AI-Supported Decision-Making under the General Data Protection Regulation

Maja Brkan
Faculty of Law, Maastricht University, The Netherlands
maja.brkan@maastrichtuniversity.nl

ABSTRACT

The purpose of this paper is to analyse the rules of the General Data Protection Regulation on automated decision making in the age of Big Data and to explore how to ensure transparency of such decisions, in particular those taken with the help of algorithms. The GDPR, in its Article 22, prohibits automated individual decision-making, including profiling. On the first impression, it seems that this provision strongly protects individuals and potentially even hampers the future development of AI in decision making. However, it can be argued that this prohibition, containing numerous limitations and exceptions, looks like a Swiss cheese with giant holes in it. Moreover, in case of automated decisions involving personal data of the data subject, the GDPR obliges the controller to provide the data subject with 'meaningful information about the logic involved' (Articles 13 and 14). If we link this information to the rights of data subject, we can see that the information about the logic involved needs to enable him/her to express his/her point of view and to contest the automated decision. While this requirement fits well within the broader framework of GDPR's quest for a high level of transparency, it also raises several queries particularly in cases where the decision is taken with the help of algorithms: What exactly needs to be revealed to the data subject? How can an algorithm-based decision be explained? Apart from technical obstacles, we are facing also intellectual property and state secrecy obstacles to this 'algorithmic transparency'.

CCS CONCEPTS

• **Security and privacy** → Human and societal aspects of security and privacy; Privacy protections;

KEYWORDS

Data protection; GDPR; automated decision-making; algorithmic transparency; right to explanation

ACM Reference format:
Maja Brkan. 2017. AI-Supported Decision-Making under the General Data Protection Regulation. In *Proceedings of ICAIL '17, London, United Kingdom, June 12-16, 2017,* 6 pages.
https://doi.org/10.1145/3086512.3086513

ICAIL '17, June 12-16, 2017, London, United Kingdom

ACM ISBN 978-1-4503-4891-1/17/06…$15.00
https://doi.org/10.1145/3086512.3086513

1 INTRODUCTION

'This is beautiful,' acclaimed Fan Hui, the multiple European Go champion, when he saw Google's AlphaGo making an unconventional move during a Go game (Metz 2016). AlphaGo eventually won the ancient game, much more complex than chess, and proved that machines could outperform humans…again. For example, an AI outperformed a human also in playing chess (AI Deep Blue) and Jeopardy (AI Watson). With the rise of intelligent machines, the input of big data and more or less complex algorithms, numerous decisions can nowadays be taken entirely automatically. Automated decision-making should be defined as taking a decision without human intervention; according to the General Data Protection Regulation (GDPR), 'automated individual decision-making' is 'a decision based solely on automated processing' (Article 22(1) GDPR). The human can of course feed the system with data – although even this can be an automatic procedure – and interpret the decision once it is taken. If the automated decision-making does not have any binding effect on data subjects and does not deprive them of their legitimate rights, such decision-making is of a low impact. However, when a decision is binding for individuals and affects their rights, by deciding for example that a client should be awarded credit, tax return or to be employed, the law has to provide sufficient safeguards to protect this individual. Further questions of efficiency and fairness in automated decision-making have been also discussed in the legal doctrine (Zarsky 2016).

The purpose of this paper is to analyse the rules of the GDPR on automated decision making in the age of Big Data and to explore how to ensure transparency of such decisions, in particular those taken with the help of algorithms.

2 GDPR AND ITS TAKE ON AUTOMATED INDIVIDUAL DECISION-MAKING

Automated decision-making seems to encompass a multitude of decision types, ranging from displaying search results, profiling, high-frequency trading (Pasquale 2015, Loveless et al. 2013), decisions on granting of a loan by a bank, administrative decisions (Perry 2017) (such as deciding which company to check for tax purposes) and to a certain extent even judicial decisions (Bench-Capon/Gordon 2015, Sartor/Branting 1998, Christin et al. 2015). The notion of automated decision-making is not a unitary concept, comprising only a particular type of decisions. Rather, it is broad, multifaceted and prone to be divided into several sub- categories. In this section, we first analyse the limitations on automated decision making stemming from the GDPR before turning to further classification of this concept.

