Distinguida dissertação de estudante da Faculdade de Ciências do Porto sobre segurança informática

written by O Cidadão | 25 de Dezembro, 2025

A dissertação de **Ana Catarina Gomes**, com o título **"Active Inference against Federated Learning: Attacks and Solutions"**, aborda a **privacidade de dados em modelos de *machine learning***, em particular em **mecanismos de aprendizagem distribuída**, como *Federated Learning* (FL), uma solução que pretende **mitigar as preocupações com privacidade dos dados** usados para treino através da descentralização.

"O meu trabalho propôs novos ataques ativos contra FL para inferir atributos sensíveis do ponto de vista da privacidade, como por exemplo se um utilizador de um smartphone está em casa. Este estudo mostra que técnicas desenvolvidas para preservar a privacidade, como FL, introduzem novas

vulnerabilidades ainda pouco exploradas, e que modelos com boa capacidade de generalização acarretam uma falsa sensação de segurança“, explica a atual estudante do Programa Doutoral em Ciência de Computadores.Na sua dissertação apresenta, por isso, **propostas alternativas de técnicas de deteção e mitigação para ataques ativos**, que vão além das existentes ao equilibrar o compromisso entre privacidade e utilidade, sendo eficazes contra ameaças ativas subestimadas. Esta é uma área cada vez mais crítica dado o crescimento exponencial da inteligêncial artificial.O trabalho da jovem investigadora, que está entre quatro distinguidos pelo IEEE, contou com a orientação do docente da FCUP e investigador do INESC TEC, **João Vilela** e de **Ricardo Mendes**, da Amazon.

Esta não é a primeira vez que **Ana Catarina Gomes** é distinguida pelo seu desempenho. A estudante recebeu recentemente a distinção de melhor média do mestrado em Ciência de Dados, na 5ª edição da Cerimónia de Prémios e Distinções da FCUP.