Transparancy Requirements for Algorithms and AI: Wishful Thinking?

Prof. Dr. Robert van den Hoven van Genderen

"*The Algorithm's coming-of-age as the new language of science promises to be the most disruptive scientific development since quantum mechanics.*"[1]

The use of artificial intelligence (AI) is a development that is considered ambivalent. On the one hand, it provides great opportunities to achieve results more efficiently and effectively by analyzing large amounts of different data ("big data") using AI. On the other hand, there is a fear that the use of self-learning algorithms and AI will result in more extensive damage to the already shrinking field of privacy and human control. As stated in the considerations of the General Data Protection Regulation (GDPR), the processing of personal data should be intended to serve mankind:[2]

Currently, many algorithms function like 'black boxes'. [3]*The algorithm give answers but no explanations. This is bad news if you are refused a mortgage ('algorithm says no') or if the police arrests you ('algorithm says yes').*[4]

Transparancy of Algorithms is required as a fundamental principle for processing personal data; but there are contravening interests: intellectual property rights, trade secrets and, interestingly enough, privacy of others to be balanced against the transparency requirements. And, of course, there is the general exception of article 8.2 European Convention on Human Rights (ECHR) on national security.

In the introduction to a research of the Ministry of Justice and Security in the Netherlands, researchers state that:

'transparency will need to be optimized; transparency will need to be balanced with security. The Ministry needs to be open and transparent 'where possible' and to provide security and safety 'where needed'.[5]

So the big question is: to what extend is transparency of algorithms feasible, necessary and even possible? Until what level do we need and want transparency? And is the European (GDPR) perspective on the requirement for transparency of algorithms wishful thinking?

Algorithms and Explainability

Although there are many definitions of what an algorithm really is, I'd like to use the following description: a set of mathematical instructions or rules that will calculate or process data by a computer to solve a problem or will create a certain result.

The research report to the European Parliament by Claude Castelluccia and Daniel Le Métayer give a broader description including the working of the algorithm. The authors describe an algorithm as an

---

[1] ***Bernard Chazelle,*** The Algorithm: Idiom of Modern Science, [https://www.cs.princeton.edu/~chazelle/pubs/algorithm.html]

[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) Consideration 4

[3] Frank Pasquale, The Black Box Society: The Secret Algorithms That Control Money and Information (1st ed. 2015)

[4] [https://responsibledatainnovation.wordpress.com/2018/05/23/transparency-of-algorithms/]

[5][https://responsibledatainnovation.wordpress.com/2018/05/23/transparency-of-algorithms/] (Informatiestrategie 2017-2022, pp 17, 23-24; and Informatieplan 2017, pp 15-19)

unambiguous procedure to solve a problem or a class of problems.[6] It is typically composed of a set of instructions or rules that take some input data and return output. As an example, a sorting algorithm can take a list of numbers and proceed iteratively, first extracting the largest element of the list, then the largest element of the rest of the list, and so on, until the list is empty.[7] Algorithms can be combined to develop more complex systems, such as web services or autonomous cars. An algorithm can be hand-coded, by a programmer, or generated automatically from data, as in machine learning.[8] "machine learning refers to an automated process of discovering correlations (sometimes alternatively referred to as relationships or patterns) between variables in a dataset, often to make predictions or estimates of some outcome."[9]

Explainability

In the Guidelines of Working Party 29 (WP29) and the European Data Protection Board (EDPB) reference is made to the recital 39 of the GDPR that concerning data processing:

"It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used" (...)

to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them.[10] This explanation is accentuated in the comments of recital 42 GDPR be it that it is compared to the explanation of transparency in consumer contracts:

"The requirement for clear and plain language means that information should be provided in as simple a manner as possible, avoiding complex sentence and language structures. The information should be concrete and definitive; it should not be phrased in abstract or ambivalent terms or leave room for different interpretations. In particular the purposes of, and legal basis for, processing the personal data should be clear."[11]

The problem with creating transparency and explainability of algorithms is that there are different addressees for this requirement. If the transparency of the technical functionality and decision tree has to be explained this is a task for the experts, the programmers and developers. The experts should be capable to make the technical structure of the algorithm logically comprehensible to the user/controller and the user or data subject should be informed about the consequences. However, is it necessary to be informed to be informed about the function and the consequences and effects but it is in my view not always required to know the in-depth processing aspects of the algorithm. The key question is how deep the explainability must go according to the legal requirements.

