Digital Investigation xxx (2015) 1–6

Contents lists available at ScienceDirect

Digital Investigation

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

Data protection in a big data society. Ideas for a future regulation

Alessandro Mantelero [a, 1], Giuseppe Vaciago [b, 2, *]

[a] Polytechnic University of Turin, Corso Duca degli Abruzzi, 24, 10129 Turin, Italy
[b] University of Insubria, Via Sant'Abbondio, 22100 Como, Italy

ARTICLE INFO

Article history:
Received 24 September 2015
Accepted 28 September 2015
Available online xxxx

Keywords:
Algorithms
Big data
Privacy
Data protection
Profiling
Decisional model
Social control
Discrimination
Reasonable suspicion
Fourth amendment

ABSTRACT

Big data society has changed the traditional forms of data analysis and created a new predictive approach to knowledge and investigation. In this light, it is necessary to consider the impact of this new paradigm on the traditional notion of data protection and its regulation.

Focussing on the individual and communal dimension of data use, encompassing digital investigations, the authors outline the challenges that big data poses for individual information self-determination, reasonable suspicion and collective interests. Therefore, the article suggests some innovative proposals that may update the existing data protection legal framework and contribute to make it respondent to the present algorithmic society.

© 2015 Elsevier Ltd. All rights reserved.

Introduction

In order to briefly depict the main challenges associated with big data analytics and suggest possible regulatory solutions, it is necessary to consider two different scenarios: the individual dimension of big data use (micro scenario) and its collective dimension (macro scenario). The first dimension concerns the way in which big data analytics affect individuals' chances of making conscious decisions about the use of their personal information, and affect individuals' expectations of privacy.[3] The second dimension focuses on the social impact of the classification approach that characterizes the logic of big data analytics and their use for decisional purposes.[4]

Regarding to the micro scenario, an interesting piece of speculative fiction written by Sara Watson envisions a future domestic world dominated by intelligent devices (IoT), which take care of their users and make decisions in the interest of their users (Watson, 2014). Obviously, although this is not considered in Watson's piece, users have received detailed information about the terms and conditions of these devices and about their privacy policies (with links to third parties privacy policies, terms and conditions, etc.).[5]

* Corresponding author.
E-mail addresses: alessandro.mantelero@polito.it (A. Mantelero), giuseppe.vaciago@uninsubria.it (G. Vaciago).

[1] Alessandro Mantelero is author of Sections Introduction, The micro scenario: beyond the "notice and consent", The macro scenario: beyond the individual dimension of data protection, and Conclusion.

[2] Giuseppe Vaciago is author of Section Reasonable suspicion and expectations of privacy in the Big Data era.

[3] See below paras. 2.1 and 2.2.

[4] See below para 3.

[5] See e.g. Fitbit Privacy Policy (August 10, 2014) <http://www.fitbit.com/uk/privacy#PrivacyPolicy> accessed August 31, 2015.

http://dx.doi.org/10.1016/j.diin.2015.09.006
1742-2876/© 2015 Elsevier Ltd. All rights reserved.

Please cite this article in press as: Mantelero A, Vaciago G, Data protection in a big data society. Ideas for a future regulation, Digital Investigation (2015), http://dx.doi.org/10.1016/j.diin.2015.09.006

In the near future, millions of sensors and devices will be connected and able to interact with each other in order to collect data about users and predict individual behaviour, support, anticipate and, in some cases, nudge users' decisions (Thaler and Sunstein, 2008; Howard, 2015). Unread legal notices (Mantelero, 2015a, 2015b; Solove, 2013; Brandimarte et al., 2010; Turow et al., 2007), and user's consent driven by must-have devices or services, will legitimate personal data use, as already happens with regard to hundreds of apps, online services, loyalty cards, etc.

Against this background, two questions arise: is this the end of the traditional idea of individual self-determination with regard personal data? Should big data analytics lead rule-makers to reconsider the way in which the idea of self-determination has been embedded in the regulation of data protection OR data protection regulations?

