**Thesis Title:**
Data Subjects in the GDPR and the Protection of Vulnerable Individuals

**Abstract:**

The new potentialities of machine learning, automated decision-making, hyper-personalization of behavioural advertising, predictive analytics are increasing the power imbalance between individuals and entities processing data in the digital environment. The increasing awareness about bounded rationality and cognitive biases is challenging the traditional notions of “average” consumer, citizen, user and data subject in the digital ecosphere. Individual conditions are more and more important to define different groups of individuals in need of protection from the unfair imbalance described above. Such a need for higher protection is evident in many EU legal fields, in particular (but not only) in the data protection framework. However, while in the EU data protection law there are clear definitions of, e.g., “data controllers” and “data processors”, there is no clear classification of data subjects.

Accordingly, the research question of this thesis is about the notion of data subject in the GDPR, considering in particular different levels of data subjects’ vulnerability, and how we can better protect vulnerable data subjects. The thesis has, thus, three related goals: 1) investigating the notion of data subject and understanding whether and how personal conditions influence the definition and the protection of data subjects; 2) reconceptualizing the notion of vulnerability in the data protection framework, proposing thus a layered, contextual, relational notion that can effectively respond to the challenges of the algorithmic environment and protect fundamental rights of individuals; 3) promoting a vulnerability-aware interpretation of the GDPR. The ultimate expected impact is, thus, to start promoting the concept of data subjects’ layered vulnerability as a heuristic tool to re-interpret the whole system of rights, duties and safeguards in the GDPR, and mostly to reconceptualize the risk-based approach on an individual-centred basis.

The thesis argues that the notion of the data subject in the GDPR, though implicit, is twofold: based both on a general notion of average data subject and on a layered concept of vulnerable subjects. Accordingly, the thesis analyses the concept of vulnerability in different domains (political philosophy, research ethics, law and economics) and in different EU legal fields, trying to adapt this concept to the needs and peculiarities of the data protection field. The accepted definition of data subject’s vulnerability is, thus, the higher risk to fundamental rights and freedoms. The proposal is to focus on a wide and extensive understanding of vulnerability, based on the layered theory of Luna and compatible with the risk-based approach in the GDPR. Under this layered perspective, this thesis identifies the two main categories of vulnerability: processing-based vulnerability (decisional vulnerability within the data processing) and effect-based vulnerability (vulnerability to the adverse outcomes of the data processing). These two kinds of vulnerability differ in terms of effects, manifestations and fundamental rights at issue.

Consequently, the thesis analyses the GDPR principles, rights and duties to assess the role of the personal conditions of data subjects (and in particular the vulnerability condition). Then, the author proposes a vulnerability-attentive model of implementation of the GDPR, following the DPIA model. Finally, possible drawbacks of this proposal are analysed, focussing also on counterarguments and alternative models de lege ferenda.