As stated in the study for the European Parliament:

---

[6] (Institut national de recherche en informatique et en automatique - Inria) at the request of the Panel for the Future of Science and Technology (STOA)

[7] See also Frederik Zuiderveen Borgesius, Discrimination, artificial intelligence and algorithmic decisionmaking, Directorate General of Democracy, Council of Europe, at 9 (2018)

[8] European Parliament, Understanding Algorithmic Decision-Making: Opportunities and Challenges, p.17 [http://www.europarl.europa.eu/RegData/etudes/STUD/2019/624261/EPRS_STU(2019)624261_EN.pdf]

[9] See David Lehr & Paul Ohm, Playing with the Data: What Legal Scholars Should Learn about Machine Learning, 51 U.C. DAVIS L. REV. 653, at 671 (2017)

[10] 17/EN WP260 rev.01 Article 29 Working PartyGuidelines on Transparency under Regulation 2016/679

[11] Idem P.8Article 5 of Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts Recital 42 states that a declaration of consent pre-formulated by a data controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms.

*Explanations (*of the working of algorithms, RHG*) can be of different types (operational, logical or causal); they can be either global (about the whole algorithm) or local (about specific results); and they can take different forms (decision trees, histograms, picture or text highlights, examples, counterexamples, etc.)*[12]

But even if the algorithm can be transparent, the outcome could be different as a result of the data input. A black box may be changed into a crystal box but one has to understand what one sees. The working of an advanced algorithm can be compared with data processing by a human child. The education, genetic information and external influences make it impossible to predict the output. A deep learning, or certainly a self learning, algorithmic system will result in a comparable unpredictable output..

The other problem is that algorithms are not a guarantee against bias. They process the given, or available, data that is based on human generated statistics and data files. One could simplify the problem statement as "bias in, bias out".[13] The awareness of these risks of the use of algorithms within decision making became a point of attention for the European Commission, by means of an in depth study, following a proposal of the European Parliament considering that:

"Algorithmic transparency is an important safeguard for accountability and fairness in decision-making. From various AI applications to ranking results in search engines, algorithms govern the way we access information online. This has large implications for consumers and businesses in areas such as online platforms. Understanding algorithmic transparency in an in-depth manner is key for informed policy-making".[14]

With reference to Lawrence Lessig it is not just technology and law but also market, architecture(nature) and social norms that ultimately determine how to cope with implementation in society.[15] I would add, or specify the constraints of Lessig, that interpretation of laws on technology also strongly depend on culture an political situation. As a result of these constraints also the interpretations of other rights and obligations covering fundamental rights, privacy, trade secrets,(national) security, public interest etc. will also limit the possibility of transparency and explainability of algorithms. This will not only be case concerning the use of algorithms used in the processing of personal data but any other application of algorithms in our algorithmic dependent society.

Covid-19

A striking example is the track&trace algorithm to follow persons and analyse their movements. The measures restricting freedom of movement and tracking systems using apps are most relevant to this. In particular, applying these apps in conjunction with public and private cameras and data analysis,… systems that use advanced algorithms (AI) can be easily misused by governments (or third parties) if not tightly regulated by existing and perhaps new privacy and security rules. The use of big (sensitive) data by third parties, such as the police, employers and tech companies produced by the app, could lead to serious breaches of everyone's privacy if not specifically controlled by, for example, the Data ©cfvProtection Authority and democratic institutions. It is therefore relevant that the regulations are clear in describing who gets access to the often sensitive data, for what specific purposes, how the data is processed, what security measures are in place, how and for how long the data is used and what

[12]http://www.europarl.europa.eu/RegData/etudes/STUD/2019/624261/EPRS_STU(2019)624261_EN.pdf Idem,
[13] Sandra G. Mayson, Bias In, Bias Out, 128 YAL. L. JOUR. 2218, 2224 (2019).
[14] https://ec.europa.eu/digital-single-market/en/algorithmic-awareness-building (study not yet available 1-1-2020)
[15] L. Lessig: The Laws of Cyberspace, https://cyber.harvard.edu/works/lessig/ laws_cyberspace.pdf.

guarantees are granted that data is not used for other purposes.[16] The European Preserving Proximity Tracing Group has developed a pan-European bluetooth proximity tracking app similar to tracking apps in China, South Korea, Singapore and India; although additional account must be taken of privacy requirements.[17] The group indicates that

"The underlying technology, which is being developed in constant exchange with data protection experts and ethicists, should make an important contribution to enabling close cross-border tracing with respect for privacy. It is scalable and open and can be used by any country."

