Risk as a subjective phenomenon.
Integrating cognitive science into the concept of risk in European data protection law

An increasing number of European regulations, especially in the area of new technologies, are based on the application of a so-called risk-based approach. It aims to ensure an appropriate level of security for activities with different levels of risk. An example would be the risk of data leakage resulting from a hacking attack using programmes that generate huge numbers of different types of passwords (so-called bruteforce). As we usually have a lot of important documents and secrets in our inboxes, unauthorised access to this information would be very painful for us. At the same time, the number of such attacks is very high. Therefore, we can see that the risk of a mailbox being hacked is high. In such a situation, we should secure our mailbox with at least a good password (recent recommendations are at least 12 characters, including upper and lower case letters, numbers and special characters). On the other hand, there is no need to apply an equally high level of security to an account on a demo version of a web application whose functionality we just wanted to check. It is therefore a question of security appropriate to the risk, but only in relation to what actually needs to be secured. This allows us to focus our resources on what actually needs it. To do this, we should carry out a risk assessment. The example given applies to ordinary users of new technologies, but analogous requirements (albeit, of course, on a correspondingly larger scale and complexity) are imposed on businesses processing personal data by the Data Protection Regulation (RODO).

The idea of adapting safeguards to the level of risk, based on the results of its analysis, is very good in theory, but over time practice has shown that conducting a risk assessment is not so easy for everyone. Besides, both the risk itself and its analysis are very subjective in nature. An entrepreneur (data controller) may assess the risk of an event as low, but a controller from a supervisory authority may arbitrarily conclude that in this case the risk is high and therefore impose a penalty on the controller for not applying adequate security measures.

In this study, we want to focus on the subjectivity of the risk estimation process; to see what psychological mechanisms affect the risk estimation process and to consider how we can improve our legal practice to make the estimation process more reliable and the control not so arbitrary.

We are conducting our study using the example of a risk analysis performed as part of the data protection impact assessment required by the RODO, but the results of the study will also be applicable to other areas of law, such as artificial intelligence law or cyber security.