Safeguards for the right not to be subject to a decision based solely on automated processing (Article 22 GDPR)

Antoni Roig[1]

Cite as Roig, A., "Safeguards for the right not to be subject to a decision based solely on automated processing (Article 22 GDPR)", in European Journal of Law and Technology, Vol 8, No 3, 2017.

ABSTRACT

WP29 has recently adopted Guidelines on Automated Individual Decision-making and Profiling for the purposes of General Data Protection Regulation 2016/679 (GDPR). Article 22 GDPR bans all decisions that affect the data subject which have been based solely on automated processing. The Article eventually allows automatic processing, conditional on application of suitable safeguards for data subject rights. These safeguards might vary substantially depending on automated processing technologies. This article describes, firstly, the general safeguards to embed legal requirements. Secondly, the article explores solutions for automatic processing based on data analysis. It is argued that, although the data controller can put in place safeguards that respect data subject rights, a parallel empowerment of external authorities will be necessary to reach both: an informed external oversight, and the full application of this right. This article seeks to provide an analysis of Article 22 GDPR in the hope that this will inform the policy debate.

Keywords: Article 22 GDPR; automated processing; data analysis; agreement technologies; multi-agent systems; internal/external oversight

1 THE RIGHT NOT TO BE SUBJECT TO A DECISION BASED SOLELY ON AUTOMATED PROCESSING

According to Article 22 of the General Data Protection Regulation (GDPR)[2], "the data subject has the right not to be subject to a decision based solely on automated processing, including profiling, when it produces legal effects concerning him or her or at least it similarly significantly affects him or her". Not all automatic processing is hence relevant for the GDPR; only that processing that has legal effects or significantly affects a person. Some conditions – contractual clauses between the data subject and the data controller, EU or Member State Law, and even a data subject's explicit consent – could alleviate the strict prohibition of Article 22 and legitimise automated processing. Decisions should not be based nonetheless on special categories of data mentioned in Article 9 (1) GDPR and should not concern a child[3].

The new Regulation is clearly concerned with the final situation of individuals confronted with automatic decisions, i.e. a situation that significantly affects them. Whilst the Article allows automated decision-making processing when the data controller has obtained informed consent of the data subject or in the light of an existing contract between the data controller and the data processor, it also calls for the application of "suitable measures to safeguard the data subject's rights and freedoms and legitimate interests." These may include:

- Specific information to the data subject
- The right to obtain human intervention
- The right to express his or her point of view
- The right to obtain an explanation of the decision reached
- The right to challenge the decision

The GDPR adopts a more general approach than the previous Article 15.1 of the Data Protection Directive of 1995[4]. According to Article 22 GDPR, not only profiling, but any automatic processing with legal effects deserves suitable safeguards. This wider perspective is interesting because it is not limited to profiling, but it also includes other systems such as decision support systems. Decision making tools can obviously rely on data analysis to get statistical inferences. The problem is that these tools can affect data subjects. The following sections will consider decision-support systems as examples of automated decision-makers that affect the data subject.

This will gain importance with the growing responsibilities of data controllers, including the requirement of data protection impact assessment (DPIA). DPIA could compile all the relevant safeguards for specific technologies and automatic processing and turn into a data generator for policy purposes (Fosch-Villaronga and Heldeweg 2017). The new obligations for data controller to conduct DPIA prior to processing are also worth noting (Article 35 GDPR). Moreover, corporations and public authorities whose main activity relies on profiling will also need a data protection officer (DPO) (Article 7 GDPR).

According to Article 14.2(g), the data controller should provide the data subject with information about "the existence of automated decision-making, including profiling, referred to in Article 22 (1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for

the data subject". It has been said that the GDPR does not include a general right to explanation of automatic decisions (Wachter, S. and others, 2017). Nonetheless, providing suitable safeguards is one key aspect to consider in a world where automatic decisions, some of them with legal effects, will be part of any citizen's daily experience[5].

The following sections will describe the general and concrete suitable safeguards for automated decisions. In Section 2, some general safeguards are suggested, like transparency, participation, internal and external oversight, traceability and informal governance platforms. In Section 3, enforced safeguards for data analysis-based automatic decisions are described. Section 4 includes legal safeguards such as traditional judicial review. We will conclude with an overview of the safeguards identified in this paper and future challenges.

2 IMPLEMENTING GENERAL SAFEGUARDS

Some traditional safeguards like transparency, participation, the internal/external combined procedure and traceability might preserve Article 22 GDPR requirements in straightforward cases. Can these ordinary safeguards also be embedded in tools? Some tools not conceived initially as safeguards, like informal governance platforms, can perhaps be revamped to embed ordinary safeguards for automatic processing, like informal governance platforms, can also offer due protection. The following sections explain the benefits and drawbacks of such safeguards.

2.1 TRANSPARENCY AND PARTICIPATION

Transparency provides specific information to the data subject, while participation allows him or her to express his or her point of view. Transparency is usually envisioned as *ex ante* transparency, in the sense that the data controller informs the data subject in advance he will use his data for automated decision-making. The subject therefore has the possibility to give informed consent or to express his or her point of view. This is part of a data minimisation-based approach, necessary but not always sufficient when dealing with automated processing, as it has been highlighted (Koops, 2013). Some automatic processing tools only require general safeguards like transparency, participation, internal/external oversight and traceability.