The World Health Organization is also convinced of the usefulness of the corona app and even states that developing and using an app is an international obligation:

"*Member States are obliged under the International Health Regulations to develop public health surveillance systems that capture critical data for their COVID-19 response, while ensuring that such systems are transparent, responsive to the concerns of communities, and do not impose unnecessary burdens, for example infringements on privacy*".[18]

Despite the positive presentation of the expected results of the use of the app by governments and, of course, by the producers, the positive effects are questionable. Experience in Iceland, the most "app-dense" country, with covid-app was not a game-changer.[19] Even pseudonymized, data collected with the right algorithm can be analyzed, making individuals identifiable. In addition, it has already been found that some apps also contain ad-generating algorithms.[20] In addition, the reliability of the app is questionable*:*

"None of the data sources […] are accurate enough to identify close contact with sufficient reliability".[21]

The choice of the platform and the underlying technology also raised doubts. There no transparency at all because the app is based on a platform developed by Google/Apple, not specifically famous for their privacy consciousness an transparency. Quite a few inaccuracies were found in a worldwide research into 80 imported corona contact apps based on the Google / Apple model that was conducted earlier this year..[22] In deciding whether or not using an app to combat the spread of the virus that will

---

[16] See R. 54 GDPR: Such processing of data concerning health for reasons of public interest should not result in personal data being processed for other purposes by third parties such as employers or insurance and banking companies.

[17] https://www.pepp-pt.org/content

[18] Ethical Considerations to Guide the Use of Digital Proximity Tracking Technologies for COVID-19 Contact Tracing Interim Guidance, 28 May 2020, Referring to the International Health Regulations - 2nd ed. Geneva; World Health Organization;

[19] [https://www.technologyreview.com/2020/05/11/1001541/iceland-ranking-c19-covid-contact-tracing/]

[20] We found code relating to Google's advertising and tracking platforms in 17 contact tracing apps. This includes AdSense, Google's advertising network that allows publishers to make money by showing ads to their users, and also the much more powerful Google Ad Manager, formerly known as DoubleClick for Publishers, which allows publishers to show ads from a huge array of sources.
[https://www.top10vpn.com/research/investigations/covid-19-digital-rights-tracker/]

[21]

Jay Stanley and Jennifer Stisa Granick, The Limits of Location Tracking in an Epidemic, ACLU, April 2020 [https://www.aclu.org/report/aclu-white-paper-limits-location-tracking-epidemic

[22] 25 apps (53%) do not disclose how long they will store users' data for; 28 apps (60%) have no publicly stated anonymity measures; 24 apps (51%) contain Google and Facebook tracking; 9 apps contain Google AdSense

be mandatory for all citizens, all competing interests of those involved authorities, service providers and the public interest - should be considered.[23] In the Netherlands it became known that also the military used the corona crisis to make use of algoritms to analyse a.o the information that came out of the use of this app (used by 4 mln citizens) and follow groups which spread "fake news". This is evident from a reconstruction of the Land Information Maneuver Center (LIMC), a unit that the defense set up in mid-March to gain insight into the corona crisis and the spread of disinformation.[24] There must be openness and transparency during the selection process under the supervision of a parliamentary committee and the privacy regulator. Even after the Privacy Impact Assessment (PIA) was carried out, it appeared that guarantees could not be given. In addition to privacy issues, it is also relevant to monitor the psychological and sociological aspects of the possible implementation of the app. That means it is imperative that the development of the app is not (only) left to a private tech company.

Interpretation of Algorithms

In the case of interpretability, the point is that the outcome of an algorithm should be explained in comprehensible language, but what is comprehensible, for which parties? [25] Technical transparency can contribute to a certain extent, but it also has its limits. The problem is a problem of choice: Which variables will be taken into account? Some algorithms can include thousands of features in their reasoning process. The outcome of the algorithm is then based on so many factors that it is difficult to see which factors were decisive for the outcome. This also makes it difficult to understand or influence the conclusion. Secondly, some models used with self-learning algorithms are inherently opaque. This is particularly the case with deep learning neural networks. It will be easier to analyze afterwards on which information an algorithm bases its outcome.

The bottleneck in the development of AI now is crossing the correlation to causality. Take a classic example: When ice cream sales rise significantly, the number of people drowning in pools an accidents at the beach escalate as well. But ice cream probably doesn't cause drowning. Under operating AI technology, we can only know the result, but don't know how and why this result is reached. This is the difficulty of explaining the relevance.

