Revista de Bioética y Derecho
Perspectivas Bioéticas
www.bioeticayderecho.ub.edu - ISSN 1886-5887

DOSSIER BIG DATA

Towards a big data regulation based on social and ethical values. The guidelines of the Council of Europe

Hacia una regulación de los datos masivos basada en valores sociales y éticos. Las directrices del Consejo de Europa

Cap a una regulació de les dades massives basada en valors socials i ètics. Les directrius del Consell d'Europa

ALESSANDRO MANTELERO *

OBSERVATORI DE BIOÈTICA I DRET DE LA UNIVERSITAT DE BARCELONA

La Revista de Bioética y Derecho se creó en 2004 a iniciativa del Observatorio de Bioética y Derecho (OBD), con el soporte del Máster en Bioética y Derecho de la Universidad de Barcelona: www.bioeticayderecho.ub.edu/master. En 2016 la revista Perspectivas Bioéticas del Programa de Bioética de la Facultad Latinoamericana de Ciencias Sociales (FLACSO) se ha incorporado a la Revista de Bioética y Derecho.

* Alessandro Mantelero. Aggregate Professor of Private Law at Politecnico di Torino. Italy. E-mail: alessandro.mantelero@polito.it.

Abstract

This article discusses the main provisions of the Guidelines on big data and data protection recently adopted by the Consultative Committee of the Council of Europe. After an analysis of the changes in data processing caused by the use of the predictive analytics, the author outlines the impact assessment model suggested by the Guidelines to tackles the potential risks of big data applications. This procedure of risk-assessment represents a key element to address the challenges of Big Data, since it goes beyond the traditional data protection impact assessment encompassing the social and ethical consequences of the use of data, which are the most important and critical aspects of the future algorithmic society.

Keywords: big data; data protection; privacy impact assessment; Council of Europe.

Resumen

Este artículo ofrece un análisis de las principales disposiciones de las Directrices sobre datos masivos y protección de datos recientemente aprobadas por el Comité Consultivo del Consejo de Europa. Después de un examen de los cambios ocurridos en el procesamiento de datos por el uso de la analítica descriptiva, el autor describe el modelo de evaluación de impacto que se sugiere en las Directrices para encarar los riesgos potenciales de las aplicaciones que utilizan la analítica de datos masivos. Este procedimiento de evaluación de riesgos es un elemento clave para gestionar los datos masivos, ya que no se limita a la evaluación tradicional del impacto en la protección de datos sino que abarca también las consecuencias sociales y éticas de su uso, aspectos que son importantes y críticos de la futura sociedad algorítmica.

Palabras clave: datos masivos; protección de datos; evaluación de impacto de la protección de datos; Consejo de Europa.

Resum

Aquest article ofereix una anàlisi de les principals Directrius sobre dades massives i protecció de dades recentment aprovades pel Comitè Consultiu del Consell d'Europa. Després d'un examen dels canvis ocorreguts en el processament de dades mitjançant l'ús de l'analítica descriptiva, l'autor descriu el model d'avaluació d'impacte que se suggereix en les Directrius a fi d'encarar els riscos potencials de les aplicacions que utilitzen l'analítica de dades massives. Aquest procediment d'avaluació de riscos és un element clau per gestionar les dades massives, ja que no es limita a l'avaluació tradicional de l'impacte en la protecció de dades sinó que inclou també les conseqüències socials i ètiques del seu ús, aspectes crítics de la futura societat algorítmica.

Paraules clau: dades massives; protecció de dades; avaluació d'impacte de la protecció de dades; Consell d'Europa.

1. Introduction

The "Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data" (hereinafter Guidelines), adopted by the Consultative Committee of Convention 108 in January 2017 represents the first international guidance on the use of big data, which is a form of data processing that rises significant questions concerning the protection of fundamental rights.[1]

The role of individual self-determination with regard to the use of data and the risk assessment of big data applications represent two of the main aspects of the Guidelines and, in this regard, the Council of Europe suggests novel solutions to address the challenges of the new data processing paradigm based on analytics.

In light of the above, this article is divided into two main parts: the second section describes the impact of the new model of predictive analysis on the main principles of data protection regulation, while the third section discusses the provisions of the Guidelines and focuses on the risk assessment procedure adopted by the Consultative Committee.

2. Big Data: a new paradigm of data processing

The advent of big data analytics[2] has suggested a new paradigm in portraying our societies, where the traditional approach adopted in statistical studies is complemented or replaced by predictive analysis. Data visualization has played a relevant role in this change, making it possible real-time analysis of streams of data and prediction of their future trends.[3] Moreover, algorithms are used to discover hidden correlations between the variables that characterize large datasets.

---

[1] Council of Europe - Consultative Committee of Convention 108. *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*. 2017. Available at: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806ebe7a> (accessed 4 March 2017).

[2] This term is used to identify computational technologies that analyse large amounts of data to uncover hidden patterns, trends and correlations. According to the European Union Agency for Network and Information Security (ENISA), the term Big Data analytics "refers to the whole data management lifecycle of collecting, organizing and analysing data to discover patterns, to infer situations or states, to predict and to understand behaviours". See ENISA, 2014.