From a different perspective, it should be noted that, in the big data context, decisions concerning individuals are assumed on the basis of group-profiling technologies (Hildebrandt and Gutwirth, 2008) and predictive knowledge provided by analytics (Mayer-Schönberger and Cukier, 2013; Bollier, 2010). Complicated and obscure data processes (Pasquale, 2015) drive decisions concerning individuals, which become mere units of one or more groups generated by analytics (FTC, 2014). Moreover, in the field of data processing for law and enforcement purposes, this poses serious questions in terms of interfering with constitutional liberties and the principle of reasonable suspicion.[6]

Focussing on the macro scenario, the algorithmic approach is creating "a new truth regime" (Rouvroy, 2014), where primetime television usage or propensity to buy general merchandise become predictor variables that are used by insurance companies to asses risks associated to segments of their clients (FTC, 2014; Garla et al., 2013). In the same way, the neighbourhood's general credit score[7] affects the chance to access to credit of the individuals living in a certain area or, in other circumstances, mere social connections with authors of serious crimes are sufficient to define lists of potential offenders (Gorner, 2013).

All these decisional models disregard the specific case and its peculiar aspects, since they adopt a classification approach in mapping our society. Nevertheless, "a map is not the territory" (Korzybski, 1933) and the logic of the author of the map, the way in which the territory is represented, as well as the potential errors of the representation, may produce different and, in some cases, biased results (Robinson and Yu, 2014; National Immigration Law Center, 2013; Gandy, 2000).

For these reasons, it is important that people affected by these representations of society are actively involved in the process and are adequately protected against biased representations or lack of accuracy in the portrayal of groups of individuals.

Moreover, a classification approach may also induce "self-fulfilling cycles of bias" and consequent discriminatory effects. This is the case of predictive policing software, which may put the spotlight on specific territorial areas and induce police departments to allocate more resources to these areas. The potential outcomes is a rise in crime detection at local level that reinforces the original prediction, while a reduced police presence in the remaining districts lowers crime detection in these areas and apparently confirm the positive prediction for these districts (Koss, 2015).

In the light of the above, a second series of questions rises: is the traditional individualistic model of data protection still adequate to face the new predictive society? In a society where group profiling is used for decision purposes, should rule makers consider the supra-individual and collective dimension of data processing?

The micro scenario: beyond the "notice and consent"

The purpose specification principle and the use limitation principle are the traditional pillars of data protection regulations and, with regard to consumer data protection, the so-called "notice and consent" model (i.e. an informed, freely given and specific consent) represents one of the most used mechanisms to legitimate data processing (Article 29 Data Protection Working Party, 2011; Van Alsenoy et al., 2014; Mayer-Schönberger, 1997; Brownsword, 2009; The White House, 2012; Ohm, 2013; Cranor, 2012).[8] Nevertheless, the "transformative" use of big data (Tene and Polonetsky, 2012) contrasts with this legal framework.

Since analytics are designed to extract hidden or unpredictable inferences and correlations from datasets, it becomes difficult to define *ex ante* the purposes of data processing (Article 29 Data Protection Working Party, 2013) and be compliant with the limitation principle. Therefore, a notice that explains all the possible uses of data is hard to be given to data subjects at the time of the initial data collection.

Not only descriptions of the purposes of data processing (notices, privacy policies) are becoming more and more "evanescent". The same idea of self-determination embodied in data subject's consent is also challenged by an increasing concentration of information in the hands of a few entities ("data barons"), both public and private (Cate and Mayer-Schönberger, 2013), and its consequences in terms of technological and social lock-in effects (Mantelero, 2014).

Finally, the complexity of data processing and legalese wording lead users to disregard privacy policies and provide their data on the basis of the mere interest in obtaining specific services or on the basis of the reputation of service providers (Mantelero, 2015a, 2015b).

For these reasons, it is necessary to reconsider the existing regime based on data subject's (pseudo) self-determination and accept that data subjects are often not able to take meaningful decisions about the use of their

[6] See below para 2.1.

[7] This score predicts credit risks referring to individuals that live in a small geographic area and is defined on the basis of aggregate credit scores.

[8] See art. 2 (h), Directive 95/46/EC and art. 4 (8) PGDPR-LIBE.

Please cite this article in press as: Mantelero A, Vaciago G, Data protection in a big data society. Ideas for a future regulation, Digital Investigation (2015), http://dx.doi.org/10.1016/j.diin.2015.09.006

Download English Version:

https://daneshyari.com/en/article/6884528

Download Persian Version:

https://daneshyari.com/article/6884528

Daneshyari.com