It does not come as a surprise that the GDPR, in its Article 22, prohibits automated individual decision- making, including profiling. According to the first paragraph of this provision, '[t]he data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.' One the one hand, this provision continues the legacy of the Directive 95/46/EC (Data Protection Directive), where such decision-making was allowed only for entering into contract or if authorised by law that also provided safeguards for the data subject's legitimate interests Article 15. On the other hand, Article 22 GDPR reflects the European scepticism towards biases and potentially false decisions that can be taken by automated means. On the first impression, the general prohibition of such automated decisions comes across as a forceful fortress for strongly protecting individuals and potentially even hampering the future development of AI in decision making. However, on a more comprehensive level of evaluation, it can be argued that this prohibition, containing numerous limitations and exceptions, looks like a Swiss cheese with giant holes in it.

On the one hand, automated decision-making, including profiling, is still allowed in certain cases. The first possibility is if such a decision is necessary to enter into or perform a contract between the data subject and a data controller (Article 22(2)(a) GDPR). These 'algorithmic contracts' (Scholz 2017) are ever more frequent in online trading, Amazon being the most used example. We argue that this 'contract exemption' will allow for automated decisions in the field of banking and insurance (e.g. loan and insurance contracts). Secondly, such decisions and profiling are allowed if they are authorised by Union or Member State law providing sufficient safeguards to the data subject. And lastly, they are allowed if based on the explicit consent of data subject. When it comes to profiling, it is questionable whether these criteria could ever be fulfilled. Profiling does not require a conclusion of contract and is neither, to our knowledge, specifically allowed by Union or Member State law – in fact, it is prohibited by GDPR. Moreover, it is often done without data subject even knowing about it (Article 29 Working Party). Whether you give explicit consent to profiling with an explicit consent to cookies is, in our view, questionable. Will the online companies, for example search engines, have to require a separate consent for profiling? Companies like Facebook can include such explicit consent into their privacy notices, whereas for search engines this is not possible. This point of GDPR therefore remains contested.

On the other hand, the prohibition of automated decision-making itself contains several limitations. The first limitation of this prohibition is that it applies only for *individual* decision-making which should be understood as prohibition applying for a particular natural person (a single data subject). Individual decisions can be binding on an individual (such as a decision on loan application, credit card application, welfare and financial decisions, granting a visa, choosing taxpayer for audit, selecting an air traveller for search) or non-binding (such as profiling). The textual interpretation of Article 22 GDPR seems to exclude *collective* decisions affecting several natural persons or a group of those together (multiple data subjects) either by virtue of their common characteristics, their belonging to a group or their living in a particular area (Mantelero 2016). An illustration of such a collective decision is, for example, a machine-based decision by the police to increase police monitoring in a certain geographical area. With the increasing importance and use of big data, collective automated decision-making is steadily increasing. Classifying multiple data subjects into a specific category (man/woman, low/high income) might influence collective decisions pertaining to this group. This circumstance of excluding collective automated decisions from the scope of application of GDPR creates an enormous imbalance in how individual and collective automated decisions are treated. It is submitted that a way to circumvent this limitation of the GDPR is to consider the decision taken regarding a group as actually being a bundle of individual decisions. We argue that a purposeful interpretation of Article 22 GDPR could lead to this result.

Secondly, the decision has to be based *solely* on automated processing. This means that as soon as a human takes the final decision, using the machine/algorithm only as decision support, such automated processing is no longer prohibited. Third, the GDPR prevents only decision-making, including profiling, which produces legal effects for the individual or significantly affects the individual. While it is relatively easy to determine which decision would have legal effects on an individual, it is less clear what kind of profiling 'significantly affects' such individual. For example, does sending advertisements by Google and Facebook 'significantly affect' an individual? We argue that this question should be answered in the negative, although it would be beneficial for the data subject if the notion of 'significantly affect' would have a broad meaning so as to include this type of profiling. Apart from the text of the GDPR, further clarifications and classifications need to be put forward. It is important to distinguish between procedural and substantive automated decision-making; algorithmic and non-algorithmic automated decision-making; and rule-based as opposed to law-based decisions.

