HUNGARIAN LABOUR LAW
E-JOURNAL

Business Secrecy as a Limit to the Right to Information on Algorithms

Noelia de Torres Bóveda[*]

1. Introduction

Over the past few decades, we have seen algorithms used in many areas, both in government (e.g. in criminal justice[1] and now even in support of court judgement writing[2]), and in private companies (e.g. banks and credit institutions). Also in workforce management, through what the authors have called algorithmic management.

Indeed, these systems offer us a multitude of benefits, such as speed, efficiency and precision. However, everything comes at a price and, in this case, the price is us[3], the citizens. Firstly, because algorithmic-based systems require huge amounts of data[4] (big data) which, if we are in the field of human resource management, will most likely be made up of employees' personal data. Furthermore, the gradual delegation of power that the employer is granting to the machine[5], means that the machine is able to make decisions that were previously only his or her; decisions that fall under the three fundamental powers of the employer: management, evaluation and control, and disciplinary[6]. We are therefore not only part of the system's input, but also of its output, by which we are affected, whether in the form of monitoring and control or automated decision-making.

[*] Teaching and research assistant, Complutense University of Madrid.

[1] See, Taylor R. Moore: *Trade secrets and algorithms as barriers to social justice.* Center for Democracy and Technology (CDT), 2017.

[2] Judgment of the 1st Labour Circuit Court of Cartagena, Colombia (Judgment No. 032). Date of ruling: 30th January 2023.

[3] Michael Kearns – Aaron Roth: *El algoritmo ético*. Madrid, La Ley Wolters Kluwer, 2020. 12.

[4] Bruno Lepri – Nuria Oliver – Emmanuel Letouz´e – Alex Pentland – Patrick Vinck: Fair, Transparent, and Accountable Algorithmic Decision-making Processes: The premise, the proposed solutions, and the open challenges. *Philosophy & Technology*, 2018. 9. As it is certainly state "in particular, we are witnessing an information asymmetry situation where a powerful few have access and use resources and tools that the majority do not have access to, thus leading to an – or exacerbating the existing – asymmetry of power between the state and big companies on one side and the people on the other side".

[5] David De Cremer: Leading by algorithm: rushing in. In: David De Cremer: *Leadership by algorithm. Who leads and who follows in the AI era?* United Kingdom, Harriman House, 2020. 29.

[6] See, Alex J. Wood: Algorithmic management. Consequences for work organisation and working conditions. *JRC Working papers series on Labour, education and technology, European Commission*, no. 7 (2021).

Companies, as might be expected, have taken the necessary measures to safeguard these tools, as they are an important source of competitive advantage. Such protection can become an obstacle to accountability and access to relevant information when decisions taken by the machine affect workers' rights. It is not possible to defend our rights, nor to apply the principles established by the law, if we do not have the necessary information to do so[7].

Intellectual property (IP) rights have evolved over the decades and, in particular, trade secrets have developed with enhanced protection as a result of the increased ease of discovery. The view of lawyers and academics on these IP rights is usually linked to this competition protection perspective, as well as to that related to the illicit access or reproduction of protected content and products. However, a minority of scholars see this legal protection as a potential obstacle to the guarantee of fundamental rights and even to effective judicial protection when algorithmic-based systems are involved. If these risks are recognised, they usually remain just a mere warning of the danger without further investigation.

The purpose of this paper is to study the legal instruments that protect algorithms and how this legal protection is likely to collide with or hinder the transparency and auditing of algorithms, which is necessary to ensure that their implementation in the company does not compromise the rights of employees. To this end, we will study the different sources of opacity, the ways in which algorithms can be protected, referring in particular to patent and trade secret protection. Of these two forms of protection, we will focus on secrecy as the most frequent form of protection and the most opaque.

Once the problem has been identified, we will move on to the "solution": transparency, analysing its content, its limits and its regulation in trade secrecy rules.

All of the above will allow us to conclude whether trade secrecy is really the obstacle it claims to be for algorithmic transparency or whether there are other factors at play.

2. Where does the opacity of algorithms come from?

One of the characteristics most emphasised by the doctrine when dealing with algorithms is their opacity[8] (algorithmic opacity). It is true that this type of technology poses serious challenges in the area of transparency, and we should therefore start by asking where this opacity comes from and,

[7] Henar Álvarez Cuesta: *El impacto de la inteligencia artificial en el trabajo: desafíos y propuestas*. Navarra, Thomson Reuters–Aranzadi, 2020. 68. Also, see Alexandra Mateescu – Aiha Nguyen: Algorithmic management in the workplace. *Data & Society*, 2019. 14. The authors reflect that "algorithmic management can create power imbalances that may be difficult to challenge without access to how these systems work, as well as the resources and expertise to adequately assess them.40 As a result, workers are often left to collect information in piecemeal ways".

[8] See Frank Pasquale: *The black box society. The secret algorithms that control money and information*. Cambridge, Harvard University Press, 2015.

more importantly, whether the algorithms embedded in the systems (especially artificial intelligence) are opaque by nature.

Regarding the first question, the scientific literature shows the existence of two types of opacity, which allows us to distinguish between what has been called "technical opacity", i.e., that which arises from the black box of the algorithm and its complexity; and "organisational opacity", which arises from a lack of information on the part of the company in this respect, as a consequence of strategic and intellectual property interests[9].

We also find doctrine that advocates not just two, but three opacity factors. In this way, the following are identified: 1) "opacity as intentional corporate or state secrecy", 2) "opacity as a technical illiteracy" and 3) "opacity as the way algorithms operate at the scale of application"[10]. The first two can be identified similarly and in fundamental terms with the technical and organisational opacity expressed above; the third, on the other hand, relates to the multi-component systems with which the algorithm programmers must contend and the difficulty this entails in uncovering their logic.

In this paper we have opted for a broader classification than those described above, identifying two main categories. Firstly, as already mentioned, we have to take into consideration an opacity that comes from the algorithm by its own configuration, to which we could attribute the name "internal opacity". In this opacity, we must include both the opacity that derives from the type of algorithm we are dealing with, and the contribution of the programmers or designers to it. We must not forget that they are the ones who develop these systems, introducing the input data and setting the reference variables[11].

Given these characteristics, it can be said that internal opacity is difficult to alter - it is at the "heart" of the algorithm, although there are ways that allow us to modulate it or at least keep it under a certain margin of control. Some of them, already widely accepted by scientific doctrine, are human supervision under a human-in-command approach, accountability or explainability, the latter of which can sometimes be difficult to put into practice, especially if we are dealing with machine learning algorithms[12].

