

REGLEMENTĂRI PRIVIND CONFIDENȚIALITATEA ȘI ROLUL ACESTEIA ÎN PROTEJAREA DREPTURILOR ANGAJAȚILOR ÎN ERA DIGITALĂ

PRIVACY REGULATIONS AND THEIR ROLE IN PROTECTING EMPLOYEE RIGHTS IN THE DIGITAL ERA

PÎSLARUC Maria,
Universitatea de Stat din Moldova,
ORCID ID: 0000-0003-1191-1232
masha.pyslaruc@gmail.com

Summary

Maintaining workplace confidentiality is essential for fostering trust and integrity within an organization. This involves safeguarding a broad spectrum of information, such as personal employee data, proprietary business information, and sensitive customer details. An understanding of privacy rights and obligations is crucial for establishing a safe and secure environment for both employees and the organization as a whole. Ultimately, it contributes to a culture of transparency, accountability, and respect, fostering a workplace where everyone can thrive.

Keywords: employee, employer, confidentiality, workplace, data protection, information, integrity, transparency, privacy, protection.

Prin noțiunea de confidențialitate înțelegem o caracteristică aplicabilă informațiilor. A proteja și păstra confidențialitatea informațiilor înseamnă a garanta că ele nu sunt făcute disponibile sau dezvăluite entităților neautorizate, iar entitățile includ atât indivizi, cât și procese. [1]

Istoric, conceptul de confidențialitate are rădăcini încă în discuțiile filozofice, cea mai cunoscută fiind distincția lui Aristotel între două sfere ale vieții: „sfera publică” a polisului, asociată cu viața politică, și „sfera privată” a polisului, asociată cu viața domestică. Filosoful și juristul Norberto Bobbio a afirmat că drepturile fundamentale sunt un produs istoric, generat treptat de lupta pentru noi libertăți împotriva vechilor puteri. [2]

La nivel european, dreptul la viața privată s-a regăsit inițial în Convenția Europeană a Drepturilor Omului din 1950, care prevedea că nu pot exista ingerințe din partea unei autorități publice în exercitarea dreptului la propria libertate individuală, cu excepția ingerințelor legale, precum măsurile necesare pentru securitatea națională, pentru siguranța publică, pentru apărarea ordinii și pentru prevenirea infracțiunilor, pentru protecția sănătății sau a moralității sau pentru apărarea drepturilor și libertăților altora.

Astăzi, confidențialitatea la locul de muncă este un aspect substanțial al menținerii încrederii în cadrul unei entități. Acesta cuprinde o gamă largă de informații, inclusiv, dar fără a se limita la date personale ale angajaților, informații comerciale și detalii sensibile ale clienților. Înțelegerea drepturilor și obligațiilor legate de confidențialitate ajută la crearea unui mediu sigur și securizat atât pentru angajați, cât și pentru organizație în ansamblu. Confidențialitatea este mai mult decât păstrarea secretelor – este vorba despre respectarea vieții private și a demnității fiecărei persoane implicate, de la angajați la clienți.

La nivel național, articolul 28 din Constituția Republicii Moldova, statuează că statul respectă și ocrotește viața intimă, familială și privată, iar alin. (1) al art.30 din legea supremă prevede că statul asigură secretul scrisorilor, al telegramelor, al altor trimiteri poștale, al convorbirilor telefonice și al celorlalte mijloace legale de comunicare, cu posibilitatea derogării de la principiul de bază, când această derogare este necesară în interesele securității naționale, bunăstării economice a țării, ordinii publice și în scopul prevenirii infracțiunilor.

Abordarea reglementării confidențialității în cadrul relațiilor de muncă implică aprofundare în albia legislației specifice raporturilor juridice de muncă. Așadar, din analiza prevederilor art.91 din Codul Muncii al RM, este clar că protecția datelor personale ale salariaților reprezintă un aspect de importanță în cadrul relației de muncă, în special actualmente când practic nu există spațiu în care tehnologiile informaționale nu și-au lăsat amprenta. Prevederile menționate, sunt menite de a asigura respectarea drepturilor și libertăților fundamentale ale salariatului, stabilind un cadru legal robust pentru protecția informațiilor personale ale angajaților în era digitală.