Wachter et al. argue that "explainability" needs not rely upon general public understanding of how algorithms function, but should be oriented on the explanation of the purpose of the use of the algorithms, more in the sense of instructing the subjects to understand the goal of the process.[26] For as

---

trackers; 11 apps contain Google conversion tracking and re-marketing code; 7 apps include code from Facebook. [https://www.top10vpn.com/research/investigations/covid-19-digital-rights-tracker/]

[23] Mittelstadt et. al. have listed a number of factors to be taken into account, including: the presence of an overriding public interest in disease prevention; the likelihood of believing that the use of a person's data will contribute to disease prevention; the risks that those involved may run; understanding the purposes of data use by data subjects; using only the smallest amount of necessary personal data; the inclusion of harm reduction strategies throughout the process. For more information: Mittelstadt B, Benzler J, Engelmann L, Prainsack B, Vayena E. "Is there a duty to participate in digital epidemiology?". Life Sci Soc policy. 2018; 14 (1): 9. Published May 9, 2018. Doi: 10.1186 / s40504-018-0074-1

[24] Quality Netherlands newspaper, NRC, 15 November: [https://www.nrc.nl/nieuws/2020/11/15/hoe-het-leger-zijn-eigen-bevolking-in-de-gaten-houdt-a4020169]

[25] See generally, JUDEA PEARL, DANA MACKENZIE, THE BOOK OF WHY: THE NEW SCIENCE OF CAUSE AND EFFECT (1st ed. 2018). 15 Michael Blastland, Just because?, BBC News

[26] Sandra Wachter, Brent Mittlestadt & Chris Russel, "counterfactual explanations without opening the black box: Automated decisions and the GDPR, Harvard Journal of Law & Technology Volume 31, Number 2 Spring 2018

far as it necessary to explain they suggest three aims for explanations directed on: understanding the decision; inform the data subject of grounds an possibility to contest the decision and create a possibility to change the decision making model in future.

In a conference on regulation of algorithms in Kyushu Japan, professor Burkhart Schäfer suggested the possibility of "algorithmic apologies" as the mirror image of Wachter's counterfactual explanations[27]. Putting the analysis in the context of recent Scottish legislative initiatives that created a legal framework for "apologies", he argues that "apologies" as a form of explanation are technologically feasible and fulfil a distinct legal purpose.[28]

Also the Netherlands Minister on Legal Protection admits that certainly with deeplearning algorithms the input data can be variable and not fixed so that it will be difficult to what extent this causes a change in the output. He states that analysis will be a very time-consuming process. Referring to the fact that there still will be a need for a certain need for all parties of society (companies, scientists, governments) to be credible in their decisionmaking, processes need to demonstrate the importance of traceable results of algorithms he also leans on the ex-post explanation. Therefore he states that against this background, when algorithms can be explained, the focus is on describing the goal that the algorithm aims to achieve, which variables have been decisive for the outcome, the type of data used, and any decision rules. Naturally, this does not affect the fact that, as for instance justice and criminal procedures as well as relating to national security there may be grounds in the light of existing laws and regulations to limit the degree of interpretability.[29] Although he does not explain how far this limitation stretches, if for instance this also should apply when algorithms are used to make predictions or to estimate risks.

High level ethical requirements as part of legal requirements?

Inherently to the character of ethical principles the requirements for ethical requirements for the programming and use of algorithms, another escape from more concrete specifications is to be expected. Every self respecting international organisation, Council of Europe, OECD and the EU has issued guidelines for ethical use of AI and/or algorithms. For the sake of clarity I will limit myself to the ethical guidelines of the European Group on Ethics in Science and New Technologies Ethical Principles and Democratic Prerequisites and the Council of Europe, be it that they are directed to the use of AI in general, not specifically on the use of algorithms.[30] The literature and perspectives of organisations though, generally mix the use of AI and the underlying algorithms.

As is to be expected, the European Ethical Guidelines on AI state very high level that AI should be robust, fair and trustworthy. According to the Guidelines, trustworthy AI should be:
(1) Lawful - respecting all applicable laws and regulations;

(2) Ethical - respecting ethical principles and values;

(3) Robust - from a technical perspective while taking into account its social environment.

This would result in the following sub requirements for ethics:

---

[27] Wachter et al proposed a model of "explanations through counterfactuals" which would allow the affected parties to improve their submissions next time round.