Procedural/substantive. The procedural/substantive divide does not refer to taking procedural or substantive decisions; it rather means that automated decisions will have to be adopted in a way that guarantees procedural and substantive fairness and accurateness. The requirement of procedural fairness requires that all decisions relating to the same or comparable facts are taken according to the same automated procedure. This procedural fairness is closely linked with substantive fairness since it would lead to the result that the same cases would have the same outcome. However, decisions also have to be substantively fair, meaning that they should not be discriminatory in any way, especially not on the basis of algorithms (Goodman 2016).

Algorithmic/non-algorithmic. Algorithmic decision-making is automated decision-making with the support of algorithms. There is no common definition of the notion of algorithm across literature. A general definition of algorithms would be, according to Coormen, "a set of steps to accomplish a task" (Coormen 2013). However, it has to be specified that, in automated decision-making, we are dealing with computer algorithms that can be defined as "a set of steps to accomplish a task that is described precisely enough that a computer can run it" (Coormen 2013). It is presumed that many – if not most – automated decisions nowadays are taken with a

support of algorithms. With the increasing use of big data and more and more complex decision-making, algorithmic intervention has become almost indispensable.

Rule-based/law-based automated decisions. In fact, both 'rule-based' and 'law-based' decisions are taken on the basis of rules, but the source of the rule for both types of decisions is different. For rule-based decisions the rule is mostly an outcome of a business decision, for example profiling for the purposes of targeted advertising (e.g. a company sending an advertisement about vacation in Bali to all people searching for vacation in Asia). The law-based decisions are based on a legal rule that is binding on everyone. If we use the example above: everyone who exceeds the speed limit gets a fine. Unless the law-based rule is very clear and precise, the decisions based on law have to face a challenge of law's open texture and notions requiring interpretation. Autonomous decision-making presupposes that the rules needed to be applied are not prone to interpretation and do not leave to the decision-maker any discretion in taking the decision. However, the authorities responsible for taking decisions (let it be administrative, judicial or other) often have a broader or narrower field of discretion when taking their decisions. Imagine there is a legal provision that entails such discretion and that would need to be applied by a machine to a particular set of facts. A human can interpret this particular provision in a way to reach this fair decision. This leads us to a consideration that the current laws are not drafted for automated decisions. If the laws, however, used 'controlled natural language', it would be much easier to take automated law-based decisions.

3 SAFEGUARDS IN AUTOMATED DECISION-MAKING: REVEALING THE LOGIC BEHIND THE DECISION

In case of automated decisions involving personal data of the data subject, the GDPR obliges the controller to provide the data subject with 'meaningful information about the logic involved' in such decision-making, regardless of whether the personal data is collected from the data subject (Article 13(2)(f) GDPR) or not (Article 14(2)(g) GDPR). These provisions fit well within the broader framework of GDPR's quest for a high level of transparency which requires that the processing of personal data should be transparent to natural persons whose personal data are 'collected, used, consulted or otherwise processed' (Recital 39 GDPR). The principle of transparency of data processing, epitomised in Article 5(1)(a) GDPR, requires not only that the information to the data subject is 'concise, easily accessible and easy to understand' (Recital 58 GDPR), but also that the data subject is informed 'of the existence of the processing operation and its purposes' (Recital 60 GDPR). Given the circumstance that the transparency within the GDPR relates to the particular individual and not to the society at large, it can be understood as 'individual transparency' as it gives the data subject rights of access, explanation and understanding the reasons behind a decision in case of automated processing. EDPS correctly points out that it is not up to individuals to seek disclosure of such logic, but that the organisations have to proactively seek for such transparency (EDPS Opinion 7/2015).

