lider.media, 27.3.2026.

Evidencijski broj / Article ID: 26619707
Naslov / Title: Umjetna inteligencija u oglašavanju traži jasna pravila – gdje su granice između inovacije i odgov...
URL: Originalni članak
OTS: 693

lidermedia.hr
27. ožujka 10:03:13

Umjetna inteligencija u oglašavanju traži jasna pravila – gdje su granice između inovacije i odgovornosti

PROMO

> *U okruženju u kojem se AI alati sve brže uvode u svakodnevne poslovne procese, organizacije se istovremeno suočavaju s potrebom za inovacijom i obvezom zaštite osobnih i poslovno osjetljivih informacija*

U okruženju u kojem se AI alati sve brže uvode u svakodnevne poslovne procese, organizacije se istovremeno suočavaju s potrebom za inovacijom i obvezom zaštite osobnih i poslovno osjetljivih informacija

Rastuća primjena **umjetne inteligencije u oglašavanju** otvara niz pitanja vezanih uz zaštitu podataka, regulatornu usklađenost i odgovorno upravljanje tehnologijom. U okruženju u kojem se AI alati sve brže uvode u svakodnevne poslovne procese, organizacije se istovremeno suočavaju s potrebom za inovacijom i obvezom zaštite osobnih i poslovno osjetljivih informacija. Na pitanja o izazovima i odgovornoj primjeni umjetne inteligencije u marketingu, s posebnim naglaskom na zaštitu podataka i regulatornu usklađenost, odgovorili su članovi Radne skupine IAB-a Croatia za privatnost i zaštitu podataka: **Mario Frančešević** (SeekandHit), **Marko Jambrešić** (dentsu Croatia), **Saša Milinović** (OMD) i **Dubravka Štefanac** (A1 Hrvatska).

Jedan od glavnih izazova uvođenja AI alata u svakodnevno poslovanje marketinških tvrtki je usklađenost s GDPR-om. Kako ističe Saša Milinović (OMD), posebno kod složenih AI sustava koji često funkcioniraju kao takozvani black box. Problem je u tome što tvrtke ponekad ne mogu jasno objasniti kako sustav obrađuje podatke ili donosi odluke. Dodatni izazov je pravo na brisanje podataka jer se podaci mogu ukloniti iz baza, ali ih je teško ukloniti iz već treniranih AI modela. Tu je i prijenos podataka izvan Europske unije budući da mnogi alati dolaze od američkih kompanija (OpenAI, Google), što zahtijeva dodatne pravne provjere koje se često zanemaruju. Velik rizik predstavlja i kada zaposlenici koriste besplatne AI alate bez kontrole poslodavca jer time često unose osjetljive podatke u takve alate bez razumijevanja gdje ti podaci završavaju. Posljedice mogu biti gubitak poslovnih tajni, kršenje ugovora o povjerljivosti i sigurnosni propusti koji mogu dovesti do visokih kazni. Zato je važno postaviti jasna pravila i koristiti sigurne, korporativne verzije alata koje ne koriste podatke za treniranje.

Govoreći o upravljanju rizicima i sigurnoj implementaciji AI alata, Mario Frančešević (SeekandHit) naglašava važnost ranog uključivanja Službenika za zaštitu podataka (DPO) u cijeli proces. Ističe kako DPO treba biti uključen već u fazi razmatranja uvođenja alata, a ne tek nakon što je tehnologija već implementirana. Takav pristup omogućuje pravovremeno prepoznavanje rizika i usklađivanje s regulatornim zahtjevima. Također ističe važnost pristupa Privacy by Design, koji podrazumijeva da se zaštita podataka ugrađuje u sam dizajn sustava.

Za svaki AI alat koji analizira ponašanje ili navike korisnika, potrebno je izraditi Procjenu učinka na zaštitu podataka (DPIA). Pravilnik o radu i ugovori bi trebali sadržavati stavke o prihvatljivom

korištenju AI alata, gdje se jasno zabranjuje zaposlenicima ubacivanje podataka klijenata i osobnih podataka korisnika u AI alate koji treniraju svoje modele na tim podacima. U praksi to znači osiguravanje transparentnosti prema korisnicima, jasno označavanje AI-generiranog sadržaja, provođenje procjena učinka na zaštitu podataka za rizičnije alate te postavljanje jasnih internih pravila o tome kako i u koje svrhe se AI alati smiju koristiti.

