

Pregatiți-va pentru impactul inteligenței artificiale: de la entuziasm la risc – este compania dumneavoastră pregatită?

**KINSTELLAR**

În anul 2022, vorbeam despre impactul promițator, dar pe atunci încă ipotetic, al inteligenței artificiale generative asupra domeniului resurselor umane – de la recrutare și evaluarea performanței până la deciziile privind promovarea – precum și despre posibilele implicații ale proiectului de Regulament european privind inteligența artificială („*Actul privind Inteligența Artificială*” sau „*AI Act*”).

Astăzi, inteligența artificială generativă nu mai este o ambiție de viitor. Companiile multinaționale integrează rapid instrumente de inteligență artificială în activitățile zilnice: de la crearea de conținut și analiza datelor până la luarea automată a deciziilor. Ceea ce cândva parea o preocupare juridică teoretică a devenit o provocare concretă de conformitate, având în vedere publicarea AI Act în 2024 și aplicarea sa integral preconizată până în august 2026.

Pe măsura ce ne apropiem de 2026, întrebarea reală nu mai este **dacă** trebuie folosită inteligența artificială, ci **dacă oamenii din organizație știu cum să o folosească**. Angajatorii nu mai pot trata IA ca pe un subiect de viitor: ea este deja aici, este puternică și, mai mult ca oricând, este supusă răspunderii.

1. ÎNȚELEGEREA RISCURILOR

Companiile se concentrează tot mai mult pe integrarea celor mai noi instrumente bazate pe inteligența artificială, însă nu este nevoie să fii specialist pentru a ști că implementarea acestor instrumente fără a pregăti corespunzător angajații reprezintă o rețetă pentru dezastru: date partinitoare care pot conduce la discriminare, încălcări ale confidențialității, interpretări eronate ale rezultatelor generate de IA și o dependență excesivă de automatizare.

Aceste riscuri se pot materializa în moduri diferite, în funcție de tipul de instrument IA utilizat.

Dacă organizația utilizează instrumente IA proprii, riscurile se concentrează asupra configurării sistemului, gradului de transparență și nivelului de înțelegere pe care îl au angajații privind utilizarea responsabilă a acestora.

Pe de altă parte, tot mai mulți angajați folosesc instrumente precum **ChatGPT**, **Copilot** sau **Gemini** pentru sarcinile lor zilnice: redactarea de e-mailuri, brainstorming, rezumarea documentelor, generarea de idei sau asistența în scrierea de cod. Utilizarea tot mai frecventă a acestor instrumente aduce cu sine propriile riscuri: date interne sensibile pot fi partajate neintenționat către sisteme terțe, rezultatele pot conține erori factuale sau prejudecăți integrate, iar obligațiile privind drepturile de autor, confidențialitatea sau protecția datelor pot fi încălcate fără intenție.

Indiferent dacă instrumentul este furnizat de companie sau accesat individual, **elementul comun rămâne comportamentul uman**. Fără politici interne clare și o conștientizare adecvată, chiar și cele mai avansate sisteme pot deveni surse de

raspundere juridica, nu de inovație.

2. TRANSFORMAREA RISCURILOR LEGATE DE IA ÎN POLITICI INTERNE

Indiferent de tipul de instrumente IA utilizate de angajați, **o politica interna privind utilizarea inteligenței artificiale nu mai este opțională**. Aceasta reprezintă cel mai eficient mijloc de a asigura alinierea la reglementările în vigoare și de a reduce riscurile operaționale și reputaționale.

O politica interna privind IA ar trebui să:

- Definească utilizările acceptabile ale instrumentelor de IA (atât pentru cele furnizate de companie, cât și pentru cele terțe);
- Stabilească modul și momentele în care este necesară supravegherea umană, în special în deciziile cu impact major;
- Precizeze limite clare privind datele ce pot fi introduse în sistemele IA, în special în ceea ce privește informațiile confidențiale, proprietatea intelectuală și datele cu caracter personal;
- Prevadă canale de escaladare pentru incidente legate de IA;
- Stabilească sancțiuni corespunzătoare pentru încălcarea obligațiilor referitoare la IA;
- Coreleze politica de IA cu obligațiile prevăzute de **AI Act** și de legislația aplicabilă în materie de protecția datelor.

Mai mult decât un simplu document de conformitate, o politica bine concepută oferă angajaților claritate și transparență, protejând în același timp angajatorul împotriva riscurilor juridice, prejudiciilor de imagine și îngrijorărilor părților terțe.

3. INSTRUIREA ANGAJAȚILOR ÎN ERA INTELIGENȚEI ARTIFICIALE

Chiar și cea mai bună politica este eficientă doar în măsura în care persoanele vizate o aplică în mod corect. De aceea, angajatorii trebuie să investească activ în **dezvoltarea competențelor digitale și a alfabetizării în domeniul IA** la toate nivelurile organizației.

Indiferent dacă folosesc instrumente IA puse la dispoziție de companie sau aplicații externe, angajații trebuie să știe **ce tipuri de date pot fi introduse în siguranță, cum să evalueze critic conținutul generat de IA, când este necesară validarea umană și cum să raporteze abaterile sau rezultatele neașteptate**.

Programele de instruire trebuie adaptate în funcție de rolul angajatului, nivelul sau tehnic și contextul de utilizare a instrumentului.

Eforturile de formare nu ar trebui să se limiteze la departamentele IT sau juridice – **conștientizarea privind IA trebuie să devină un element esențial al culturii organizaționale**.

4. CAZUL SPECIAL AL APLICAȚIILOR DE HR BAZATE PE IA

Deși inteligența artificială poate aduce eficiența, **sistemele IA utilizate în luarea deciziilor legate de angajare** (de exemplu, recrutare, evaluarea performanței, decizii de promovare, concediere etc.) necesită o atenție deosebită, întrucât sunt clasificate drept **sisteme cu risc ridicat** potrivit AI Act. Aceste instrumente vor fi permise doar în condiții stricte, ce includ cerințe de documentare, transparență și supraveghere umană.

Sistemele de **recunoaștere a emoțiilor la locul de muncă**, care încearcă să deducă starea mentală sau emoțională a unei persoane pe baza expresiilor faciale sau a tonului vocii, sunt **în mod expres interzise**.

În acest context, profesioniștii din domeniul resurselor umane trebuie să joace un rol central, fiind implicați nu doar în implementarea și utilizarea acestor sisteme, ci și în guvernarea internă privind IA.

5. CE TREBUIE SĂ FACĂ ANGAJATORII ÎNCĂ DE ACUM

Pe măsura ce se apropie momentul aplicării integrale a **AI Act**, organizațiile trebuie să adopte o abordare proactivă:

- €€€€€€€€ sa identifice sistemele IA utilizate în prezent;
- €€€€€€€€ sa le clasifice în funcție de nivelul de risc;
- €€€€€€€€ sa evalueze riscurile juridice și operaționale;
- €€€€€€€€ sa implementeze politici interne adecvate;
- €€€€€€€€ și să investească în programe de instruire adaptate fiecărui rol.

Inteligența artificială transformă fundamental mediul de lucru. Succesul se va măsura prin capacitatea organizațiilor de a înțelege, gestiona și comunica schimbarea – la toate nivelurile. În era IA, fiecare angajat este parte a soluției.