În primul rând, este important de subliniat că prelucrarea datelor personale ale salariaților este permisă doar în scopuri bine definite, cum ar fi îndeplinirea cerințelor legale, acordarea de asistență la angajare și avansarea în serviciu. Aceasta trebuie să se facă în conformitate cu legislația în vigoare și să fie limitată strict la nevoile entității în care lucrează salariatul. În plus, angajatorul are obligația de a respecta confidențialitatea și integritatea datelor personale ale salariaților, precum și de a proteja aceste informații împotriva utilizării ilegale sau a pierderii. Acest lucru implică elaborarea și implementarea unor măsuri de securitate adecvate, care să prevină accesul neautorizat la date și să protejeze informațiile sensibile. De asemenea, este esențial ca angajatorul să respecte drepturile salariaților în ceea ce privește confidențialitatea datelor lor personale. Aceasta înseamnă că informațiile referitoare la convingerile politice și religioase, viața privată și apartenența la diverse organizații nu pot fi obținute sau prelucrate fără acordul scris al salariaților. Un alt aspect important este faptul că salariații trebuie să fie informați cu privire la drepturile lor în ceea ce privește protecția datelor personale și să nu fie obligați sau constrânși să renunțe la aceste drepturi în niciun fel. Acest lucru poate fi realizat prin familiarizarea acestora cu politica de confidențialitate a organizației și prin asigurarea că au acces la informații despre modul în care datele lor personale sunt prelucrate și protejate.

În viziunea unei organizații de leadership [3], informațiile confidențiale la locul de muncă pot fi împărțite în trei categorii:

- informații de afaceri.
- informații de management;
- informații despre angajați.

Informațiile de afaceri includ date de proprietate, adesea numite secrete comerciale, care nu sunt ușor accesibile publicului sau concurenților. Exemplele includ software, planuri financiare și documente strategice. Încălcări ale unor astfel de informații ar putea permite concurenților să reproducă procesele, potențial sporindu-și fluxurile de venituri.

La categoria informațiilor de management se atribuie situații interne manageriale, cum ar fi relațiile cu angajații, acțiunile disciplinare și soluționarea conflictelor. Deși nu este restricționată legal de la divulgare, partajarea unor astfel de date poate genera tensiune și eroda încrederea la locul de muncă.

Confidențialitatea informațiilor despre angajați se referă la datele personale de identificare ale persoanei. Aceasta acoperă elemente precum contractele de muncă, numerele permisului de conducere, etc.. Cadru legal impune atât stocarea în siguranță, cât și eliminarea adecvată a acestor

informații după perioada de păstrare. Încălcarea acestei confidențialități ar putea să nu afecteze direct clienții sau beneficiarii, dar ar putea genera repercusiuni legale din partea angajaților afectați, vătămați de încălcări ale confidențialității.

În esență, angajații au mai puține drepturi la locul de muncă decât în afara locului de muncă, dar protecția confidențialității rămâne a fi valabilă, fapt conturat atât de prevederile legislației citate cât și de jurisprudența Curții Europene pentru Drepturile Omului. După cum s-a desprins din cauza *Bărbulescu vs. România* [4], așteptările salariatului, în lipsa unei politici de confidențialitate, joacă un rol diriguitor la examinarea cazurilor particulare de încălcare a vieții private la locul de muncă. În cele mai multe cazuri, angajatorii pot interveni în spațiul de lucru al unui angajat. Angajații ar putea să nu aibă o așteptare de confidențialitate în privința birourilor, dulapurilor ce aparțin angajatorului, care reprezintă spațiul lor de lucru oferit pentru muncă. În același timp, angajații vor avea o așteptare rezonabilă și întemeiată de confidențialitate în privința lucrurilor lor personale aflate la locul de muncă, iar angajatorul nu va putea verifica geanta fără știrea și acordul salariatului. În virtutea specificului activității companiei, angajatorul ar putea avea o politică de efectuare a verificării bagajelor salariaților la ieșire de pe teritoriu de exemplu, doar cu condiția că angajații vor cunoaște această politică înainte de a începe orice verificare. Important este de menționat că o astfel de măsură va fi adoptată de angajator pentru a-și proteja proprietatea contra unor acțiuni ilicite sau altor scopuri legitime, nu din motivul curiozității.

