

Systemy informacyjne wokół nas przetwarzają ogromną ilości danych. Niektóre powinny być ukryte albo tak zmienione, aby nie można było za wiele powiedzieć o osobach, których one dotyczą. Jest to nie tylko kwestia naszego poczucia bezpieczeństwa, ale też przestrzegania coraz bardziej wymagającego prawa (*vide* dyrektywa GDPR (UE) 2016/679).

Pewnych danych nie możemy po prostu zaszyfrować, bo staną się zupełnie bezużyteczne. Nie chcemy na przykład swoim znajomym ujawniać ile zarabiamy, jednak już podanie średniej zarobków obywateli z całego kraju nie zagraża przecież naszej osobistej prywatności. Co więcej, taka informacja może być bardzo przydatna dla ogółu. Podobnie możemy zaakceptować gromadzenie pewnych danych przez radiową sieć ad hoc zbudowaną między innymi z naszych urządzeń mobilnych. Nie możemy jednak dopuścić do tego, aby ujawnione zostały zbyt szczegółowe informacje geolokalizacyjne czy te dotyczące naszych preferencji konsumenckich.

Tego typu problemami zajmować chcemy się w naszym projekcie. Badania nasze dotyczyć mają wielu, pozornie odległych od siebie zagadnień, takich jak zbieranie/agregacja danych, wnioskowanie na podstawie ogromnych zbiorów danych czy sieci społecznościowych. W pracach wykorzystywać będziemy różne techniki algorytmiczne i statystyczne. Użyjemy także zaawansowane techniki kryptograficzne, aby ujawniać dokładnie te informacje, jakie mają być ujawnione, a pozostałe ukryć. Nasze badania oparte będą na podejściu formalnym, matematycznym. Wierzimy, że tylko takie podejście może zagwarantować nam odpowiedni poziom bezpieczeństwa.