GENOMICS AND GENETICS IN CHECK: ALGORITHMIC OPACITY IN THE ESSENCE OF THE HUMAN BEING

Juliana Abrusio* & Lara Rocha Garcia**

ABSTRACT: It seems impossible to imagine a world without algorithms, whether they are for decision making or for prediction. In one analysis, their benefits seem to be sufficient to promote the discussions inherent to the subject and shed light on questions still without guaranteed answers. However, research pushes boundaries precisely by questioning. Considering that the basis of personalized medicine is the study of genomics, whose genetic information is fully available in global databases, how to make data manipulation and prediction compatible without, however, promoting discrimination and opacity? This is the research question that permeates this article that, from the literature analysis of the main international institutions in health and genome - *Human Genome Project*, the World Medical Association and the World Health Organization – ponders risks and guidelines for health algorithms to continue as a factor of human and social development aimed at better quality of life. Otherwise, it could become a source of exclusion, discrimination and opaque decisions.

KEYWORDS: algorithm; data protection; artificial intelligence; opacity; human genome.

I. Introduction

It seems impossible to imagine a world without algorithms, whether they are for decision making or for prediction. In one analysis, their benefits seem to be sufficient to promote the discussions inherent to the subject and shed light on questions still without guaranteed answers. However, research pushes boundaries precisely by questioning.

Considering that the basis of personalized medicine is the study of genomics, whose genetic information is fully available in global databases, how to make data manipulation and prediction compatible without, however, promoting discrimination and opacity?

This is the research question that permeates this article that, from the literature analysis of the main international institutions in health and genome - *Human Genome Project*, the World

* PhD in Law from Pontifícia Universidade Católica de São Paulo (2019). Master in Roman Legal System, Unification of Law and Integration Law from Università degli Studi di Roma Tor Vergata (2006), with a revalidated diploma from University of São Paulo (2008). Graduate in Business Law from Mackenzie Presbyterian University (2003). Law degree from Mackenzie Presbyterian University (2001). Professor at the Faculty of Law and permanent professor of Stricto Sensu Graduate Program in Political and Economic Law at Mackenzie Presbyterian University. Coordinator of Innovation and Technologies at Mackenzie Presbyterian University. Director of the Legal Grounds for Privacy Design Institute (LGPD Institute). Effective member and Vice President of the Artificial Intelligence Committee of IASP - Instituto dos Advogados de São Paulo (Institute of Attorneys of São Paulo). Coordinator of the Digital Law Committee of CESA-Centro de Estudos das Sociedades de Advogados (Study Center of Attorneys Associations). Guest professor of the postgraduate course Law and Information Technology PECE POLI/USP. Visiting professor of Fundação don Cabral. Guest professor of the Insper Digital Law extension course. Nominated by Whos who Legal International Directories (2015, 2016, 2017, 2018, 2019 and 2020, 2021); Best Lawyers in Brazil (2013, 2014, 2016, 2019 and 2020), Client Choice (2020) and the Legal 500 Latin America (2015 and 2014). Appointed by the National Directory Analysis (2018, 2019, 2020, 2021). Partner of Machado & Meyer Advogados.

** PhD in political and Economic Law from Mackenzie Presbyterian University, Visiting Scholar from Columbia Law School (USA Master's degree in Political and Economic Law from Mackenzie Presbyterian University, focusing on Innovation and Health. Specialist in innovation and entrepreneurship by Stanford Graduate School of Business (USA). Professor and lawyer of Digital Law, Innovation, compliance and Data Protection. Former Innovation Manager of the Israeli hospital Albert Einstein and former leader of the product sector of Dr. Consulta.).

Medical Association and the World Health Organization – ponders risks and guidelines for health algorithms to continue as a factor of human and social development aimed at better quality of life. Otherwise, it could become a source of exclusion, discrimination and opaque decisions.

In the first part of the article, we present international literature to technically examine the concepts that are necessary to answer our research question, understanding how the black box works, why it receives this designation, what types of opacity and their elimination vectors, as well as challenges of regulation for such.

Next, in the second item, we discuss the importance of personal data and sensitive personal data in the protection of health, as well as the latest recommendations including data protection, artificial intelligence and gene manipulation to, finally, in the third item we discuss proposals for transposing the challenge.

II. Algorithmic opacity as a transposition challenge

When we mentioned the 'black box' character of algorithms, we saw that this picture is related to the variation in the possibilities of algorithms being understood. Some algorithms are more amenable to verification than others. For Jenna Burrell, opacity seems to be at the center of new concerns about "algorithms," both among law scholars and among social scientists[175].

In this way, speaking of transparency in an algorithm context means referring to the degree to which the elements that make up a given algorithm can be accessed, read (as programming code) and understood. On the subject, as explained by the authors Jatinder Singh, Ian Walden, Jon Crowcroft and Jean Bacon:

> For instance, exposing the features of the data the learned model takes into account, the associations and rules that were derived, and the extent to which the model relies on these. Notions of control are very much related, concerning how algorithms can be managed and constrained, for example to prevent particular associations being made, or setting bounds on outputs[176].

While algorithms are tools used to simplify decisions, increase efficiency and offer convenience – and, on the other hand, they are extremely positive – when there is opacity and you cannot understand how they work or even if they work, we enter a nebulous scenario that can be negative. According to Nicole Kobie's hypothesis, if a data broker include a false fact in a person's profile, or if the analysis makes an incorrect assumption, this can negatively affect someone's life[177]. And how do we know if, in fact, there was an insertion without consequences, or if this incorrect assumption occurred?