The second source of opacity that we find is that which arises as a consequence of the existence of the algorithm in society, in a specific legal sphere. The latter type of opacity can be referred to as "external opacity", in that it does not stem from the algorithm itself, but from the fact that it exists in a given legal system. It can therefore be observed that, with regard to the first of the categories, the

[9] Mohammad Hossein Jarrahi – Gemma Newlands – Min Kyung Lee – Christine T. Wolf – Eliscia Kinder – Will Sutherland: Algorithmic management in a work context. *Big Data & Society*, 2021. 8.

[10] Jenna Burrell: How the machine 'thinks': Understanding opacity in machine learning algorithms. *Big Data & Society*, 2016. 2–5.

[11] In relation to the introduction of biases, Valerio De Stefano: Negotiating the algorithm: automation, artificial intelligence and labour protection. *International Labour Office*, 2018. 9.

[12] Maayan Perel – Niva Elkin-Koren: Black box tinkering: beyond disclosure in algorithmic enforcement. *UF Law Scholarship Repository*, 2017. 190. The code of machine learning algorithms is mysterious in that the steps it performs may be understandable, but getting an explanation of why it performs certain things "requires understanding how it evolved and what 'experiences' it had along the way".

reasons or features of opacity remain static, although, of course, they vary according to the type of algorithm used. In the second case, the factors leading to opacity fluctuate more, as they depend on international, EU and national legislation in this respect, all of which can be altered by the legislator according to needs.

External opacity thus manifests itself through the protection of the algorithm under different types of intellectual property rights, each with different protection regimes. Therefore, when we speak of trade secrets, we speak of a *legal backing of opacity*, in favour of business competitiveness.

As to the question of whether algorithms are opaque by nature, the answer is yes[13], notwithstanding the fact that not all algorithms pose the same challenges and are not equally impenetrable. A fundamental difference will be whether they are part of symbolic AI systems – which require strong human intervention – or sub-symbolic AI systems – which do not require human intervention except in design, as they learn on their own from available data –[14], such machine learning and neural networks. In the latter case – sub-symbolic AI systems – the problems of transparency will clearly be more relevant, among other things, because in many cases we cannot explain the output offered by the algorithm[15]. At this point, it should be asked whether the use of this type of system should be valid[16] in matters that may affect fundamental rights, as is the case in the field of labour.

3. The protection of algorithmic systems under intellectual property rights

Algorithmically based systems may enjoy legal protection when they are considered intellectual property. However, it should be emphasised that "legal protection of inventions" is not automatically synonymous with "opacity"; in fact, some IP institutions are endowed with an obligation of publicity, which allows the disclosure of new discoveries, inventions and works, with the aim of promoting scientific and technological development. The conflict is mainly found when the systems are protected under the figure of a trade secret, where, by its very nature, the information is of a confidential and restricted character.

[13] See, Perel–Elkin-Koren op. cit. 189. While it is true that some algorithms, especially the simpler ones, are based on the introduction of the specific steps that the algorithm must follow to obtain the result, the reality is that "many systems spring more simply informal or notional specifications, where developers work from a poorly specified goal rather than a clear set of requirements". Deven R. Desai – Joshua A. Kroll: Trust but verify: a guide to algorithms and the law. *Harvard Journal of Law & Technology,* vol. 31, no. 1 (2017). The greater degree of autonomy that these systems are endowed with is directly related to a greater degree of opacity.

[14] Aleksandr Christenko – Vaida Jankauskaitė – Agnè Paliokaitė – Egidius Leon van den Broek – Karin Reinhold – Marina Järvis: Artificial intelligence for worker management: an overview. *European Agency for Safety and Health at Work*, (2022). 11.

[15] David Leslie – Christopher Burr – Mhairi Aitken – Josh Cowls – Mike Katell – Morgan Briggs: *Artificial Intelligence, human rights, democracy and the rule of law. The Alan Turing Institute and the Council of Europe*, 2021. 15.

[16] *Unboxing Artificial Intelligence: 10 steps to protect Human Rights.* Council of Europe, 2019. 9–10. [hereinafter: Council of Europe (2019)]. Here the Council states that systems that do not allow for adequate transparency should not be used.

Intellectual property law encompasses various types of protection, from patent or copyright to trade secret protection. According to the World Intellectual Property Organisation (WIPO) there are two types or categories of IP[17]. First, industrial property, in which are included invention patents, trademarks, industrial designs and geographical indications and, secondly, copyright and related rights, i.e. literary, artistic and scientific works, including performances and broadcasts. Trade secrets are part of IP[18], although this international organisation does not expressly classify them in either of the two previous categories.

The regulatory framework for this set of rights is governed by international norms, which set the minimum standards that states must respect. This framework is composed of the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) from the World Trade Organisation (WTO), the Paris Convention for the Protection of Industrial Property, the Patent Law Treaty (PLT), the Berne Convention for the Protection of Literary and Artistic Works, the Treaty on Intellectual Property in respect of Integrated Circuits, among others.

In the European context, attention should mainly be drawn, as far as this work is concerned, to the Munich Convention on the Grant of European Patents, the Implementing Regulations of the Convention on the Grant of European Patents and Directive 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure.

The above rules are left to the national development of each of the Member States of the Union, which means that in practice we find different levels of protection depending on the territory in which we are located.

3.1. Legal protection of the algorithm: the patent

An algorithm is a sequence of steps aimed at achieving a specific result[19], which can be in either a common language or a programming language[20]. Consequently, we are dealing with abstract entities[21], as well as, in most cases, with mathematical methods. As we will have the opportunity to see below, as a consequence of this definition, we will find a protection framework that is certainly limited.

The Agreement on Trade-Related Aspects of Intellectual Property Rights, states that "patents shall be available for any inventions, whether products or processes, in all fields of technology, provided

[17] *What is intellectual property?* WIPO, 2020. https://www.wipo.int/edocs/pubdocs/en/wipo_pub_450_2020.pdf

[18] According to Art. 1(2) of the Agreement on Trade-Related Aspects of Intellectual Property Rights from the World Trade Organisation. It refers to them as "undisclosed information". (Section 7, Part II).

[19] Leslie–Burr–Aitken–Cowls–Katell–Briggs op. cit. 8. An algorithm is a "computational process or set of rules that are performed to solve some problem".

[20] Mariateresa Maggiolino: EU trade secrets law and algorithmic transparency. *Bocconi Legal Studies*, no. 3363178, (2019) 5. Also, with regard to the programming language, Diego Alejandro Morales Oñarte: Implicaciones jurídicas del algoritmo: derechos intelectuales y privacidad, *Foro: Revista de Derecho*, no. 36, (2021) 118.