This quest for transparency, however, raises several questions: what exactly needs to be revealed to the data subject? How detailed does the explanation have to be? If we link this information to the rights of data subject, we can see that the information about the logic involved needs to enable the data subject to express his or her point of view and to contest the automated decision (Article 22(3) GDPR). However, we argue that this information goes beyond the information that needs to be offered to the data subject in all cases of data processing, such as the identity of a controller or the purposes for which personal data is processed (Articles 13 and 14 GDPR). Therefore, we submit that the meaningful information about the logic involved should comprise at least: (a) information about the data that served as the input for automated decision, (b) information about the list of factors that influenced the decision, (c) information on the relative importance of factors that influenced the decision, and (d) a reasonable explanation about *why* a certain decision was taken (textual information).

Thus, in order to comply with the GDPR requiring that the logic behind the decision must be explained to the data subject, it is not enough to ensure merely what Kroll et al. (2017) term 'procedural regularity'. Such procedural regularity ensures only that the decisions are based on the same decision policy, that the policy was determined before knowing the inputs and that the outcomes can be reproduced. It therefore addresses only aggregate procedural regularity of all cases, safeguarding that all cases are decided upon the same rules. However, the concept of procedural regularity does not answer the question of *why* the algorithm reached a certain decision with a certain dataset as an input. The transparency required by the GDPR is of a different kind: the data subject has to understand reasons behind the decision.

The individual transparency relating to non- algorithmic automated decisions will not pose particular problems regarding the explanation of the logic behind the decision. For example, if a camera detecting the speed of the driver communicates to the public authorities that the speed limit was exceeded, the issuing of speeding ticket follows automatically. The logic behind the decision as well as the rule on which the decision is based can be easily explained to the data subject: speeding ticket is issued if the speed limit is exceeded (taking into account the correction factor if applicable).

Differently, automated decision-making based on algorithms faces numerous complications when it comes to the explanation of the reasons underlying a decision. As the technology advances and the use of algorithms for decision-making is exponentially growing, both the legal regulation and academic work requires more transparent algorithmic decision-making, often described with the buzzword 'algorithmic transparency'. The basic quest of proponents of algorithmic transparency is to reveal the logic behind the algorithm that adopts a certain decision. While some commentators consider that it is near to impossible to explain an algorithm because even its developers cannot exactly pinpoint the reasons why a particular decision was taken (Metz 2016), others take a more optimistic approach (Kroll et al. 2017) and even propose technical solutions (Datta et al. 2016) that would lead to a higher algorithmic transparency. Algorithmic transparency is deemed to cover different transparency degrees from revealing a source code to an explanation of its functioning. For the purposes of this paper, we believe that the algorithmic transparency, legally speaking, should

encompass transparency of the process of algorithmic decision-making to the extent that this is necessary to ensure the respect of rights under the GDPR, notably the information to the data subject about meaningful information about the logic involved. Technically speaking, the degree to which the functioning of the algorithm is revealed might be different for different decisions.

4 OBSTACLES TO ALGORITHMIC TRANSPARENCY

It is submitted that there are several obstacles that stand in a way of giving a data subject a meaningful explanation of logic behind algorithmic decisions. Burell distinguishes between three types of opacity of algorithms: corporate or state secrecy; technical illiteracy; and opacity arising from characteristics of machine learning (Burrell 2016). Among the obstacles to algorithmic transparency are therefore the following: (1) technical obstacles, (2) intellectual property obstacles and (3) state secrets and other confidential information of state authorities.

4.1 Technical obstacles

The amount of technical obstacles standing in a way of explaining algorithmic-based autonomous decisions depends on the complexity of an algorithm. Many authors claim that it is nearly impossible to explain the logic behind an algorithm taking a decision. The reasons for a decision on the basis of a simple decision tree could perhaps still be explained. However, if the algorithm used is a neural network, working with big data and prone to very fast learning, then it will be close to impossible to explain the reasons behind its decision. Masnick claims that the faster the machine learns, the more difficult it is to understand the reasons behind its decisions (Masnick 2016). Moreover, Metz points out that deep neural networks 'generate complex algorithms that can be opaque even to those who put these systems in place' (Metz 2016, *cf* also Goodman 2016). However, Datta et al. developed a system called Quantitative Input Influence (QII) that could explain autonomously-made decisions (Datta et al. 2016). The idea behind QII is that the degree of influence from input data to output data could be measured. It seems that, in order to reach the transparency of an algorithm, another algorithm would need to be developed to clarify which factors were taken into account and what was their weight (AI Room document). It appears that requiring a human to explain a decision made by an artificially intelligent software (or machine) runs into difficulties. We therefore submit that it would be more appropriate to let software explain an automated decision. A better approach to algorithmic transparency would thus be to explain the logic behind an algorithm with help of another algorithm. Of course, a cost-benefit analysis of such an approach would need to be made.