Frank Pasquale uses the term *defective by design* as a critical expression of infrastructure that can harm people, but not issue corrections[178]. If a certain stigma is inserted into reputation systems, there should be some way to allow it to be removed as quickly as it spreads. We add

---

[175] BURRELL, Jenna. How the machine 'thinks': understanding opacity in machine learning algorithms. In: Big Data & Society, jan.-jun. 2016. Available at: <http://journals.sagepub.com> Access on: 21 Oct. 2018, p. 1.

[176] SINGH, Jatinder; WALDEN, Ian; CROWCROFT, Jon; BACON, Jean. Responsibility and machine learning: part of a process. Published: 27 Oct. 2016. Available at: <https://ssrn.com/abstract=2860048>. Access on: 18 Oct. 2018, p. 4. Translation: for example, exposing the characteristics of the data that the learned model considers, the associations and rules that have been derived, and to what extent the model is based on them. The notions of control are very related, about how algorithms can be managed and constrained, for example, to prevent specific associations from being made or to set limits on outputs.

[177] KOBIE, Nicole. Who do you blame when an algorithm gets you fired? Available at: <https://www.wired.co.uk/article/make-algorithms-accountable>. Access: 24 Dec. 2018.

[178] PASQUALE, Frank. The black box society: the secret algorithms that control money and information. Harvard University Press, Cambridge, Massachusetts, 2015, p. 4-5.

that to have the right to removal, it is necessary to exist, *ex ante*, the right to know the personal data used to crystallize certain stigma.[179]

From another perspective, the opacity of algorithms can be considered a social problem, given that several social classification mechanisms often depend on algorithms and, lately, depend on the technique of machine learning to do this sorting work, for example: spam filters, credit card fraud detection, search engines, news reading suggestion, advertising, insurance, fitness to borrow, credit score, etc[180]. According to Jenna Burrel, these algorithms operate personal data, and in situations where part or all of the mechanism of the algorithm is unknown, questions arise: What are the reasons for this state of not knowing? Would it be because the algorithm is of proprietary nature? Because it is complex or highly technical? Or are there, perhaps, other reasons? In the words of the author:

> The algorithms in question operate on data. Using these data as input, they produce an output; specifically, a rating (that is, if you give a loan to an interested party or mark an email as spam). They are opaque in the sense that if someone is a receiver of the output from the algorithm (from the classification decision), rarely does anyone have a concrete sense of how or why a particular classification was achieved by the inputs. In addition, the inputs can be totally unknown or only partially known. The question that naturally arises is: what are the reasons for this state of not knowing? Is it be because the algorithm is of proprietary nature? Because it is complex or highly technical? Or are there, perhaps, other reasons?[181]

It offers a classification regarding the forms of opacity and whose division can clarify the paths in the face of the formulated questions. According to the author, there are three distinct forms of opacity:

> (1) opacity as self-protection and intentional corporate or institutional concealment and, with it, the possibility of knowing the deception; (2) opacity arising from the current state of affairs where writing (and reading) code is a specialized skill and; (3) an opacity arising from the mismatch between mathematical optimization in high dimensionality characteristic of machine learning and the demands of human scale reasoning and semantic interpretation styles[182].

The third form of opacity - often confused with the second form as part of the general sense that algorithms and code are very technical and complex – is the particular focus of the article developed by Jenna Burrell. By analyzing this form of opacity, The author points out the

[179] ABRUSIO, Juliana. Proteção de dados na cultura do algoritmo. São Paulo: Editora D'Plácido, 2020.
[180] BURRELL, Jenna. How the machine 'thinks': understanding opacity in machine learning algorithms. In: Big Data & Society, jan.-jun. 2016. Available at: <http://journals.sagepub.com>. Access on: 21 Oct. 2018, p. 1.
[181] BURRELL, Jenna. How the machine 'thinks': understanding opacity in machine learning algorithms. In: Big Data & Society, jan.-jun. 2016. Available at: <http://journals.sagepub.com>. Access on: 21 Oct. 2018, p. 1. Original excerpt: The algorithms in question operateon data. Using this data as input, they produce na output; specifically, a classification (i.e. whether to give an applicant a loan, or whether to tag an email as spam). They are opaque in the sense that if one is a recipient of the output of the algorithm (the classification decision), rarely does one have any concrete sense of how or why a particular classification has been arrived at from inputs. Additionally, the inputs themselves may be entirely unknown or known only partially. The question naturally arises, what are the reasons for this state of not knowing? Is it because the algorithm is proprietary? Because it is complex or highly technical? Or are there, perhaps, other reasons?
[182] This classification is made by BURRELL, Jenna. How the machine 'thinks': understanding opacity in machine learning algorithms. In: Big Data & Society, jan.-jun. 2016. Available at: <http://journals.sagepub.com> Access on: 21 Oct. 2018, p. 2. Original excerpt: (1) the opacity of the intentional corporate or institutional self-protection, and concealment, and, along with it, the possibility for knowing deception; (2) the opacity stemming from the current state of affairs, where the writing (and reading) code is a specialist skill, and; (3) an existing page that stems from the mismatch between the mathematical optimization in the high-dimensionality characteristic of machine learning and the demands of the humanscale reasoning and styles of the semantic interpretation.

shortcomings around the 'audits' of algorithms, even as a way of evaluating the discriminatory classification[183].

Sometimes opacity, at a certain level, exists due to proprietary concerns. The algorithms are closed precisely to keep the competitive advantage and the secrets of the business. Given this, it would be very unlikely that the algorithms will be fully revealed. For Gianclaudio Malgieri, the balance rules in data protection law and trade secret law are vague and schizophrenic[184].

As an antidote to this scenario, Jenna Barrell proposes the use of open source codes in the elaboration of the algorithms[185]. However, it seems clear to us that the use of the proprietary model within the free market initiative cannot be prevented. Another proposal of the author is to educate a wider range of society in relation to code programming and computational skills in order to reduce the problem of a reduced elite of technical people who understand the subject. However, the author herself admits that the algorithms involved in *machine learning* they are a challenge that goes far beyond, as machines learn from themselves and can escape full human understanding-even for those with expert training and computer scientists[186].