[21] Michelle Azuaje Pirela – Daniel Finol González: Transparencia algorítmica y la propiedad intelectual e industrial: tensiones y soluciones. *Revista la Propiedad Inmaterial*, no. 30. (2020) 120.

that they are new, involve an inventive step and are capable of industrial application" [Art. 27(1)]. This provision is reproduced almost verbatim by the European Patent Convention in Article 52(1) and as can be seen, this provision does not contain a definition of patent *strictu sensu*. In fact, the legislator opted for a negative definition of this institution, stating what a patent is not. In this way, the Convention includes a series of excluded assumptions, among which are "mathematical methods" [art. 52(2)(a)], "schemes, rules and methods for performing mental acts, playing games or doing business, and programs for computers" [art. 52(2)(c)].

As the European Patent Office recognises in this respect, in its Guidelines for Examination, "mathematical methods play an important role in the solution of technical problems in the fields of technology. However, they are excluded from patentability under Art. 52(2)(a) when claimed as such [Art. 52(3)]"[22]. This last subparagraph ("as such") is of vital importance, as it clearly delimits the scope of the exclusion. Hence, those formulae that involve the use of technical means, such as a computer or other type of device, would be in principle covered by the patent right, as they would be integrated into the patented system[23].

The mathematical method must therefore contribute to the technical character[24] of the patentable invention. Such a contribution can be made in two ways. Firstly, when the mathematical method produces a technical effect that serves the technical purpose of the invention by its application to a field of technology. In these cases, the technical purpose must be specific, to which is added that "the claim is to be fuctionally limeted to the technical purpose, either explicity or implicity"[25] -there must be a causal link between the method and the technical effect-.

Secondly, the technical effect is considered to be fulfilled when the objective is specific technical implementation of the mathematical method, in which case the method must be specifically adapted for such implementation. This adaptation is manifested in that its design is underpinned by the technical considerations of the internal workings of the system. Technical effects due to implementation are considered independently of any kind of technical application[26], i.e. it is not necessary that the first of the assumptions is fulfilled as it is sufficiently relevant to generate the necessary technical character that leads to patent protection.

Notwithstanding the above, it should be borne in mind that the mere fact that an algorithm is in a computer carrying out its functions does not automatically mean that it is protected by patent law. As

[22] *Guidelines for Examination in the European Patent Office.* European Patent Office (EPO), March 2022 (last version available). [Hereinafter: EPO (2022)]

[23] Johan Axhamn: Transparency in automated algorithmic decision-making: perspectives from the fields of intellectual property and trade secret law. In: Liane Colonna – Stanley Greenstein (eds.): *Law in the era of artificial intelligence*. Stockholm, The Swedish Law and Informatics Research Institute, 2022. 172–173. As the author states, in those cases "a technical character is conferred on the subject-matter as a whole, enabling patent eligibility".

[24] This technical character has no legal definition, although it is implicit in the cases that are excluded from the rule since they are not considered inventions. Esperanza Gallego Sánchez: La patentabilidad de la inteligencia artificial. La compatibilidad con otros sistemas de protección. La Ley mercantil, Wolters Kluwer, no. 59, (2019) 4.

[25] EPO (2022) op. cit.

[26] EPO (2022) op. cit.

has already been pointed out "even if the algorithm fulfils the technical consideration criterion, it often lacks an inventive step and novelty"[27]. Moreover, patent protection does not attach to the individual computer program, for example, but to the combination of several technical elements resulting in a technological advance (an invention), i.e. when combined with physical components, the algorithms and their instructions must yield innovative results[28].

If we talk about the specific protection of artificial intelligence, we must consider that we are dealing with a software technology, which is commonly linked to hardware. An obvious example of the latter would be the physical bodies of robots that are brought to "life" by AI. The fact that AI often has hardware as a necessary component means that the technical effect necessary to enjoy patent protection is in principle fulfilled, if the aspects set out in the previous section are present and the requirements of novelty and inventive step are met. In such cases, algorithms that are part of artificial intelligence would enjoy patent protection. According to the European Parliament in this regard, "mathematical methods and computer programs may be protected by patents under Article 52(3) of the EPC when they are used as part of an AI system that contributes to producing a further technical effect", adding that "the impact of such potential patent protection should be thoroughly assessed"[29].

Even so, we have to conclude that, in general, algorithms are excluded from patentability, unless they materialise technical effects and meet above mentioned requirements. The difficulty that companies may face in protecting the algorithm under patent, may lead them to opt for trade secret protection[30].

3.2. The algorithm as a trade secret

It is common to refer to trade and business secrets as equivalent concepts[31], although the reality is that we are dealing with two different terms. Business secrets relate to all confidential information held by

[27] Axhamn op. cit. 173.

[28] Marco Antonio Mariscal Moraza: *Protección jurídica del software*. Madrid, Editorial Reus, 2022. 481. Here the author cites José Carlos Erdozaín López: Un ensayo sobre algunos aspectos de la protección de los programas de ordenador y su consideración jurídica. *Revista de Propiedad Intelectual*, 2001. 77.

[29] *Report on intellectual property rights for the development of artificial intelligence technologies (2020/2015(INI), 2020).* European Parliament, 2020. 3 4. [Hereinafter: European Parliament (2020)] https://www.europarl.europa.eu/doceo/document/TA-9-2020-0277_EN.pdf

[30] Azuaje Pirela – Finol González op. cit. 120–121. As the authors point out, patentability requirements are often not met, leading to companies resorting to trade secrets.

[31] In fact, the Spanish law transposing the European Directive on this matter is called "Ley sobre Secretos Empresariales" (Business Secrets Act).

the company[32], whereas a trade secret relates only to information that meets the requirements of the Trade Secrets Directive. In consequence, business secrecy has a broader content than trade secrecy[33].

When the company opts for trade secret protection of the algorithm[34], the following requirements must be met: 1) the information must be secret, 2) it must have commercial value, and 3) efforts must be made to keep the information confidential (Art. 2(1) Directive 2016/943 on trade secrets, which reproduces what was established by Art. 39(2) TRIPS). This, of course, in the knowledge that the object of secrecy will be *any information or procedure that generates value for the company*, which translates into the acquisition of competitive advantage. In particular, this includes technological information, business information and know-how, provided that there is a legitimate interest in their confidentiality[35].