This is the case, for instance, with automated processing based on semantic annotation[6]. Some metadata are added to the text so that it automatically links different texts with related meaning. This can be used for classification and legal information retrieval and thus can fuel decision-making. These tools can easily preserve legal requirements because the links are based on legal knowledge. Legal ontologies can also be privacy-friendly automated decision tools[7]. The ontology is a formal structure with links between legal concepts that can be used by an algorithm or decision-making tool to perform automatic processing. If legal knowledge acquisition is properly implemented, these tools allow legal compliance. Indeed, some automated processing tools can favour general safeguard effectiveness. This does not mean that all automatic processing is harmless. On the contrary, some tools are clearly challenging for the general safeguards mentioned here and would require additional protection (see below, section 3).

2.2 INTERNAL/EXTERNAL OVERSIGHT AND TRACEABILITY

Ex-ante transparency and participation have limited effect in practice. The so-called decision transparency (Koops, 2013) focusses on the output of the decision-making. The safeguards for automatic processing need to also integrate decision-making. The ideal situation is real-time oversight, but this seems impossible or unnecessarily complicated. Indeed, a combination of regular internal monitoring and occasional external auditing might provide sufficient protection.

We should avoid external blind review of automated processing, only based on the proportionality principle or reasonability. The latter would occur when a court, a data protection authority (DPA) or another authority, with no relevant information on the monitored decision-making, decides whether the outcome is proportionate or reasonable[8]. But how can a judge assess the necessity or adequacy of a processing without closely monitoring the internal process? Internal monitoring, for instance by a DPO, is thus crucial for subsequent review. Only if the DPO, or equivalent, has access to the decision making, can it eventually evaluate real-time outcomes. The DPA or court external review indeed relies on the accuracy of the inner oversight. This is therefore a combined perspective of the safeguards, which complements transparency and participation, and contributes to GDPR compliance in the following manner:

- Internal supervision

  The desirable procedure would be prior confirmation or validation by a human expert. Some machine-to-machine (M2M) tools will make it impossible for humans to confirm in real time the extent of the decision-making. Therefore, a confirmation or validation after the automatic decision is needed. Some tools use machine-learning techniques to improve future recommendations with past events. This can reinforce automatic decision making, and hence the confirmation of "trends" will also require human oversight.

  The Data Protection Officer (DPO) or other expert is in charge of the internal supervision:

  - The DPO or expert should be a member of the decision-making staff, an expert with field knowledge of the decision-making.
  - In the performance of his duties, he should follow instructions from no one.
  - He should ensure, in an independent manner, compliance with Article 22.
  - He should ensure that a written record of transmission and receipt of personal data is kept according to the rules of procedure and under secure conditions. He should concretely ensure that the logs are kept.
  - He should ensure that data subjects are informed of their rights at their request.
  - To support these tasks, the expert or DPO shall have access to all the data processed by the automated decision tool.

  Should the DPO or the expert find the processing does not comply with the GDPR, s/he then shall inform the decision-making board and refer the matter to the external supervisor. This could improve GDPR compliance and maybe exonerate the DPO from further responsibilities, although this should need further exploration.

- External supervision

  Not only internal oversight can help the implementation of Article 22, but external supervision also has a key role for this purpose. National Data Protection Authorities (DPA) or other more specialised institutions can evaluate *posteriori* the DPO criteria adopted on case-by-case basis or explicitly held in best practices or codes of conduct of the company.

The implementation of accountability measures can also have a negative side: the introduction of breach risks. Managing access to logs and traceability is thus a priority for efficient external oversight. Koops provides some interesting examples of transparency legislation that could enhance control structure and procedures (Koops, 2013). He suggests preserving not only the process transparency, but also the decision or outcome transparency[9]. He also claims for receptors capable of understanding and using the information, which adds a new perspective to the external supervision: can we rely on Courts and DPA for this important task? We therefore need to enhance legal safeguards, and we will suggest some ways to do it below (see, section 4).

2.3 SAFEGUARDS EMBEDDED IN INFORMAL GOVERNANCE PLATFORMS

The NanoSafetyCluster[10], a platform for safety assessment, is perhaps the best example of informal governance platforms that could eventually evolve into a legal decision-making tool for nanotechnology. Such informal clusters or platforms could effectively provide transparency and internal/external oversight, all in an integrated package. Not initially conceived as legal decision-making tools nor safeguards, they however fail in one crucial point: they do not include the public interest. Stakeholders suggest and agree on lists of risks and criteria, and afterwards some of the results are included in EU recommendations. Moreover, there is always the danger of capture of the lawmaker by the stakeholders and other representatives of legitimate, but not general, interests[11].

However, the fact that these platforms were not initially conceived as safeguarding tools does not necessarily mean they could not effectively serve this purpose. Indeed, they could play a role in automated processing if they evolve from governance platforms to an institutional framework, and if they include embedded transparency and internal/external oversight. They currently only provide a dynamic decision-making framework on legal principles, including experts and stakeholders. Perhaps the Global Privacy Enforcement Network (GPEN), which strengthens public authorities' capacities for cross-border cooperation, and the European Data Protection Board (EDPD) can also have an important role[12].

3 NEW CHALLENGES DUE TO DATA ANALYSIS-BASED AUTOMATED PROCESSING

Automatic decisions based on data analysis will require enforced safeguards. The general safeguards mentioned in section 2 cannot offer effective protection against this kind of automatic decision-making.

3.1 GENERAL SAFEGUARDS WILL NOT WORK WITH DATA ANALYSIS-BASED AUTOMATED PROCESSING

Data analysis raises challenges for at least the following legal areas: "transparency and information obligations of data controllers; consent (including consent in case of repurposing); the need to balance public interest and the interests of data subjects for legitimising personal data processing; the regulation of profiling; and proper safeguarding of digital rights in case of data transfers to third parties and third countries and access to EU data"[13]. A complete Big Data threat landscape is now available[14]. The combination of big data with statistical correlations is most challenging for automatic processing from the perspective of Article 22. The reason is that statistical correlations completely neglect legal theories or legal requirements, in this case the GDPR. It is difficult to embed legal requirements such as those envisaged in Article 22 GDPR in the decision-making tool.

