

LES PÍNDOLES DEL DPD

PÍNDOLA 54.- 10 MALENTESOS SOBRE EL MACHINE LEARNING

L'Agència Espanyola de Protecció de Dades i el Supervisor Europeu de Protecció de Dades han publicat un nou document conjunt en el que exposen els 10 malentesos més comuns relacionats amb el Machine Learning (aprenentatge automàtic) i aporten una anàlisi de quin hauria de ser l'enfocament correcte.

L'aprenentatge automàtic (Machine Learning o ML) és una branca específica de la intel·ligència artificial, aplicada a la resolució de problemes específics i limitats, com tasques de classificació o predicció. A diferència d'altres tipus d'intel·ligència artificial que intenten emular l'experiència humana; el comportament dels sistemes d'aprenentatge automàtic no està definit per un conjunt predeterminat d'instruccions.

Els models de ML s'entrenen utilitzant conjunts de dades. Durant el seu entrenament, els sistemes de ML s'adapten de manera autònoma als patrons trobats en les diferents variables d'un conjunt de dades donat, creant correlacions. Un cop entrenat, el sistema utilitzarà els patrons apresos per a generar un resultat.

A diferència d'altres tipus de sistemes d'intel·ligència artificial, el rendiment dels models de ML depèn en gran mesura de la precisió i la representativitat de les dades utilitzades pel seu entrenament (dades d'entrenament).

L'objectiu del document és dilucidar els conceptes erronis més comuns que envolten els sistemes de Machine Learning, a més de subratllar la importància d'implementar aquestes tecnologies d'acord amb els valors de la UE, els principis de protecció de dades i el respecte als drets de les persones.

Els 10 malentesos que es descriuen en el document són:

1. Correlació implica causalitat. → realitat: causalitat és més que només establir correlacions.
2. Al desenvolupar sistemes d'aprenentatge automàtic, quantes més dades i major sigui la varietat, millor. → realitat: els conjunts de dades d'entrenament de ML han de seleccionar-se per complir llistats de precisió i representativitat.
3. El ML necessita dades d'entrenament completament lliures d'errors. → realitat: per aconseguir un bon rendiment els models de ML calen dades d'entrenament amb tan sols una qualitat superior a un cert llistat.
4. El desenvolupament de sistemes de ML requereix grans repositoris de dades o l'intercanvi de conjunts de dades de diferents fonts. → realitat: l'aprenentatge federat permet el desenvolupament de sistemes d'aprenentatge automàtic sense compartir dades d'entrenament.
5. Els models de ML milloren automàticament amb el temps. → realitat: una vegada implementats, el rendiment dels models de ML pot deteriorar-se i no millorarà a menys que rebí entrenament addicional.
6. Les decisions automàtiques preses pels algorismes de ML no poden ser explicades. → realitat: un model de ML ben dissenyat pot produir decisions comprensibles per a totes les parts interessades rellevants.

LES PÍNDOLES DEL DPD

7. La transparència en ML viola la propietat intel·lectual i no és entesa per l'usuari. → realitat: és possible proporcionar una transparència significativa als usuaris d'intel·ligència artificial sense fer malbé la propietat intel·lectual.
8. Els sistemes de ML estan subjectes a menys biaixos que els propis humans. → realitat: els sistemes de ML estan subjectes a diferents tipus de biaixos i alguns d'aquests provenen de biaixos humans.
9. El ML pot predir amb precisió el futur. → realitat: les prediccions d'un sistema de ML només són precises quan els esdeveniments futurs reproduïxen tendències passades.
10. Els interessats són capaços d'anticipar les possibles sortides que els sistemes de ML poden donar amb les seves dades. → realitat: la capacitat de ML per trobar correlacions no evidents en les dades pot acabar revelant informació personal addicional, sense que l'interessat en sigui conscient.

Per a més informació, podeu consultar el document complet a través del següent enllaç:

<https://www.aepd.es/es/documento/10-malentendidos-machinelearning-es.pdf>

Per qualsevol dubte o aclariment addicional podeu adreçar-vos al DPD de Salut:

dpd@ticsalutsocial.cat

<https://ticsalutsocial.cat/oficina-dpd/>

Tel.: 93 553 26 42 (9:00 a 14:00 h.)