For Russell, the automated decision made by algorithms is not necessarily bad. He attributes the possibility of two extremes: to provide exceptional benefits, on the one hand; and, on the other, to be catastrophic.[187] For him, datification consolidates itself as a phenomenon of transforming the entire human experience into data and, consequently, also in the phenomenon of mathematization. Transforming social questions and types of intelligence and mathematical calculations, for him, would be the same as reducing the human being, and all its social, cultural and biological complexity, to a single dimension.

The data creation and the mathematization of the human being, mainly aim at two purposes: increase of efficiency and possibility of prediction.

Such a prediction, it is important to remember, would happen on bases which are probabilistic, therefore subject to change over time.

However, if there are deterministic inferences in something that should be probabilistic, it would be possible to change someone's life decisively by discrimination, something condemned not only by our legal system.

This discrimination can happen by human interpretation, but also by algorithmic opacity. t This can even happen without being perceived due to the characteristic of being a black box.

Deconstructing the black boxes is no easy task. Even if there is a willingness to expose their methods to the public, there would be a very big challenge to understand such methods. Frank Pasquale, for his part, points out three strategic ways to keep the black boxes closed: royal secrecy, legal secrecy and obfuscation[188].

Real secrecy can be understood as the situation that establishes a barrier between hidden content and unauthorized access to such content. An example of this case is the email we protect with a password.

---

[183] BURRELL, Jenna. How the machine 'thinks': understanding opacity in machine learning algorithms. In: Big Data & Society, jan.-jun. 2016. Available at: <http://journals.sagepub.com>. Access on: 21 Oct. 2018, p. 2.

[184] MALGIERI, Gianclaudio. Trade secrets *v.* personal data: a possible solution for balancing rights. International Data Privacy Law, v.6, 2. 1 ed. May 2016, p.102-116. Available at: <https://doi.org/10.1093/idpl/ipv030>. Access: 16 Oct. 2018.

[185] BURRELL, Jenna. How the machine 'thinks': understanding opacity in machine learning algorithms. In: Big Data & Society, jan.-jun. 2016. Available at: <http://journals.sagepub.com> Access on: 21 Oct. 2018, p. 4.

[186] BURRELL, Jenna. How the machine 'thinks': understanding opacity in machine learning algorithms. In: Big Data & Society, jan.-jun. 2016. Available at: <http://journals.sagepub.com> Access on: 21 Oct. 2018, p. 10.

[187] RUSSELL, Stuart. Human Compatible: Artificial Intelligence and the problem of control. New York: Penguin Books, 2020, p. 9.

[188] PASQUALE, Frank. The black box society: the secret algorithms that control money and information. Harvard University Press, Cambridge, Massachusetts, 2015, p. 4-5.

Legal secrecy, in turn, obliges certain data and information to keep its contents confidential, for example, a bank employee who is obliged either by law or by virtue of the employment contract not to disclose the balance of his customers to third parties.

Obfuscation is related to deliberate acts of concealment when secrecy cannot be alleged in the situation. As an example, company can be mentioned as, in response to a request for information, delivering thousands of pages of documents, forcing the interested party to waste time, like the task of finding a needle in a haystack.

For Frank Pasquale all, these forms (royal secrecy, legal secrecy and obfuscation) can be considered *opacity*, to which the author attributes the meaning of "remediable incomprehensibility"[189].

When analyzing the incompatibility of transparency and auditing of algorithms against the intellectual property behind them, Howard Yu ponders that the problem is that legislation does not protect the most precious data for technology companies, those inferred and produced by algorithms and used by advertisers[190]. In this sense, the author questions the opacity of the algorithms, protected by intellectual property rights, but discovered as to the right to protection of personal data.

According to Howard Yu, this, however, is not insoluble. He suggests that technology companies could be required to appoint independent reviewers, computer scientists and academic researchers to conduct algorithm audits to ensure that profiling and automated decisions are unbiased and ethical.

For Frank Pasquale, many companies that process data claim that they maintain strict secrecy techniques to preserve their respective intellectual properties, "but their darker motives are also obvious"[191]. According to the author, companies hide behind the shield of legal protection of intellectual property. In this tran of thought, Frank Pasquale ponders that more transparency would help analysts verify in markets of "irrational exuberance" misconduct that can be easily hidden nowadays. It could, for example, expose unfair competition and discriminatory practices.

Frank Pasquale suggests the path of regulation. Recognizing, however, that this is not enough, he argues that any transparency solution to black box problems must be specific on three main issues: how much does the company need to disclose? Whom should he reveal it to? What is the deadline of the revelation? Therefore, there are three vectors to be fulfilled: depth of revelation, scope of disclosure, and term of revelation[192].

For Andrew Tutt, in the future most algorithms will be *trained* and not *designed*. This means that the operation of many algorithms will be opaque and there will be significant difficulty in what the author calls "to predict in border cases" and in addition, the responsibility for your damages will be diffuse and difficult to assign. In addition, according to Andrew Tutt, although *designed* algorithms already play important roles in many life-or-death situations (from emergency landings to automated braking systems), there will be an increase in more and more *trained* algorithms deployed in these mission-critical applications[193].

---

[189] PASQUALE, Frank. The black box society: the secret algorithms that control money and information. Harvard University Press, Cambridge, Massachusetts, 2015, p.6.

[190] YU, Howard. GDPR isn't enough to protect us in an age of smart algorithms. The Conversation, 29 May 2018. Available at: <https://theconversation.com/gdpr-isnt-enough-to-protect-us-in-an-age-of-smart-algorithms-97389>. Access: 01 Dec. 2018.