In this section, we argue that general safeguards – specific information to the data subject; the right to obtain human intervention; the right to express his or her point of view; the right to obtain an explanation of the decision reached; and the right to challenge the decision – may not work in the case of data analysis-based automated processing:

- Right to be informed: Similar to the right to access under Article 12(a) of the Data Protection Directive ("communication to him [the user] in an intelligible form of the data undergoing processing and of any available information as to their source") it is only a very first step towards an effective safeguard against the effects of a decision-making.
- Right to obtain human intervention: When a decision is based on data analysis, human intervention cannot alter the result, unless it simply takes into consideration the statistical correlation. This implies a clear risk: human intervention may in the future be only a formal requisite, but with no actual effect on the automatic processing. This will push future DPO or equivalent internal human officer knowledge on data analysis so as he can discriminate relevant correlations from other irrelevant statistical links with no value for the decision-making. Another consideration has to do with the purpose of such human intervention, which it is not only to exclude discrimination and profiling of minors, but also to reduce false positives[15]. The possibility of having false positives due to meaningless statistical correlations is a major risk scenario to be tackled by human expert data analyst intervention. Obviously, even without false positives the tool can also discriminate and have negative effects on citizens.

Therefore, the right to express his or her point of view is also needed. But it will be difficult to contest an automatic decision without a clear explanation of the decision reached. To challenge such an automatic data-based decision, only a multidisciplinary team with data analysts will be able to detect false positives and discriminations. The human intervention has thus a crucial double role: on the one hand, it must filter false positives; and on the other hand it must allow future strict scrutiny of the decision-making by the external monitoring institution (DPA, courts or other accredited institutions).

3.2 BIG DATA ANALYTICS VALUE CHAIN PET, NOT CONCRETE AND ISOLATED PET

The privacy by design strategies described by ENISA in its 2014 Report still offers valuable general principles to solve the privacy risks related to data analysis-based automatic processing in a collaborative manner[16]. These include: data minimisation, guidance on hidden data, separate data, aggregate data, informing data subjects, data subjects control of their data, privacy policy and compliance by stakeholders. Data analysis-based automated processing will require more than mere technological measures for compliance.

The application of such principles will require continuous legal monitoring and a technical solution update. In a nutshell, PbD when dealing with data analysis tools will require strategic capabilities: an alignment between IT and the legal requirements. PbD will resemble, in this case, a regulatory process dealing with IT options. This alignment will only be achieved if DPA, data controllers and big data analytics actively and permanently interact to implement PbD.

Although no concrete or isolated privacy-enhancing technology (PET) pack can provide enough protection unless it considers the so-called "big data analytics value chain"[17], it has been argued that "big data with privacy" is technically possible[18]. More than a singular measure, privacy-preserving for data analysis tools requires a general approach: automated policy definitions and enforcement defined with semantics and relevant standards, and cryptographic implementation. This promotes a clash between utility and privacy, which is usually managed by some techniques like k-anonymity for data releases, differential privacy for data queries and perturbative approaches for streaming data. Local anonymization and collaborative anonymization can also offer better protection than centralised anonymization. In some cases, lawyers will not only have to call for technical support; they will have to cooperate with computer scientists at the risk of leaving the data analysis to engineers who do not possess legal background/expertise.

3.3 PRIVACY-PRESERVING AUTOMATED DECISIONS

Is there any privacy-friendly automated processing alternative to PETs mentioned in 3.2? Some artificial intelligence (AI) techniques called E-institutions, Social Artificial Intelligence, Multi-agent Systems, Social Technical Systems, and also Hybrid Online Social Systems (HOSS) could provide new possibilities in this respect[19].

E-Institutions, like conventional institutions, facilitate coordination between agents through a restricted context where only some objects and entities exist, with interactions allowed according to institutional constraints. This is from a social AI or Artificial Social Intelligence perspective, where agent actions cause an electronic state. Compliance rules and principles are part of these tools, and thus legal theories can be enshrined at the core of these automatic decision-making institutions. Indeed, compliance and enforcement become crucial for electronic institutions, and there is always a descriptive specification of the rules or conventions. According to these rules, agents can enter an organisation, play a role in it, or even leave it. In some of these e-institutions, agents are even allowed to violate rules, although the tool tries to encourage compliance imposing sanctions. These electronic institutions involve many activities or meetings, which are connected according to the characteristics of the institution. Some possible dialogues between agents are defined, according to their

respective role in the institution. This leads to a scene network, and agents move from one scene to another. The institution thus provides an interaction framework with atomic interactions, but also social ones, like joining or leaving the institution and creating or terminating scenes. Therefore, the different parts to define include scenes networks, transitions, electronic institution and institutional state. As a result, a restricted virtual environment is built, with all interactions taking place according to the institutional rules or conventions: it is called a "normative multi-agent system", where the electronic institution creates the institutional reality: procedural and functional conditions for the interaction of agents[20].

