Transparency and Disclosure Risk in Data Privacy

Vicenç Torra
University of Skövde, Sweden

ABSTRACT

k-Anonymity and differential privacy can be considered examples of Boolean definitions of disclosure risk. In contrast, record linkage and uniqueness are examples of quantitative measures of risk. Record linkage is a powerful approach because it can model different types of scenarios in which an adversary attacks a protected database with some information and background knowledge.

Transparency holds in data privacy when data is published together with details on their processing. This includes the data protection method used and its parameters. Intruders can use this information to improve their attacks. Specific record linkage algorithms can be defined to take into account this information, and to define more accurate disclosure risk measures.

Machine learning and optimization techniques also permits us to increase the effectiveness of record linkage algorithms.

This talk will be focused on disclosure risk measures based on record linkage. We will describe how we can improve the performance of the algorithms under the transparency principle, as well as using machine learning and optimization techniques.

Short Bio

Vicenç Torra is a professor in the School of Informatics at the U. of Skövde in Sweden. Until 2014 he was Associate Prof. - Research Track at the Artificial Intelligence Research Institute of the Spanish National Research Council (IIIA-CSIC). His fields of interest are data privacy, information fusion and approximate reasoning.

He is ECCAI Fellow (2010), Elected Member of ISI (2013). He has published over 200 publications and 4 books. One undergraduate course on artificial intelligence (in Catalan and Spanish), one graduate text (Modeling decisions, Springer, 2007; with Y. Narukawa), a book on the history of computer science (From the Abacus to the digital revolution, RBA, 2010) published in Spanish, Portuguese, Italian, French, English, Polish, Russian, and another one on decisions and elections (The mathematics of elections, RBA, in press).

He founded and is the editor in chief of the journal Transactions on Data Privacy (http://www.tdp.cat/). He is associate editor of Information Sciences (Elsevier) and member of the editorial board of Fuzzy Sets and Systems (2004-), Progress in Artificial Intelligence (2011-), J. of Advanced Computational Intelligence and Intel. Informatics (2007-), Int. J. of Computational Intelligence System (2008-). He founded the annual MDAI conference series in 2004 and is PC co-chair ever since. His research has been funded by national and international agencies.