From the content described above, it can be concluded that we are dealing with a very broad protection[36], which covers *all types of information* provided that the above requirements are met. This implies that the training data that feeds the algorithm, as well as other data related to it, may be covered by the secrecy[37]. When these data include personal data – which will often be the case given the purpose of the systems – the situation is of particular concern[38].

In our opinion, in such cases, we would be dealing with an unlawful system from the beginning, unless the personal data had been collected on a valid basis and authorised by law. In the event that such data were taken from workers, this reasoning would be complicated, since, as the Working Party has already shown, the consent of the workers is generally invalid and the justification for

[32] Reflected in Art. 339 from the Treaty on the Functioning of the European Union: "The members of the institutions of the Union, the members of committees, and the officials and other servants of the Union shall be required, even after their duties have ceased, not to disclose information of the kind covered by the obligation of professional secrecy, in particular information about undertakings, their business relations or their cost components".

[33] *Opinion on the proposal for a directive of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure.* European Data Protection Supervisor, 2014. 4. https://edps.europa.eu/sites/edp/files/publication/14-03-12_trade_secrets_en.pdf

[34] Elizabeth A. Rowe – Nyja Prior: Procuring algorithmic transparency. *Alabama Law Review*, vol. 74, no. 2. (2022) 40. "Information that meets the definition of a trade secret is property to the extent it can be precisely defined and is maintained within the exclusive control of the putative trade secret owner".

[35] Recital 14, Directive 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure.

[36] Sandra Wachter – Brent Mittelstadt: A right to reasonable inferences: re-thinking data protection law in the age of big data and AI. *Columbia Business Law Review*, no. 2. (2019) 116. According to the authors "the final framework to discuss as a potential barrier to the right to reasonable inferences is a "catch all" framework that may pose a substantial barrier to learning the justification behind inferences. […] the new EU Trade Secrets Directive458 is likely to substantially limit controllers' transparency obligations459".

[37] Axhamn op. cit. 174.

[38] *Opinion on the proposal for a directive of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure.* European Data Protection Supervisor, 2014. 2 and 5. https://edps.europa.eu/sites/edp/files/publication/14-03-12_trade_secrets_en.pdf

Already at the time, The European Data Protection Supervisor pointed out that this definition should be more precise and have clearer safeguards regarding data protection rights. It also added that the norm should "take account of the obligations of the holders of trade secrets as data controllers towards the individuals where their personal information is considered to be a trade secret".

the processing of the data on the basis of the contract may also not be sufficient, as it is subject to a restrictive interpretation[39].

3.3. Determining the most appropriate protection

From a business point of view, both patents and trade secrets have disadvantages. On the patent side, the main disadvantage is the difficulty of simply gaining access to patent protection for algorithmically based systems. In addition, the company or individual wishing to patent will have to comply with a series of formalities, as well as the obligation to register the innovation. Patent protection has an expiry date, as the patent has a duration of 20 years (Article 33 TRIPS), without prejudice to the provisions of each national legal system, which means that once this period has expired, competitors may reproduce the invention.

Finally, we must not forget that the patent is a territorial right, i.e. it is subject to a specific geographical scope. Therefore, if the company wishes to protect the invention globally, it will have to patent it in the different countries in which it operates[40].

Patents have been identified as the recommended form of protection for artificial intelligence systems[41]. Patent protection provides publicity for the invention[42], which results in greater transparency of these systems. This is especially important as the private sector is predominant in the development of these technologies[43]; a sector with a fierce degree of competition driven by the quest to achieve the maximum possible profit.

In this attempt to protect the invention as a source of competitive advantage, we find the trade secret, which allows us to keep the system away from competitors[44]. These have a very broad scope of protection, do not require specific formalities and their duration is unlimited, of course, provided they

[39] Article 29 Working Party: Guidelines on consent under Regulation 2016/679*,* 2017. https://ec.europa.eu/newsroom/article29/items/623051;
Article 29 Working Party: Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 2017. https://ec.europa.eu/newsroom/article29/items/612053/en

[40] This explains why "many patent applications are extended to more than one jurisdiction. One-third of all AI patent applications are filed in additional jurisdictions after their first filing and 8 percent are filed in five or more jurisdictions". *Technology trends. Artificial Intelligence.* WIPO, 2019. 16. https://www.wipo.int/edocs/pubdocs/en/wipo_pub_1055.pdf

[41] *Patenting artificial intelligence. Conference Summary.* EPO, 2018. 4.

[42] As it has been explained, "there is a risk that an intelligent agent is considered to be a non-statutory mathematical discovery. If it is not statutory subject matter, a patent cannot be granted and the patent does not, therefore, provide an incentive to disclose the invention". Gregory Hagen: AI and patents and trade secrets. In: Florian Martin – Teresa Scassa: *Artificial intelligence and the law in Canada*. New York, Lexis Nexis, 2021. 5.

[43] Technology trends. Artificial Intelligence. WIPO, 2019. 15. https://www.wipo.int/edocs/pubdocs/en/wipo_pub_1055.pdf. "Companies represent 26 out of the top 30 AI patent applicants, while only four are universities or public research organisations".

[44] Andrew A. Schwartz: The Corporate Preference for Trade Secret. *Ohio State Law Journal*, vol. 74, no. 4. (2013) 640. "A patent application freely shares with the world-including direct competitors-all the hard-earned knowledge that one has developed after spending a lot of time and money".

are not discovered[45]. Despite this flexibility and apparent duration *ad infinitum*, this legal protection is more difficult to deploy in practice, as it requires a high and constant effort – which can translate into monetary costs – on the part of the holder – as well as the licensees, if applicable – to keep this information secret. In addition, other problems are found, such as the difficulty of proving that a third party has unlawfully discovered the protected information. This is further complicated by the fact that the third party may claim to have obtained the information by so-called "reverse engineering"[46], which *is* a lawful way of making the information available.

In our view, the most appropriate protection for algorithms would be patent protection, where possible, as it provides greater transparency to the system. However, the above-mentioned aspects lead to the frequent use of trade secrets[47]. It is for this reason, as well as for the greater opacity it provides to algorithms, that this study will focus on the latter formula.

4. Algorithmic transparency versus trade secrets: reconciling two opposing rights

Algorithm-based systems are used by companies, either for automated decision-making or to carry out control functions over production processes, as well as over the workers themselves. This means that employees in these companies are subject to a high degree of intrusiveness, especially when the activity of the algorithm may affect their fundamental rights[48].

For this reason, one of the guarantees most often invoked by authors and institutions in the face of the opacity of these systems is that of establishing transparency mechanisms. This guarantee, which may seem obvious, is certainly complex in practice. Complexity that, as we shall explain, reaches both the state of the art and the law itself, when algorithms are protected by business secrecy. We could even say that, in those cases in which they are protected by patent, the opacity remains when it comes to systems based on machine learning algorithms[49].

