SABEU QUÈ SÓN ELS "ZRP O ZERO RETENTION PROMPTS"?

- **Són instruccions o prompts que no s'emmagatzemen com a informació pels grans models de llenguatge i, a priori, no són utilitzats per entrenar-los (només per un període molt determinat).**

- **Aquesta política de ZRP està relacionada amb la quantitat ingent d'informació que es processa en la IA generativa i amb la necessitat i requeriments que les dades dels usuaris estiguin molt més protegides, principalment en termes de seguretat i privacitat.**

- **Malgrat que els LLM contenen grans quantitats de dades, actualment no tenen les màximes garanties de seguretat i, això, és preocupant en general i especialment preocupant en àmbits altament sensibles com els de la salut, justícia o educació.**

- **Cal tenir present que segons la Normativa de protecció de dades o GDPR (Art.5), les dades s'han d'emmagatzemar durant el menor temps possible però no especifica quant de temps és això, només que la durada s'ha de justificar i aquesta decisió s'ha de documentar.**

- **En aquest sentit, les polítiques de ZRP demostren que és possible avançar en termes de seguretat i privadesa a través d'una innovació molt marcada pels requeriments legals com són el dret de supressió o dret a l'oblit o bé els requeriments que han fet organismes de protecció.**

- **El més notori fou el de l'Autoritat Italiana de Protecció de Dades (Il Garante), que va ordenar a Open AI que interrompés temporalment el tractament de dades personals de ChatGPT a Itàlia degut a les presumptes infraccions amb la GDPR.**

- Principalment, aquestes infraccions foren la manca d'informació relacionada amb la transparència requerida sobre el tractament de les seves dades personals per part de ChatGPT als usuaris i altres parts interessades sobre les dades recopilades per ChatGPT.

- L'absència d'una base legal per al tractament de dades personals amb finalitats de formació dels models i del seu perfilat, així com que la informació proporcionada per ChatGPT no sempre coincideix amb les dades reals.

- L'acció de Il Garante reflecteix una atenció creixent per part de les autoritats en els LLM, i sembla poc probable que sigui l'última tenint en compte que l'acumulació innecessària de dades està contraposada amb la supressió total de les dades personals que contempla la GDPR.

- Evidentment, com les dades sovint serveixen com a evidència en procediments legals, aquesta disposició legal de la GDPR i les polítiques de ZRP també poden dificultar la capacitat d'una organització per defensar-se o presentar reclamacions si les dades no estan disponibles.

- D'aquí que la mateixa normativa i la política més actual de ZRP sigui la d'estipular en els contractes uns períodes curts de conservació d'aquests tipus de dades (generalment durant un màxim de 30 dies) en cas que existeixin reclamacions i les dades no estan disponibles.

- Si bé això significa que, més enllà d'aquest període, no es faran servir indicacions o prompts d'entrada per entrenar models ni per perfilar com s'utilitzen els models, és possible que es continuïn utilitzant metadades agregades per aquestes i altres activitats.

- Així doncs, la política de ZRP és només un petit canvi ja que l'actual model és encara d'acumulació de dades i els canvis més significatius no seran exclusivament en termes de seguretat i privacitat, sinó també pels costos associats a l'emmagatzematge constant de dades.