În spațiul virtual angajatorii au aceleași drepturi de monitorizare a acțiunilor salariaților, atât a fluxului de informații cât și a conținutului acesteia. Un punct de delimitare constituie faptul că angajatul nu doar să fie informat cu privire la posibilitatea generală a monitorizării și interzicerea utilizării resurselor companiei în scopuri personale, dar să fie conștient că o astfel de monitorizare ar putea avea loc în condiții clare, or, cu alte cuvinte salariatul să fie informat cu privire la amploarea și natura activităților de monitorizare ale angajatorului său sau despre posibilitatea ca angajatorul să aibă acces la conținutul real al comunicărilor sale. După cum relevă și jurisprudența Curții Europene pentru Drepturile Omului în contextul art. 8 din Convenție, instrucțiunile angajatorului nu pot reduce viața socială privată la locul de muncă la zero.

Nu în ultimul rând, este important de reținut că consimțământul salariatului nu presupune renunțarea la obligații din partea angajatorului privind confidențialitatea. Cu alte cuvinte, dacă un salariat și-a exprimat consimțământul ca informațiile sale personale să fie prelucrate într-un mod oarecare, entitatea încălcând limitele va fi pasibilă de răspundere juridică.

În cele ce urmează, prezintă interes prevederile art.91 lit.f) din Codul Muncii al RM, care stabilește că la adoptarea unei decizii care afectează interesele salariatului, angajatorul nu este în drept să se bazeze pe datele personale ale salariatului obținute exclusiv în urma prelucrării automatizate sau pe cale electronică. Același principiu îl găsim în norma art.17 al Legii nr.133/2011 privind protecția datelor cu caracter personal, care indică că, orice persoană are dreptul de a cere anularea, în totalitate sau parțială, a oricărei decizii individuale care produce efecte juridice asupra drepturilor și libertăților sale, fiind întemeiată exclusiv pe prelucrarea automatizată a datelor cu caracter personal destinată să evalueze unele aspecte ale personalității sale, precum competența profesională, credibilitatea, comportamentul și altele asemenea.

Din analiza normelor prevederilor indicate mai sus, reiese că angajatorul constatând o abatere a salariatului manifestată prin utilizarea în scopuri vădit neprofesionale ori personale în timpul de muncă a dispozitivelor puse la dispoziția acestuia pentru exercitarea funcției, pe lângă analiza fluxului și/sau conținutului informației trebuie să implice și alt probatoriu obținut nu prin

prelucrarea automatizată a datelor cu caracter personal pentru a putea adopta o decizie individuală în privința salariatului, care în mod cert va produce efecte juridice asupra drepturilor acestuia.

Trebuie de înțeles că angajatorul nu are obligația legală de a permite utilizarea telefonului sau internetul în scopuri personale. Cu toate acestea, o anumită utilizare privată a telefonului sau internetului, atâta timp cât acest lucru nu interferează cu munca, nu poate fi restricționată.

Pentru a respecta cadrul legal, nu este suficientă o informare vagă precum că spațiul virtual poate fi monitorizat, ci trebuie să persiste o înțelegere clară a momentului în care sunt colectate informațiile, motivele colectării, cum vor fi utilizate și cine va avea acces la ele.

La capitolul monitorizării corespondenței angajaților, conform recomandărilor din Ghidul privind datele personale și comunicațiile electronice în instituțiile UE, pentru a minimiza nevoia de a accesa cutiile poștale personale în absența angajaților, Autoritatea Europeană pentru Supravegherea Datelor recomandă măsuri de asigurare în privința e-mail-urilor de serviciu, precum ar fi:

- instruirea angajaților să salveze toate e-mailurile relevante în dosare electronice, cum ar fi în sistemele de gestionare a documentelor sau a cazurilor sau să arhiveze corespondența în dosare pe hârtie;

- introducerea de cutii poștale funcționale pentru anumite unități/servicii/sectoare care sunt accesibile tuturor angajaților relevanți. Destinatarii li se poate cere apoi să copieze toată corespondența legată de afaceri în aceste cutii poștale;

- instruirea angajaților care părăsesc instituția să furnizeze note complete de predare.[5]

În susținerea poziției date vine art. 93 din Codul Muncii al RM, care prevede drepturile specifice ale salariaților atunci când datele lor sunt prelucrate și anume:

- dreptul de a primi informația deplină despre datele sale personale și modul de prelucrare a acestora;

- dreptul de a avea acces liber și gratuit la datele sale personale, inclusiv dreptul la copie de pe orice act juridic care conține datele sale personale, cu excepția cazurilor prevăzute de legislație;

- dreptul de a-și desemna reprezentanții pentru protecția datelor sale personale;

- dreptul de a avea acces la informația cu caracter medical ce-l vizează, inclusiv prin intermediul lucrătorului medical, la alegerea sa;

- dreptul de a cere excluderea sau rectificarea datelor personale incorecte și/sau incomplete, precum și a datelor prelucrate cu încălcarea cerințelor cadrului legal. În cazul în care angajatorul refuză să excludă sau să rectifice datele personale incorecte, salariatul este în drept să notifice în scris angajatorului dezacordul său motivat;

- dreptul de a ataca în instanța de judecată orice acțiuni sau inacțiuni ilegale ale angajatorului admise la obținerea, păstrarea, prelucrarea și protecția datelor personale ale salariatului.

