LIBERTATEA DIGITALĂ A SALARIAŢILOR

CZU: 349.22:004.738.5

Maria PÎSLARUC

Școala doctorală Științe Juridice,
Universitatea de Stat din Moldova

DIGITAL FREEDOM OF EMPLOYEES

The digitalization of processes within companies has seen a significant increase, so that employers can not give up control over the use of the Internet or devices by employees, because this aspect is related to work discipline. The objective of the article is to clarify the concept of digital freedom in the context of labor relations and the legal coverage provided by national and international norms. The analysis of the criteria that legitimize the monitoring of the digital activity of the employees will allow highlighting the limits of exercising the freedom of information and good practices.

Keywords: *employee, employer, digital freedom, private life, workplace, monitoring, internet, information.*

Noțiunea de libertate este definită ca posibilitatea de a acționa după propria voință sau dorință [1]. În cadrul raporturilor juridice de muncă, fără a şterbi din esența conceptului de libertate, posibilitatea salariatului de a acționa după propria voință este configurată de disciplina muncii şi de ierarhia subiecților, specifică relațiilor de muncă.

Libertatea digitală poate fi definită ca acces necenzurat la internet deschis, telefoanele mobile, sau la alte tehnologii informaționale, cu respectarea libertății de exprimare, a accesului la informații, a dreptului la viața privată şi a libertății de întrunire în întreaga lume.

Potrivit Rezoluției nr.38/7 din 17.07.2018 a Consiliului pentru Drepturile Omului al ONU privind promovarea, protecția şi exercitarea drepturilor omului pe internet, statele semnatare au afirmat că aceleaşi drepturi pe care oamenii le au offline trebuie, de asemenea, protejate online, în special libertatea de exprimare, în conformitate cu articolul 19 din Declarația Universală a Drepturilor Omului şi cu Pactul internațional privind drepturile civile şi politice din 1966. Rezoluția în cauză recunoaşte şi reiterează importanța protecției drepturilor omului şi libera circulație a informațiilor în mediul online [2].

Aceeaşi Rezoluție stabileşte că prevederile menționate trebuie să încurajeze întreprinderile comerciale să lucreze pentru a permite soluții tehnice pentru securizarea şi protejarea confidențialității comunicațiilor digitale, care pot include măsuri de criptare şi anonimat.

Recomandarea Comitetului de Miniştri din cadrul Consiliului Europei către statele membre privind prelucrarea datelor cu caracter personal în contextul angajării, adoptată la 1 aprilie 2015, prescrie respectarea demnității umane şi a vieții private în cazul prelucrării datelor cu caracter personal în scopuri de angajare, în special pentru a permite dezvoltarea gratuită a personalității angajatului, precum şi pentru posibilități de relații individuale şi sociale la locul de muncă [3].

Revenind la cadrul național, menționăm că art.9 alin.(2) lit.a), d) din Codul muncii al Republicii Moldova [4] stabileşte că salariatul este obligat să-şi îndeplinească conştiincios obligațiile de muncă prevăzute de contractul individual de muncă şi să respecte disciplina muncii.

Corelativ, angajatorul are dreptul (consacrat de art.10 alin.(1) lit.b) din Codul muncii) să ceară salariaților îndeplinirea obligațiilor de muncă şi manifestarea unei atitudini gospodăreşti față de bunurile acestuia.

Actualmente, în baza normelor generale nominalizate mai sus, angajatorul are prerogativa de a supraveghea şi controla device-urile puse la dispoziția salariaților.

Mai nou, în anul 2020 Codul muncii a fost completat cu Capitolul IX[1] care reglementează munca la distanță, aceasta fiind definită că formă de organizare a muncii în domeniile de activitate, prin care salariatul îşi îndeplineşte atribuțiile specifice ocupației, funcției sau meseriei pe care o deține în alt loc decât cel organizat de angajator, folosind inclusiv mijloace din domeniul tehnologiei informației şi a comunicațiilor.