We suggest that these electronic institutions can effectively support legal compliance and become privacy-preserving automated processing. They have been used so far to support a wide variety of applications:

- Fish markets: agents interact by means of communication, making a bid in the fish market. Some auction scenes or meetings are implemented, in which buyers compete to purchase fish. A variation of the traditional Dutch auction protocol provides the principal scene: an auction. The auctioneer choses an item, opens a bidding, and for each successive price the auctioneer calls, one, several or no buyers, submit a bid; and this is repeated until there are no more goods left[21].
- Water virtual market: each basin institution is under the supervision of the government authority, according to a concrete contractual agreement. Specific guidelines based on legal documents are not only welcomed but also required for the proper functioning of the tool. Based on this, there is also the need for coherence and traceability of the normative environment. As a result, a virtual market for water rights is proposed, with traceable rights parameters, buyer, seller profiles and populations[22].
- Agent based simulation for archaeology and cultural heritage is another example of normative – with technical constraints, not obviously legal rules – multi agent system. Concretely, a 3D virtual world is integrated into an institutional framework and enables automatic generation of the corresponding 3D environment, if needed. The autonomous agents reproduce the way of life of ancient people in 3000 B.C Mesopotamia in virtual worlds, with regulation of interactions[23].
- Other applications have been also envisioned as applications for mutual support, scientific assessment and hotel management, for instance.

These current applications are certainly far from what legal automated decisions will require, but they represent the main components of what a future automated processing tool may look like in the future. Privacy-preserving electronic institutions are technically possible, and could empower future legal automated processing to have automatically compliant tools instead of mere data analysis-based automated processing with no legal roots.

Instead of simply building safeguards for existing automated processing, the legal domain should suggest a PbD automatic processing that naturally embeds the safeguards – and the rights – into them. Contrary to what has been argued in the literature (Koops and Leenes 2014), there do not seem to be technical problems precluding data analysis in electronic institutions like the ones we have described here. This can be an option to the existing PET for data analysis-based automated processing: its embedment into a privacy-friendly electronic

institution. This may certainly add costs to the data-driven initial tools, but in the end it may suffice to have a privacy-friendly resulting framework.

4 ENHANCING LEGAL SAFEGUARDS

Apart from building technical standards and encouraging privacy-friendly automated processing, there is a complementary perspective to consider: to empower legal safeguards when dealing with automated decisions. This can be achieved by empowering an external oversight, which could be a court, a DPA or another authority[24]. If we take the requirement of human intervention seriously, both the internal oversight and the external monitoring should be empowered. As said before, the internal oversight must be accurate enough to allow future external auditing. We should now try to describe how we could obtain an enhanced informed external oversight.

The efficiency of the external oversight will largely depend on the authority entitled to review the automated decision and the inner monitoring. A regular judge, for instance, may not be equipped enough to assess the level of protection afforded by the tool and the internal oversight[25]. An independent authority could perhaps fulfil better this task, but one cannot neglect the role of judicial review[26]. Although it may require education and the provision of additional tools and systems, this is a good occasion to empower courts for this crucial new commitment: the external monitoring of automated processing and due process with human intervention. As mentioned before, decision transparency may be a good complement to process transparency. This has one (un)solvable challenge: the decision logic might not be understood, and effective monitoring is thus at risk. Therefore, the internal and external oversight need to be modelled together, not independently, in order the former provides all the relevant information to the latter to evaluate the adopted decision.

Coordination and reporting will be, therefore, key aspects of this combined safeguard. This may result in having one single monitoring process carried out by two different authorities: one permanent oversight of the DPO or equivalent, and another one, occasional and accessed by the user. In such case, the latter should in any case provide a latent monitoring to the former, and should provide indications or guidance. This basically means that the DPA, court or accredited authority will have permanent information from the DPO or equivalent oversight, to react if necessary as soon as possible. This requires technical and human expert support to shift external oversight into a sort of latent monitoring. Courts usually do not decide *ex officio* and only proceed once the previous court/authority has adopted a decision. Therefore, these are aspects that will have to be carefully considered if the external oversight of automated processing is assigned to courts.

Moreover, in this paper we have always considered non-legal automatic decisions. But judicial automated decision support systems might soon appear[27]. So, the general framework here depicted will have to include in the future this new scenario and extend the general safeguards to it.

5 CONCLUSIONS

According to Article 22 GDPR, automated processing, including profiling, can produce legal effects concerning people and this should be banned. As a potential remedy, the European lawmaker envisions in this case the need for human intervention. Moreover, a contractual clause, a Union or Member State law or explicit consent can legitimate automated decision-making. Even though this Article bans discrimination for special categories and child's data for this purpose, it eventually allows automatic processing, conditional on suitable safeguards. Our contribution has shed light on these safeguards, considering different automated processing in order to protect the rights and freedoms and legitimate interests of the data subject.

We have first identified general safeguards for respectful techniques, like semantic annotation or legal ontologies, prone to embed legal requirements. These general safeguards are transparency and participation, internal and external oversight and traceability. We also argue that these safeguards can even be technically embedded in informal governance platforms, and this could be beneficial to a discussion between law-makers and stakeholders.

The current state of the art reveals that automatic processing tools based on data analysis are more challenging because statistical correlations completely neglect legal requirements like Article 22 provisions. Because of that, they will require enhanced safeguards. The PET or Transparency Enhancing Technologies (TET) communities are now discussing on Big Data Analytics Value Chain PET. Instead of a single measure, data analysis requires a process involving a combination of PET.

We also considered the possibility of privacy-preserving automated decisions, e.g. enshrining legal safeguards into electronic institutions. These automatic tools can even embed data analytics and then provide legal requirements to data-driven tools. In the future, these electronic institutions may not only serve governance or compliance purposes, but can also play an important role as enhanced legal safeguards. It is too soon to forecast what type of safeguard will eventually prevail, but future revisions or guidelines on the application of the GDPR could perhaps contemplate such possibility.

As a side note, monitoring automated processing requires close latent scrutiny of the daily or weekly activity of the DPO or equivalent internal institution. Moreover, automatic processing tools may also require other improvements such as the empowerment of Courts and other external authorities as external oversights. Traditional legal safeguards are not yet conceived for such a review. Meanwhile, new scenarios are appearing and will have to be added to those here described: some risk assessment tools might soon evolve into predictive algorithms for judicial review. Therefore, automatic legal decisions will also be technically possible.