Obligațiile de confidențialitate referitoare la informațiile angajaților se aplică în general nu numai angajaților actuali, ci și potențialilor și foștilor angajați.

Nu putem nega faptul că așteptarea confidențialității poate varia de la un loc de muncă la altul, în funcție de atribuții încredințate. Un completator de mărfuri ar putea avea o așteptare mai „puternică” a confidențialității convorbirilor la telefonul de serviciu în comparație cu un operator a cărui sarcină constă în interacțiunea zilnică cu clienții companiei din numele acesteia.

La capitolul proporționalității măsurilor adoptate de angajator, sunt relevante concluziile Curții Constituționale din Spania pe marginea unui caz examinat în anul 2000, în care a fost aplicat

un test de proporționalitate, iar Curtea spaniolă considerând că dispozitivele de înregistrare video și audio amplasate la casă și pe o masă de joc dintr-un cazinou, au fost o măsură disproporționată, rezultând o interferență majoră cu dreptul angajaților și clienților la respectarea vieții lor private. În acest caz, instanța a reținut că angajatorul nu a demonstrat modul în care înregistrarea sonoră, care era deosebit de intruzivă pentru dreptul la viață privată al celor în cauză, a fost necesară pentru protejarea drepturilor și intereselor sale legitime. [6]

Tot în contextul dat, este relevant art.43 alin. (1) din Codul civil al RM, potrivit căruia în condițiile legii, orice persoană fizică are dreptul la viață, la sănătate, la integritate fizică și psihică, la libera exprimare, la nume, la onoare, demnitate și reputație profesională, la propria imagine, la respectarea vieții intime, familiale și private, la protecția datelor cu caracter personal, la respectarea memoriei și corpului său după deces, precum și la alte asemenea drepturi recunoscute de lege. În sensul art.46 din Codul civil al RM, vor fi considerate ca atingeri aduse vieții private interceptarea fără drept a unei convorbiri private, săvârșită prin orice mijloace tehnice, sau utilizarea, în cunoștință de cauză, a unei asemenea interceptări, ținerea vieții private sub observație, prin orice mijloace, în afară de cazurile prevăzute expres de lege, difuzarea de materiale conținând imagini privind o persoană aflată la tratament în unitățile de asistență medicală, precum și a datelor cu caracter personal privind starea de sănătate, problemele de diagnostic, prognostic, tratament, circumstanțe în legătură cu boala și cu alte diverse fapte, inclusiv rezultatul autopsiei, fără consimțământul persoanei în cauză, iar în cazul în care aceasta este decedată, fără consimțământul familiei sau al persoanelor îndreptățite; difuzarea sau utilizarea corespondenței, manuscriselor ori a altor documente personale, inclusiv a datelor privind domiciliul, reședința temporară, precum și numerele de telefon ale unei persoane sau ale membrilor familiei sale, fără consimțământul persoanei căreia acestea îi aparțin sau care, după caz, are dreptul de a dispune de ele.

Angajatorul în virtutea poziției sale în cadrul raportului juridic de muncă este „depozitarul” unui șir de informații foarte complexe despre salariați, pe care trebuie să o gestioneze în așa mod încât să nu depășească acele limite specifice relației de muncă.

O situație de risc în privința prelucrării legitime a informațiilor personale ar putea servi practica solicitării de la angajatorii naționali a informațiilor privind cuantumul și modul de decontare a veniturilor salariaților de către companiile colectoare de datorii, care au preluat creanța în privința salariatului de la o entitate care a oferit împrumut către acesta (bancă sau organizație de microfinanțare).

Situația dată, reieșind din prevederile normelor legale depășește scopul angajatorului de a prelucra datele cu caracter personal al salariatului, dat fiind faptul că art.91 lit.a) din Codul Muncii al RM, prevede că prelucrarea datelor personale ale salariatului poate fi efectuată exclusiv în scopul îndeplinirii prevederilor legislației în vigoare, acordării de asistență la angajare, instruirii și avansării în serviciu, asigurării securității personale a salariatului, controlului volumului și calității lucrului îndeplinit și asigurării integrității bunurilor unității.

