“Understanding the risk-based approach to data protection: An analysis of the links between law, regulation, and risk” - Abstract

The main goal of this dissertation is to provide an understanding of what is commonly referred to as “the risk-based approach to data protection”. Its starting point is that this risk-based approach is a method of regulation through risk. One can thus argue that data protection (with a specific focus on EU law, and hence the GDPR) is a legal framework pervaded by risk management duties, which are constitutive of a method of regulation. The dissertation therefore studies the risk-based approach to data protection from the perspective of law, regulation, risk, their multiple entanglements, and their respective literatures. It is the thread that guides the whole dissertation. In this sense, one can argue that this thesis actually contains two coextensive research questions. On the one hand it seeks to explain the risk-based approach to data protection per se. On the other hand, the use of this model of regulation entails that data protection is about regulation in the very first place.

The thesis therefore studies in depth the notions of risk, regulation, and their links. It also analyses data protection law from the perspective of regulation theory. Finally, and in the light of these findings, it analyses and explains the risk-based approach to data protection. This analysis is both conceptual and practical. It first puts the adoption of the risk-based approach into perspective, highlighting its theoretical and historical roots. It then goes on to describe the modalities of the adoption of the risk-based approach in the most prevalent data protection statutes (e.g., GDPR, PIPEDA, etc.). It also provides a number of methodological discussions and insights around the main tool used for the risk-based approach (i.e., so-called data protection impact assessments). Finally, it also contains a number of lessons gathered from the use of risk-based approaches in other fields.