As a closing remark, it is important to state once again the importance of interdisciplinarity as an indispensable condition for the successful application of the GDPR. If lawyers continue to overlook the technical sides of the regulation, not only will Article 22 of the GDPR (among others) not be appropriately implemented, but the rights of the data subjects will also be at risk.

ACKNOWLEDGEMENTS

The work was supported by a Spanish Project on The Ethical and Legal Dimensions of the web of data and the Regulation and Rights in current States, I+D National Research Program, Subprogram of Knowledge Generation (DER2016-78108-P), 2016-2018, awarded to Dr. Pompeu Casanovas and Dr. Antoni Roig. I would like to thank the anonymous reviewers of this commentary for their suggestions.

REFERENCES

Agarwal, S. (2016) 'Developing a Structured Metric to Measure Privacy Risk in Privacy Impact Assessments', in David Aspinall, Jan Camenisch, Marit Hansen, Simone Fischer-Hübner and Charles Raab (Eds.), Privacy and Identity Management Time for a Revolution? 10th IFIP WG 9.2, 9.5, 9.6/11.7, 11.4, 11.6/SIG 9.2.2 International Summer School Edinburgh, UK, August 16–21, 2015 Revised Selected Papers, pp. 141-155.

Albrecht, J. P. (2016) 'Regaining Control and Sovereignty in the Digital Age', in Wright, David and De Hert, Paul (Eds.), Enforcing Privacy. Regulatory, Legal and Technological Approaches, Springer, pp. 473-488.

Alnemr, R., Cayirci, E., Dalla Corte, L., Garaga, A., Leenes, R., Mhungu, R., Pearson, S., Reed, C., Santana de Oliveira, A., Stefanatou, D., Tetrimida, K.and Vranaki, A. (2016) 'A Data Protection Impact Assessment Methodology for Cloud', in B. Berendt et al. (Eds.), APF 2015, LNCS 9484, pp. 60–92.

Bier, C., Kühne, K. and Beyerer, J., (2016) 'PrivacyInsight: The Next Generation Privacy Dashboard', in S. Schiner et al. (Eds.), *APF 2016*, LNCS 9857, pp. 135–152.

Boella, G., Di Caro, L., Humphreys, L., Robaldo, L., Rossi, P and van der Torre, L. (2016) 'Eunomos, a legal document and knowledge management system for the Web to provide relevant, reliable and up-to-date information on the law', Artif Intell Law, 24, pp. 245–283.

Bogdanovych, A., Rodríguez, J.A., Simo?, S., Cohen, A.and Sierra, C., 'Developing Virtual Heritage Applications as Normative Multiagent Systems' (2011) in M.-P. Gleizes and J.J. Gomez-Sanz (Eds.), *AOSE 2009*, LNCS 6038, pp. 140–154.

Botti, V., Garrido,V., Giret, A. and Noriega, P., 'The Role of MAS as a Decision Support Tool in a Water-Rights Market' (2012) in F. Dechesne et al. (Eds.), *AAMAS 2011 Workshops*, LNAI 7068, pp. 35–49.

Büscher, C., (2015) 'Risk Calculation as Experience and Action—Assessing and Managing the Risks and Opportunities of Nanomaterials', *Nanoethics*9, pp. 277–295.

Caballero-Díaz, E., Simonet, B.m., and Valcárcel, M. (2013) 'The social responsibility of Nanoscience and Nanotechnology: an integral approach', J Nanopart Res 15, p.1534.

Chibba, M. and Cavoukian (2015) 'A., Privacy, Consumer Trust and Big Data: Privacy by Design and the 3 C'S', in *International Telecommunication Union, Proceedings of the 2015 ITU*

Kaleidoscope Academic Conference Trust in the Information Society, Barcelona, Spain (9-11 December 2015) pp. 233-237.

CORDIS (2015) NANODEFINE periodic report summary 1. European Commission. http://cordis.europa.eu/result/rcn/163274_en.htm, accessed 15 June 2017.

CORDIS (2015) PROSAFE - promoting the implementation of safe by design. European Commission. http://cordis.europa.eu/project/rcn/194431_en.html, accessed 15 June 2017.

D'Inverno, M., Luck, M., Noriega, P., Rodríguez-Aguilar, J.A. and Sierra, C. (2012) 'Communicating Open Systems', Arti?cial Intelligence, 186, pp. 38–94.

Döhmann, I.S.g., Tambou, O., Bernal, P., Hu, M., Molinaro, C.A., Negre, E., Sarlet, I.W., Mendes, L., Schertel, W.N. and Yger, F., (2016) 'The Regulation of Commercial Profiling – A Comparative Analysis', European Data Protection Law Review, Vol. 2, Num. 4, pp. 535-554.

Dorbeck-Jung, B., and Shelley-Egan, C. (2013) 'Meta-Regulation and Nanotechnologies: The Challenge of Responsibilisation Within the European Commission's Code of Conduct for Responsible Nanosciences and Nanotechnologies Research', Nanoethics, 7, pp.55–68.

ENISA (2015) Privacy by design in big data. An overview of privacy enhancing technologies in the era of big data analytics, Final 1.0.

ENISA (Jan. 2016) Rekleitis, E. (ed.), Big Data Threat Landscape and Good Practice Guide.

ENISA, Schiffner S. (Ed.) (Dec. 2015) Readiness Analysis for the Adoption and Evolution of Privacy Enhancing Technologies Methodology, Pilot Assessment, and Continuity Plan, approved version 1.0.