[28] Conference on Multidisciplinary Perspectives on Algorithms,Regulation, Governance, Markets, Kyushu University,21-23 november [https://www.kyushu-university-law.com/]

[29] Based on the explanation of the minister of Legal protection in:

Tweede Kamer der Staten-Generaal 2018-2019 26643 nr. 570

[https://zoek.officielebekendmakingen.nl/kst-26643-570.html#ID-857880-d36e228]

[30] [https://ec.europa.eu/research/ege/pdf/ege_ai_statement_2018.pdf]

(a) Human dignity: respect for the human values in the use of algorithmic processing
(b) Autonomy: of humans (not AI entities!)
(c) Responsibility: AI research and application to align with a plurality of fundamental human values and rights
(d) Justice, equity, and solidarity: non discriminatory equal access to 'autonomous' technologies and fair distribution of benefits and equal opportunities across and within societies
(e) Democracy: publically informed key decisions on the regulation of AI development
(f) Rule of law and accountability: unbiased access to justice and the right to redress and a fair trial
(g) Security, safety, bodily and mental integrity

The Council of Europe, to be precise , the Consultative Committee Of The Convention For The Protection Of Individuals With Regard To Automatic Processing Of Personal Data, in her Guidelines proposes a comparable set, logically more specifically oriented on the aspect of privacy as it concerns Convention 108:

Key Elements of this Approach are:

- lawfulness, fairness, purpose specification, proportionality of data processing, privacy-by-design and by default, responsibility and demonstration of compliance(accountability),
- transparency, data security and risk management.
- AI applications should allow meaningful control by data subjects over the data processing and related effects on individuals and on society.[31]

Is this enough to instruct governments and industry to use AI in a human friendly and respectful way and could it also be considered of elements on regulating the development and use of algorithms? There is a broad range of ethical aspects that could be taken in consideration but not needs to be engraved in legal norms. As stated before it all depends on the use and functionality of the algorithmic processing of personal data. The use in governmental decisionmaking or as part of court decisions requires different explanation than the use of data for surgery or autonomous vehicles. Therefore it is necessary to have knowledge about the technical aspect of the working of algorithms as well as to know what the influence of the use of algorithms has on our daily life. In this influence there are always two sides of the medal; algorithms can enhance knowledge and improve efficient en well informed decision making, creating better results and less faults. On the other side the use of algorithms can have a negative influence on our privacy, can create dependency on those applications, can create bias and can disturb social contacts and transparency of decision making and legal procedures.

Therefore the European Commission strives for Algorithm awareness building:

Algorithmic transparency is an important safeguard for accountability and fairness in decision-making. From various AI applications to ranking results in search engines, algorithms govern the way we access information online. This has large implications for consumers and businesses in areas such as online platforms. Understanding algorithmic transparency in an in-depth manner is key for informed policy-making.[32]

In the following paragraphs I will scrutinize the necessity of legal requirements for transparency of algorithms and the means of actual controlling the technical working of algorithms and transparency of the process as being understandable for the data subject.

The use of AI and algorithms by government and industries.

[31] [https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8]
[32][https://ec.europa.eu/digital-single-market/en/algorithmic-awareness-building]

There is a natural tendency to use any new technology to improve control of the public, be it for governing or to sell products. Airbnb, Google, LinkedIn, Tesla, Microsoft and hundreds of other companies are using algorithms to profile their customer to ”create better services.” Will it be possible to create a legal framework that will take into account the ethical aspects as well a practical measures to scrutinize the development and application of algorithms in a broad sense? Or is the variety for the application and use of algorithms inherently so big that only high level principles could present a guideline how to deal with an “algorithmized” society? Too many rules could be detrimental, working as”chilling factor’ to the further development and use of algorithms. To regulate this multi-differential multi-technical and multi-functional engine for AI systems, robots and human behaviour is a very difficult task. Fear of the unknown should in any case not be a guideline for restrictive regulations for the development and application of algorithms. However, the prevention of negative aspects of the application of algorithmically supported decision-making must be taken into account.

The actual use of algorithms for profiling, Algorithm Based Decision making (ADS) Use for Risk assessment in Criminal behaviour and Fraud Investigations

Government and business are happy to resort to the use of AI for profiling citizens and customers. In addition, (deep / self) learning algorithms are fed with (big) data, which form the basis of the system. Analyzing that data leads to results that lead to analysis that lead to results that form the basis for decision-making.

Well-known examples of support in the use of Algorithm based decision (ADS) making are face recognition, license plate registration and population screening based on background and behavioural data of citizens. Systems in the Netherlands such as SyRi (System Risk Indication) - in which the government combines the personal data of citizens to detect various forms of fraud, abuse and violations - seem to be surpassing their goal.

On 5 February 2020, the Court of The Hague ruled that SyRI (System Risk Indication) legislation is contrary to the European Convention on Human Rights.[33] This case was brought by a large number of civil society organizations against the use by the State of the Netherlands to detect and combat fraud in a number of "risk areas" with the help of data linking and analysis using algorithms. The court ruled that there was insufficient balance between the use of new technologies such as AI, data analysis, algorithms, deep learning or self-learning systems - and respect for private life as set out in Article 8 of the ECHR. According to the court, there is also a risk of discrimination. The law is insufficiently transparent and verifiable and therefore unlawful. This could be an (European) Landslide case.

