COMPUTER LAW & SECURITY REVIEW 34 (2018) 754–772

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/CLSR

Computer Law & Security Review

AI and Big Data: A blueprint for a human rights, social and ethical impact assessment

*Alessandro Mantelero**

Department of Management and Production Engineering, Polytechnic University of Turin, Torino, Italy

ARTICLE INFO

Article history:

Keywords:
Data protection
Impact assessment
Data protection impact assessment
Human rights
Human rights impact assessment
Ethical impact assessment
Social impact assessment
General Data Protection Regulation

ABSTRACT

The use of algorithms in modern data processing techniques, as well as data-intensive technological trends, suggests the adoption of a broader view of the data protection impact assessment. This will force data controllers to go beyond the traditional focus on data quality and security, and consider the impact of data processing on fundamental rights and collective social and ethical values.

Building on studies of the collective dimension of data protection, this article sets out to embed this new perspective in an assessment model centred on human rights (Human Rights, Ethical and Social Impact Assessment-HRESIA). This self-assessment model intends to overcome the limitations of the existing assessment models, which are either too closely focused on data processing or have an extent and granularity that make them too complicated to evaluate the consequences of a given use of data.

In terms of architecture, the HRESIA has two main elements: a self-assessment questionnaire and an ad hoc expert committee. As a blueprint, this contribution focuses mainly on the nature of the proposed model, its architecture and its challenges; a more detailed description of the model and the content of the questionnaire will be discussed in a future publication drawing on the ongoing research.

1. Introduction

Risk assessment models today play an increasing role in data protection, as recently confirmed by the EU General Data Protection Regulation (hereinafter GDPR).[1] Various types of assessment models can be adopted: they may be mandatory or voluntary, self-assessments or third-party/licensing schemes. They can only assess specific kinds of data processing or types of risk. They may be risk/benefit assessments or rights-based assessments. Finally, they may only focus on the legal issues or encompass societal issues as well.

Against this background, the first question we need to ask when defining an assessment model is whether the model is to be sector-specific or general. This is an important question, since data uses are not circumscribed by a specific domain or technology.

It hardly seems possible to adopt a technology-specific approach, for example, an IoT impact assessment, a Big Data impact assessment, a smart city impact assessment or an AI

* Corresponding author: Department of Management and Production Engineering, Politecnico di Torino, C.so Duca degli Abruzzi, 24, Torino 10120, Italy.
E-mail address: alessandro.mantelero@polito.it

[1] See Articles 25 and 26, GDPR.

https://doi.org/10.1016/j.clsr.2018.05.017

impact assessment.[2] All these technologies use data processing for decision-making: they differ in their methods but not in their scope. For this reason, and because the rights and values to be safeguarded are the same in these different contexts - regardless of the technology used, the model proposed here is not a technological assessment,[3] but a rights-based and values-oriented model.

In the context of data-driven applications, an assessment focused on a specific technology looks to be inadequate and only partially effective.[4] On the other hand, taking into account the various application domains (e.g. healthcare or crime prevention), different sets of rights, freedoms and values should be considered. So, a sector-specific approach focuses on the rights and values in question rather than the technology.

Thus, sectoral models concentrate their attention, not on the technology, but on the context and the values that assume relevance in that context.[5] This does not mean that the nature of the technology has no importance in the assessment process as a whole: a given technology determinates the most appropriate measures to take to safeguards the benchmark values.

Adopting a value-oriented approach, the assessment should focus on the societal impact of data use. This impact encompasses the potential negative outcomes on a variety of fundamental rights and principles and also takes into account the ethical and social consequences of data processing.[6]

In addressing these issues, this article builds on the results of previous research on data protection regulation in the context of data-intensive applications for decision-making processes. These works point out the criticisms affecting data protection in this context – which is dominated by an extensive use of Big Data analytics, algorithms and AI – and suggest the development of broader forms of data protection impact assessment, which also looks at the social impact and encourage a values-oriented use of data.[7]

In an initial approach, a mandatory multiple impact assessment was suggested to address these issues in an attempt to provide stronger safeguards for individuals.[8] However, a mandatory procedure encompassing societal issues was perceived as excessively burdensome and complex by business. This article therefore reconsiders the nature of the assessment and recommends a voluntary model,[9] which retains data controllers' freedom of decision, making this assessment a more acceptable solution than compulsory provisions.