Esquivel-Quirós, L.G. and Barrantes, E.G. (2016) 'An Experience with a De-Identifying Task to Inform About Privacy Issues', in David Aspinall, Jan Camenisch, Marit Hansen, Simone Fischer-Hübner, Charles Raab (Eds.), Privacy and Identity Management Time for a Revolution? 10th IFIP WG 9.2, 9.5, 9.6/11.7, 11.4, 11.6/SIG 9.2.2 International Summer School Edinburgh, UK, August 16–21, 2015 Revised Selected Papers, pp. 49-60.

Felici, M. and Pearson, S. (2015) 'Accountability for Data Governance in the Cloud', in M. Felici and C. Fernández-Gago (Eds.), *A4Cloud 2014*, LNCS 8937, pp. 3–42.

Fernandez-Gago, C., Pearson, S., D'Errico, M., Alnemr, R., Pulls, T. and Santana de Oliveira, A. (2016) A4Cloud Workshop: Accountability in the Cloud, in David Aspinall, Jan Camenisch, Marit Hansen, Simone Fischer-Hübner, Charles Raab (Eds.), Privacy and Identity Management Time for a Revolution? 10th IFIP WG 9.2, 9.5, 9.6/11.7, 11.4, 11.6/SIG 9.2.2 International Summer School Edinburgh, UK, August 16–21, 2015 Revised Selected Papers, pp. 61-78.

Fosch Villaronga, E. and Heldeweg, M.A. (2017). Regulering voor Experimenteren met Emergente Robot Technologie [Regulation for Experimenting with Emergent Robot Technology] in: Daskalova, V.I. and M.A.Heldeweg (eds.) (2017). Constitutionele mogelijkheden en beperkingen voor experimenteel handelen en experimentele wetgeving. Staatsrechtconferentie 2016. Publikaties van de Staatsrechtkring – Staatsrechtconferenties nr. 20. Oisterwijk: Wolf Legal Publishers (ISBN: 9789462404441), pp. 89-107.

Garcia, E., Miles, S., Luck, M. and Giret, A. (2015) 'Evaluating how agent methodologies support the speci?cation of the normative environment through the development process', Auton Agent Multi-Agent Syst , 29, pp.104–106.

González Fuster, G. and Scherrer, A. (Sept. 2015) Big Data and smart devices and their impact on privacy, *Study*. Document Requested by The Committee On Civil Liberties, Justice And Home Affairs.

Gutwirth, Serge and De Hert, Paul (2008) "Regulating Profiling in a Democratic Constitutional State", in Hildebrandt, Mireille, Gutwirth, Serge (Eds.), Profiling the European Citizen. Cross-Disciplinary Perspectives (Springer) pp. 271-302.

Hansen, M., Hoepman, J.H, Jensen,M. and Schiffner, S. (2016) 'Report on the Workshop on Assessing the Maturity of Privacy Enhancing Technologies', in David Aspinall, Jan Camenisch, Marit Hansen, Simone Fischer-Hübner, and Charles Raab (Eds.*), Privacy and Identity Management Time for a Revolution?* 10th IFIP WG 9.2, 9.5, 9.6/11.7, 11.4, 11.6/SIG 9.2.2 International Summer School Edinburgh, UK, August 16–21, 2015 Revised Selected Papers, pp. 96-110.

Hester, K., Mullins, M., Murphy, F. and Tofail, S.A.M. (2015) 'Anticipatory Ethics and Governance (AEG): Towards a Future Care Orientation Around Nanotechnology', *Nanoethics,* 9, pp.123–136.

Jahnel, J. (2015) 'Conceptual Questions and Challenges Associated with the Traditional Risk Assessment Paradigm for Nanomaterials', Nanoethics 9, pp. 261–276.

Jasmontaite, L. and Verdoodt, V. (2016) 'Accountability in the EU Data Protection Reform: Balancing Citizens' and Business' Rights', in *David Aspinall, Jan Camenisch, Marit Hansen, Simone Fischer-Hübner, and Charles Raab (Eds.), Privacy and Identity Management Time for a Revolution?* 10th IFIP WG 9.2, 9.5, 9.6/11.7, 11.4, 11.6/SIG 9.2.2 International Summer School Edinburgh, UK, August 16–21, 2015 Revised Selected Papers, pp. 156-169.

Kohnstamm, J. (2016) 'Getting Our Act Together: European Data Protection Authorities Face Up to Silicon Valley', in Wright, D. and De Hert, P. (Eds.), Enforcing Privacy. Regulatory, Legal and Technological Approaches (Springer) pp. 455-472.

Koops, Bert-Jaap, (2013) 'On Decision Transparency, or how to enhance data protection after the computational turn', in Hildebrandt, Mireille and de Vries, Katja (Eds.), *Privacy, Due Process and the Computational Turn. The philosophy of law meets the philosophy of technology* (Routledge) pp. 196-220.

Koops, B.-J. and Leenes, R. (2014) 'Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data-protection law', International Review of Law, Computers & Technology, 28, 2, pp. 159-171.

Lammerant, H. and De Hert, P. (2016) 'Visions of Technology. Big Data Lessons Understood by EU Policy Makers in Their Review of the Legal Framework on Intellectual Property Rights, Access to and Re-use of PSI and the Protection of Personal Data', in Gurtwirth, S., Leenes, R. and De Hert, P. (Eds.), Data Protection on the Move. Current Developments in ICT and Privacy/Data Protection (Springer) pp. 163-194.

Leenes, R. (2008) 'Adressing the Obscurity of Data Clouds' in Hildebrandt, Mireille and Gutwirth, Serge (Eds.), *Profiling the European Citizen (*Springer) pp. 293-300.