4.2 IP-related obstacles: a paper tiger?

To a certain extent, intellectual property rights can also build obstacles for algorithmic transparency. We submit that this is not the case as far as patent and copyright are concerned. Differently, trade secrets or confidential information can stand in a way of algorithmic transparency.

Even though the European Patent Convention (EPO) allows for patenting "computer-implemented inventions" (Article 52(2)(c)), it is not enough that the software is inventive, but it also has to allow for an industrial application (Article 52(1)). Along this line of reasoning, the EPO does not allow to patent a computer algorithm, as the "programmer must have had technical considerations beyond 'merely' finding a computer algorithm" (Opinion of EPO G 0003/08). However, even if the algorithm was subject to a patent, this would still not create an obstacle for algorithmic transparency as having a patent would oblige the patent holder to disclose the composition and the modalities of functioning of an algorithm.

Copyright protection of a computer software leads to a similar result: while both the Agreement on Trade- Related Aspects of Intellectual Property Rights (TRIPS) agreement (Article 10(1)) and the World Intellectual Property Organization (WIPO) copyright treaty (Article 4) allow for copyright protection of software from the moment of its creation, it is not entirely clear whether algorithms themselves can be a subject matter of copyright protection (Stern, 1995, Swinson 1991). It seems that the EU does not allow for such protection and this approach is in line with some other non-European jurisdictions, such as Japan (Karjala 1991). In any event, it is worth mentioning that the Directive 2009/24/EC (EU computer programmes directive) allows the user of a computer program "to observe, study or test the functioning of the program in order to determine the ideas and principles which underlie any element of the program". In practice this means that a user of a computer programme is allowed to determine the functioning of the algorithm and, if it is technically possible, to reveal the importance of particular factors involved in the algorithmic decision-making. That would imply that even if the software and/or algorithm are protected by a copyright, such protection could not stand in a way of algorithmic transparency.

However, an IP right that does stand in the way of algorithmic transparency is a trade secret (confidential or undisclosed information). According to TRIPS, trade secret allows natural and legal persons to prevent that the information is disclosed to or used by others in a way that goes against honest commercial practices if that information is secret, has commercial value and steps have been taken to keep it secret (Article 39(2)). In its recently adopted Directive 2016/943/EU (EU Trade Secrets Directive) which follows this definition, the EU however provides for an exception that allows for suspension of a trade secret "for the purpose of protecting a legitimate interest recognised by Union or national law" (Article 5(d)). Explaining an algorithmic decision to a data subject could fall under this exception as it is provided by the GDPR and seeks to protect a legitimate interest.

Even if that exception is not applicable, we argue that algorithmic transparency does not necessarily need to run against trade secrets. In order to provide for such transparency within the GDPR, the source code or even the way the algorithm operates does not need to be disclosed. The 'logic behind the decision' from GDPR points to the (argumentative) tool that was deployed by an algorithm without the necessity to fully disclose that tool. Per analogy with computational journalism Diakopoulos points out that algorithmic transparency would command merely "the disclosure of certain key

pieces of information, including aggregate results and benchmarks" (Diakopoulos 2016).

4.3 State secrets and other confidential information

The biggest obstacles to algorithmic transparency are state secrets or other information held by public authorities that cannot be revealed to the public. It is in the interest of the state and those authorities that they do not reveal exactly why a certain decision was taken. For example, a tax authority will not reveal the algorithm that chooses taxpayers whose tax (ir)regularity needs to be checked. Likewise, customs authorities will not reveal the pattern-match system that chooses which company needs to undergo customs check. Equally, police authorities will not disclose the rule behind the choice of neighbourhood or persons to monitor, for example for the purposes of prevention of terrorism or drug trafficking.