[191] PASQUALE, Frank. The black box society: the secret algorithms that control money and information. Harvard University Press, Cambridge, Massachusetts, 2015, p. 9.

[192] PASQUALE, Frank. The black box society: the secret algorithms that control money and information. Harvard University Press, Cambridge, Massachusetts, 2015, p.141-142.

[193] TUTT, Andrew. An FDA for algorithms. Published: 15 Mar. 2016. In: 69 Admin. L. Rev. 83, 2017. Available at: <https://ssrn.com/abstract=2747994>, p. 94. Access: 18 Nov. 2018. Interestingly, Prof. Tutt is from the area of oncology, medicine.

There can be several applications with this mission-critical nature. Commonly, there is the warning of the authors to the risks in the financial and internet market, by virtue of their ability to influence the economy and political paths. However, in this article, we would like to discuss other mission-critical applications that are beginning to gain popular contours, such as human genome analysis, which we will discuss in the following item.

III. Personalized medicine as the future of health

Health, by essence, is guided by data analysis: clinical exams, laboratory exams, imaging exams, family history analysis, patient history, behavioral analysis, risk factors, among others.

Medical Conduct is decided on the basis of scientific evidence crossed with the individual reality of each patient. Still, even with all the care and zeal dedicated by the professionals involved and the dedication of the patient, the conduct does not always achieve its goal.

In this context, as another element to aid decision-making, comes the genetic and genomic analysis of the patient.

The analysis of the genetic composition of the patient is configured as the greatest personalization of the treatment insofar as it allows to perceive characteristics that, otherwise, are not achievable.

Since the mapping of the human genome, which began in the 90s, but only went public in 2003[194], this element has become popular, especially since, with each new gene discovered, with its functions and consequences, a new addition is made to the genetic and genomic databases available for international use.

In a simplified way, when a patient performs his individual mapping, either of the complete genome or of specific genes, he is crossed with the mapped genes and stored in the global banks and, from the existing knowledge, the probabilities are presented: to develop conditions or diseases, to detect some existing ones, to confirm compatibility (or resistance) with drugs and treatments, among others.

With the advances of science, with each new gene discovered, it is possible to expand the mapping and add new elements to the medical conduct.

It can be seen, therefore, that not only medicine is guided by personal data, mostly sensitive, but also personalized medicine, by essence, consists of the management of genetic and genomic databases.

The potential benefit is indisputable, that is why so much is invested in this type of research. The risks of manipulation and discrimination, both of banks and genes individually, also exist.[195]

> Although the risks of algorithmic decision-making are all too real, as we have shown throughout this book, avoiding those risks does not require giving up entirely in the benefits. [196]

In this regard, the World Medical Association also has the same position - it demonstrates concern with regard to genetic manipulation and alteration, although it understands that there may be benefits and therefore makes the following recommendations:

[194] NATIONAL HUMAN GENOME RESEARCH INSTITUTE. The Human Genome Project. Available at: https://www.genome.gov/human-genome-project . Access: 05 Sep. 2021.

[195] KEARNS, Michael and ROTH, Aaron. The ethical algorithm: the science of socially aware algorithm design. New York: Oxford University Press, 2019, p. 192.

[196] Author's translation: Although the risks of algorithmic decision-making are real, as we demonstrate in this work, avoiding these risks does not mean giving up their benefits entirely. KEARNS, Michael and ROTH, Aaron. The ethical algorithm: the science of socially aware algorithm design. New York: Oxford University Press, 2019, p. 192.

> Governments should: Develop robust and enforceable regulatory frameworks for genome editing in their own countries and Urge continued development of an international consensus, grounded in science and ethics, to determine permissible therapeutic applications of germline genome editing. Member should: Develop and promote ethical guidelines for genome editing for their members, taking into consideration societal perspectives, professional consensus, national laws and regulations, and international standards.[197]

It is noticed that the WMA even recognizes that regulation can be a way to build consensus in an area that still lacks pacification and, therefore, can be a source of opacity or discrimination. The concern of the institution also lies in the risk of eugenics. It worries that the international scenario presents standards that would be transformed into law in national environments, with the due enforcements and socio-cultural adaptations.

In Andrew Tutt's proposal, algorithmic regulation will require federal uniformity, expert judgment, political independence, and pre-market analysis to prevent – without stifling innovation – the introduction of unacceptably dangerous algorithms into the market. The author proposes that a new specialized regulatory agency be created to regulate algorithmic security. It is what the author calls an FDA for algorithms:

> This federal Consumer Protection Agency must have three powers. First, it must have the power to organize and classify algorithms into regulatory categories by its design, complexity and potential for harm (both in common use and for misuse). Second, it must have the power to prevent the introduction of algorithms into the market until their safety and effectiveness have been proven through evidence-based, pre-market testing. Third, the agency must have broad authority to impose disclosure requirements and usage restrictions to prevent misuse of algorithms.[198]

The use of the expression "An FDA for algorithms" is due to Andrew Tutt stating that the concerns that drive the regulation of food, medicine and cosmetics resemble the concerns that should drive the regulation of algorithms. This is because with regard to the functioning of many drugs, the exact mechanisms that can produce – both benefits and generate harm – are not well understood. According to the author, the same will occur, very briefly, in relation to the main algorithms used in the future and the ones potentially dangerous[199].

In our opinion, to use the subterfuge of the absolute duality of transparency versus intellectual property protection ends up deflecting the real agenda of the debate. Uncorking the 'black box ' character does not imply violating intellectual property rights.[200] Business secrecy and intellectual property rights must remain untouchable. What is advocated is that these rights - keeping them preserved, it should be emphasized – do not form insurmountable walls at the expense of the cardiac principles of transparency, explainability and *accountability.* It is possible to follow, for example, Howard Yu's idea of independent reviewers, or even a model of depositing relevant data to a trusted third party[201], or in the application of the XAI model.