În corespundere cu art.292[3] alin.(2) din Codul muncii, contractul individual de muncă privind munca la distanță trebuie să conțină, în afara clauzelor prevăzute la art.49, clauze privind: a) condițiile de prestare a muncii la distanță; b) programul în cadrul căruia angajatorul este în drept să verifice activitatea salariatului şi privind modalitatea de realizare a controlului; c) modalitatea de evidență a orelor de muncă prestate de salariatul cu munca la distanță; d) condițiile privind suportarea cheltuielilor aferente activității în regim de muncă la distanță; e) alte condiții convenite de părți.

Astfel, potrivit normei citate, angajatorul trebuie să coordoneze în prealabil cu salariatul un program în cadrul căruia acesta are dreptul să verifice activitatea angajatului şi modalitatea exactă de realizare a controlului.

În această ordine de idei, este de menționat că instrumentele internaționale tot mai pronunțat îndeamnă statele să adopte, să pună în aplicare şi, dacă este necesar, să reformeze reglementările, astfel încât să fie asigurată protecția datelor cu caracter personal şi protecția confidențialității online pentru a preveni, atenua şi remedia colectarea, păstrarea, prelucrarea, utilizarea sau divulgarea de date cu caracter personal pe internet ,care ar putea încălca drepturile omului, arbitrare sau ilegale.

În prezent există diverse modalități prin care angajatorul poate monitoriza digital activitatea salariatului, cum ar fi: monitorizarea internetului, monitorizarea utilizării telefonului de serviciu, monitorizarea GPS, supravegherea video a salariaților, sistemul de control intrare/ieşire.

Controlul traficului internet al salariatului este o modalitate frecventă de monitorizare, care se poate realiza prin:

- interzicerea completă a internetului în cadrul entității;

Deşi internetul constituie o distragere a atenției la locul de muncă, în acelaşi timp acesta este un element esențial pentru majoritatea proceselor de afaceri, majoritatea companiilor moderne fiind bazate pe activități online. Având în vedere dependența atât de considerabilă de internet, interzicerea acestuia în totalitate este o măsură discutabilă şi uneori nejustificată, care depinde de specificul muncii.

- interzicerea accesului la unele pagini web particulare (spre exemplu: facebook, instagram, youtube, odnoklassniki etc.);

Realitatea denotă că există sute de site-uri diferite în care salariatul şi-ar putea petrece timpul. Totuşi, blocând cele mai utilizate rețele de socializare, angajatorul are drept scop să focuseze atenția salariatului asupra sarcinilor de muncă. Concomitent, nu sunt rare cazurile când angajatul poate avea nevoie să utilizeze astfel de site-uri web în scopuri legate de muncă, cum ar fi cazul unei agenții de marketing pentru rețelele de socializare. În acest caz, rețelele de socializare vor fi privite ca parte integrantă din operațiunile de muncă ale salariatului şi nu ca divertisment în timpul orelor de muncă.

În cazul în care salariatul foloseşte computerul personal pentru serviciu, limitarea accesului la anumite site-uri web poate implica restricții mai pronunțate asupra vieții private şi a libertății informaționale a salariatului.

- utilizarea diferitor IT instrumente pentru a monitoriza întreaga activitate digitală a angajaților (keyloggers, video loggers).

În prezent, există diverse instrumente prin intermediul cărora activitatea digitală a salariatului poate fi monitorizată. Cu titlu de exemplu, tehnologiile ,,keyloggers" oferă posibilitatea de a urmări tastele apăsate de un angajat la computer. Video loggers este software care înregistrează sau face capturi de ecran ale ecranului computerului unui angajat în timp ce lucrează. O astfel de monitorizare având caracter intruziv în viața privată a persoanei urmează a fi justificată temeinic de către angajator:

- monitorizarea timpului de utilizare a internetului de către angajați şi/sau accesarea aplicațiilor (metodă folosită de Apple, Verizon);

Monitorizarea timpului de utilizare a internetului permite vizualizarea de către angajator a informației privind site-urile web şi aplicațiile care au fost utilizate de fiecare angajat şi cât timp le-au folosit. Dacă salariatul este plătit pe oră, metoda în cauză permite de a afla dacă cineva trece ore libere ca ore lucrate.

