In: Emre Bayamlıoğlu, Irina Baraluic, Liisa Janssens and Mireille Hildebrandt (eds), BEING PROFILED:COGITAS ERGO SUM. 10 Years of Profiling the European Citizen, 2018: Amsterdam University Press, 42-45. DOI 10.5117/9789463722124/CH6.

Why data protection and transparency are not enough when facing social problems of machine learning in a big data context

*Anton Vedder**

Abstract

Neither data protection nor transparency are effective answers to large part of the social challenges coming along with Machine Learning in a Big Data context (henceforth MLBD). Data protection is not enough, simply because input and output data of MLBD need not qualify as personal data according to the definition stipulated in relevant legislation such as the GDPR, nor do they have to be about human beings at all, in order to affect humans in a way that may be questionable. Transparency falls short for another reason. Although the opacity due to technical and contextual dimensions are basic problems in attempts to cope with ethical and legal problems concerning MLBD, transparency can only play a role at the very first start. For the actual observation, articulation and solution of possible problems a broader normative framework and deliberations using the framework are needed.

Keywords: Profiling, KDD, Big Data, Machine Learning, ethics, law.

Introduction

Neither data protection nor transparency are effective answers to large part of the social challenges of Machine Learning in a Big Data context (MLBD). Data protection is not enough, because input and output data of MLBD need not qualify as personal data according to the definition stipulated in relevant legislation such as the General Data Protection Regulation (GDPR), nor do they have to be about human beings at all, in order to affect humans in questionable ways. Transparency falls short for another reason. Although the opacity due to technical and contextual dimensions is a basic problem for the solution of ethical and legal problems concerning MLBD (Vedder, Naudts 2017; Burrell 2016; Kroll et al. 2017), transparency can only play a role at the very first start of the deliberations. For the actual observation, articulation and solution of possible problems a broader normative framework (ethical or legal) is needed. What are the problems for which data protection and transparency do not suffice?

Problems concerning group profiling but not necessarily involving personal data

MLBD searches for patterns, correlations and commonalities hidden within large datasets. The resulting information can serve as an immediate differentiation ground for discriminating, amongst others, between (groups of) individuals. MLBD can group together individuals on an aggregate level based upon previously unknown shared commonalities found within large data sets. The groups thus created, might not be easily definable, nor in real practice easily recognizable, due to their seemingly random nature.

Where such groups are involved, the resulting group characteristic will often be *non-distributive*, meaning that the characteristic is primarily a characteristic of the group, while it can only be attributed to the individual members of the group in their quality of being members of that particular group rather than to those individuals in their own right. If the latter would be the case, the characteristic would be distributive (Vedder 1999). Take, for example, a group consisting of people who happen to have a red Opel Corsa and a Jack Russell Terrier. Suppose that MLBD shows that this group – coincidentally? – runs an on average relatively high risk of a specific incurable fatal disease. Then, Mary who currently happens to possess both a red Opel Corsa and the Jack Russell Terrier will share in this characteristic. If the characteristic is non-distributive and Mary would get rid of the Opel Corsa or the little dog, or of both, she might not be considered to be at high risk anymore. If the characteristic would have been distributive, she still would have been.

The attribution of a non-distributive property can be true or false depending on the perspective of the assessor. While a person may, as a member of a seemingly random group, run a statistically high risk of developing a disease, she may as an individual in her own right be the healthiest person on earth with a health prognosis for which many would envy her. Due to the non-distributivity in this case of the "being at high risk for the disease" property, both statements – "Mary is at high risk for developing the disease" and "Mary is the healthiest person in the world with excellent health prospects" can be simultaneously true from different perspectives. Their actual use will depend on the context and the perspective of the user (Vedder 1999, 258). The notion of 'data determinism' introduced by Edith Ramirez (2013, 7-8) helps to understand this issue. Seeing and understanding the outcomes of this form of MLBD will be difficult. The groups can often only be identified by those who defined them for a specific purpose, or those who obtain the results of the MLBD directly (Vedder 1999).

MLBD involving data on human beings can very easily result directly or indirectly in discrimination in the sense of prejudicial treatment or judgement. Over the last years, many scholarly works in law and ethics have been dedicated to intentional and unintentional discrimination by MLBD on the traditional grounds for unlawful discrimination: race/ethnic background, gender, sexual orientation, religious/ideological background, political convictions, health condition et cetera (Le Métayer and Le Clainche 2012; Barocas and Selbst 2016; Diakopoulos 2016; Kroll et al. 2017). What has received relatively little attention is that MLBD has the inherent potential to provide for a plethora of new grounds for discriminating among individuals and groups. Not only, however, it is difficult to recognize the exact grounds for differentiation or the definition of the groups distinguished. It often is also difficult to exactly understand the possible unfair or discriminatory character of the attribution of characteristics to individuals and groups if these do not coincide directly or indirectly with the traditional grounds for discrimination mentioned in law (Vedder 2000; Naudts 2017). What many people may intuitively grasp, however, is that adverse judgement (for instance stigmatization) or treatment based on the mere membership of a group or category of people comes very close to the traditional phenomena of discrimination, while judging or treating persons adversely on the basis of a group characteristic that is unknown to themselves or – due to its non-distributiveness – is dependent on their (seemingly random!) circumstances rather than on themselves in their own right may be unfair and go against the individuality of persons as a fundamental value in its own right.