Chiar dacă salariatul a semnat acordul de prelucrare a datelor cu caracter personal în momentul nașterii raportului de împrumut, oferirea ulterioară de către angajator, conform solicitării persoanelor terțe, a informației confidențiale despre salariat va constitui o depășire a limitelor legale. Totuși, dacă părțile au convenit că oferirea informațiilor către terțe persoane este oportună, angajatorul ar trebui să obțină consimțământul expres al angajatului înainte de a utiliza datele personale în scopuri nelegate de muncă și să ofere informații clare despre modul în care aceste date au fost transmise.

Rezumând cele comentate, pot fi profilate câteva aspecte importante legate de confidențialitatea digitală a salariaților:

Existența politicilor interne privind confidențialitatea. Multe organizații au politici specifice care guvernează modul în care datele personale ale angajaților sunt colectate, stocate, procesate și utilizate. Aceste politici trebuie să fie conforme cu reglementările legale relevante naționale, ținând cont inclusiv de Regulamentul General privind Protecția Datelor (GDPR) în Uniunea Europeană.

Accesul la date. Angajatorii ar trebui să aibă politici clare cu privire la cine are acces la datele personale ale angajaților și în ce scopuri. Accesul la aceste date ar trebui să fie limitat strict la personalul autorizat și să fie justificat în funcție de necesitatea de a îndeplini sarcinile de lucru. În acest sens, art.30 alin. (2) și (2¹) din Legea nr.133/2011 privind protecția datelor cu caracter personal, a fost ajustat în 2023, prin completarea reglementării care prevede că în cazul în care prelucrarea datelor cu caracter personal este efectuată pe seama și în numele operatorului, acesta va împuternici o persoană care va asigura respectarea garanțiilor referitoare la măsurile adecvate de securitate tehnică și de organizare privind prelucrarea ce urmează să fie efectuată. Persoana împuternicită de operator nu recrutează o altă persoană împuternicită de operator fără a primi prealabil o autorizație scrisă, specifică sau generală, din partea operatorului. În cazul unei autorizații generale scrise, persoana împuternicită de operator informează operatorul cu privire la toate modificările preconizate privind adăugarea sau înlocuirea altor persoane împuternicite de operator, oferind astfel posibilitatea operatorului de a prezenta obiecții față de modificările respective. Mai mult ca atât, în cazul în care o persoană împuternicită de un operator recrutează o altă persoană împuternicită pentru efectuarea de operațiuni de prelucrare specifică în numele operatorului, aceleași obligații privind protecția datelor cu caracter personal, prevăzute în contractul sau în alt act juridic încheiat între operator și persoana împuternicită de operator, revin și celei de-a doua persoane împuternicite, în temeiul unui contract sau al unui alt act juridic, în special care să furnizeze garanții suficiente pentru punerea în aplicare a unor măsuri tehnice și organizatorice adecvate, astfel încât prelucrarea să îndeplinească cerințele prezentei legi. În cazul în care cea de-a doua persoană împuternicită nu își respectă obligațiile privind protecția datelor cu caracter personal, persoana împuternicită de operator continuă să poarte răspundere deplină față de operator în ceea ce privește îndeplinirea obligațiilor celei de-a doua persoane împuternicite. Norma în cauză a fost inspirată din GDPR care a reglementat numirea unui responsabil de protecția datelor dacă entitatea este o autoritate sau un organism public sau dacă desfășoară anumite tipuri de activități de prelucrare.

Securitatea informațiilor. Protejarea datelor personale ale angajaților împotriva accesului neautorizat sau a utilizării incorecte este esențială. Acest lucru poate implica măsuri precum utilizarea de parole puternice, criptarea datelor sensibile și implementarea altor controale de securitate cibernetică. Potrivit art.30 alin. (1) din Legea nr.133/2011 privind protecția datelor cu caracter personal, la prelucrarea datelor cu caracter personal, operatorul este obligat să ia măsurile organizatorice și tehnice necesare pentru protecția datelor cu caracter personal împotriva distrugerii, modificării, blocării, copierii, răspândirii, precum și împotriva altor acțiuni ilicite, măsuri menite să asigure un nivel de securitate adecvat în ceea ce privește riscurile prezentate de prelucrare și caracterul datelor prelucrate.