In the United States and China the use of ADS in support of governmental decision making is even more wide spread. Exemplary is the well known case, concerning the use of the “Correctional Offender Management Profiling for Alternative Sanctions (COMPAS)” in the “State v. Loomis” is good example of the (negative) effect of algorithmic based decision making. In 2013, the Circuit Court for La Crosse County, Wisconsin charged Eric Loomis with attempting to flee a traffic officer

[33] http://bit.ly/2S090Yo.

http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBDHA:2020:865.

and operating a motor vehicle without the owner's consent.[34] The trial court based its decision for a part on a COMPAS risk assessment, which indicated Loomis might have extremely high risk to reoffend, sentenced Loomis to six years of imprisonment and five years of extended supervision. Loomis challenged the court's using COMPAS in deciding his sentence in two aspects, including due process rights and considering gender at sentencing. In 2016, the Supreme Court of Wisconsin dismissed Loomis' appeal, stressing the positive functionality of the use of COMPAS, "COMPAS has the potential to provide sentencing courts with more complete information to address enhanced need." Concerning the question of due process, the court suggested that only when the risk assessment score was the determinative or role factor the judge considered shall the claim succeed. Moreover, the court concluded that Loomis could challenge the data that put into the algorithmic system, because the data was publicly available, such as administrative data, public records, and self- reporting and interviews from the defendant, Loomis could correct and determine the accuracy of his risk assessment score[35]. And to the question of gender, the court found that the use of gender as a factor in assessment served to promote accuracy, with no discriminatory intention, so there was no violation to Loomis' constitutional rights. Though the court didn't accept Loomis' claims, it concerned the future using of COMPAS and outlined permissible using situations. Interesting is that the case raised attention from the whole society, and triggered a series of debates over whether it is appropriate to use such algorithm at sentencing in criminal judicial system. Although risk assessment will not be banished the relatively of the outcome was recognized

In the study for the European Parliament on the effects of the deployment of ADS it is concluded that this process forms a threat to privacy and data protection in many different ways. The first is related to the massive collection of personal data required to train the algorithms. Even when no external attack has been carried out, the mere suspicion that one's personal data is being collected and possibly analysed can have a detrimental impact on people. For example, several studies and even have provided evidence of the chilling effect resulting from fear of online surveillance. Altogether, large-scale surveillance and scoring could narrow the range of possibilities and choices available to individuals, affecting their capacity for self-development and fulfilment. Scoring also raises the fear that humans are increasingly treated as numbers, and reduced to their digital profile. Reducing the complexity of human personality to a number can be seen as a form of alienation and an offence to human dignity.[36]

Transparency and Compliance with EU and GDPR Requirements
Transparancy.

How is transparency considered in European law in general and important is transparency in European perspective? The WP 29 refers to the principle as one of the fundamental principles of the European legal system. Article 1 of the TEU refers to decisions being taken "as openly as possible and as close to the citizen as possible". Article 11(2) states that "The institutions shall maintain an open, transparent and regular dialogue with representative associations and civil society"; and Article 15 of the TFEU refers amongst other things to citizens of the Union having a right of access to documents of Union institutions, bodies, offices and agencies and the requirements of those Union institutions, bodies, offices and agencies to ensure that their proceedings are transparent. Therefore transparency is considered to create trust towards the citizens of the EU. It further is considered an element of the principle of fairness for the processing of personal data as laid down in Article 8 of the Charter of Fundamental Rights of the European Union.

[34] See more, State v. Loomis. (2017, March 10). Retrieved November 1, 2019, from https://harvardlawreview.org/2017/03/state-v-loomis/.
[35] Washington, A. L. (2018). How to argue with an algorithm: Lessons from the compas- propublica debate. Colorado Technology Law Journal, 17(1), 139-141.
[36] Study for the European Parliament, Understanding algorithmic decision-making: Opportunities and challenges, 2019
[http://www.europarl.europa.eu/RegData/etudes/STUD/2019/624261/EPRS_STU(2019)624261_EN.pdf]

Technical Transparency and Explainability

If we look at the extent to which algorithms can be made transparent in a more general sense, it is important to realize that transparency is not an end in itself, but a means: transparency can contribute to the confidence that people are using it of algorithms by the government, and the possibilities of possibly resisting an outcome of their use.