[3] See Bollier, 2010.

Like in the past, with regard to the traditional statistical studies, this kind of analysis is not exclusively carried on for mere scientific purposes, but is mainly conducted to provide insights about individuals and society to decision-makers. This relationship between data processing and the adoption of strategic decisions —which affect individuals in different contexts (e.g. financial services, healthcare services, urban planning)— has become progressively stronger by reason of the increased availability of data as a result of the so-called datification process.

This is an ongoing process to "capture quantifiable information"[4], which aims to transform reality into data.[5] In this sense, even human beings can be considered as aggregates of information,[6] which represent their private or public identities. This relationship between individual nature and personal data has been recognised by the courts in various decisions concerning the right to privacy and —more recently— the right to be forgotten.[7]

Nevertheless, the complexity of human beings cannot be reduced to a mere aggregate of data, since they are primarily persons. For this reason, the information referring to them are not neutral or raw data that, in the present digital economy, can be freely used and assimilated to mere goods, regardless they are qualified as private or common. Personal data, as well as the other forms of expression of a given person, are part of her identity and, therefore, should be safeguarded within the framework of personality rights and fundamental rights and freedoms.[8]

According to this theoretical framework, individual name, image and social identity (i.e. reputation and honour) have been recognised as attributes of human beings and safeguarded by law over the centuries. Against this scenario, the right to the protection of personal data represents the most recent development of the category of personality rights, since its origin is strictly related to the early stages of the digitalisation of information, which is the foundational stone of the present process of datafication and of our (big) data-driven society.

---

[4] See Mayer-Schönberger and Cukier, 2013, 78. See also Lycett, 2013; Ericsson, 2014.

[5] An early step in this strategy of datafication was made by the Auto-ID Center which, set up in 1999, was a not-for-profit consortium created with the aim "to develop a system for using the Internet to identify goods anywhere in the world".

[6] See Floridi, 2014, 96-98 ("the fourth revolution has brought to light the intrinsically informational nature of human identity") and Mayer-Schönberger and Cukier, 2013, 93 ("Datafication is not just about rendering attitudes and sentiments into an analysable form, but human behavior as well").

[7] See Court of Justice of the European Union, 13 May 2014, case C-131/12, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González. Available at: http://curia.europa.eu (accessed 4 March 2017).

[8] On the notion of personality right see, inter alia, Resta, 2014; Cannataci, 2008; Alpa and Resta, 2006.

Like the right to privacy was the answer to the assault to the private sphere conducted by the penny press at the end of the XIX century,[9] the right to the protection of personal information is the answer given by legislators in the '70s to the rising citizens' concern about the risks of new forms of computer-based social control. Over the years, this risk has changed its nature and source, from the original concern about government surveillance and economic exploitation of personal information to the present public and private partnership in surveillance and the adoption of information-based predictive decision-making systems.

This increasing exploitation of personal information and the development of data processing technologies led legislators to adopt different procedural regulations on data protection and, since the so-called second generation of data protection laws,[10] the right to the protection of personal information was placed in the wider context of fundamental rights. In this sense, the Convention 108 on the Protection of Individuals with regard to Automatic Processing of Personal Data, adopted by the Council of Europe in 1981, considers data protection as an expression of the broader right to privacy.[11]

Although nowadays the right to data protection is —more correctly— considered as an autonomous right, which differs from the right to privacy, the qualification provided by the Convention 108 was consistent with the theoretical framework at that time. Anyway, the most important element of this qualification consists in the level of protection accorded to personal information. In this sense, the protection of personal information is put at the highest level, in the context of fundamental rights.

More recently, the Charter of Fundamental Rights of the European Union has expressly recognised the "right to the protection of personal data"[12] as an autonomous right, different from the right to respect for private and family life, and has grant to everyone "the right to the protection of personal data concerning him or her".

Against this scenario, the European model of data protection is based on the safeguard of the data subject's individual right to control "his or her personal data and the processing of such data".[13] This is in line with the original notion of data protection as data control that was

[9] See Schudson, 1992; Mantelero, 2007, ch. 1.

[10] See Mayer-Schönberger, 1997, 219-241.

[11] See Article 1, Convention 108. See also Parliamentary Assembly of the Council of Europe, Recommendation 509 (1968) on Human rights and modern scientific and technological developments (1968).

[12] See Charter of Fundamental Rights of the European Union, Article 8.

[13] See the Preamble of the Draft Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data (hereafter Draft Modernised Convention 108). Consolidated text of the modernisation proposals of

elaborated by legal scholars in the '70s,[14] which led legislators to adopt a model of protection primarily focused on the individual dimension.[15]

Nevertheless, both this idea of control over personal information and the notion of data protection as an individual right show their limits in the context of the present forms of data processing based on analytics. In this sense, on the one hand, the traditional paradigm of "notice and consent" does not adequately address the complexity of data processing[16] and, on the other hand, data collection and analysis are even more focused on the collective dimension, due to their attempt to understand, predict and orient the behaviour of groups of persons.