Finally, group profiles may contain previously unknown and undesired information for all or some of the members of the group involved. Take again the example of Mary. Suppose, Mary happens to have a special interest in epidemiology. Her favourite journal publishes a special issue on the prevalence of as yet incurable fatal diseases. Mary reads about the remarkable discovery of people having a red Opel Corsa and a Jack Russell terrier who run a relatively high risk of developing the incurable fatal disease. Mary looks at the dog, then, through the window, at her car, and trembles…

Ever since the rise of predictive medical testing and screening in the 1980’s, patient law in many countries provides people with a right not to know unintended side-results of testing and screening. Should people be protected in similar ways against the exposure to possibly undesired information that results from BDA or should bad news disclosure by MLBD be considered as mere collateral damage?

Distributive group profiles can sometimes qualify as personal data and therefore fall within the scope of data protection laws. This is also the case with non-distributive profiles as soon as they are applied to demonstrable individual persons. Concerning the latter, one should be aware that application to individuals is often not part of the automatic process itself, but an additional step in which humans interpret the outcomes of that process and take decisions on the basis of it. If data protection laws apply, these may provide legal solutions for the problems mentioned. [1] When group profiles cannot be considered as personal data, the problems remain and must be dealt with in another manner.

Broader framework

In the GDPR, transparency is defined as a responsibility of the controllers towards the legislator and towards the data-subject. The responsibilities towards the data-subject receive most attention and a high degree of specification.[2] Of course, this will make some sense in the case of MLBD involving personal data.

In MLBD without personal data, such an obvious addressee is lacking. More importantly, as may have become clear in the previous sections, complexity of the underlying technological process is only one issue to grapple with. The perspective-dependence of the recognisability of profiles is another, while the involvement of a very broad set of possibly relevant values, rights and interests, ranging from fair access to the MLBD infrastructure and information, over individuality and justice, to a right not to know and the rights to data protection and privacy is further adding to the difficulties of finding a satisfactory approach. For that approach transparency is not the end, it is just the beginning.

Given these particularities, a regulatory regime that in the first place enables deliberations about the possible impacts on humans would be desirable. Such a regime could lay down a basis for those deliberations by assigning accountabilities to the parties that could be identified as the controllers of the BDA data processing. It could stipulate mechanisms of for instance processing records, impact assessments, transparency rules, and obligations to report to data authorities – not merely *personal* data authorities. In order to effectively identify possible rights, legitimate interests, and values affected by data processing activities, broadly composed authorities seem to be called for. In order to help especially with the articulation of possible moral and legal problems, a broadly composed authority should not only consist of representatives from various possible stakeholders, such as corporations and NGOs, but also of ethicists and lawyers.

Notes

* Anton Vedder is a professor of IT Law at KU Leuven, board member of the Centre for IT and IP Law (CiTiP) in Leuven, and program director of the master's program of IP and ICT Law of KU Leuven in Brussels.

[1] The relevant right not to be subject to automated decision-making (Art. 22 GDPR; Recital 71 GDPR) cannot be discussed in this paper for reasons of conciseness.

[2] Art. 12 GDPR.

References

Barocas, Solon, and Andrew D. Selbst. 2016. "Big Data's Disparate Impact" California Law Review 104: 671–732.

Burrell, Jenna. 2016. "How the machine 'thinks': Understanding opacity in machine learning algorithms" Big Data & Society 3(1): 1-12.

Diakopoulos, Nicholas. 2016. "Accountability in Algorithmic Decision Making" Communications of the ACM, 59(2): 56-62.

Le Métayer, Daniel, and Julien Le Clainche, 2012. "From the Protection of Data to the Protection of Individuals: Extending the Application of Non-Discrimination Principles." In European Data Protection: In Good Health?, edited by Serge Gutwirth, Ronald Leenes, Paul De Hert, and Yves Poullet, 315-29. Dordrecht Heidelberg London New York: Springer.

Kroll, Joshua, Joanna Huey, Solon Barocas , Edward W. Felten, Joel R. Reidenberg, David G. Robinson, and Harlan Yu. 2017. "Accountable Algorithms." University of Pennsylvania Law Review 165(3): 633-705. https://scholarship.law.upenn.edu/penn_law_review/vol165/iss3/.

Naudts, Laurens. 2017. "Fair or Unfair Differentiation? Luck Egalitarianism as a Lens for Evaluating Algorithmic Decision-making." Data for Policy. London, 6-7 September 2017. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3043707.

Ramirez, Edith. 2013. "Keynote Address at the Tech. Policy Inst. Aspen Forum, The Privacy Challenges of Big Data." http://www.ftc.gov/sites/default/files/documents/public_statements/privacy-challenges-big-data-view-lifeguard%E2%80%99s-chair/130819bigdataaspen.pdf.

Vedder, Anton. 1999. "KDD: The challenge to individualism." Ethics and Information Technology 1: 275-28

Vedder, Anton. 2000. "Medical data, new information technologies and the need for normative principles other than privacy rules." In Law and Medicine, edited by Michael Freeman and Andrew D. E. Lewis, 441-59. Oxford: Oxford University Press.

Vedder, Anton, and Laurens Naudts. 2017. "Accountability for the use of algorithms in a big data environment." International Review of Law, Computers & Technology 31(2): 206-24.