dimecres, 08 de juliol de 2026

La Comissió presenta un pla d'acció sobre IA i ciberseguretat

Font: Comissió Europea

a Comissió Europea ha presentat un Pla d'Acció per donar una resposta estructurada sobre com abordar els riscos i aprofitar les oportunitats dels models avançats d'intel·ligència artificial (IA) en l'àmbit de la ciberseguretat.

Els nous models avançats d'IA estan redefinint la ciberseguretat. La IA es pot utilitzar indegudament per identificar vulnerabilitats, automatitzar atacs i augmentar l'escala i la velocitat dels incidents cibernètics a una velocitat sense precedents.

Sobre la base del marc jurídic únic de la UE per a la IA i la ciberseguretat, el Pla d'Acció reunirà els estats membres, la indústria i organitzacions a escala de la UE per reforçar la ciberseguretat del nostre panorama digital davant les vulnerabilitats que planteja la IA avançada.

Avaluació dels models d'IA

Per a que la seguretat sigui efectiva cal comprendre en detall quin pot ser l'ús, l'ús indegut i l'explotació de les noves tecnologies. En virtut de la Llei d'IA [https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai], abans d'introduir-los al mercat de la UE, els models avançats d'IA s'han d'avaluar i les mesures de mitigació s'han d'examinar detingudament.

Per fomentar els coneixements especialitzats a la UE, la Comissió Europea publicarà una convocatòria per crear una capacitat d'avaluació de la UE que abasti la ciberseguretat, que s'espera que estigui operativa el 2027. Aquesta nova capacitat contribuirà a la funció reguladora de l'Oficina d'IA en reforçar l'avaluació per part de tercers de les capacitats i els riscos de la IA a escala mundial.

Accés a models avançats d'IA

Europa també necessita condicions clares i transparents per accedir als sistemes d'IA més avançats.

La Comissió treballarà amb l'Agència de la UE per a la Ciberseguretat (ENISA [https://www.enisa.europa.eu/]) per definir un pla rector europeu per a l'accés estructurat a capacitats avançades d'IA en l'àmbit de la ciberseguretat. Aquestes orientacions donaran suport a aquelles organitzacions públiques i privades europees pertinents per accedir a models avançats d'IA.

Posar a prova la IA en l'àmbit de la ciberseguretat

ENISA i el Centre Comú de Recerca [https://joint-research-centre.ec.europa.eu/index_en] de la Comissió Europea crearan una plataforma segura per posar a prova la IA en l'àmbit de la ciberseguretat, també amb l'ús d'entorns simulats. Això farà que els operadors de sectors crítics, com les finances, l'energia, la salut, el transport i l'administració pública, ampliïn els seus coneixements tècnics sobre l'ús segur de la IA.

Reforçar la ciberseguretat de la UE i corregir les vulnerabilitats

La UE ha de protegir les seves infraestructures crítiques contra les vulnerabilitats derivades del possible ús indegut d'aquestes tecnologies.

Tal com preveuen les normes de ciberseguretat de la UE, les organitzacions haurien d'intensificar les pràctiques de ciberhigiene, les mesures de gestió de riscos i els principis de seguretat des del disseny.

Les organitzacions haurien de començar a utilitzar les capacitats d'IA ja disponibles, també a través de models de codi obert, per identificar i corregir les vulnerabilitats més ràpidament, i per prevenir i respondre als ciberatacs.

Per ajudar les organitzacions en aquesta transició, ENISA donarà suport i facilitarà les associacions entre les autoritats públiques, les empreses i les comunitats de codi obert en l'ecosistema cibernètic. Això inclourà orientació, recomanacions i millors pràctiques, així com una campanya per assegurar el programari de codi obert crític.

Expandir les capacitats europees d'IA per a la ciberseguretat

Per a estimular l'expansió del mercat europeu, la Comissió posarà en marxa un gran repte de la UE en matèria d'IA per a la ciberseguretat. Aquesta competició reunirà empreses, investigadors i organitzacions per desenvolupar solucions d'IA per a la ciberseguretat.

La UE ha de continuar invertint en desenvolupar les seves pròpies capacitats avançades d'IA, aprofitant la infraestructura proporcionada per les fàbriques d'IA i les futures gigafàbriques [https://digital-strategy.ec.europa.eu/en/policies/ai-factories]. En aquest context, la futura capacitat europea de capital en l'àmbit de les tecnologies, anunciada en el Paquet de mesures de sobirania tecnològica [https://ec.europa.eu/commission/presscorner/detail/es/ip_26_1187], podria atraure inversió privada per ampliar les capacitats pròpies d'IA.

Rerefons

La UE disposa d'un marc jurídic adequat per abordar la ciberseguretat en l'era de les tecnologies emergents, com la IA. La Llei d'IA exigeix avaluar i mitigar els riscos derivats dels models d'IA, mentre que el Codi de bones pràctiques per a la IA d'ús general [https://digital-strategy.ec.europa.eu/en/policies/contents-code-gpai] especifica els requisits i facilita el compliment per part dels proveïdors de models avançats. Aquestes disposicions començaran a aplicar-se el 2 d'agost de 2026.

La Llei de ciberresiliència [https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act], aplicable abans de finals de 2027, exigeix la seguretat des del disseny per als productes de maquinari i programari. A més, la Directiva sobre seguretat de les xarxes i els sistemes d'informació [https://digital-strategy.ec.europa.eu/es/policies/nis2-directive], o Directiva SRI 2, pretén impulsar la seguretat de sectors crítics com el transport i l'energia, juntament amb la Llei relativa a la resiliència operativa digital del sector financer [https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32022R2554&from=ES] (DORA). La Llei de cibersolidaritat [https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity] reforça les capacitats de la UE per detectar amenaces i atacs de ciberseguretat significatius i a gran escala, preparar-s'hi i respondre-hi.

Més informació

Pla d'Acció de la UE sobre Ciberseguretat i Intel·ligència Artificial [https://digital-strategy.ec.europa.eu/en/news-redirect/946754]

Pàgina d’informació [https://digital-strategy.ec.europa.eu/en/news-redirect/947210]

(Font: Comissió Europea)