The use of big data analytics creates "a new truth regime",[17] in which general strategies are adopted on a large scale on the basis of descriptions of society generated by algorithms,[18] which predict future collective behaviour.[19] These strategies are then applied to specific individuals, given the fact that they are part of one or more groups generated by analytics.[20]

Nevertheless, this "categorical" approach characterizing the use of analytics[21], leads decision-makers to adopt common solutions for individuals belonging to the same cluster generated by analytics, without considering each individual *per se*, her unique identity that may differ from the stereotypical models created by algorithms.

Convention 108 finalised by the CAHDATA (meeting of 15-16 June 2016). Available at: http://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806af964 (accessed 6 March 2017). See also Recital no. 7 of the Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) ("[...] Natural persons should have control of their own personal data. Legal and practical certainty for natural persons, economic operators and public authorities should be enhanced").

[14] See Westin, 1970, 158-168, 298-326; Breckenridge, 1970, 1-3. See also Solove, 2008, 4-5.

[15] See Bygrave, 2004, 324-325; Solove, 2008, ch. 2. See also Bennett and Raab, 2003, ch. 1; Post, 1989; Cohen, 2000, 1426-1428. The collective dimension of this right has been recognised in the U.S. and Europe, but protected mainly indirectly, as an aggregation of individual privacy issues and not as an autonomous dimension. See Mantelero, 2016.

[16] See Mantelero, 2014; Rubinstein, 2013.

[17] See Rouvroy, 2014, 9.

[18] Pasquale, 2015; Mayer-Schönberger and Cukier, 2013; Rubinstein, 2013; Bollier, 2010.

[19] See Pasquale, 2015; Mayer-Schönberger and Cukier, 2013; Bollier, 2010; McKinsey Global Institute, 2011. See also Bellagio Big Data Workshop Participants, 2014; Boyd and Crawford, 2011; Boyd and Crawford, 2012; Tene and Polonetsky, 2012.

[20] Federal Trade Commission, 2014, 20 and Appendix B; Bollier, 2010; Hildebrandt, 2006.

[21] See also Vedder, 1997, 215–226.

In this sense, the use of big data analytics to support decisions exceeds the boundaries of the individual dimension and assumes a collective dimension,[22] with potential harmful consequences for some groups.[23] Therefore, the potential prejudice is no longer circumscribed to the well-known privacy-related risks (e.g. illegitimate use of personal information, data security), but it also concerns the negative impact on other fundamental rights, such as the right to non-discrimination.[24]

Against this background, the adoption of a fundamental rights impact assessment has been proposed by the United Nations Special Rapporteur on the right to privacy (Joe Cannataci), but it seems still far from being developed at global level. Nevertheless, a first step in this direction is the Privacy, Ethical and Social Impact Assessment (PESIA),[25] which has been adopted by the Council of Europe in its Guidelines on Big Data. This model of assessment goes beyond the traditional impact assessment focused on data quality and data security, since it also encompasses the societal consequences of data uses and the analysis of their potential conflicts with ethical values.

Moreover, the intent of the Guidelines to take into account the collective dimension of the use of personal information[26] is not only evident in the scope of PESIA, but also in the participatory model adopted in the assessment procedure, which aims to give voice to the different stakeholders potentially affected by data processing.[27]

Although there are several provisions of these Guidelines that suggest novel approaches in protecting personal information and fundamental rights in the big data environment (e.g. the provisions concerning the role of the human intervention in Big Data-supported decisions[28]) the

---

[22] See Mantelero, 2017, 139-158. See also Vedder, 1997.

[23] See also Crawford et al., 2013, 6-7; Boyd, Levy, and Marwick, 2014, 56.

[24] With regard to the right to non-discrimination, see also Article 11 of the UNESCO Universal Declaration on Bioethics and Human Rights. See also The White House, Executive Office of the President, 2014; Zarsky, 2013, 1510-1513; Vedder, 1997; Barocas and Selbsr, 2016. See also European Parliament. European Parliament resolution of 14 March 2017 on fundamental rights implications of big data: privacy, data protection, non-discrimination, security and law-enforcement (2016/2225(INI)). 2017. Available at: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2017-0076+0+DOC+XML+V0//EN&language=EN (accessed 16 March 2017).

[25] Regarding the PESIA model, see also the H2020 project "VIRT-EU: Values and ethics in Innovation for Responsible Technology in Europe". Available at: http://www.virteuproject.eu/ (accessed 16 March 2017). With regard to the ethical assessment in research and innovation, see Shelley-Egan et al., 2014, 42-44.

[26] See Mantelero, 2016.

[27] A similar participatory approach is also adopted by the UNESCO Universal Declaration on Bioethics and Human Rights (Article 18).