The General Data Protection Regulation sets rules for the processing of personal data. Although the European governments are supposed to handle the personal data of its citizens with care; the requirements for processing personal data in the GDPR, whereby processing must be lawful, decent and transparent, do not always meet the same requirements. The data subject (that is the person whose personal data is being processed) has the right to know the logic behind the processing. In addition, the person has the right not to be subject to profiling that leads to a decision with legal consequences.

The advisory group on data protection and privacy, WP 29, now European Data Protection Board EDPD), isued guidelines concerning the requirements of transparency, probably because these requirements were not so transparent.[37]

According to the EDPD these (revised) guidelines should provide practical guidance concerning the and interpretation from the Article 29 Working Party (WP29) on the new obligation of transparency concerning the processing of personal data under the General Data Protection Regulation1 (the "GDPR").

According to the Guidelines:
Transparency is an overarching obligation under the GDPR applying to three central areas: (1) the provision of information to data subjects related to fair processing; (2) how data controllers communicate with data subjects in relation to their rights under the GDPR; and (3) how data controllers facilitate the exercise by data subjects of their rights.[38]

The technical working of the processing as such is not mentioned but could be considered so in a ample interpretation of the first mentioned area. Even stronger, in a note to this introduction the Guidelines are explained to: *set out general principles in relation to the exercise of data subjects' rights rather than considering specific modalities for each of the individual data subject rights under the GDPR.* This is recognized by the WP 29 itself because the Working Party already notices that:

these guidelines cannot address the nuances and many variables which may arise in the context of the transparency obligations of a specific sector, industry or regulated area. However, these guidelines are intended to enable controllers to understand, at a high level, WP29's interpretation of what the transparency obligations entail in practice and to indicate the approach which WP29 considers controllers should take to being transparent while embedding fairness and accountability into their transparency measures.

So also these guidelines can be considered as rather high level, but it we will see if they can be of relevance to the specific position of algorithms because of the general opinion of many lawyers and scholars that the GDPR gives a clear requirement for the transparency of algorithms.

The GDPR

Although Transparency is not defined in the GDPR "It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what

[37] Guidelines on transparency under Regulation 2016/679, 17/EN WP260 rev.01
[38] Guidelines, p.4

extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used (…) to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them.[39]

The leading principle from the GDPR is that personal data must be processed in a manner that is transparent with regard to data subjects (Article 5, first paragraph, under a). This principle is elaborated in various information obligations. A general framework for this can be found in Article 12 of the GDPR. If a government department processes personal data using algorithms, it follows from that article that it must provide information about this processing that is concise, transparent, comprehensible and easily accessible. This information must be provided in clear and simple language, especially if the information is intended for children. If the processing is in the nature of automated decision-making, the GDPR also requires the data processor to inform the data subject. At least if this decision-making is based on profiling as is referred to in article 22, it must also provide useful information about the underlying logic and the importance and the expected consequences of that processing for the data subject (Article 13, second paragraph, under f, and 14, second paragraph, under g, GDPR. The clearest requirement for transparency and explainability of the processing mechanism is given in Article 22 of the GDPR as described in Recital 71:

"The data subject should have the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her or similarly significantly affects him or her, such as automatic refusal of an online credit application or e-recruiting practices without any human intervention. (…)

In any case, such processing should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision.

The problem is that data-subjects probably does not know they are subjected to algorithms with legal consequences because there are data processing activities under the notable surface taking place.

Regulating the use of Algorithms by Law?

There are several signs that organizations as the EU and the Council of Europe want to set rules to control the use of algorithms. The Council of Europe state in a leaflet that certainly algorithms concerning decision making should be regulated to specify accountability:

"*Public entities should be held accountable for the decisions they take based on algorithmic processes. Impacts should be considered 'high risk' as they often carry significant legal weight for individuals and opting-out is either impossible or associated with negative consequences. Effective mechanisms must be in place that enable redress for individuals that are negatively impacted by algorithmically informed decisions".*[40]

[39] Recital 39 GDPR

[40] Algorithmic accountability and transparency from a human rights perspective[https://rm.coe.int/leaflet-algorithms-and-human-rights-en/168079cc19]

The European parliament issued a study about algorithmic decision making systems concerning the explainability of the algorithms as it could be regulated or at least be interpreted in the light of the GDPR:

"Explainability is defined as the availability of explanations about the ADS. In contrast to transparency, explainability requires the delivery of information beyond the ADS itself. Explanations can be of different types (operational, logical or causal); they can be either global (about the whole algorithm) or local (about specific results); and they can take different forms (decision trees, histograms, picture or text highlights, examples, counterexamples,(…)[41]