Marko Jambrešić (dentsu Croatia) upozorava da najčešći propusti dolaze iz korištenja generičkih ugovora koji nisu prilagođeni AI sustavima. Često nisu jasno definirane uloge, pa pružatelj alata nije nužno samo izvršitelj obrade, već može imati i širu ulogu, primjerice ako koristi podatke za treniranje modela. Također, ugovori često ne preciziraju svrhu obrade ni koriste li se podaci samo za uslugu ili i za razvoj tehnologije. Dodatni problem je nedostatak jasnoće oko podizvršitelja, posebno kada su uključeni cloud pružatelji izvan Europske unije, pa je važno da ugovori jasno definiraju odgovornosti i način korištenja podataka. Pseudonimizacija podataka može pomoći u smanjenju rizika jer otežava povezivanje podataka s pojedincem, ali takvi podaci i dalje se smatraju osobnima jer ih je moguće ponovno identificirati. Zato ona nije dovoljna sama po sebi, već služi kao dodatna zaštitna mjera, uz obvezu postojanja zakonite osnove obrade i drugih sigurnosnih mjera. Organizacijama se pritom preporučuje i da se, u kontekstu nadolazećih pravila poput EU Artificial Intelligence Acta, upoznaju s mjerama za odgovorno upravljanje podacima i rizicima u AI sustavima.

Govoreći o razlikama između open source i komercijalnih AI alata, Mario Frančešević (SeekandHit) navodi da za obje vrste vrijede ista pravila zaštite podataka. Open source modeli mogu biti sigurniji jer se koriste lokalno, pa nema dijeljenja podataka s trećim stranama. No s druge strane, u tom slučaju tvrtka preuzima veću odgovornost za eventualne pogreške, netočne rezultate ili pristranosti modela koje mogu utjecati na korisnike ili klijente. Kada je riječ o brzini implementacije, u praksi često postoji napetost između želje za brzim uvođenjem AI rješenja i potrebe za usklađenošću s regulativom. Tehnologija se razvija vrlo brzo, dok pravni okvir zaostaje, pa marketing i menadžment često guraju brže uvođenje, dok pravni timovi usporavaju proces kako bi osigurali usklađenost. Ipak, ta dva cilja ne moraju biti u sukobu ako postoji jasan interni proces. Kao rješenje ističe se uvođenje jednostavnog AI onboarding procesa kojim se definira koje alate tvrtka smije koristiti i pod kojim uvjetima. Također je korisno unaprijed odobriti određene sigurne alate koje zaposlenici mogu koristiti bez dodatnih provjera. Važno je da takvi procesi ne usporavaju poslovanje, već da pomažu tvrtkama da uvedu AI na siguran i kontroliran način.

Sukob između brzine implementacije AI rješenja i regulatorne usklađenosti sve je izraženiji u praksi, jer se tehnologija razvija znatno brže od pravnog okvira. Dubravka Štefanac (A1 Hrvatska) objašnjava kako poslovni timovi teže brzom uvođenju kako bi ostali konkurentni, dok pravne i compliance funkcije usporavaju proces kako bi osigurale usklađenost. Kao rješenje ističe uvođenje jasnih internih procesa, poput AI onboarding modela, koji omogućuju kontrolirano uvođenje alata, uz unaprijed odobrene i sigurne opcije za zaposlenike, ali bez nepotrebnog usporavanja poslovanja. Važno je pritom da takvi procesi budu u funkciji poslovnih ciljeva, uz istovremeno pokrivanje svih pravnih zahtjeva i smanjenje rizika. Zaštita intelektualnog vlasništva klijenata zahtijeva pristup na više razina, s važnosti jasnog definiranja korištenja AI alata u ugovorima, korištenja sigurnih verzija alata koje ne koriste podatke za treniranje te edukacije zaposlenika da ne unose povjerljive informacije. Uz to, preporučuje se vođenje evidencije sadržaja generiranog uz pomoć AI-ja kako bi se mogao dokazati njegov nastanak i odgovornost. Transparentnost prema klijentima pritom vidi kao ključan element povjerenja, a ne samo regulatornu obvezu.