---

[197] WORLD MEDICAL ASSOCIATION. Statement on Human Genome Editing. Available at: https://www.wma.net/policies-post/wma-statement-on-human-genome-editing/. Access: 10 Aug. 2021.

[198] TUTT, Andrew. An FDA for algorithms. Published: 15 Mar. 2016. In: 69 Admin. L. Rev. 83, 2017. Available at: <https://ssrn.com/abstract=2747994>. Access: 18 Nov. 2018, p. 20. Original excerpt: Such a federal consumer protection agency should have three powers. First, it should have the power to organize and classify algorithms into regulatory categories by their design, complexity, and potential for harm (in both ordinary use and through misuse). Second, it should have the power to prevent the introduction of algorithms into the market until their safety and efficacy has been proven through evidence-based pre-market trials. Third, the agency should have broad authority to impose disclosure requirements and usage restrictions to prevent algorithms' harmful misuse.

[199] TUTT, Andrew. An FDA for algorithms. Published: 15 Mar. 2016. In: 69 Admin. L. Rev. 83, 2017. Available at: <https://ssrn.com/abstract=2747994>. Access: 18 Nov. 2018, p. 119.

[200] ABRUSIO, Juliana. Proteção de dados na cultura do algoritmo. São Paulo: Editora D'Plácido, 2020.

[201] Frank Pasquale, about this path, explains that a fully transparent society would be a nightmare of invasion of privacy, voyeurism and infringement of intellectual property. One of the possible paths to orderly and productive research would be to entrust the work to a trustworthy third party. (PASQUALE, Frank. The black box society:

For Luca Bolognini, Enrico Pelino and Camila Bistolfi, the data subject must know at least the logic of automated processing and the personal data assigned to him as a result of profiling or automated processing[202].

The disclosure of the first layer can indicate which personal data is being used, in compliance with the rule of informational self-determination. However, in addition to the control over the data that consists of input from the first layer, there is the right to know the purpose for which they are intended. This is because the right to know the purpose of computerized data is currently a particularly relevant right to informational self-determination[203]. In adittion, what data will be inferred by the algorithmic machine. Furthermore, it is important to keep the principle of respect for context in perspective. According To Helen Nissenbaum:

> To assess the privacy interests, it is crucial to know the context — who is gathering the information, the who is analyzing it, who is disseminating, and to whom, and the nature of the information, and the relationships among the various parties, and the even larger, institutional, and social circumstances[204].

One can not fail to mention that the president of one of the largest companies in the world in Information Technology and Intelligent Systems, said, in 2018, in the capacity of the position she held: "we must be transparent (...), we must explain why algorithms make the decisions they make. And if a company cannot do it, their products should not be on the market"[205].

Under another approach, it could be considered that the path of high punishments, of pecuniary character[206], could guarantee the enforcement, and bring greater protection to personal data in this ecosystem. However, without disregarding that this retributive regime must also exist, we do not end up in it as a way of solving the problem of opacity.

Furthermore, the complexity of the algorithms, moreover, cannot serve as a justification for not providing information to data subjects. In this regard, examples[207] brought by the document

---

the secret algorithms that control money and information. Harvard University Press, Cambridge, Massachusetts, 2015, p.144).

[202] BOLOGNINI, Luca; PELINO, Enrico; BISTOLFI, Camilla. Il regolamento privacy europeo. Milan-Italy: Giuffrè, 2016, p. 272.

[203] CANOTILHO, J. J. Gomes; MOREIRA, Vital. Constituição da República Portuguesa Anotada. v.1. São Paulo: RT; Coimbra: Coimbra, 2007, p.550. "Hence the legal-constitutional requirements regarding the purposes of the information: (1) legitimacy; (2) determinability; (3) explicitation; (4) adequacy and proportionality; (5) accuracy and timeliness; (6) time limitation all these requirements allow the control of the purposes, preventing, in particular, that there is processing of data relating to non-legitimate or unspecified purposes, excessive in relation to these same purposes or that have as reference inaccurate or outdated data or unjustified thunderstorms".

[204] NISSENBAUM, Helen. Privacy in context: technology, policy, and the integrity of social life. Stanford, CA: Stanford University Press, 2009. Words in the original: To assess the privacy interests, it is crucial to know the context — who is gathering the information, the who is analyzing it, who is disseminating, and to whom, and the nature of the information, and the relationships among the various parties, and the even larger, institutional, and social circumstances.

[205] ROMETTY, Virginia. We need a new era of data responsibility. In: World Economic Forum, 21 Jan. 2018. Available at: <https://www.weforum.org/agenda/2018/01/new-era-data-responsibility/>. Access: 10 Aug. 2019. Original text: When it comes to the new capabilities of artificial intelligence, we must be transparent about when and how it is being applied and about who trained it, with what data, and how. Does it reflect professional expertise? Are unintended biases built in? We must explain why its algorithms make the decisions they do. If a company can't do that, their products shouldn't be on the Market (free translation).

[206] On the guidelines for the application and fixing of fines for the purposes of the GDPR, see document prepared by the Working Group of Article 29, WP 253, adopted on 03 Oct. 2017.

[207] A controller uses a credit score to evaluate and reject a person's loan application. The score may have been transmitted by a credit reference agency or calculated directly on the basis of information held by the controller. Regardless the source (information on the source should be provided to the data subject in accordance with Article 14, number 2, point f), where the personal data are not collected from the data controller), if the controller is based

WP251 demonstrate the separation of subjects, and how opacity can be broken, in order to meet the right of the data subject, without violating the intellectual property right of the controller, especially when dealing with sensitive personal data.

