# Sécurité Appliquée-TP 2
# Protection de la vie privée-PVP

Jean-François COUCHOT
couchot[arobase]femto-st[point]fr

18 novembre 2022

On considère le jeu de données Adults de l'UCI présentant un extrait des données de recensement en 1994/1995 aux USA et dont l'objectif initial était de prédire si telle ou telle personne allait avoir un salaire supérieur à 50K$ par an. On s'intéresse dans ce TP à publier des statistiques sur les statuts maritaux.

## 1 Publication d'histogramme respectueux de la vie privée

**Exercice 1.1 (Initialisation).**

1. *Récupérer le jeu de données.*
2. *Mémoriser (dans un dictionnaire) les fréquences originales des statuts maritaux.*
3. *Les représenter l'aide d'un histogramme.*

**Exercice 1.2 (Histogramme respectueux, à la main avec un bruit laplacien).**

1. *On souhaite publier un histogramme à l'aide de l'$\epsilon$-DP. Montrer que la sensibilité d'une telle requête est 1.*
2. *Implanter un algorithme qui construit un histogramme répondant à la question 1.*

**Exercice 1.3 (Histogramme respectueux avec `diffprivlib`).** *Maintenue par IBM, `DiffprivLib` est une bibliothèque en protection de la vie privée à base de confidentialité différentielle.*

1. *Installer cette bibliothèque.*
2. *En s'inspirant du site github de diffprivlib consacré aux histogrammes reprendre l'exercice précédent.*
3. *Faire varier $\epsilon$ dans $\{0.001, 0.001, 0.01, 0.1, 1, 10, \infty\}$ et afficher à chaque fois l'histogramme. Quelle semble être la distribution pour $\epsilon = 0.001$ ? Et pour $\epsilon = \infty$ ?*
4. *Comprendre l'alerte suivante générée par l'outil. Pourquoi particulièrement cela correspond-il à une fuite d'information.*

```
PrivacyLeakWarning: Range parameter has not been specified.
Falling back to taking range from the data.
To ensure differential privacy, and no additional privacy leakage,
the range must be specified independently of the data (i.e., using domain knowledge).
"specified independently of the data (i.e., using domain knowledge).", PrivacyLeakWarning)
```

5. *Pourrait-on fournir les intervalles pour éviter cette fuite ? Comment ? Le faire.*

## 2 Mécanisme exponentiel

**Exercice 2.1 (Statut marital le plus fréquent).** *On souhaite répondre à la question : quel est le statut marital le plus fréquent dans la base, sachant que celle-ci va progressivement évoluer.*

1. *Quel mécanisme peut-on utiliser ?*
2. *On propose de choisir la fonction d'utilité $u(D, r)$ qui retourne le nombre de fois où $r$ apparaît dans $D$. Montrer que $\Delta_u$ vaut 1.*
3. *Montrer que l'on ne va pas pouvoir évaluer $\exp(\frac{\epsilon u(D,r)}{2\Delta_u})$ pour certains couples de valeurs de $(epsilon, r)$. Pourquoi ?*
4. *Proposer une fonction qui retourne le statut marital le plus fréquent, tout en respectant l'$\epsilon$-DP pour des valeurs de $\epsilon$ (très) petites.*
5. *Évaluer cette fonction sur 1000 tirages en prenant $\epsilon \in [10^{-5}, 10^{-4}, 10^{-3}, 0.01, 0.1]$ et représenter graphiquement le résultat.*