[45] In this sense, it does not matter whether they are discovered on a lawful or unlawful basis in terms of their effects on the market (not, of course, in terms of possible responsibilities when they have been obtained illegally) because once discovered, they are available to the public at large.

[46] Article 3(1)(a) and Recital 16. The latter states that "in the interest of innovation and to foster competition, the provisions of this Directive should not create any exclusive right to know-how or information protected as trade secrets. Thus, the independent discovery of the same know-how or information should remain possible. Reverse engineering of a lawfully acquired product should be considered as a lawful means of acquiring information, except when otherwise contractually agreed. The freedom to enter into such contractual arrangements can, however, be limited by law".

[47] Perel–Elkin-Koren op. cit. 185. As the authors state, "algorithmic decision-making is essentially concealed behind a veil of a code, which is often protected by trade secret law".

[48] It is because of this potential that the European Union has qualified these systems in the workplace as high-risk systems. See, Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts (ANNEX III, 4).

[49] Among other things, because they do not require the establishment of specific and well-defined variables to achieve the final output, but they themselves establish the necessary patterns to achieve the set objective. What is produced during this process to obtain the result is easily unknown, both for the employer who applies it and even for the expert who designed it.

4.1. Conceptualising transparency: the right to be informed

It should be kept in mind that there is currently no standard or unanimous definition of transparency in the context of these systems[50]. Thus, the fact that transparency is configured as a broad concept means that concepts such as access to or openness of these systems, information obligations or accountability mechanisms can be integrated into it.

However, institutions and doctrine have pronounced themselves on the abstract principle of algorithmic transparency, giving it content. In this way, it is said that "transparency may consist in a disclosure of the AI applications used, a description of their logic or access to the structure of the AI algorithms and – where applicable – to the datasets used to train the algorithms"[51].

It is also made clear that compliance with transparency standards can come about in two ways. First, through public disclosure of system information or, second, in the form of an audit of the system, which must be "independent, comprehensive, and effective"[52]. Some authors even include this obligation of transparency in the employer's duty of good faith[53] in the administration of labour relations in the company.

What is clear is that, while transparency is a multifaceted concept[54], the main component of it is the collection and transmission of information about the system, or as already noted, "the demand for transparency (where it exists) translates into a kind of right of access to the algorithm"[55]. A component which, in effect, is the cause of collision between transparency – manifested in the right to information – and opacity – manifested in the right to trade secrecy –.

Now, we are talking about access to information about the system, but it is necessary to determine what type of information, in what form and to whom it will be necessary to transmit it in order to make effective compliance with the duty to provide information and, consequently, the principle of transparency. In this sense, the type of information to be provided in order to understand that the obligation has been fulfilled must be that which allows us to know the logic of the algorithm, that is, to understand it. Specifically, it has been said that the information disclosure should include "the system in question, its processes, direct and indirect effects on human rights, and measures taken to identify and mitigate against adverse human rights impacts of the system"[56]. But more importantly,

[50] Axhamn op. cit. 169 and 176.

[51] Alessandro Mantelero: Data processing and the risks of Artificial Intelligence. *Derecho Digital e Innovación. Digital Law and Innovation Review*, no. 1. (2019) 3.

[52] Council of Europe (2019) op. cit. 9–10.

[53] Antonio José Valverde Asencio: *Implantación de sistemas de inteligencia artificial y trabajo*. Albacete, Editorial Bomarzo, 2020. 25. Also, see Roberto Padilla Parga: El derecho de los trabajadores a la información sobre el algoritmo y el interés corporativo como fuente de opacidad. *Revista Justicia & Derecho*, vol. 5, no. 1. (2022) 8–9.

[54] Heike Felzmann – Eduard FoschVillaronga – Christoph Lutz – Aurelia TamòLarrieux: Towards Transparency by Design for Artifcial Intelligence. *Science and Engineering Ethics, Springer*, no. 26. (2020) 3335. In particular, it is said that transparency "can refer to explainability, interpretability, openness, accessibility, and visibility".

[55] Translated by the autor. Azuaje Pirela – Finol González op. cit. 115.0

[56] Council of Europe (2019) op. cit. 9–10.

transparency – information – it has been described as a principle "which does not involve revealing codes but rather ensuring that the parameters and criteria used to make decisions are understandable". Adding that "there must always be provision for appeal to a human"[57]. Hence, compliance with transparency standards rests on "explanation and meaning", i.e. the ability to convey the reason and manner in which the action was taken[58].

The above allows us to affirm that more relevant than a mere disclosure of the algorithm is access to *meaningful information* about the algorithm; among other things because the mere access to the algorithm is very likely to be useless[59]. This meaningful information is to be understood in the terms of the General Data Protection Regulation, which is also the reference in matters such as the artificial intelligence Regulation proposal (AI Act) and the Directive proposal on improving working conditions of platform workers. This means that to fulfil this obligation, information must be sufficient for the data subject -employee, in this case- to comprehend the reasoning behind the decision, which is accomplished by explaining to the worker the steps used by the algorithm to arrive at a certain outcome[60]. This information should be conveyed in a clear and plain language [Art. 12(1) GDPR][61].

The fact that the fundamental goal is to achieve understandability[62] of the system that allow us to overcome an unfair decision or algorithmic impact, let us conclude that simple access to meaningful information does not necessarily imply disclosure of the subject matter of trade secret protection. This is because knowing or understanding the logic behind the system does not directly involve access to the source of competitive advantage. Proof of the foregoing is the 33rd Recital of the proposal for a Directive on improving working conditions in platform work as it declares that

> "digital labour platforms should not be required to disclose the *detailed functioning* of their automated monitoring and decision-making systems, including algorithms, *or other detailed data* that contains commercial secrets or is protected by intellectual property rights. *However, the result of those considerations should not be a refusal to provide all the information required* by this Directive".

[57] *Artificial intelligence: anticipating its impact on jobs to ensure a fair transition (own-initiative opinion), (INT/845-EESC-2018-).* European Economic and Social Committee, 2018. 8. In a similar way, see European Parliament (2020) op. cit. *Session document A9-0176/2020.* 16.

[58] Cary Coglianese – David Lehr: Transparency and Algorithmic Governance. *Administrative Law Review*, vol. 71, no. 1, 2019. 37.

[59] Hagen op. cit. 18.

