



CENTRE GOUVERNEMENTAL
DE CYBERDÉFENSE

SI-19(06)

Confidentialité différentielle

Juill. 2026



Intégrité des systèmes et des données

System and Information Integrity

SI-19(06) – Confidentialité différentielle (Pb--)

Énoncés :

Prévenir la divulgation de renseignements personnels en ajoutant du bruit non déterministe aux résultats des opérations mathématiques avant de faire rapport des résultats.

Responsable : Aucun

Discussion :

La définition mathématique de la confidentialité différentielle indique que le résultat de l'analyse du jeu de données devrait être approximativement le même avant et après l'ajout ou la suppression d'un seul enregistrement de données (que l'on présume être les données d'un seul individu). Dans sa forme la plus fondamentale, la confidentialité différentielle s'applique uniquement aux systèmes d'interrogation en ligne. Elle peut toutefois être utilisée pour produire des classificateurs statistiques d'apprentissage automatique et des données synthétiques. La confidentialité différentielle est assurée au détriment de l'exactitude des résultats, forçant les organisations à quantifier le compromis entre la confidentialité et l'exactitude, la pertinence et l'utilité globales des jeux de données dépersonnalisés. Le bruit non déterministe peut comprendre l'ajout de petites valeurs randomisées aux résultats des opérations mathématiques dans l'analyse des jeux de données.