The question of whether the algorithm should be revealed to the data subject in these situations depends on the balancing of privacy with competing interests. It is obvious that state secret or confidential information will stand in a way of algorithmic transparency, but the latter is not an ultimate value in our society that would need to always prevail over other interests. In such cases, revealing the logic behind the automated decision will depend on the proportionality analysis in each particular case.

5 CONCLUSION

On a final note, eliminating the obstacles to algorithmic transparency would not only enable the data subject to gain an insight on the reasons for which it was taken, but it would also be important in two other respects. On the one hand, it would help to eliminate the discriminatory biases in the decision-making process itself. (Newell/Marabelli 2015) Discrimination in algorithmic decision-making can arise because the datasets with which an algorithm operates might be biased and therefore the algorithm learns to be biased itself. However, some authors argue that removing biased data from the automated process can nevertheless lead to biased results (Calders and Žliobaitė 2013, Žliobaitė and Custers 2016). Recognising and being able to determine the bias is an important step in removing it and making the substantive decision fairer (Goodman 2016). On the other hand, closely linked to algorithmic transparency is accountability (sometimes also termed 'algorithmic accountability'). In fact, transparency is a predisposition for accountability. Who should be responsible if an algorithm makes a mistake or takes a discriminatory decision – the developers, the user or even the autonomous agent itself? Who is accountable if a search engine uses an algorithm that favours a particular political party instead of being politically neutral; or if it displays results regarding certain companies above the others and aims to run competitors out of business? These are challenging topics which raise questions for further research.

ACKNOWLEDGMENTS

The author would like to thank Dr. Ana Ramalho for useful insights on intellectual property protection of algorithms and Prof. dr. ir. Sjir Nijssen for helpful discussion on automated decision-making and its use by the Dutch tax and customs authorities.

REFERENCES

Agreement on Trade-Related Aspects of Intellectual Property Rights. https://www.wto.org/english/docs_e/legal_e/27-trips_01_e.htm accessed 11 November 2016.

Article 29 Working Party 2013. 'Advice paper on essential elements of a definition and a provision on profiling within the EU General Data Protection Regulation', adopted on 13 May 2013, http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20130513_advice-paper-on-profiling_en.pdf accessed 11 November 2016.

'Artificial Intelligence, Robotics, Privacy and Data Protection'. Room document for the 38th International Conference of Data Protection and Privacy Commissioners, October 2016.

Trevor Bench-Capon, Thomas F. Gordon 2015. 'Tools for Rapid Prototyping of Legal Cased-Based Reasoning' ULCS-15-005, University of Liverpool, United Kingdom.

Jenna Burrell 2016. 'How the machine 'thinks': Understanding opacity in machine learning algorithms' *Big Data & Society* 1-12.

Toon Calders, Indrėe Žliobaitė 2013. 'Why Unbiased Computational Processes Can Lead to Discriminative Decision Procedures' in Bart Custers et al. (eds.), *Discrimination and Privacy in the Information Society. Data Mining and Profiling in Large Databases*. Springer, 43-57.

Thomas H. Coormen 2013. *Algorithms Unlocked*. MIT Press.

Angèle Christin, Alex Rosenblat, Danah Boyd 2015. 'Courts and Predictive Algorithms'. Data & Civil Rights: A New Era of Policing and Justice http://www.law.nyu.edu/sites/default/files/upload_documents/Angele%20Christin.pdf accessed 16 January 2017.

Anupam Datta, Shayak Sen and Yair Zick 2016. 'Algorithmic Transparency via Quantitative Input Influence'. https://www.andrew.cmu.edu/user/danupam/datta-sen-zick-oakland16.pdf accessed 10 December 2016.

Nicholas Diakopoulos 2016. 'Accountability in Algorithmic Decision Making'. *Communications of the ACM* 56: 58-59.

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, OJ L 281, 23.11.1995, p. 31.

Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs, OJ L 111, 5.5.2009, p. 16.

Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, OJ L 157, 15.6.2016, p. 1.