[60] Article 29 Working Party: Guidelines on automated individual decision-making and profiling, 2017. In this regard, Recital 47 form the AI Act states that "users should be able to interpret the system output and use it appropriately. High-risk AI systems should therefore be accompanied by relevant documentation and instructions of use and include concise and clear information, including in relation to possible risks to fundamental rights and discrimination, where appropriate".

[61] Article 29 Working Party: Guidelines on transparency under Regulation 2016/679, 2017. 8. In this sense, Art. 6(3) platform workers Directive establishes that "the information shall be presented in a concise, transparent, intelligible and easily accessible form, using clear and plain language".

[62] Lepri–Oliver–Letouz´e–Pentland–Vinck op. cit. 9.

Thus, in principle and as a general rule, transparency does not endanger trade secrets. However, in the event that it does, the well-known principle of proportionality[63] would have to be applied to assess the rights at stake. As the European Parliament itself considers, "the protection of intellectual property must always be reconciled with other fundamental rights and freedoms"[64].

In applying this balancing formula, it is important to bear in mind the nature of both rights. Firstly, the right to be informed – like the right to be consulted – is a right with long tradition in national legal systems, but also at the supranational level[65]. This right(s) is proclaimed as a fundamental right of the European Union (Article 27 of the Charter of Fundamental Rights of the European Union (CFREU)[66]). On the other hand, the right to protect trade secrets – not general business secrets –, appears to be included in Article 17.2 CFREU since, as we have noted earlier in this paper, trade secrets are part of the compendium of intellectual property rights[67]. Although, apparently, we encounter equality between both rights – being considered fundamental – the law has established a clear hierarchy in their interaction. In this way, our attention should be drawn to Article 3(1)(c) of the Directive 2016/943 on the protection of trade secrets, according to which the acquisition of the object of the trade secret is considered lawful when it is necessary for the "exercise of the right of workers or workers' representatives to information and consultation in accordance with Union law and national laws and practices"[68]. Consequently, when the right to information of employees or their representatives is in conflict with the right to secrecy, the former shall prevail over the latter, ie. "trade secrets protection must not exist or take a step back"[69]. And, there is no doubt about it, where such a right to information is necessary to ensure the protection of fundamental rights and freedoms of workers[70].

[63] Explicitly referred in Recital 21.

[64] *Report on intellectual property rights for the development of artificial intelligence technologies (2020/2015(INI)).* European Parliament, 6. https://www.europarl.europa.eu/doceo/document/TA-9-2020-0277_EN.pdf

[65] For instance, we can refer to ILO Convention 135 (art. 2) and ILO Recommendation 143 (Part IV, para. 13), where it is established that the company must provide the necessary facilities and maintain effective communication with the representatives so that they can carry out their functions. It is also necessary to mention the European Social Charter (ESC), which specifically regulates the rights of information and consultation, and of participation, in Arts. 21 y 22, respectively.

[66] "Workers or their representatives must, at the appropriate levels, be guaranteed information and consultation in good time in the cases and under the conditions provided for by Community law and national laws and practices".

[67] Although this may be paradoxical if we stop to think about the content of trade secrets, which comprise not only innovations or know-how, but also any kind of confidential business information that generates economic value. The latter includes, for example, customer lists, which admittedly are not the result of human intellectual activity.

[68] Likewise, in this regard see Recital 18 of the Directive.

[69] Maggiolino op. cit. 15. Also, see Guido Noto la Diega: Against the dehumanisation of decision-making: algorithmic decisions at the crossroads of intellectual property, data protection, and freedom of information. *Journal of Intellectual Property, Information, Technology and E-Commerce Law*, vol. 9, no. 1. (2018) 13.

[70] Maggiolino op. cit. 15. Although the author in this point refers to the right to freedom of expression, the claim that "it is common knowledge that a Directive cannot rule out the application of a fundamental right" is perfectly transferable to the right to information analysed in this section, as it is also a fundamental right. Moreover, it is important to highlight that the means and proceedings adopted to protect trade secrets cannot put at risk or infringe fundamental rights and liberties (Recital 21 Directive).

4.2. Algorithmic transparency in trade secret law: the guarantees provided by the EU Directive

The Directive on trade secrets works to limit the right of secrecy or, in other words, to recognise its non-absolute nature[71]. In doing so, it has been identified that the standard opens up two ways of ensuring algorithmic transparency in the company.

Firstly, through Article 3(1), which lists a series of cases in which the disclosure of secrecy is admissible[72], i.e. when it is discovered or created by another subject independently, when the information is obtained through the analysis, disassembly or testing of a product that is accessible to the public or that is lawfully in possession of the same, without the subject carrying it out being limited to do so by law and, finally, when it is discovered in the exercise of the rights of information and consultation of the representatives and/or workers. This last case, therefore, recognises the prevalence of the rights of information and consultation over secrecy in the event of a collision between the two. This recognition allows these rights to be effectively articulated as a measure of accountability on the part of the employer towards his or her staff, and can be materialised both in the implementation stages of algorithmic-based systems and when they are already in operation or undergo modifications.

Of particular interest in this respect is the express provision for the right to consultation, with dialogue with the company being a clear manifestation of employee participation in matters and allowing these decisions not to be left to the sole consideration of the employer; although the latter, unless expressly provided for in the national legislation, will be free to adopt, unilaterally, any decisions he or she deems appropriate by virtue of his or her right to freedom to conduct his or her business.

The second avenue for algorithmic transparency that has been identified is the established by Article 5(c), which provides, as one of the exceptions to the right to request secrecy protection measures under the Directive, that the alleged disclosure of the secret has occurred as a consequence of its communication by employees to their representatives, where this is necessary for the proper performance of their duties. As can be seen, reference is made to functions in general and not to information and consultation in particular, which opens up the prism of protection. These cases could include, for example, situations of risk for the violation of workers' fundamental rights that require the attention of representatives.

Also in this second pathway, letters (b)[73] and (d)[74] should be taken into consideration, which, although they do not directly refer to the field of employment, are susceptible to application in this field.

[71] David Vaver: Intellectual property: the state of the art. *Victoria University of Wellington Law Review*, vol. 32, no. 1, 2001. 17. Intellectual property has to be reconciled with other values, which are of equal importance. Therefore, "intellectual property cannot be treated as an absolute value".

[72] It is important to note the open-ended nature of the list of cases referred to (Article 3(1)(d)), which implies that more situations than those expressly referred to in the provision may be considered.

[73] Relating to the discovery of an irregularity or illegal activity, where the defendant acted in the general interest.

[74] In order to protect a legitimate interest.