Concerning the developments of regulations authors require a more cautious direction:

Different types of legal instruments can be used to enhance the accountability of ADS. Considering that technology and its use evolve very quickly in this area, it is wise to avoid hasty legislation that could create more problems than it solves. New regulation should be enacted only when the matter has been properly understood, the recommended public debate has taken place and it is established that existing laws are insufficient to address the identified issues.[42]

Possibly in sequence of the above sited study the European Parliament issued a resolution to regulate civil accountability and accountability of AI systems in general, differentiating between high risk (autonomous) AI that would be risk based liability and other, more understandable AI, where responsible actors could be identified.[43] Another initiative to regulate the use of algorithms in certain sense has developed in Amsterdam, and the Helsinki. These two capitals are the first in the world, who came up with a register that charts the use of algorithms for all kind of different applications. This register shows what the municipality uses the algorithms for, such as when reporting waste lying around in public spaces, during parking checks and when tracing illegal holiday rentals or movements of tourists. Also the used datasets and source code are considered to be available but this aspect is still under construction.[44]The allover question will be if the explainability will give any understandable information for data subject.

Conclusion

The impression is created that the GDPR controls the application of algorithms. The GDPR does not specifically regulate the operation and application of algorithms. The words algorithm or artificial intelligence (AI) appear neither in the regulation nor in the explanation. This "high level" (meaning "vague") regulation is the result of a lengthy process, started at a time when there was hardly any thought about AI. The GDPR sets requirements for the processing of personal data in a general sense, with the aim of technology neutrality. The GDPR stipulates, among other things, that the processing must be lawful, proper and transparent. The explanation of article 22 refers to the wish to make the processing (by use of algorithms) transparent and explainable so that a party (the processor) can be held accountable for the result if this result has (legal) consequences for the data subject.

---

[41] Claude Castelluccia and Daniel Le Métayer (Institut national de recherche en informatique et en automatique - Inria) ,at the request of the Panel for the Future of Science and Technology (STOA)Understanding algorithmic decision-making: Opportunities and challenges,
https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624261/EPRS_STU(2019)624261_EN.pdf

[42] Ibidem. p.VI

[43] European Parliament resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence (2020/2014(INL))
https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_EN.html

[44] https://algoritmeregister.amsterdam.nl/

It is argued that the GDPR includes the requirement of fairness and social justice for the processors of personal data. This is "wishful thinking". Not just because explanation is difficult but also because of the resentfulness of parties to be transparent. Goodman and Flaxman cite Burrell who already in 2016 distinguishes between three barriers to transparency: (1) intentional concealment on the part of corporations or other institutions, where decision-making procedures are kept from public scrutiny; (2) gaps in technical literacy, which mean that, for most people, simply having access to underlying code is insufficient; and (3) a

"mismatch between thematically optimization in high-dimensionality characteristic of machine learning and the demands of human-scale reasoning and styles of interpretation."[45]

It has to be considered what requirements are possible and realistic in using algorithms and AI for the processing of personal data and for which purposes. Only then a credible regulation for the use of algorithms and AI can form the basis for personal data processing in international environment. The question is if it is necessary to explain the working of the algorithm for this purpose. It is more important to know which data is selected and what the result of the processing is. The weighing of the data, as in the Compass case is more important as well as the result in the sense that subject wants to know what the influence is on the decision making, to be explained by the decision makers in an ex-post explanation. This is necessary to know when one has to recur to the possibility to object to this decision. For that democratic right in my view the transparency of the algorithms is not required. What seems to be the main problem is –as always- a problem of insufficient communication. The programmers and developer of algorithms are not conscious of the requirements concerning transparency, explainability and privacy in general. Next to the well known requirement of "privacy by design", the commissioner of the work to develop and AI system has to include also an instruction to integrate transparency and explainability by design on code and input level. These requirements could be set as soft laws by self regulation of the industry that could develop into hard law by acceptance in normalization institute as the European standardisation organizations and acceptance as conformity to the requirements in the GDPR. On the other hand the practical problems of creating explainability of the selection of data by self learning algorithms to the datasubjects seem to be far from reality.

As stated by Arthur Conan Doyle: When have eliminated the impossible, whatever remains, however improbable, must be the truth.

[45] Bryce Goodman, Seth Flaxman ,European Union Regulations on Algorithmic Decision Making and a "Right to Explanation" AI magazine, Vol. 38 No. 3: Fall 2017 DOI: https://doi.org/10.1609/aimag.v38i3.2741