The genetic heritage of humanity is made up of contributions and individuals, which, in addition to biological material, deposit expectations and fears. To the extent that the NHGRI (National Human Genome Research Institute), in its data sharing policy, repeatedly stipulates the sharing of data, always with the consent of the holder, when applicable, and anonymized, when possible, at four levels of time of submission and publication. If the algorithms of analysis, prediction and indication of decision-making are opaque, rather than a patrimony that can increase the quality of human life, perhaps we would be faced with one of the largest global discriminatory banks.

Similarly, this bank, in itself, might not be opaque but, if those who access it deviate from the use, the uncontrolled could be, as Pasquale would say, catastrophic.

IV. Opacity at the heart of personalized medicine

Frank Pasquale, in his most recent work[208], dialogues with Isaac Asimov on the creation of new laws of robotics: i) *Robotic Systems and AI should complement professionals, not replace them;* (ii) *Robotic Systems and AI should not counterfeit humanity*; (iii) *Robotic Systems and AI should not intensify zero-sum races*; (iv) *Robotic Systems and AI must always indicate the identity of their creator (s), controllers (s) and owner (s)*.[209]

Concerned about the future of health, its dependence on sensitive personal data in digital systems and platforms, WHO published two reports in 2020 and 2021, one of them being *Data, Analytics and delivery for Impact*[210] and the other, Digital Health Strategy 2020-2025[211], whose agenda has as an essential basis to treat health data, in a generic way, not only genetic data, with a common good, supranational, with WHO as the main manager. The spirit of this recommendation follows the same of AMM and the Human Genome Project, which are noble, focused on the common good, but impossible to ignore the risks and harm containment, if any.

While there is a genuine and widespread concern under the use of algorithms and the opacity of decision automation, it is understood that in health the use of these algorithms as a "right arm of the doctor" becomes necessary. So much so that the World Medical Association drafts

on this score, he/she should be able to explain it and substantiate the underlying logic with the data controller. The controller explains that this process helps you make fair and responsible lending decisions. It provides data on the main characteristics considered in the decision-making, the source of such information and its relevance, which may include, for example: the information provided by the data subject in the application form; information on the previous own management of the account, including possible delays in payments; and information from official public records, such as information from fraud and insolvency records. The controller must also include information to indicate to the data subject that the credit scoring methods used are periodically tested to ensure their fairness, effectiveness and impartiality. The controller must provide the data subject with contacts through which he can request that any decision of refusal be reviewed in accordance with Article 22 (3) (WP 251).

[208] PASQUALE, Frank. New Laws of Robotics: Defending Human Expertise in the Age of AI. Cambridge: Belknap Harvard, 2020.

[209] Translation: i) Robotics and Artificial intelligence systems must complement the human being and not replace them; ii) Robotics and Artificial intelligence systems must not falsify humanity; iii) robotics and Artificial Intelligence systems must not intensify zero-sum races; iv) Robotics and Artificial Intelligence systems must always indicate the identity of their creator(s), controller(s) and owner(s).

[210] WORLD HEALTH ORGANIZATION. Data, analytics & delivery for impact. Available at: https://www.who.int/data/ddi. Access: 10 Aug. 2021.

[211] WORLD HEALTH ORGANIZATION. Global strategy on digital health. Available at: https://cdn.who.int/media/docs/default-source/documents/gs4dhdaa2a9f352b0445bafbc79ca799dce4d.pdf?sfvrsn=f112ede5_75 , Access:10 Aug. 2021.

same current on the use of "enhanced intelligence"[212], expression by her coined to replace artificial intelligence or algorithm.

World Medical Association suggests that treating sensitive personal data as a common good, coupled with the use of enhanced intelligence, is necessary to expand access to health.

When we think about what exists regarding the maximization of the use of data and "enhanced intelligence", we come across the promise of personalized medicine with the use of genetic data.

The human gene, in Brazil, is not subject to intellectual property protection every new gene discovered, it begins to compose international gene banks, which can be used by any natural person or legal entity under public or private law, anywhere in the world.[213]

World Health Organization and the institution Patients Like Me have created a genome bank from human material collected and donated voluntarily by patients themselves in the project Digital Me[214] and, with each new discovery, it redoes the automated cross-referencing of this information and outputs with recommendations. For approximately two years, 2,500 samples were collected with respective patient questionnaires. At the moment, they no longer accept new samples.

Russell argues that machine intelligence should be aligned with human intelligence through common goals:

> Because machines, unlike humans, have no objectives of their own, we give them objectives to achieve. In other words, we build optimizing machines, we feed objectives into them.[215]

Having as a premise that the algorithm, in itself, is not born with a purpose defined by him, Russel puts that this would be the beginning: to ensure that in fact the machine is developing compactly with human beings, with their values and interests. For health, this alignment of purpose could go as far as eradicating diseases and even raising the reach in mental health.

Despite this, two concepts about the use of artificial intelligence are emphasized by the author: the Gorilla problem[216] and King Midas[217]. The first refers to the fear of humans losing their supremacy in a world where there are machines with superior intelligence. The second refers to the Greek mythology of the king who, when turns into gold everything he touches. It sounds great, but it becomes a curse to the extent that things that he would not want to turn into the noble metal also mutate, such as food or people, for example. In the analogy with artificial intelligence, it would be the possibility of misalignment of the algorithmic system with human values and interests, allowing the existence of opacity or algorithmic discrimination.

However, defining human purposes accurately and completely becomes a challenge in itself, independent of the algorithm by virtue of the diversity of societies. Therefore, it is sometimes possible for an algorithm to promote discrimination even if this was not its main goal. The presence of opacity can also happen due to the absence of the possibility of explanation, not

[212]WORLD MEDICAL ASSOCIATION. Statement on Augmented Intelligence in Medical Care. Available at: https://www.wma.net/policies-post/wma-statement-on-augmented-intelligence-in-medical-care/. Access: 10 Aug. 2021.