Linkov, I., Kurth, M.H., Hristozov, D. and Keisle, J.M. (2015) 'Nanotechnology: promoting innovation through analysis and governance', Environ Syst Decis, 35 pp. 22–23.

Malsch, I., Subramanian, V., Semenzin E., Hristozov, D. and Marcomini, A., "Supporting decision-making for sustainable nanotechnology", *Environ Syst Decis,* 2015, 35, pp. 54–75.

Meyer, D.E. and Upadhyayula, V. K. K. (2014) 'The use of life cycle tools to support decision making for sustainable nanotechnologies', Clean Techn Environ Policy, 16, pp. 757–772.

Murphy, T.H. (Fall 2013) 'Mandating Use of Predictive Coding in Electronic Discovery: An Ill-Advised Judicial Intrusion', American Business Law Journal, Volume 50, Issue 3, pp. 609–657.

NANoREG - A common European approach to the regulatory testing of nanomaterials, 2013, European Commission. http://cordis.europa.eu/project/rcn/107159_en.html, www.nanoreg.eu, accessed 15 June 2017.

Nissan, E. (14 Oct.2015) 'Digital technologies and arti?cial intelligence's present and foreseeable impact on lawyering, judging, policing and law enforcement', AI & Soc.

Noriega, P. and de Jonge, D. (2016) 'Electronic Institutions: the EI/EIDE Framework', in Aldewereld, H., Boissier, O., Dignum, V., Noriega, P. and Padget, J. (eds.), *Social Coordination Frameworks for Social Technical Systems*, Springer, p. 47-76.

OCDE, Series on the Safety of Manufactured Nanomaterials (07-07-2015) no.57, Guidance Manual towards the Integration of Risk Assessment into Life Cycle Assessment of Nano-Enabled Applications.

Parra-Arnau, J., Rebollo-Monedero, D. and Forné, J. (2014) 'Privacy-Enhancing Technologies and Metrics in Personalized Information Systems' in Navarro-Arribas, G. and Torra, V. (Eds.), Advanced Research in Data Privacy, Springer, Volume 567 of the series Studies in Computational Intelligence, pp 423-442.

Pearson, S. (2014) 'Accountability in Cloud Service Provision Ecosystems', in K. Bernsmed and S. Fischer-Hübner (Eds.), NordSec 2014, LNCS 8788, pp. 3–24.

Remus, D. A. (2014) 'The Uncertain Promise of Predictive Coding', Iowa Law Review, Vol. 99, pp. 1691-1724.

Wachter, Sandra, Mittelstadt, Brendt and Floridi, L. (2017) Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, International Data Privacy Law.

Walker, W.C., Bosso, C.J., Eckelman, M., Isaacs, J.A., and Pourzahedi, L. (2015) 'Integrating life cycle assessment into managing potential EHS risks of engineered nanomaterials: reviewing progress to date', J Nanopart Res, pp. 17:344.

WP29, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, Adopted on 3 October 2017 (WP251).

WP29, Guidelines on transparency under Regulation 2016/679 (WP260)

Wright, D. (2016) 'Enforcing Privacy', in Wright, David and De Hert, Paul (Eds.), Enforcing Privacy. Regulatory, Legal and Technological Approaches (Springer) pp. 13-49.

FOOTNOTES

[1] IDT-UAB Institute of Law and Technology, Universitat Autònoma de Barcelona, Spain, antoni.roig@uab.cat

[2] Regulation (EU) 2016/679 of the European Parliament and of 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, GDPR). See also Recital 71 GDPR.

[3] Not only transparency, but also opacity, in the sense of prohibition of racial profiling or discrimination is required. Some authors have claimed Americain constitutional tradition has offered more precise and comprehensive solutions than the European general prohibition on automated decisions (Gutwirth, Serge and De Hert, Paul, "Regulating Profiling in a Democratic Constitutional State", in Hildebrandt, Mireille and Gutwirth, Serge (Eds.), Springer, 2008, pp. 271-302). However, Ronald Leenes rightly replies opacity is a limited instrument (ibídem, 300)).

[4] Article 15 of the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. A comparative analysis of commercial profiling, with also references to Article 22 GDPR and automated profiling at Indra Spiecker genannt Döhmann et al., "The Regulation of Commercial Profiling – A Comparative Analysis", European Data Protection Law Review, Vol. 2, Num. 4, 2016, pp. 535-554.

[5] A general perspective on privacy enforcement at Wright, David, "Enforcing Privacy", in Wright, David and De Hert, Paul, Enforcing Privacy. Regulatory, Legal and Technological Approaches, Springer, 2016, pp. 13-49.

[6] Zeni N., Mich L., Mylopoulos J., "GaiusT 2.0: Evolution of a Framework for Annotating Legal Documents", in Garoufallou E., Subirats Coll I., Stellato A., Greenberg J. (Eds), Metadata and Semantics Research, MTSR 2016, col. Communications in Computer and Information Science, vol 672, Springer.

[7] Sartor. Giovanni, Casanovas, Pompeu, Biasiotti, Maria Angela, Fernánedz-Barrera, Meritxell (Eds.), Approaches to Legal Ontologies. Thoeries, Domains, Methodologies, Springer, 2011.

[8] Sartor has described the possibilities to formalise the reasonableness in legal decision-making (Sartor, Giovanni, "A Suf?cientist Approach to Reasonableness in Legal Decision-

Making and Judicial Review", in G. Bongiovanni et al. (Eds.), Reasonableness and Law, Law and Philosophy, Library 86, 2009, pp. 17-68). Although this is a valuable effort to enhance judicial review, it is not clear in our opinion it can effectively empower the oversight unless it is complemented by other measures.