Furthermore, a voluntary approach is more consistent with the existing legal framework, which seems to have difficulties in going beyond mere data protection in information use. In this sense, the GDPR – which provides one of the most advanced examples of regulation in this area – focuses on risk

[2] See AI Now Institute, 'Algorithmic Impact Assessments: Toward Accountable Automation in Public Agencies' (2018) <https://medium.com/@AINowInstitute/algorithmic-impact-assessments-toward-accountable-automation-in-public-agencies-bd9856e6fdde> accessed 4 March 2018.

[3] See Barbara Skorupinski and Konrad Ott, 'Technology assessment and ethics' (2002) 1(2) Poiesis & Praxis 95–122.

[4] In some cases, it is hard to define the borders between the different data processing fields and the granularity of the subject matter (e.g. the blurred confines between well-being devices/apps and medical devices).

[5] Specific impact assessments for Big Data analytics and for AI are not necessary, but we do need separate impact assessments for data-driven decisions in healthcare and another for smart cities, given the different values underpinning the two sectors. Whereas, for example, civic engagement and participation and equal treatment will be the driving values behind smart city technologies impact assessment, in healthcare freedom of choice and no-harm principle may play a more critical role. Differing contexts have different "architectures of values" that should be taken into account as a benchmark for the assessment models.

[6] See also Skorupinski and Ott (n 3) 101 ("Talking about risk […] is not possible without ethical considerations […] when it comes to a decision on whether risk is to be taken, obviously an orientation on norms and values is unavoidable").

[7] See Alessandro Mantelero, 'Personal data for decisional purposes in the age of analytics: from an individual to a collective dimension of data protection' in this Review (2016), vol 32, issue 2, 238–255; Alessandro Mantelero, 'The future of consumer data protection in the E.U. Rethinking the 'notice and consent' paradigm in the new era of predictive analytics' in this Review (2014), vol 30, issue 6, 643–660. See also Alessandro Mantelero, 'Regulating Big Data. The guidelines of the Council of Europe in the Context of the European Data Protection Framework' in this Review (2017), vol 33, issue 5, 584-602.

[8] See Mantelero, 'The future of consumer data protection in the E.U.' (n 7), p. 654–659. See also David Wright, 'A framework for the ethical impact assessment of information technology (2011) 13(3) Ethics and Information Technology 199–226; Paul M. Schwartz, 'Data Protection Law and the Ethical Use of Analytics' Data Protection Law and the Ethical Use of Analytics' (The Centre for Information Policy Leadership, 2011) <http://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/data_protection_law_and_the_ethical_use_of_analytics__paul_schwartzwhite_paper_2010_.pdf> accessed 18 December 2017.

[9] An important contribution in refining this proposal came from the Guidelines on Big Data issued by the Council of Europe in 2017, where a focus on the ethical and social consequences of data use was adopted by the members of the Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data. However, the discussion, which also engaged representatives of various stakeholders, outlined the difficulties in adopting a mandatory ethical and social assessment as part of the traditional data protection assessment. See Council of Europe, 'Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data', adopted in January 2017 and available at <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806ebe7a> accessed 4 May 2017. Disclosure: the author had the privilege to be appointed as consultant expert in drafting the text of the guidelines and to follow the discussion of the proposal by the representatives of the Parties to Convention 108 in the Bureau of the Consultative Committee of Convention 108 and the Plenary Meeting. Concern about the mandatory nature of the proposed assessment and its consequences in terms of use of resources was also expressed by several commentators, some belonging to sectors of industry, during the presentation of my proposal on a mandatory assessment in the European workshop on "Algorithmic decision making and human rights implications" (Alexander von Humboldt Institute for Internet and Society - Hans-Bredow-Institute for Media Research, Berlin 2017), the Amsterdam Privacy Conference (Amsterdam, 2015) and the 9th International Conference on Legal, Security and Privacy Issues in IT Law (Lisbon, 2014).