- monitorizarea particulară a anumitor activități (email de serviciu, rețea intranet, soft specializat);

Angajatorul trebuie să monitorizeze doar ceea ce este legat de lucru şi ce a pus la dispoziția salariatului. Totuşi, chiar dacă angajatorul monitorizează strict informațiile ce țin de muncă, salariatul chiar şi în aceste condiții beneficiază de protecția vieții private, iar dacă angajatorul nu respectă unele condiții, această monitorizare poate fi catalogată drept încălcare.

Pe măsură ce locurile de muncă devin din ce în ce mai tehnologizate, devine pertinentă protecția angajaților de riscuri şi prevenirea daunelor ce pot fi cauzate de utilizarea tehnologiilor intruzive.

Există condiții de care ambele părți ale raportului juridic de muncă trebuie să țină cont pentru a-şi valorifica drepturile digitale şi pentru a echilibra asimetria de putere care decurge din utilizarea tehnologiilor informaționale de supraveghere.

În această ordine de idei, orice libertate, inclusiv libertatea digitală a salariaților, este în corelație cu alte drepturi şi libertăți, atât ale angajatorilor, cât şi ale altor salariați, care urmează să respecte un şir de condiții pentru ca o măsură de monitorizare să fie legitimă:

- informarea clară şi prealabilă despre natura monitorizării;

Informarea poate fi comunicată personalului în diverse moduri, în funcție de circumstanțele specifice fiecărei cauze. Curtea Europeană a Drepturilor Omului consideră că măsurile pot fi considerate conforme cu cerințele art.8 din Convenția Europeană pentru Drepturile Omului, dacă informarea este clară în ceea ce priveşte natura monitorizării şi prealabilă punerii în aplicare a acesteia. Dacă angajatorul are un scop legitim bine argumentat, consimțământul salariatului nu va constitui un element esențial, cu condiția ca acesta să fi fost informat în prealabil suficient de clar. Negarea consimțământului nu are caracter absolut. Condiția consimțământului apare dacă ulterior apar alte scopuri decât cele legate nemijlocit de executarea CIM-ului, care nu au fost discutate la negocierea contractului de muncă şi la care salariatul nu se aşteaptă în mod rezonabil (de exemplu, plasarea pozei pe site). În aceste cazuri, consimțământul trebuie solicitat suplimentar. Condiția descrisă este ghidată de principiul transparenței şi previzibilității. Urmează a fi furnizată, după caz, o descriere deosebit de clară şi completă a categoriilor de date cu caracter personal care pot fi colectate de TIC, inclusiv supravegherea video şi posibila lor utilizare [5].

- evaluarea şi stabilirea amplorii monitorizării;

În această privință, trebuie să se facă distincție între monitorizarea fluxului comunicărilor şi cea a conținutului acestora. În plus, trebuie luat în considerare dacă au fost monitorizate toate comunicările sau doar o parte a acestora şi dacă monitorizarea a fost sau nu limitată în timp, precum şi numărul persoanelor care au avut acces la rezultatele acesteia. Acelaşi lucru este valabil şi pentru limitele spațiale ale monitorizării [6].

- existența motivelor legitime pentru monitorizare;

Monitorizarea salariaților şi, în special, monitorizarea conținutului comunicărilor fiind, prin natura sa, o metodă mult mai invazivă, necesită justificări mai serioase (riscuri în privința proprietății angajatorului, alte tipuri de infracțiuni). Spre exemplu, angajatorul poate justifica necesitatea monitorizării prin faptul că acțiunile salariatului ar puteau aduce atingere sistemelor informatice ale întreprinderii şi ar genera eventual răspunderea întreprinderii în cazul unei activități ilicite în spațiul virtual, precum şi pentru a se evita să se dezvăluie secretele comerciale ale acesteia. Totuşi, din considerentele expuse, pentru a nu fi catalogate doar ca indicații teoretice, riscurile în cauză trebuie să fie reale şi proprii domeniului în care salariatul îşi desfăşoară activitatea [7].

- evaluarea oportunității instituirii unui sistem de monitorizare mai puțin intruziv;

În acest sens, este necesar să se aprecieze, în funcție de circumstanțele specifice fiecărei cauze, dacă scopul urmărit de către angajator putea fi atins fără ca acesta să aibă acces direct şi integral la conținutul comunicărilor angajatului [8].