[213] NATIONAL HUMAN GENOME RESEARCH INSTITUTE. Genomic Data Sharing Policy. Available at: https://www.genome.gov/about-nhgri/Policies-Guidance/Genomic-Data-Sharing/data-standards#guidance. Access: 21 Aug. 2021.

[214] PATIENTSLIKEME. Digital Me. Available at: https://www.patientslikeme.com/research/digitalme. Access: 10 Aug. 2021.

[215] RUSSELL, Stuart. Human Compatible: Artificial Intelligence and the problem of control. New York: Penguin Books, 2020, p. 10.

[216] RUSSELL, Stuart. Human Compatible: Artificial Intelligence and the problem of control. New York: Penguin Books, 2020, p. 132.

[217] RUSSELL, Stuart. Human Compatible: Artificial Intelligence and the problem of control. New York: Penguin Books, 2020, p. 137.

because the algorithm chose different purposes, but because it *has learned* and moved on its own.

Still, Russell argues that there is the possibility of mitigation because, in the opposite sense, it would invalidate this technology and this discussion – risks of opacity and discrimination – would simply have no reason to exist. That is, it exists because the benefits of a general purpose technology can be proven and the negative points must be transparently and seriously discussed so that they can be transposed.

> If there were no potential benefits of AI, there would be no economic or social impetus for AI research and hence no danger of ever achieving human-level AI. We simply wouldn't be having this discussion at all. Second, if the risks are not successfully mitigated, there will be no benefits.[218]

Failure to transpose would imply a setback in what we understand by the dimensions of human rights and, possibly, the effort to reverse the damage would be greater than non-use. This does not mean that efforts and investments in research, development, and application in artificial intelligence systems in products and services should be stagnant, but rather, that they be carried out multidisciplinary.

In health, an emblematic case of the use of artificial intelligence was the FDA approval of the algorithm that identifies diabetes through the retina, developed by Google.[219] Based on a multicenter trial, to ensure the diversity of people and ocular structures, the first approved software has an accuracy of more than 87% of almost instantaneous detection of this disease that affects more than 30 million Americans.

What if, from the understanding of the human genome, with the aim of improving people's lives, there is genetic alteration to avoid serious disease conditions? Building an algorithm which is capable of reading the still embryonic genome, indicating which should undergo editing with the aim of helping humanity and eradicating diseases, providing poor quality of life, seems fantastic. And scary at the same time.

What are these conditions? Why can a disabled person be considered an inferior human being? In another hypothetical situation, a person is diagnosed with the need for organ transplantation. For this queue, age, cognitive and health criteria would be evaluated. Analyzing genetic compatibility could be, in theory, a factor of increasing transplant success.

But what if in this analysis the probability of developing another serious condition in the future is identified? Would this determine the refusal of the transplant?

Consider also the learning ability of the algorithm when machine learning is applied, as mentioned before. It could then learn and exclude conditions it considered inappropriate without human knowledge and, perhaps, without being able to explain his logic.

How to deconstruct this black box? For some situations, there is a need for real secrecy, protecting the data, with password and other mechanisms. It also makes sense to apply legal secrecy in such cases. With the training of the algorithm, would we know how to explain what and how it became opaque?

Kearns and Roth explain that the algorithmic promise of assertive decision-making seems misguided, since even human decision-making is not based on logical and linear constructions, and that even humans themselves have difficulty outsourcing their decision-making method.

---

[218] RUSSELL, Stuart. Human Compatible: Artificial Intelligence and the problem of control. New York: Penguin Books, 2020, p. 157.

[219] US FOOD AND DRUG ADMINISTRATION. FDA permits marketing of artificial intelligence-based device to detect certain diabetes-related eye problems.Available at: https://www.fda.gov/news-events/press-announcements/fda-permits-marketing-artificial-intelligence-based-device-detect-certain-diabetes-related-eye. Access: 10 Aug. 2021.

> All decision making – including that carried out by human beings – is ultimately algorithmic. The difference is that human decision-making is based on logic or behaviors that we struggle to precisely. If we humans had the ability to describe our own decision-making processes precisely enough, then we could in fact represent them as computer algorithms. So the choice is not whether to avoid using algorithms or not, but whether or not we should use precisely specified algorithms.[220]

They understand that society's response to this has been regulation, essential in this process, but insufficient to achieve the necessary results. The role of regulation, whether national or international, lies in explaining what society wants or not. However, its biggest problem is the lack of scalability. In this sense, they have another suggestion:

> So while laws and regulations are important, we have argued in this book that the solution to the problems introduced by algorithmic decision-making should itself be in large part algorithmic.[221]

This means to say that, for the authors, regulation should guide the developments, but the resolution that has the scope to actually stagnate the problem of opacity, offering the possibility of depth of disclosure and scope for such, within a reasonable time, in order to avoid or correct possible discrimination, would happen within the algorithm itself. It would be developed with this understanding of being able to explain himself. Perhaps the challenge is not to unravel the black box, but to train it to such an extent that it itself understands that it must explain how it works, without losing this ability (or *feature*) throughout your continuous learning.

V. Final considerations

The genetic heritage of humanity has the potential to benefit humanity from understanding – and changing - the human being at its innermost biological core, its own DNA. Human Genome Project, World Medical Association and World Health Organization, as international parastatal institutions, are concerned with editing international guidelines and guidelines.

Such documents, even if they do not have the force of law, are intended to stimulate consensus, reduce possible ethical dilemmas and reinforce the need for states and members to act in favor of data protection and the development of artificial intelligence algorithms. However, such documents recognize important risks that can turn their benefits into setbacks.