4.3. Guarantees in the Spanish legislation

Focusing our attention on Article 3(1)(c), we note that the Directive sets the rights of information and consultation in direct relation to national legal systems, which implies that the scope of action of the holders of this right will be subject to the specific Member State in which it operates, with a broader or narrower right depending on the case.

In Spain, to observe the scope of these guarantees, we must refer to *Ley 1/2019, de 20 de febrero, sobre secretos empresariales* (Law 1/2019, of 20 February, on business secrets), which is responsible for transposing the Directive. However, this scope is limited, as an analysis of the law in this area shows that it merely reproduces what is already provided for in the European standard itself, although with a different arrangement of the legal text. We find, then, that the measures referred to in Article 3(1)(c) and 5(1)(c) of the Directive are included in a single provision together, in Article 2(1)(c) and 2(3)(c) of the Spanish law. Therefore, we cannot see any development by the national rule with respect to the European rule in this regard.

Nevertheless, Spanish legislation does not leave these rights aside, but decides to establish a specific regulation through labour legislation. Indeed, the *Estatuto de los Trabajadores* (Worker's Statute) dedicates an extense provision (Article 64) to the exclusive development of information and consultation rights. As far as we are concerned, we must turn to Article 64(4)(d), which expressly recognises, for the first time since 2021[75], the right to information on algorithms. This provision declares the right to:

> "be informed by the company of the parameters, rules and instructions on which algorithms or artificial intelligence systems are based that affect decision-making that may have an impact on working conditions, access to and maintenance of employment, including profiling"[76].

The content of this right is based on the concept of "understandability" and "explainability", as the aim is to obtain information about the logic of the algorithm, leaving aside the technical core of it. Even so, it is a precept with certain shortcomings, such as 1) the temporal ambiguity, as the information shall be provided "at appropriate intervals"[77], 2) the restricted compendium of matters in respect of which the information is to be provided, 3) the sole consideration of decision making, without taking into account other possible areas of the use of these systems – as relevant as those of employment for monitoring and

[75] *Artículo único. Uno de la Ley 12/2021, de 28 de septiembre, por la que se modifica el texto refundido de la Ley del Estatuto de los Trabajadores, para garantizar los derechos laborales de las personas dedicadas al reparto en el ámbito de plataformas digitales* (Sole article. One of Law 12/2021, of 28 September, which amends the revised text of the Workers' Statute Law in order to guarantee the labour rights of people dedicated to delivery in the field of digital platforms). This law has been popularly known as the "Rider Law", although this is a misnomer as the amendments introduced do not only affect digital platform workers.

[76] Translated by the author from the original Article.

[77] Beginning of Article 64(4).

control of labour performance –[78] and 4) probably one of the most notable shortcomings: the absence of a right to consultation[79] and, where appropriate, the issuing of a report.

Furthermore, it should be noted that this is a right of collective exercise, in that it is entrusted to the workers' representatives, whether internal to the company – works council – or trade unions, assuming that the workers themselves cannot directly request this information from the employer, but that the intervention of their representatives will be required.

Lastly, it is necessary to mention, at least, the very recent Article 23 *Ley 15/2022, de 12 de julio, integral para la igualdad de trato y la no discriminación* (Law 15/2022, of 12 July, on equal treatment and non-discrimination), on "artificial intelligence and automated decision-making mechanisms", which requires Spanish public administrations to ensure that the algorithms they use to make decisions comply with minimum standards that make it possible to reduce the biases of these systems and, consequently, to address their discriminatory impact. In addition, transparency provisions are established, as public administrations must prioritise "transparency in design and implementation and the ability to interpret the decisions taken by them"[80].

With all of the above, Spanish law, like EU law, places the right to information above secrecy and, furthermore, gives it content by developing a specific legal framework for algorithms and artificial intelligence. In particular, the first part of the wording of Article 64(4)(d) of the *Estatuto de los Trabajadores* is to be considered positively, as it does not set up the obligation with regard to the source code or technical aspects of it, but to its logic; allowing to transfer relevant information about the algorithm without disclosing the trade secret.

4.4. The real challenge: internal opacity and the problem of trust

After addressing all these guarantees, one might think that trade secret law is not really the problem in terms of algorithmic opacity that everyone seems to acknowledge: the law provides us with safeguards and mechanisms that seem to let us access the algorithm when necessary. But, if this is not the main obstacle for transparency, we must ask ourselves where the problem lies.

We have found two fundamental aspects that keep algorithms a black box.

[78] In this respect, the proposal for a Directive on digital platforms is right to consider "automated monitoring systems which are used to monitor, supervise or evaluate the work performance of platform workers through electronic means" [Article 6(1)(a)].

[79] Paradoxically, this right was recognised in the drafts prior to the current precept. However, in the end, a much more conservative regulation was chosen, which is the one currently in force. If you would like to learn more about the legislative process of this article, as well as the development of its drafts, I recommend reading Francisco Pérez Amorós: ¿Quién vigila al algoritmo?: los derechos de información de los representantes de los repartidores en la empresa sobre los algoritmos de las plataformas de reparto. *e-Revista Internacional de la Protección Social*, vol. 6, no. 1, (2021).

[80] Article 23(2). Translated by the author.

First and foremost, the obscure nature of these systems or, in the terms already expressed, their technical or internal opacity. The fact that algorithms are opaque by nature[81] leads to significant problems in enforcing the right of information that results in compliance with the requirements of algorithmic transparency provided by law[82]. The solution that is found to this problem is the establishment of accountability systems that allow us to know the logic behind the system, although it happens that, depending on the type of system we are talking about, the possibilities of auditing it from a technical point of view will be subject to fluctuation and to important limitations. Again, this is especially problematic when it comes to machine learning algorithms, as they enjoy autonomy in achieving the output. As has been rightly pointed out, "the difficulty is that given the "black box" nature of AI, the software can be a "human-illegible chunk of math" that operates "without providing their creators (or anyone else) any meaningful information insight as to the underlying logic of the system"[83].

Therefore, the problem is not so much the existence of a secret that protects the algorithm, but the algorithm itself. If it is not possible to know the logic, the process or the purpose behind the operations that the system carries out, it becomes unfeasible to be able to convey meaningful information about it in the terms expressed in the previous sections.

In addition, the means currently available to corroborate that systems are fair and respectful of rights are limited. The fact that the legislator imposes guarantees of transparency will not be enough to ensure the development of human-centred algorithms or AI. As has been pointed out by some authors, sometimes the law set standards of transparency that, in practice, are impossible to reach[84].