- evaluarea consecințelor monitorizării pentru salariați;

Condiția enunțată impune analiza modului în care angajatorul a utilizat rezultatele măsurii de monitorizare, în special dacă rezultatele respective au fost folosite în vederea atingerii scopului declarat al măsurii [9].

- existența unor garanții suficiente pentru apărarea drepturilor şi intereselor legitime.

Aceste garanții trebuie, în special, să permită împiedicarea accesului angajatorului la conținutul efectiv al comunicărilor în cauză, atunci când angajatul nu a fost informat în prealabil cu privire la o astfel de posibilitate. În acest context, Curtea Europeană a Drepturilor Omului precizează că, pentru a prospera, raporturile de muncă trebuie să se bazeze pe încrederea între persoane [10].

În cele din urmă, salariații a căror activitate digitală a fost monitorizată pot beneficia de o cale de atac în fața unui organ judiciar care are competența de a se pronunța, cel puțin în esență, cu privire la respectarea criteriilor nominalizate mai sus, precum şi asupra legalității măsurilor disputate [11].

În concluzie putem spune că deşi angajatorul are dreptul să stabilească politici de monitorizare sau să restricționeze accesul la unele surse informaționale pentru a limita sustragerea salariaților în timpul programului de lucru, acest fapt nicidecum nu înseamnă anihilarea dreptului persoanei la viață privată în timpul orelor de muncă.

Sarcina cadrului normativ este de a contura nişte limite sau criterii cu privire la cât de intruzive pot fi software-urile de monitorizare a salariaților, deoarece lucrătorii nu sunt doar maşini de productivitate, ci ființe sociale cu dreptul la viața privată de bază, la o viață personală separată de muncă şi la demnitate în viața profesională, inclusiv la un nivel de respect şi încredere din partea angajatorului.

Referințe:

1. Disponibil: https://dexonline.ro/definitie/libertate
2. Rezoluția Consiliului pentru Drepturile Omului al ONU privind promovarea, protecția şi exercitarea drepturilor omului pe internet, nr.38/7 din 17.07.2018.
3. Recomandarea Comitetului de Miniştri din cadrul Consiliului Europei către statele membre privind prelucrarea datelor cu caracter personal în contextul angajării, nr.CM/Rec(2015)5 din 1 aprilie 2015.
4. Codul muncii al Republicii Moldova, nr.154-XV din 28.02.2003. În: *Monitorul Oficial al Republicii Moldova*, 2003, nr.159-162/648.
5. Disponibil:https://www.constcourt.md/libview.php?l=ro&id=1685&idc=179&t=/Rezumate-CEDO/2019/strongLopez-Ribalda-i-altii-v-Spania-MCstrong-Supravegherea-video-ascunsa-de-catre-angajator-a-casierilor-i-a-asistentilor-de-vanzari-din-supermarketuri-Nicio-incalcare/?l=ro&id=1685&idc=179&t=/Rezumate-

CEDO/2019/strongLopez-Ribalda-i-altii-v-Spania-MCstrong-Supravegherea-video-ascunsa-de-catre-angajator-a-casierilor-i-a-asistentilor-de-vanzari-din-supermarketuri-Nicio-incalcare/

6. Case *Ozpinar vs. Turkey* (2018). Disponibil: https://hudoc.echr.coe.int/eng#{%22languageisocode%22:[%22RUM%22],%22appno%22:[%2220999/04%22],%22documentcollectionid2%22:[%22CHAMBER%22],%22itemid%22:[%22001-123481%22]}
7. Case *Centre for Democracy and the Rule of Law vs. Ukraina* (2020). Disponibil: https://hudoc.echr.coe.int/eng#%20
8. Case *Barbulescu vs. Romania* (2016). Disponibil: https://hudoc.echr.coe.int/spa#{%22itemid%22:[%22001-177082%22]}
9. Case *Kopke vs. Germany* (2007). Disponibil: https://hudoc.echr.coe.int/spa#{%22fulltext%22:[%22kopke%22],%22itemid%22:[%22001-101536%22]}
10. Disponibil: https://digitalfreedomfund.org/empowering-workers-through-digital-rights/
11. Disponibil: https://www.worktime.com/12-most-asked-questions-on-us-employee-monitoring-laws#C1