University of Abou Bekr Belkaid –Tlemcen
Faculty of sciences

Computer science department

2^{year} A.I MASTER

Lab N°=6 DL (Privacy and machine learning)

Problem specification

- Using the code named ‘simpleresnet-dp.ipynb’:
- Apply it on the diabetic retinopathy dataset (or you can apply it on Cifar10 by changing the number of classes and the path of the dataset).
- Answer the following questions:

- **(1) Privacy Budget Impact**
  Run the model with different epsilon values and complete the table:

Epsilon (ε)	Test Accuracy	Training Time
1.0		
2.0		
8.0		

- **(2) : Privacy vs Utility Trade-off**
- 1. Plot the privacy-utility curve
- 2. Find the best compromise using the harmonic mean : (2*criterion1*crterion2)/(criterion1+criterion2)

- **(3) Bonus Challenges**
  1. Try different models (architectures such as resnet 152, densenet 121)
  2. Plot the privacy-utility curve