Information systems around us process huge amounts of data. Part of this information should be hidden or transformed in such a way, that it is hard to infer anything about particular individuals, who it concerns. It is not only the matter of our security and privacy, but also the law is becoming more restrictive in these matters (*vide* guideline GDRP (UE) 2016/679)

One approach to this problem is encrypting the data. However, such operation transforms data into a different domain, where its properties are lost, rendering it useless or very hard to process. Still, the need for processing original data in order to retrieve some of its *cumulative* properties is a desired feature. We do not want our friends to know our salary, but revealing the average or median salary of all people in the whole country does not endanger our privacy. Moreover, such information could be very useful. Similarly, we can accept gathering some information from an ad hoc radio network of our mobile devices, however we need to protect ourselves from revealing too much information about our location or preferences.

These are the problems we want to tackle in our project. The research will concern many, seemingly unconnected fields - collecting/aggregating data, statistical reasoning based on Big Data or social networks. To achieve our goals we plan to use various methods and algorithms. We would also need to exploit some advanced cryptographic protocols to determine exactly what should be revealed and protect anything else. Our research will be based on formal, mathematical methodology. We believe that only such approach can guarantee appropriate security and privacy level to the solutions we will develop.