Gdańsk 10 listopada 2022 r.

STRESZCZENIE ROZPRAWY DOKTORSKIEJ

Prawne instrumenty oceny prawidłowości procesów przetwarzania danych osobowych w aspekcie normalizacji

Autor rozprawy: mgr Tomasz Soczyński
Promotor: dr hab. Wojciech Wiewiórowski

Uniwersytet Gdański
Wydział Prawa i Administracji

Tempo zmian technologicznych i masowe przetwarzanie danych osobowych z użyciem technologii teleinformatycznych rodzi nowe wyzwania w zakresie zapewnienia bezpieczeństwa danych w procesie przetwarzania. Stanowienie prawa w sposób zapewniający godzenie obligatoryjności normy prawnej (nakaz wypełnienia treści przepisu prawa) z dobrowolnym stosowaniem normy technicznej (wybór sposobu spełnienia określonych standardów normalizacyjnych), to jeden ze sposobów odzwierciedlenia postępu technologicznego w porządku prawnym.

Celem głównym rozprawy jest wykazanie potrzeby uwzględnienia standardów normalizacyjnych w instrumentach prawnych stosowanych do oceny prawidłowości i modelowania procesów przetwarzania danych osobowych. Celowe jest zatem odniesienie instrumentów prawnych wprowadzonych przepisami RODO do możliwości i potrzeby odwołania do norm technicznych, dokonanie przeglądu norm właściwych dla tych instrumentów, ustalenie związku wymogów zgodności rozwiązań przewidzianych w przepisach RODO z właściwymi normami technicznymi. Celowi głównemu służy wykazanie zasadności tworzenia opartych o normy techniczne narzędzi oceny zgodności (kodeksy postępowania, ocena skutków przetwarzania dla danych osobowych, mechanizmy certyfikacji oraz ochrona danych w fazie projektowania), ze szczególnym podkreśleniem roli oceny skutków przetwarzania dla danych osobowych (DPIA) oraz wskazanie przykładów modelowego wykorzystania DPIA w ramach oceny skutków regulacji (OSR) projektowanych rozwiązań prawnych.

Uzasadnienie wyboru tematu rozprawy doktorskiej, cel rozprawy, określenie przedmiotu badań, przedstawienie hipotezy badawczej i metod badawczych zawiera rozdział 1. Podstawowe pojęcia instrumentu prawnego, prywatności, ochrony danych osobowych oraz zmianę podejścia do tych danych omawia rozdział 2.

Rozdział 3 poświęcony jest wybranym zagadnieniom z zakresu normalizacji, w tym przywołaniu definicji normy, rodzajów norm, procesu ich tworzenia, poziomów normalizacji, znaczenia normalizacji europejskiej i krajowej oraz przeglądowi światowych organizacji normalizacyjnych. W tym rozdziale rozważany jest problem reagowania systemu prawa na zmiany technologiczne, aktualizowanie norm technicznych oraz zagadnienie powoływania norm w przepisach prawa.

W rozdziale 4 na gruncie przepisów RODO scharakteryzowano istotę nowego podejścia do ochrony danych osobowych. Ochrona danych osobowych traktowana jest jak jeden z procesów w organizacji, zarządzany zgodnie z normami technicznymi z rodziny ISO, uwzgledniający poziom zarzadzania jakością i zgodnością w organizacji oraz poziom zarzadzania ryzykiem i bezpieczeństwem danych.

W rozdziale 5 poddano analizie zależności pomiędzy stosowaniem prawnych instrumentów ochrony danych osobowych a normami technicznymi, z podkreśleniem roli administratora danych osobowych i podmiotu przetwarzającego, kryteriów bezpieczeństwa IT, ram prywatności, zapewnienia adekwatnego do występujących ryzyk bezpieczeństwa danych, rejestrów czynności przetwarzania jako funkcji prekontroli oraz uprzednich konsultacji z organem nadzorczym.

Rozdział 6 dotyczy stosowania mechanizmów autoregulacyjnych z wykorzystaniem norm technicznych odpowiednich dla kodeksów postępowania i certyfikacji oraz przedstawia proces ich wdrażania.

W rozdziale 7 omówione zostało stosowanie oceny skutków przetwarzania dla danych osobowych (DPIA) w oparciu o normy i wytyczne, sposoby mitygowania ryzyka w procesie przetwarzania danych, wspomaganie wykonywania DPIA przez organy nadzorcze w UE oraz rekomendowane przez nie narzędzia wspomagające DPIA.

Rozdział 8 poświęcony jest lepszemu stanowieniu prawa na poziomie europejskim i krajowym oraz roli oceny skutków regulacji (OSR). Analizie poddano realizację obowiązku przeprowadzenia DPIA w ramach przygotowania OSR dla siedmiu projektów aktu prawnego, którego przepisy wymagają przetwarzania danych osobowych. Praktykę tę zestawiono z doświadczeniami dokonywania DPIA i OSR w państwach europejskich.

W rozdziale 9 przedstawiono rozwiązanie problemu badawczego w postaci autorskiej propozycji modelu DPIA do celów OSR, służącego realizacji treści normy prawnej w oparciu o międzynarodowe normy techniczne.

Rozważania kończą uwagi i wnioski zawarte w rozdziale 10, podsumowujące wyniki rozważania problemu prawnych instrumentów oceny prawidłowości procesu przetwarzania danych osobowych w aspekcie normalizacji, ze szczególnym akcentowaniem potrzeby dokonywania DPIA na etapie projektowania rozwiązań prawnych związanych z przetwarzania i ochrony danych osobowych.