[9] Other authors simply consider transparency too limited and suggest other frameworks (Zarsky, Tal, "The Trouble with Algorithmic Decisions: An Analytic Road Map to Examine Efficiency and Fairness in Automated and Opaque Decision Making", Science, Technology, & Human Values, 2016, Vol. 41, 1, pp. 118-132).

[10] http://www.nanosafetycluster.eu/

[11] Lobbies are obviously yet present in the current legal drafting and perhaps with informal platforms the origin of the amendments will be more transparent. See, for instance, the description of lobbyists' activities during the GDPR drafting at Albrecht, Jan Philipp, "Regaining Control and Sovereignty in the Digital Age", Enforcing Privacy. Regulatory, Legal and Technological Approaches, Springer, 2016, pp. 473-488.

[12] http://www.privacyenforcement.net. Joined enforcement authorities in a "sweep", or collaboration for a concrete task, is a good example of joining forces to offer better safeguards. Kohnstamm, Jacob, "Getting Our Act Together: European Data Protection Authorities Face Up to Silicon Valley", in Wright, David and De Hert, Paul, Enforcing Privacy. Regulatory, Legal and Technological Approaches, Springer, 2016, pp. 455-472. The EDPS in the Opinion 8/2016, on coherent enforcement of fundamental rights in the age of big data, on 23 September 2016, suggests also a Digital Clearing House for enforcement in the EU digital sector, a voluntary network of regulatory bodies to share information.

[13] ENISA, Privacy by design in big data. An overview of privacy enhancing technologies in the era of big data analytics, Final 1.0 December 2015.

[14] ENISA, Rekleitis, E. (ed.), Big Data Threat Landscape and Good Practice Guide, January 2016.

[15] Discrimination not only affects ethnic minorities, but also people with mental illness (Monteith, Scott and Glenn, Tasha, "Automated Decision-Making and Big Data: Concerns for People with Mental Illness", Curr Psychiatry Rep, 2016, Num. 18, 112).

[16] ENISA, Privacy and Data Protection by Design – from policy to engineering, December 2014.

[17] Lammerant, Hans and De Hert, Paul, "Visions of Technology. Big Data Lessons Understood by EU Policy Makers in Their Review of the Legal Framework on Intellectual Property Rights, Access to and Re-use of PSI and the Protection of Personal Data", in Gurtwirth, Serge, Leenes, Ronald and De Hert, Paul (Eds.), Data Protection on the Move. Current Developments in ICT and Privacy/Data Protection, Springer, 2016, pp. 163-194 [165-167].

[18] ENISA, Privacy by design in big data. An overview of privacy enhancing technologies in the era of big data analytics, Final 1.0 December 2015.

[19] Noriega, P. and de Jonge, D., "Electronic Institutions: the EI/EIDE Framework", in Aldewereld, H., Boissier, O., Dignum, V., Noriega, P. and Padget, J. (Eds.), Social Coordination Frameworks for Social Technical Systems, Springer, 2016, pp. 47-76.

[20] D'Inverno, M., Luck, M., Noriega, P., Rodríguez-Aguilar, J.A. and Sierra, C., "Communicating Open Systems", Arti?cial Intelligence 186, 2012, pp. 38–94.

[21] Noriega, Pablo (1999), Agent-mediated auctions, The Fishmarket metaphor. Ph.D. thesis, Universitat Autònoma de Barcelona. Number 8 IIIA-CSIC monograph series.

[22] Botti, V., Garrido,V., Giret, A. and Noriega, P., "The Role of MAS as a Decision Support Tool in a Water-Rights Market", in F. Dechesne et al. (Eds.): AAMAS 2011 Workshops, LNAI 7068, 2012, pp. 35–49.

[23] Bogdanovych, A., Rodríguez, J.A., Simo?, S., Cohen, A.and Sierra, C., "Developing Virtual Heritage Applications as Normative Multiagent Systems", in M.-P. Gleizes and J.J. Gomez-Sanz (Eds.), AOSE 2009, LNCS 6038, 2011, pp. 140–154.

[24] In the same vein, Danaher claims for "some combination of reviewability and enhancement" (Danaher, John, "The Threat of Algocracy: Reality, Resistance and Accommodation", Philos. Technol. (2016) 29, pp.245–268).

[25] In the same vein, see Coudert, Fanny, "The Legitimacy of Bulk Transfers of PNR Data to Law Enforcement Authorities under the Strict Scrutiny of AG Mengozzi", European Data Protection Law Review, Vol. 2, Num. 4, 2016, pp. 596-601.

[26] Gutwirth and De Hert claim for bringing profiling demands to the judges. They suggest the US Google case has included judicial concrete analysis of the necessity of the profiling and this could be also interesting for European courts (Gutwirth, Serge and De Hert, Paul, "Regulating Profiling in a Democratic Constitutional State", in Hildebrandt, Mireille and Gutwirth, Serge (Eds.), Springer, 2008, pp. 271-302).

[27] Zhang, Sheldon X, Roberts, Robert E. L. and Farabee, David, "An Analysis of Prisoner Reentry and Parole Risk Using COMPAS and Traditional Criminal History Measures", Crime & Delinquency, 2014, Vol. 60 (2) pp. 167 –192; Hamilton, Zachary, Campagna, Alex K.M., Barnoski, Robert, Lee, Stephen, Van Wormer, Jacqueline, Block, Lauren, "The Development and Validation of the STRONG-R Recidivism Risk Assessment", Criminal Justice and Behavior, 2016, Vol. 43, No. 2, February 2016, pp. 230 –263.