[28] See Guidelines, Section IV, para 7.

risk assessment procedure represents the core of the Guidelines. In this sense, the risk assessment procedure[29] plays a central role with regard to different elements concerning the social and ethical dimensions of data uses, data subject's self-determination, the relationships between the purposes of data collection and data uses,[30] the by design approach[31] and the use of anonymous data[32] and open data.[33]

3. The PESIA model in the context of the Guidelines of the Council of Europe

The Guidelines adopted by the Consultative Committee of Convention 108 are non‑legally binding practical and operative instructions provided by the Council of Europe to the Parties of the Convention. This is in line with the regulatory model of the Council of Europe, which adopts a principle-based approach complemented by guidelines that provide a sector-specific interpretations of the principles of the Convention. Through the adoption of its guidelines, the Consultative Committee aims to facilitate an effective application of the principles of the Convention.[34] In this sense, the Guidelines are primarily addressed to data controllers and data processors.

The main limit of these Guidelines regards their scope, since they concern a given technology in general (i.e. big data), rather than its application in a given sector (e.g. healthcare services). For this reason, the reached result is not completely satisfactory for various operators, who would like to have specific answers with regard to the applications of analytics in given fields.

This outcome is inevitable due to the wide range of big data applications, but the awareness of this limit led the Consultative Committee of the Convention to recognise in the Guidelines that "given the expanding breadth of Big Data in various sector-specific applications, the present

---

[29] A central role to risk assessment and risk management is also recognised by the UNESCO Universal Declaration on Bioethics and Human Rights, see Article 20.

[30] See Guidelines, Section IV, para 3.1 ("Exposing data subjects to different risks or greater risks than those contemplated by the initial purposes could be considered as a case of further processing of data in an unexpected manner"). On the purpose limitation principle, see also Article 9 of the UNESCO Universal Declaration on Bioethics and Human Rights.

[31] See Guidelines, Section IV, para 4.

[32] See Guidelines, Section IV, para 6.

[33] See Guidelines, Section IV, para 8.

[34] See Guidelines, Section II (Scope).

Guidelines provide a general guidance, which may be complemented by further guidance and tailored best practices on the protection of individuals within specific fields of application of Big Data (e.g. health sector, financial sector, public sector such as law enforcement)".[35]

Apart from this limit, the Guidelines represent an important step in regulating big data use, since the issues concerning analytics are not specifically addressed by the most recent data protection regulations, such as Regulation (EU) 2016/679.[36]

The main instrument to address the potential negative impact of big data on individuals and society is represented by risk management. In defining the key principles for risk management, the Guidelines suggest the adoption of a precautionary approach to regulating data protection in the field of big data.[37]

The precautionary approach is adopted with regard to any new application of technology that may produce potential risks for individuals and society, which cannot be exactly calculated or quantified in advance.[38] In this sense, the obscurity of big data uses, the uncertainty characterising the concrete applications of data science and the potential high impact of big data analytics on essential aspects of society may warrant the adoption of this approach as the default setting.[39]

Regarding the scope of risk assessment, while in the Regulation (EU) 2016/679 – as well as in Directive 95/46/EC – it mainly focuses on data security and data quality, in the Guidelines the Data Protection Impact Assessment evolves into a broader and more complex Privacy, Ethical and

---

[35] See Guidelines, Section II (Scope).

[36] See Mayer-Schönberger and Padova, 2016, 326, 332. See also Moerel, 2014.

[37] See Guidelines, Section IV, para 2.1 ("Given the increasing complexity of data processing and the transformative use of Big Data, the Parties should adopt a precautionary approach in regulating data protection in this field"). On the distinction between the precautionary approach and the precautionary principle, see Peel, 2004.

[38] See Guidelines, Section IV, para 2.1 ("Given the increasing complexity of data processing and the transformative use of Big Data, the Parties shall adopt a precautionary approach in regulating data protection in this field"). Only few contributions in law literature take into account the application of the precautionary approach in the field of data protection, see Costa, 2012; Gonçalves, 2017; Gellert, 2015. See also Council of Europe, 2005, para 10; Pieters, 2011, 455. On the precautionary approach in data protection, see also Narayanan, Joanna and Felten, 2016, 357-385; Böröcz, 2016, 476-477; Raab, and Wright, 2012, 364; Lynskey, 2015, 83; Raab, 2004.

[39] Moreover, in Section IV, Paragraph 2.2, the Guidelines require data controllers to adopt "preventive policies" to adequately address and mitigate the potential risks related to the use of big data analytics. This is consistent with Article 8bis (2) of Draft Modernised Convention 108, which focuses on risk analysis and requires that data processing is designed "in such a manner as to prevent or minimise the risk of interference with […] rights and fundamental freedoms". On the precautionary principle, see also Tosun, 2013; Aven, 2011; Stirling and Gee, 2002.