An algorithm does not understand concepts such as morality, justice or non-discrimination, but requires the introduction of specific variables[85] that lead it to obtain results in accordance with these human concepts; concepts that also do not have the same meaning for all people, as they are subjective. If we ask an algorithm not to discriminate, for example, it will be necessary to develop a specification that will allow computer scientists to make such a request feasible[86].

[81] Perel–Elkin-Koren op. cit. 188.

[82] In fact, the rules themselves are aware of this problem. Thus, we find that the proposed IA Regulation acknowledges that it is not possible to guarantee full transparency, since, as it states that "*a certain degree* of transparency should be required for high-risk AI systems" (Recital 47 AI Act). Similarly, Article 13(1) establishes that "high-risk AI systems shall be designed and developed in such a way to ensure that their operation is *sufficiently transparent* to enable users to interpret the system's output and use it appropriately. *An appropriate type and degree of transparency* shall be ensured, with a view to achieving compliance with the relevant obligations of the user and of the provider". Likewise, Article 23 Ley 15/2022 provides that that "public administrations shall encourage the implementation of mechanisms so that the algorithms involved in decision-making used in public administrations take into account criteria of minimisation of bias, transparency and accountability, *whenever technically feasible*".

[83] Hagen op. cit. 9. Citing Stacy Rush: The Challenges of Patenting Artificial Intelligence. *Canadian Lawyer Magazine*, 2017.

[84] Desai–Kroll op. cit. 5. Thus, "from a technical perspective, general calls to expose algorithms to the sun or to conduct audits will not only fail to deliver critics' desired results but also may create the illusion of clarity in cases where clarity is not possible".

[85] For example, introducing specific cases in which discrimination is considered to be occurring in order to prevent the system from replicating it. The problem with this parameterisation is that it would have to be programmed indefinitely, as the discrimination scenarios are endless.

[86] Desai–Kroll op. cit. 25.

As a result, the mere requirement for transparency is insufficient to keep systems audited[87].

The second challenge identified is the exercise of the right to information itself and the problem of trust.

On the assumption that it is possible to obtain such logic and understandability of the algorithm, we continue to find challenges to transparency. Firstly, because of the imbalance of power between the social and business sides, which can lead to difficulties in demanding the information that the Directive allows them to obtain. This imbalance is accentuated when this right is exercised by the employees themselves.

It is also difficult to determine in which cases a request for information is appropriate, since, as the system is under trade secret protection, even the employees subject to it may not be aware of its existence, or, in other words, they may be ignorant of the fact that the source of the infringement was a system responsible for making a certain decision, and not a human being. However, if the AI Regulation is adopted as currently drafted, it will be mandatory for persons interacting with AI systems to be informed of their existence (Article 52(1) Regulation), yet there is silence on whether persons who do not interact with these systems, but who are affected by them, should be informed.

Finally, there is what could be called a problem of trust, because the representatives and/or the employees, in the exercise of the right to information, will have to believe the information on the logic of the algorithm transmitted by the employer to be true, and it will not be possible to verify its veracity. As we are in the private sphere, the employer "is free to determine what specific information to disclose in accordance with their private, financial interests"[88].

Thus, everything is left to the good faith of the employer, unless there are provisions imposing obligations to audit these systems and consequently to ensure accountability[89]. This is, of course, without prejudice to access to this information through a legal claim or when workers or representatives with technical expertise in this respect access the system.

5. Concluding remarks

The study has allowed us to conclude that algorithmic transparency in itself does not endanger trade secrets, which are so valuable to any company's business. The fact that enforcing transparency

[87] Perel–Elkin-Koren op. cit. 188. The authors point the inadequacy of transparency as a guarantor of accountability, based on four reasons: 1) the great complexity involved in reading and interpreting the code under which the algorithms are, 2) the irrelevance of transparency requirements when there is trade secrecy, 3) the impracticality of reviewing all the information disclosed, and 4) when algorithms have a margin of discretion to carry out their own determinations, transparency in inputs and outputs is insufficient to know the reasoning behind a given action.

[88] Perel–Elkin-Koren op. cit. 194. The authors expressly refer to online intermediaries, although this statement is perfectly applicable to our context.

[89] Provisions of this type exist in the proposal for a Regulation on IA with regard to high-risk systems (Title III). The regulation of the rest of the IA systems with respect to the obligations of Chapter II of Title III is left to the will of the subjects through the drafting of a code of conduct (Title IX).

obligations requires the provision of meaningful information about the logic of the algorithm makes it possible to promote a balance between the needs of both sides of the employment relationship. However, in the event that disclosure is necessary, the law give prevalence to the exercise of the rights of information and consultation.

As a consequence of the above, the premise that started this work, which positioned secrecy as a fundamental obstacle, is refuted, as the reality is that it is a complementary obstacle to the natural opacity of the algorithm.

Moreover, the notion that transparency in itself is the solution to opacity has proven to be wrong, as it is technically impossible to achieve a fully transparent system. A combination of means and approaches is therefore necessary to achieve accountability of algorithms. Hence, it is not surprising that the European Parliament itself recognises that the evaluation of artificial intelligence applications is a challenge that requires the development of new techniques[90]. In this way, transparency obligations should be clear and specific, taking into account and adapting to technical limitations in order to build a framework that fills these transparency gaps, always allowing for a final review by a human being.

It is necessary to emphasise the importance of implementing transparency measures from the start, through an *ex ante* approach. This approach may be even more important than the *ex post* approach, depending on the system in question[91]. In this respect, we speak of prospective transparency and retrospective transparency[92].

We believe that there is a need to enhance the involvement of employee representatives with the company regarding algorithmic systems, especially when they are protected by trade secrecy. The representatives should have all the information and be empowered to talk to the employer about the measures taken with regard to algorithms, always, of course, respecting professional secrecy (Article 4(3)(b) Directive and Article 65 Workers' Statute). Let us say that, in this sense, the representatives would be like the insider in matters concerning secrecy.

Similarly, workers or outsiders with expert knowledge could be brought in to monitor the systems, shielding secrecy through contractual confidentiality and post-contractual non-competition clauses.

To conclude, it is essential to guarantee channels of complaint and protection mechanisms for those who face violations, either because they have been direct victims of the system or because they have become aware of a risk from it. A good example is the regulation established by the digital platform workers Directive (Articles 7(3), 17 and 18).

[90] European Parliament (2020) op. cit. Session document A9-0176/2020. 16.

[91] European Parliament (2020) op. cit. It is appreciated that in the case of adaptive learning systems some *ex ante* disclosures may be ineffective on their own, as these systems are able to recalibrate themselves with each input.

[92] Axhamn op. cit. 176.