DISTORTION IN REAL-WORLD ANALYTIC PROCESSES

PETER KIESEBERG, LUKAS DANIEL KLAUSNER, AND ANDREAS HOLZINGER

ABSTRACT. In discussions on the General Data Protection Regulation (GDPR), anonymisation and deletion are frequently mentioned as suitable technical and organisational methods (TOMs) for privacy protection. The major problem of distortion in machine learning environments, as well as related issues with respect to privacy, are rarely mentioned. The *Big Data Analytics* project addresses these issues.

People are becoming increasingly aware of the issue of data protection, a concern that is in part driven by the use of personal information in novel business models. The essential legal basis for considering the protection of personal data in Europe has been created in recent years with the General Data Protection Regulation (GDPR). The data protection efforts are confronted with a multitude of interests in research [NSG14] and business [Cir15], which are based on the provision of often sensitive and personal data. We analysed the major challenges in the practical handling of such data processing applications, in particular the challenges they pose to innovation and growth of domestic companies, with particular emphasis on the following areas (see also summary in Figure 1):

- *Anonymisation:* For data processing applications to be usable, it is essential, particularly in the area of machine learning, that the obtained results are of high quality. Classical anonymisation methods generally distort the results quite strongly [MKWH]. Mere pseudonymisation, typically used up to now as a replacement, can no longer be used as a privacy protection measure, since the GDPR explicitly stipulates that these methods are not sufficiently effective. At present, however, there is no large-scale study on these effects which considers different types of information. Also, the approaches to mitigate this distortion are currently still mostly proofs of concept and purely academic. Concrete methods are needed to reduce this distortion and to deal with the resulting effects.
- *Transparency:* The GDPR prescribes transparency in data processing, i. e. the fact that a data subject has the right to receive information about the data stored about them at any time, and to know how they are used. At present, no practical methods exist to create this transparency whilst avoiding possible data leaks. Furthermore, the commonly used mechanisms currently in use are not designed to ensure transparency in the context of complex evaluations using machine learning algorithms. Guaranteeing transparency is also an important prerequisite for the deletion of personal information as well as for ensuring responsibility and reproducibility.
- *Deletion:* An important aspect of the GDPR is informational self-determination: This includes the right to subsequent withdrawal of consent and, ultimately, the right to data deletion. Processes must accomodate

this right; therefore, methods for the unrecoverable deletion of data from complex data-processing systems are needed, a fact which stands in direct opposition to the design criteria that have been employed since the advent of computing. Deletion as a whole is also a problem with respect to explainability and retraceability, thus opening up a substantial new research field on these topics.

- *Data security*: The GDPR not only prescribes privacy protection of personal data, but also data security. Various solutions already exist for this; the challenge does not lie in the technical research but in the concrete application and budgetary framework conditions.
- *Informed consent*: Consent is another essential component of the GDPR. Henceforth, users will have to be asked much more clearly for their consent to using their data for more explicitly specified purposes. The academic and legal worlds have already made many suggestions in this area, so, in principle, this problem can be considered solved.
- *Fingerprinting*: Often data is willingly shared with other institutions, especially in the area of data-driven research, where specialised expertise by external experts and/or scientists is required. When several external data recipients are in the possession of data, it is important to be able to detect a leaking party beyond doubt. Fingerprinting provides this feature, but most mechanisms currently in use are unable to detect a leak based on just a single leaked record.

FIGURE 1. Important aspects of data science affected by the GDPR

Within the framework of the *Big Data Analytics* project, methods for solving these challenges will be analysed, with the aim of coming up with practical solutions, i.e. the problems will be defined from the point of view of concrete users instead of using generic machine learning algorithms on generic research data. In our testbed, we will implement several anonymisation concepts based on k-anonymity and related criteria, as well as several generalisation paradigms (full domain, sub-tree, sibling) combined with suppression. Our partners from various data-driven business areas (e.g. medical, IT security, telecommunications) provide complete use cases, combining real-life data with the respective machine learning workflows. These use cases will be subjected to the different anonymisation strategies, thus allowing the actual distortion introduced by them to be measured. This distortion will be evaluated with respect to the use cases' quality requirements.

In summary, this project addresses the question of whether the distortion introduced through anonymisation hampers machine learning in various application

domains, and which techniques seem to be most promising for distortion-reduced privacy-aware machine learning.

REFERENCES

- [Cir15] Stéphane Ciriani, *The Economic Impact of the European Reform of Data Protection*, Communications & Strategies **97** (2015), no. 1, pp. 41–58, [SSRN: 2674010](#).
- [MKWH16] Bernd Malle, Peter Kieseberg, Edgar Weippl, and Andreas Holzinger, *The Right to Be Forgotten: Towards Machine Learning on Perturbed Knowledge Bases*, Proceedings of the 11th International Conference on Availability, Reliability and Security (ARES 2016), 2016, pp. 251–266, [DOI: 10.1007/978-3-319-45507-5_17](#).
- [NSG14] Olof Nyrén, Magnus Stenbeck, and Henrik Grönberg, *The European Parliament Proposal For the New EU General Data Protection Regulation May Severely Restrict European Epidemiological Research*, Eur. J. Epidemiol **29** (2014), no. 4, pp. 227–230, [DOI: 10.1007/S10654-014-9909-0](#).

INSTITUTE OF IT SECURITY RESEARCH, ST. PÖLTEN UNIVERSITY OF APPLIED SCIENCES, MATTHIAS-CORVINUS-STRASSE 15, 3100 ST. PÖLTEN, AUSTRIA

Email address: peter.kieseberg@fhstp.ac.at

INSTITUTE OF IT SECURITY RESEARCH, ST. PÖLTEN UNIVERSITY OF APPLIED SCIENCES, MATTHIAS-CORVINUS-STRASSE 15, 3100 ST. PÖLTEN, AUSTRIA

Email address: mail@l17r.eu

URL: <https://l17r.eu>

HUMAN-CENTERED ARTIFICIAL INTELLIGENCE LAB, INSTITUTE FOR MEDICAL INFORMATICS, STATISTICS AND DOCUMENTATION, MEDICAL UNIVERSITY OF GRAZ, AUENBRUGGERPLATZ 2/V, 8036 GRAZ, AUSTRIA

Email address: andreas.holzinger@medunigraz.at

URL: <http://www.aholzinger.at/>