Social Impact Assessment (PESIA) to encompasses the societal consequences of data uses mentioned above.[40]

Obviously, an assessment concerning the compliance of data use with ethical and social values is more complicated than the traditional data protection assessment, since social and ethical values are necessarily context-based and change from one community to another.[41] In this sense, the Guidelines recognise the relative nature of social and ethical values.[42]

To address this issue, the Guidelines urge both data controllers and data processors to use personal information in a manner that is not in conflict with the "ethical values commonly accepted in the relevant community or communities and should not prejudice societal interests, values and norms".[43]

Moreover, in order to provide a general benchmark of values to be taken into account in conducting the PESIA, the Guidelines identify "the common guiding ethical values" in the international charters of human rights and fundamental freedoms, such as the European Convention on Human Rights.[44]

Nevertheless, international charters and ethical values commonly accepted in a community[45] may only provide a high-level guidance. For this reason, the Guidelines combine this general suggestion with a more tailored option, represented by "ad hoc ethics committees",[46] which should identify the specific ethical values to be safeguarded with regard to a given use of data, providing more detailed and context-based guidance for risk assessment.

In conclusion, the PESIA model is based on a system of values which is organised on three different layers with a progressive granularity: the "common guiding ethical values" provided by the international charters of human rights, the values and social interests of given communities

---

[40] Definition of the PESIA model is still in its infancy, see above fn. 25.

[41] See Guidelines, Section IV, para 1.

[42] On the different ethical values and their harmonization, with regard to ethics assessment of research and innovation, see Bray et al., 2015.

[43] Guidelines, Section IV, para 1.2.

[44] See also, in this sense, Wright, 2011, 201–202.

[45] On the importance of cultural diversity and pluralism see also Article 12 of the UNESCO Universal Declaration on Bioethics and Human Rights.

[46] See Guidelines, Section IV, para 1.3 ("the assessment of the likely impact of an intended data processing described in Section IV.2 highlights a high impact of the use of Big Data on ethical values, controllers could establish an ad hoc ethics committee, or rely on existing ones, to identify the specific ethical values to be safeguarded in the use of data"). With regard to the role played by ethics committees, see also Article 19 and 22.2 of the UNESCO Universal Declaration on Bioethics and Human Rights.

and the tailored application of these values provided by ethics committees, which focuses on a given use of data.

Regarding the procedure of assessment, the Guidelines adopt the traditional circular scheme that characterises the risk-assessment,[47] which is divided into four stages:[48] 1) identification of risks, 2) analysis of the potential impact of these risks, 3) selection and adoption of the measures to prevent or mitigate the risks, 4) regular review of the effectiveness of the measures.[49]

With regard to the measures to prevent or mitigate the risks, the Guidelines also make an explicit reference to by-design and by-default solutions.[50] The existing strict relationship between risk assessment and solutions by design implies that any change in the nature of the assessment affects the architectural solutions adopted. Thus, the multiple impact assessment suggested by the Council of Europe necessarily leads data controller to consider a broader range of by-design solutions to mitigate the additional ethical and social concerns.[51]

Given the complexity of this assessment and the various aspects that should be taken into account, it cannot be conducted only by data protection experts, but "should be carried out by persons with adequate professional qualifications and knowledge to evaluate the different impacts, including the legal, social, ethical and technical dimensions".[52]

Finally, the collective dimension of the potential impact of the use of data leds the Consultative Committee to encourage the involvement of all the relevant stakeholders, giving voice to the different groups of persons potentially affected by the use of data.[53]

---

[47] See, e.g., CNIL, 2015.

[48] See Guidelines, Section IV, para 2.5.

[49] See Guidelines, Section IV, para 2.9. Moreover, to enable subsequent control of the effective level of compliance, data controllers should document both the risk assessment and the measures adopted, see Guidelines, Section IV, para 2.10. See also Koivisto and Douglas, 2015.

[50] These two kinds of solutions, which are also mentioned in Regulation (EU) 2016/679, represent a key component of the modern risk-based approach to data protection.

[51] See Wright, 2011.

[52] See Guidelines, Section IV, para 2.6. See also, with regard to the Regulation (EU) 2016/679, Article 29 Data protection Working Party, 2017.

[53] See Guidelines, Section IV, para 2.7 ("With regard to the use of Big Data which may affect fundamental rights, the Parties should encourage the involvement of the different stakeholders (e.g. individuals or groups potentially affected by the use of Big Data) in this assessment process and in the design of data processing"). See also Wright, and De Hert, 2012, 467. On ethical values and stakeholder analysis, see Shelley-Egan et al., *SATORI Deliverable D2.2*, 2015; Shelley-Egan et al. *Ethical Assessment of Research and Innovation*, 2015, 28-29.

4. Conclusions

The Guidelines on the protection of individuals with regard to the processing of personal data in the big data context represent the first attempt to provide practical guidance to address the issues related to the use of big data and to reduce their potential negative impacts on society.

These Guidelines, as well as the Privacy, Ethical and Social Impact Assessment that they outline, confirm the importance of going beyond the mere declarations of fundamental rights and to provide practical instructions and operative methodologies to put them into practice.