Consensul și informarea. Angajatorii ar trebui să solicite consimțământul angajaților înainte de a colecta sau utiliza datele personale în scopuri care nu sunt legate direct de sarcinile de

lucru, oferind informații clare, transparente și suport cu privire la modul în care datele personale sunt prelucrate.

Drepturile angajaților. Angajații au drepturi privind datele lor personale, cum ar fi dreptul de acces la date, dreptul de rectificare a informațiilor inexacte sau incomplete și dreptul de a solicita ștergerea datelor lor în anumite circumstanțe, justificate și permise de cadrul legal. [7]

Restricții de confidențialitate nu se referă doar la angajator ci sunt aplicabile inclusiv pentru a împiedica un angajat (sau o altă persoană care lucrează în cadrul companiei) să folosească informațiile private pe care le colectează în timp ce lucrează, într-un mod care ar putea afecta drepturile subiecților.

Respectarea confidențialității angajaților ajută la crearea unui mediu de lucru în care oamenii se simt confortabil și concentrați. Atunci când angajații sunt încrezători că confidențialitatea lor este respectată, este mai probabil să se concentreze asupra muncii lor fără distragere a atenției sau îngrijorări cu privire la utilizarea greșită a informațiilor lor personale. [8]

Concluzii

În final, este important ca angajatorii, salariații și reprezentanții lor să colaboreze în elaborarea și implementarea măsurilor de protecție a datelor personale ale salariaților. Prin această colaborare, se poate asigura că toți cei implicați în relația de muncă înțeleg și respectă importanța confidențialității datelor personale și contribuie la crearea unui mediu de lucru sigur și de încredere în era digitală. Menținerea confidențialității la locul de muncă necesită o combinație de politici clare, instruire a angajaților și măsuri solide de securitate a informațiilor personale. Prin respectarea drepturilor angajaților și îndeplinirea obligațiilor de a proteja informațiile sensibile, organizațiile pot promova o cultură a încrederii și integrității, păstrându-și în același timp reputația și bunurile.

Indivizii au o dorință paradoxală atât pentru confidențialitate, cât și pentru partajarea conținutului personal online, ceea ce duce la riscuri crescute. Notificarea angajaților cu privire la supraveghere ajută la gestionarea așteptărilor lor cu privire la confidențialitate.

Jurisprudența Curții Europene a Drepturilor Omului conturează tendința de a echilibra drepturile angajatorilor și ale angajaților în contextul confidențialității la locul de muncă. În timp ce angajații au dreptul la confidențialitate, acest drept trebuie să fie echilibrat cu interesele legitime ale angajatorilor, cum ar fi asigurarea productivității, prevenirea abaterilor și protejarea informațiilor sensibile. Angajatorii trebuie să stabilească politici și proceduri clare cu privire la monitorizarea comunicărilor angajaților și să se asigure că orice activități de monitorizare sunt proporționale și limitate în sferă.

Bibliografia și resursele Web

1. <http://dexcert.ro/iso-27001/confidentialitatea.html> [Accesat la 27.04.2024]
2. Di Armando Iadevaia, E Marzia De Luca. Protection of privacy: the right to confidentiality in working relationships, ISSN 2384-9169, Fascicolo n. 3, 2020 rivista.eurojus.it, pag. 87. [Accesat la 27.04.2024]
3. <https://www.kellerexecutivesearch.com/insight/confidentiality-in-the-workplace/> [Accesat la 28.04.2024]
4. <https://globalfreedomofexpression.columbia.edu/cases/case-barbulescu-v-romania/> [Accesat 27.04.2024]

5. Guidelines on personal data and electronic communications in the EU institutions. EDPS. December 2015, pag.14. Link: https://www.edps.europa.eu/sites/default/files/publication/15-12-16_ecommunications_en.pdf [Accesat la 05.04.2024]
6. Di Armando Iadevaia, E Marzia De Luca. Protection of privacy: the right to confidentiality in working relationships, ISSN 2384-9169, Fascicolo n. 3, 2020 rivista.eurojus.it, pag. 103. [Accesat la 27.04.2024]
7. <https://www.goethena.com/post/confidentiality-in-the-workplace/#:~:text=Only%20share%20confidential%20information%20on,about%20using%20and%20disseminating%20it> [Accesat 25.04.2024]
8. <https://harperjames.co.uk/article/how-to-deal-with-an-employee-breach-of-confidentiality/> [Accesat la 25.04.2024]