In this context, these institutions are consolidated with the theoretical frameworks presented here – Brunell, Tutt, Russell, Pasquale, Kearns and Roth in search of a solution to opacity and algorithmic discrimination, which, although good faith prevails in the development process, are not entirely removed.

The regulation is proposed as a solution indicated by the institutions and authors indicated, however, in practice, they recognize that it can be fragile due to the difficulty of identifying cases and, also, of enforcement. However, it is still necessary to strengthen the paths and pacify development models.

As tautological as it may seem, the solution so far discussed for opacity and discrimination is in the algorithm itself, in being developed from ethical principles and deep knowledge of existing legislation to avoid retrogression, alignment with human values and that it is self-explainable. Its explainability within a time frame, with depth and possibility of reversal, would achieve the scalability required to follow the algorithm.

[220] KEARNS, Michael and ROTH, Aaron. The ethical algorithm: the science of socially aware algorithm design. New York: Oxford University Press, 2019, p. 191.
[221] KEARNS, Michael and ROTH, Aaron. The ethical algorithm: the science of socially aware algorithm design. New York: Oxford University Press, 2019, p. 192.

VI. References

ABRUSIO, Juliana. Proteção de dados na cultura do algoritmo. São Paulo: Editora D'Plácido, 2020.

BOLOGNINI, Luca; PELINO, Enrico; BISTOLFI, Camilla. Il regolamento privacy europeo. Milan-Italy: Giuffrè, 2016.

BURRELL, Jenna. How the machine 'thinks': understanding opacity in machine learning algorithms. In: Big Data & Society, jan.-jun. 2016. Available at: <http://journals.sagepub.com> Access on: 21 Oct. 2018.

CANOTILHO, J. J. Gomes; MOREIRA, Vital. Constituição da República Portuguesa Anotada. v.1. São Paulo: RT; Coimbra: Coimbra, 2007.

FINANCIAL Times Lexicon. Available at: <http://lexicon.ft.com/term?term=principal/agent-problem>. Access: 24 Dec. 2018.

GARCIA, Lara Rocha. Inovação tecnológica e direito à saúde: aspectos jurídicos, econômicos, tecnológicos e de políticas públicas. Curitiba: Juruá, 2017.

KEARNS, Michael and ROTH, Aaron. The ethical algorithm: the science of socially aware algorithm design. New York: Oxford University Press, 2019.

KOBIE, Nicole. Who do you blame when an algorithm gets you fired? Available at: <https://www.wired.co.uk/article/make-algorithms-accountable>. Access: 24 Dec. 2018.

MALGIERI, Gianclaudio. Trade secrets *v.* personal data: a possible solution for balancing rights. International Data Privacy Law, v.6, 2. 1 ed. May 2016, p.102-116. Available at: <https://doi.org/10.1093/idpl/ipv030>. Access: 16 Oct. 2018.

NATIONAL HUMAN GENOME RESEARCH INSTITUTE. The Human Genome Project. Available at: https://www.genome.gov/human-genome-project . Access: 05 Sep. 2021.

NISSENBAUM, Helen. Privacy in context: technology, policy, and the integrity of social life. Stanford, CA: Stanford University Press, 2009.

PATIENTSLIKEME. Digital Me. Available at: https://www.patientslikeme.com/research/digitalme. Access: 10 Aug. 2021.

PASQUALE, Frank. The black box society: the secret algorithms that control money and information. Harvard University Press, Cambridge, Massachusetts, 2015, p.144).

PASQUALE, Frank. New Laws of Robotics: Defending Human Expertise in the Age of AI. Cambridge: Belknap Harvard, 2020.

ROMETTY, Virginia. We need a new era of data responsability. In: World Economic Forum, 21 Jan. 2018. Available at: <https://www.weforum.org/agenda/2018/01/new-era-data-responsibility/>. Access: 10 Aug. 2019.

SINGH, Jatinder; WALDEN, Ian; CROWCROFT, Jon; BACON, Jean. Responsibility and machine learning: part of a process. Published: 27 Oct. 2016. Available at: <https://ssrn.com/abstract=2860048>. Access: 18 Oct. 2018.

TUTT, Andrew. An FDA for Algorithms. Published: 15 Mar. 2016. In: 69 Admin. L. Rev. 83, 2017. Available at: <https://ssrn.com/abstract=2747994>. Access: 18 Nov. 2018.

US FOOD AND DRUG ADMINISTRATION. FDA permits marketing of artificial intelligence-based device to detect certain diabetes-related eye problems.Available at: https://www.fda.gov/news-events/press-announcements/fda-permits-marketing-artificial-intelligence-based-device-detect-certain-diabetes-related-eye. Access: 10 Aug. 2021.

WORLD HEALTH ORGANIZATION. Data, analytics & delivery for impact. Available at: https://www.who.int/data/ddi. Access: 10 Aug. 2021.

WORLD HEALTH ORGANIZATION. Global strategy on digital health. Available at: https://cdn.who.int/media/docs/default-source/documents/gs4dhdaa2a9f352b0445bafbc79ca799dce4d.pdf?sfvrsn=f112ede5_75. Access: 10 Aug. 2021.

WORLD MEDICAL ASSOCIATION. Statement on Augmented Intelligence in Medical Care. Available at: https://www.wma.net/policies-post/wma-statement-on-augmented-intelligence-in-medical-care/. Access: 10 Aug. 2021.

WORLD MEDICAL ASSOCIATION. Statement on Human Genome Editing. Available at: https://www.wma.net/policies-post/wma-statement-on-human-genome-editing/. Access: 10 Aug. 2021.

YU, Howard. GDPR isn't enough to protect us in an age of smart algorithms. The Conversation, 29 May 2018. Available at: <https://theconversation.com/gdpr-isnt-enough-to-protect-us-in-an-age-of-smart-algorithms-97389>. Access: 01 Dec. 2018.