In light of the above, these Guidelines confirm the attention of part of our society to the potential implications of the use of data, adopting a viewpoint that refuses vague notions (such as "citizen empowerment" or "digital sovereignty") often used to provide a mere formal protection to personal data, but looks ahead to concrete and robust forms of assessment of the compliance of data use with the ethical and social values accepted in a given community.[54]

Bibliography

- ALPA, G. and RESTA, G. *Le Persone e la Famiglia. 1. Le persone fisiche e i diritti della personalità*. UTET, Torino, 2006.
- ARTICLE 29 DATA PROTECTION WORKING PARTY. *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*. 2017. Available at: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137 (accessed 13 April 2017).
- AVEN, T. "On Different Types of Uncertainties in the Context of the Precautionary Principle", *Risk Analysis* 31(10), 2011:1515–1525. Available at: http://onlinelibrary.wiley.com/doi/10.1111/j.1539-6924.2011.01612.x/abstract (accessed 8 March 2017).

[54] See also, in this sense, Llàcer, M.R., Casado, M. and Buisan, L. (eds) *Document on bioethics and Big data: exploitation and commercialisation of user data in public health care*. Universitat de Barcelona, Barcelona, 2015. Available at: http://www.publicacions.ub.edu/refs/observatoriBioEticaDret/documents/08209.pdf.

- BAROCAS, S. and SELBSR, A.D. "Big Data's Disparate Impact", *California Law Review* 104 (3), 2016:671-732.
- BELLAGIO BIG DATA WORKSHOP PARTICIPANTS, *Big data and positive social change in the developing world: A white paper for practitioners and researchers*. Oxford Internet Institute, Oxford 2014. Available at: http://www.rockefellerfoundation.org/uploads/files/c220f1f3-2e9a-4fc6-be6c-45d42849b897-big-data-and.pdf (accessed 18 December 2017).
- BENNETT, C.J. and RAAB, C.D. *The Governance of Privacy. Policy instruments in global perspective*. Ashgate, Aldershot, 2003.
- BOLLIER, D. *The Promise and Perils of Big Data*. Aspen Institute, Washington, DC, 2010. Available at: http://www.aspeninstitute.org/sites/default/files/content/docs/pubs/The_Promise_and_Peril_of_Big_Data.pdf (accessed 27 February 2017).
- BÖRÖCZ, I. "Risk to the Right to the Protection of Personal Data: An Analysis through the Lenses of Hermagoras*", European Data Protection Law Review* 2(4), 2016:467-480.
- BOYD, D. and CRAWFORD, K. "Critical Questions for Big Data: Provocations for a Cultural, Technological, and Scholarly Phenomenon", *Information, Communication, & Society* 15(5), 2012:662-679.
- Boyd, D. and CRAWFORD, K. *Six Provocations for Big Data* (paper presented at Oxford Internet Institute's "A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society", Oxford, September 21, 2011). Available at: <http://ssrn.com/abstract=1926431 (accessed 16 April 2017).
- BOYD, D., LEVY, K., and MARWICK, A. "The Networked Nature of Algorithmic Discrimination". In GANGADHARAN, S.P., EUBANKS, V. and BAROCAS, S. *Data and Discrimination: Collective Essays*. Open Technology Institute and New America, 2014. Available at: http://www.newamerica.org/downloads/OTI-Data-an-Discrimination-FINAL-small.pdf (accessed 14 April 2017).
- BRAY, P. ET AL. *International differences in ethical standards and in the interpretation of legal frameworks SATORI Deliverable D3.2*. (2015). Available at: http://satoriproject.eu/work_packages/legal-aspects-and-impacts-of-globalization/ (accessed 20 February 2017).
- BRECKENRIDGE, A.C. *The Right to Privacy*. University of Nebraska Press, Lincoln, 1970.

- BYGRAVE, L.A. "Privacy Protection in a Global Context. A Comparative Overview", *Scandinavian Studies in Law* 47, 2004: 324-325.
- CANNATACI, J.A. *Lex Personalitatis & Technology-driven Law*. (2008) 5(1) SCRIPTed 1–6.
- CNIL. *Privacy Impact Assessment (PIA). Methodology (how to carry out a PIA)*. 2015. Available at: https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-1-Methodology.pdf (accessed 25 February 2017).
- COHEN, J.E. "Examined Lives: Informational Privacy and the Subject", *Stanford Law Review* 52, *2000*: 1373-1437.
- COSTA, L. "Privacy and the precautionary principle*", Computer Law and Security Review* 28(1), 2012:14–24.
- COUNCIL OF EUROPE. *Progress report on the application of the principles of Convention 108 to the collection and processing of biometric data*. 2005, para 10. Available at: https://rm.coe.int/16806840ba (accessed 4 May 2017).
- CRAWFORD, K. ET AL. *Big Data, Communities and Ethical Resilience: A Framework for Action*. 2013, 6-7. Available at: http://www.rockefellerfoundation.org/app/uploads/71b4c457-cdb7-47ec-81a9-a617c956e6af.pdf (accessed 5 April 2017).
- ENISA. *Privacy by design in big data. An overview of privacy enhancing technologies in the era of big data analytics*. 2014. Available at: https://www.enisa.europa.eu/publications/big-data-protection (accessed 4 February 2017).
- ERICSSON. *The Impact of Datafication on Strategic Landscapes*. 2014. Available at: https://www.ericsson.com/assets/local/news/2014/4/the-impact-of-datafication-on-strategic-landscapes.pdf (accessed 20 March 2017).
- EUROPEAN PARLIAMENT. *European Parliament resolution of 14 March 2017 on fundamental rights implications of big data: privacy, data protection, non-discrimination, security and law-enforcement* (2016/2225(INI)). 2017. Available at: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2017-0076+0+DOC+XML+V0//EN&language=EN (accessed 16 March 2017).
- FEDERAL TRADE COMMISSION. *Data Brokers: A Call for Transparency and Accountability*. Washington, DC, 2014, 20 and Appendix B. Available at: https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf (accessed 27 February 2017).