European Data Protection Supervisor 2015. 'Opinion 7/2015. Meeting the challenges of big data. A call for transparency, user control, data protection by design and accountability'. https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-11-19_Big_Data_EN.pdf accessed 15 November 2016.

European Patent Convention in combination with Guidelines for Examination, point 3.6 Programs for computers, available at https://www.epo.org/law-practice/legal-texts/html/guidelines/e/g_ii_3_6.htm accessed 20 December 2016.

Bryce Goodman 2016. 'Discrimination, Data Sanitisation and Auditing in the European Union's General Data Protection Regulation'. *European Data Protection Law Review* 493.

Bryce Goodman, Seth Flaxman 2016. 'European Union regulations on algorithmic decision-making and a "right to explanation"'. https://arxiv.org/abs/1606.08813v3 accessed 1 September 2016.

Dennis S. Karjala 1991. 'Japanese Courts Interpret the 'Algorithm' Limitation on the Copyright Protection of Programs'. *Jurimetrics Journal* 233.

Joshua A. Kroll et al. 2017. 'Accountable Algorithms' (forthcoming) 165 *University of Pennsylvania Law Review*, 1, 18.

Jacob Loveless et al. 2013. 'Online Algorithms in High-frequency Trading. The challenges faced by competing HFT algorithms' 11 acmqueue 1.

Alessandro Mantelero 2016. 'Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection'. *Computer Law & Security Review* 32, 2: 238–255.

Mike Masnick 2016. 'Activists Cheer On EU's 'Right To An Explanation' For Algorithmic Decisions, But How Will It Work When There's Nothing To Explain?' https://www.techdirt.com/articles/20160708/11040034922/activists-cheer-eus-right-to-explanation-algorithmic-decisions-how-will-it-work-when-theres-nothing-to-explain.shtml accessed 10 January 2016.

Cade Metz 2016. 'The Sadness and Beauty of Watching Google's AI Play Go'. https://www.wired.com/2016/03/sadness-beauty-watching-googles-ai-play-go/ accessed 21 November 2016.

Cade Metz 2016. 'Artificial Intelligence Is Setting Up the Internet for a Huge Clash With Europe'. https://www.wired.com/2016/07/artificial-intelligence-setting-internet-huge-clash-europe/ accessed 10 January 2016.

Sue Newell, Marco Marabelli 2015. 'Strategic opportunities (and challenges) of algorithmic decision- making: A call for action on the long-term societal effects of 'datification''. *Journal of Strategic Information Systems* 24: 3–14.

Opinion of EPO G 0003/08 (Programs for computers) of 12.5.2010, ECLI:EP:BA:2010:G000308.20100512, point 13.5.

Frank Pasquale 2015. *The Black Box Society. The Secret Algorithms That Control Money and Information*. Harvard University Press, 2015.

Melissa Perry 2017. 'iDecide: Administrative Decision-Making in the Digital World'. *Australian Law Journal* (forthcoming).

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), OJ L 119, 4.5.2016, p. 1.

Giovanni Sartor, Luther Branting (eds.) 1998. *Judicial Applications of Artificial Intelligence*. Springer.

Lauren Henry Scholz 2017. 'Algorithmic Contracts'. *Stanford Technology Law Review*, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=274770 accessed 10 November 2016.

Richard H. Stern 1995. 'On Defining the Concept of Infringement of Intellectual Property Rights in Algorithms and Other Abstract Computer-Related Ideas'. *AIPLA Quarterly Journal* 23: 401.

John Swinson 1991. 'Copyright or Patent or Both: An Algorithmic Approach to Computer Software Protection'. *Harvard Journal of Law & Technology* 5: 145.

Tal Zarsky 2016.'The Trouble with Algorithmic Decisions: An Analytic Road Map to Examine Efficiency and Fairness in Automated and Opaque Decision Making'. *Science, Technology, & Human Values* 41: 118–132.

Indrė Žliobaitė, Bart Custers 2016. 'Using sensitive personal data may be necessary for avoiding discrimination in data-driven decision models'. *Artificial Intelligence and Law* 24: 183–201.