului fără a fi necesară analizarea conținutului de pe site. Dacă se poate evita utilizarea greșită (de exemplu, prin utilizarea filtrelor web), angajatorul nu are niciun drept general de monitorizare.

În plus, o interdicție generală aplicată cu privire la comunicarea în interes personal nu este practică, iar asigurarea respectării acesteia poate presupune un nivel de monitorizare care ar putea fi disproporționat. Ar trebui să se acorde mai multă importanță prevenirii decât detectării, interesele angajatorului fiind mai bine servite dacă se previne utilizarea greșită a internetului prin mijloace tehnice, decât dacă se utilizează resurse pentru detectarea utilizării greșite.

Pe cât posibil, ar trebui să se reducă la minimum informațiile înregistrate ca urmare a monitorizării permanente, precum și informațiile prezentate angajatorului. Angajații ar trebui să aibă posibilitatea de a dezactiva temporar funcția de urmărire a localizării, în cazul în care există circumstanțe care justifică acest lucru. Pot fi concepute soluții care, spre exemplu, urmăresc vehicule pentru a înregistra datele privind poziția fără ca acestea să fie prezentate angajatorului.

Angajatorii trebuie să țină cont de principiul reducerii la minimum a datelor atunci când decid să utilizeze tehnologii noi. Informațiile ar trebui să fie stocate pe perioada minimă necesară, cu indicarea perioadei de păstrare. Ori de câte ori există informații care nu mai sunt necesare, acestea ar trebui să fie eliminate.

6.5 Servicii cloud, aplicații online și transferuri internaționale

În cazul în care angajații trebuie să utilizeze aplicații online care prelucrează date cu caracter personal (cum ar fi aplicațiile de birou online), angajatorii ar trebui să aibă în vedere acordarea permisiunii angajaților de a desemna anumite spații private la care angajatorul nu poate avea acces sub nicio formă, cum ar fi o poștă electronică privată sau un dosar de documente.

Utilizarea majorității aplicațiilor în cloud va determina transferul internațional de date privind angajații. Ar trebui să garanteze că transferul datelor cu caracter personal într-o țară terță din afara UE este efectuat numai în cazul în care se asigură un nivel de protecție adecvat și faptul că datele partajate în afara UE/SEE și accesul ulterior al altor entități din cadrul grupului rămân limitate la minimul necesar în scopurile prevăzute.

* * *

Adoptat la Bruxelles, la 8 iunie 2017

Pentru Grupul de lucru,
Președinta
Isabelle FALQUE-PIERROTIN