- FLORIDI, L. *The 4th Revolution: How the Infosphere is Reshaping Human Reality*. Oxford University Press, Oxford, 2014.
- GELLERT, R. "Data protection: a risk regulation? Between the risk management of everything and the precautionary alternative", *International Data Privacy Law* 5(1), 2005:3-19.
- GONÇALVES, M.E. "The EU data protection reform and the challenges of big data: remaining uncertainties and ways forward", *Information & Communications Technology Law* 26 (2), 2017:20 Published online: 28 February 2017.
- HILDEBRANDT, M. *Profiling: "*From Data to Knowledge. The challenges of a crucial technology", *Datenschutz und Datensicherheit* 30(9), 2006:548-552.
- KOIVISTO, R. and DOUGLAS, D. *Principles and Approaches in Ethics Assessment. Ethics and Risk. Annex 1.h Ethical Assessment of Research and Innovation: A Comparative Analysis of Practices and Institutions in the EU and selected other countries. Project Stakeholders Acting Together on the Ethical Impact Assessment of Research and Innovation – SATORI. Deliverable 1.1*. (2015). Available at: http://satoriproject.eu/work_packages/comparative-analysis-of-ethics-assessment-practices/ (accessed 15 February 2017).
- LLÀCER, M.R., CASADO, M. and BUISAN, L. (eds) *Document on bioethics and Big data: exploitation and commercialisation of user data in public health care*. Universitat de Barcelona, Barcelona, 2015. Available at: http://www.publicacions.ub.edu/refs/observatoriBioEticaDret/documents/08209.pdf
- LYCETT, M. "'Datafication': making sense of (big) data in a complex world*"*, *European Journal of Information Systems* 22(4), 2013:381–386.
- LYNSKEY, O. *The Foundations of EU Data Protection Law*. Oxford University Press, Oxford, 2015.
- MANTELERO, A. "From Group Privacy to Collective Privacy: Towards a New Dimension of Privacy and Data Protection in the Big Data Era". In TAYLOR, L., FLORIDI, L. and VAN DER SLOOT, B. (eds). *Group Privacy: New Challenges of Data Technologies*. Springer International Publishing, Cham, 2017.
- MANTELERO, A. *Il costo della privacy tra valore della persona e ragione d'impresa*. Giuffrè, Milano, 2007.
- MANTELERO, A. "Personal data for decisional purposes in the age of analytics: from an individual to a collective dimension of data protection", *Computer Law and Security Review* 32(2), 2016:238-255.

- MANTELERO, A. "The future of consumer data protection in the E.U. Rethinking the "notice and consent" paradigm in the new era of predictive analytics", *Computer Law and Security Review* 30(6), 2014:643-660.
- MAYER-SCHÖNBERGER, V. and CUKIER, K. *Big Data. A Revolution That Will Transform How We Live, Work and Think*. John Murray, London, 2013
- MAYER-SCHÖNBERGER, V. and PADOVA, Y. "Regime Change? Enabling Big Data through Europe's Data Protection Regulation", *Columbia Science and Technology Law Review* XVII, 2016:315-335.
- MAYER-SCHÖNBERGER, V. "Generational development of data protection in Europe?". In AGRE, P. and ROTENBERG, M. (eds). *Technology and privacy: The new landscape*. MIT Press, Cambridge, MA, 1997.
- MCKINSEY GLOBAL INSTITUTE. *Big data: The next frontier for innovation, competition, and productivity*. 2011. Available at: http://www.mckinsey.com (accessed 16 January 2017).
- MOEREL, L. *Big Data Protection: How to Make the Draft EU Regulation on Data Protection Future Proof*. Tilburg University, Tilburg, 2014. Available at: http://www.debrauw.com/wp-content/uploads/NEWS%20-%20PUBLICATIONS/Moerel_oratie.pdf (accessed 15 October 2016).
- NARAYANAN, A., JOANNA, H., and FELTEN, E.W. "A Precautionary Approach to Big Data Privacy". In GUTWIRTH, S., LEENES, R., and DE HERT, P. (eds). *Data Protection on the Move*. Springer Netherlands, Dordrecht, 2016, 357-385;
- PASQUALE, F. *The Black Box Society. The Secret Algorithms That Control Money and Information*. Harvard University Press, Cambridge, MA, 2015.
- PEEL, J. *Precaution - A Matter of Principle, Approach or Process?* (2004) 5(2) Melb. J. Int. Law 483. Available at: http://www.austlii.edu.au/au/journals/MelbJlIntLaw/2004/19.html (accessed 4 February 2017).
- PIETERS, W. "Security and Privacy in the Clouds: A Bird's Eye View". In GUTWIRTH, S., POULLET, Y., DE HERT, P., and LEENES, R. (eds.). *Computers, Privacy and Data Protection: an Element of Choice*. Springer, Dordrecht, 2011.
- POST, R.C. "The Social Foundations of Privacy: Community and Self in the Common Law Tort", *California Law Review* 77, 1989:957-1010.
- RAAB, C., and WRIGHT, D. "Surveillance: Extending the Limits of Privacy Impact Assessment". In WRIGHT, D., and DE HERT P. (eds), *Privacy Impact Assessment*. Springer, Dordrecht, 2012.

