IPoP: Interdisciplinary Project on Privacy

Antoine Boutet (Insa-Lyon), Vincent Roca (Inria)

February 3, 2023

Abstract

IPoP est un projet inscrit dans le PEPR (Programme et Équipement Prioritaires de Recherche) Cybersécurité financé dans le programme France 2030 débuté en 2022 pour une durée de 6 ans. Le projet IPOP s'intéresse à étudier les menaces vis-à-vis de la vie privée introduites par l'usage des nouvelles technologies et nouveaux services émergents (par exemple avec les dispositifs de santé connectés ou encore les assistants personnels) en toute compatibilité avec les réglementations en vigueur en Europe et en préservant la qualité d'expérience des utilisateurs. Les problématiques soulevées doivent répondre à la fois à des défis technologiques, sociétaux, juridiques, économiques, politiques et éthiques.

Défi sociétal : Protéger les données personnelles

IPoP est un projet interdisciplinaire sur la protection des données personnelles, il mélange informatique en lien étroit avec les sciences humaines et sociales ou encore législatif en lien avec le RGPD. Le programme scientifique se focalise sur :

- Effectuer une veille sur les nouvelles formes de collecte d'informations personnelles et les pratiques de l'écosystème associé, identifier les vecteurs de fuite, de quantifier les informations collectées et proposer des contre-mesures.
- Optimiser l'usage du Machine Learning et de l'IA exploitant des données personnelles afin de fournir un niveau de confidentialité interprétable et transparent pour les utilisateurs (coopération avec le PEPR Santé Numérique pour les cas d'usage de données de santé).
- Proposer un environnement contrôlé pour évaluer la sécurité des algorithmes d'anonymisation.
- Étudier et sécuriser l'usage de systèmes personnels de gestion de données permettant de redonner aux utilisateurs un contrôle sur leurs données personnelles.
- Trouver un meilleur compromis entre utilité et vie privée dans les approches de confidentialité différentielle.
- Traiter les défis juridiques (la place du droit de la protection des données à caractère personnel face aux enjeux de cybersécurité, et de l'articulation des sources du droit dans le champ de la santé numérique), sociétaux (analyses sociologiques sur la perception des risques pour la vie privée) et éthiques (analyses des pratiques de manipulation des utilisateurs).

Cette vision holistique du problème de la protection des données personnelles permet à la fois de proposer des solutions aux défis scientifiques et techniques, de confronter ces solutions sous différentes formes dans le cadre de collaborations interdisciplinaires, et de proposer des recommandations en matière de régulation et d'encadrement juridique.

Ce programme scientifique fédérateur interdisciplinaire rassemble des équipes de recherche travaillant sur la protection des données et reconnues internationalement, issues d'universités, d'écoles d'ingénieurs et d'organismes nationaux de recherche, ainsi que la CNIL (Commission nationale de l'informatique et des libertés). Plus précisément, le consortium est composé de INRIA, CNRS, INSA Val de Loire, INSA Lyon, Université Versailles Saint-Quentin en Yvelines, Université de Lille, Université Grenoble Alpes, Edhec, Université de Rennes 1, ainsi que la CNIL.