- RAAB, C. *The future of privacy protection*. (2004) Cyber Trust & Crime Prevention Project 15. Available at: https://www.piawatch.eu/node/86 (accessed 28 April 2017).
- RESTA, G. "Personnalité, persönlichkeit, personality", *Comparative Perspectives on the Protection of Identity in Private Law* 1(3), 2014:215-243.
- ROUVROY, A. *Des données sans personne: le fétichisme de la donnée à caractère personnel à l'épreuve de l'idéologie des Big Data*. (2014) 9. Available at: http://works.bepress.com/antoinette_rouvroy/55 (accessed 8 March 2017).
- RUBINSTEIN, I.S. "Big Data: The End of Privacy or a New Beginning?", *International Data Privacy Law* 3(2), 2013:74–87.
- SCHUDSON, M. *Discovering the news: a social history of American newspapers*. Basic Books, New York, 1992.
- SHELLEY-EGAN, C. ET AL. SATORI *Deliverable D2.1 Report (handbook) of participatory processes.* (2014), 42-44. Available at: http://satoriproject.eu/work_packages/dialogue-and-participation/ (accessed 15 February 2017).
- SHELLEY-EGAN, C. ET AL. *Ethical Assessment of Research and Innovation: A Comparative Analysis of Practices and Institutions in the EU and selected other countries. Deliverable D1.1*. (2015) 28-29. Available at: http://satoriproject.eu/work_packages/comparative-analysis-of-ethics-assessment-practices/ (accessed 13 February 2017).
- SHELLEY-EGAN, C. ET AL. *SATORI Deliverable D2.2 (public version): Views of civil society organisations, government agencies/policymakers and media actors regarding ethics assessment of research and innovation*. (2015). Available at: http://satoriproject.eu/work_packages/dialogue-and-participation/ (accessed 13 February 2017).
- SOLOVE, D.J. *Understanding Privacy*. Harvard University Press, Cambridge, Ma, 2008.
- STIRLING, A., and GEE, D. "Science, precaution, and practice", *Public Health Reports* 117(6), 2002: 521–533. Available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1497477/ (accessed 8 March 2017).
- TENE, O. and POLONETSKY, J. "Privacy in the Age of Big Data. A Time for Big Decisions", *Stanford Law Review Online* 64, 2012:63-69. Available at: http://www.stanfordlawreview.org/sites/default/files/online/topics/64-SLRO-63_1.pdf (accessed 14 March 2017).

- THE WHITE HOUSE, EXECUTIVE OFFICE OF THE PRESIDENT. *Big Data: Seizing Opportunities, Preserving Values*. Washington, DC, 2014. Available at: https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf (accessed 26 March 2017).
- TOSUN, J. "How the EU Handles Uncertain Risks: Understanding the Role of the Precautionary Principle", *Journal of European Public Policy* 20(10), 2013:1517-1528. Available at: http://www.tandfonline.com/doi/abs/10.1080/13501763.2013.834549 (accessed 8 March 2017).
- VEDDER, A.H. "Privatization, Information Technology and Privacy: Reconsidering the Social Responsibilities of Private Organizations". In Moore, G. (ed), *Business Ethics: Principles and Practice*, Business Education Publishers, 1997.
- WESTIN, A.F. *Privacy and Freedom*. Atheneum, New York.
- WRIGHT, D., and DE HERT, P. "Findings and Recommendations". In Wright and De Hert. *Privacy Impact Assessment*. Springer, Dordrecht, 2012.
- WRIGHT, D. "A framework for the ethical impact assessment of information technology", *Ethics and Information Technology* 13(3), 2011:199-226.
- WRIGHT, D. A framework for the ethical impact assessment of information technology. (2011) 13 Ethics Inf. Technol. 199–226.
- ZARSKY, T.Z. "Transparent Predictions", *University of Illinois Law Review* 4, 2013:1503-1569.

Fecha de recepción: 5 de junio de 2017
Fecha de aceptación: 30 de junio de 2017