https://doi.org/10.22364/iscflul.8.2.27

Liva Rudzite, *Mg. iur., doctoral degree candidate*
Faculty of Social Sciences, University of Tartu, Estonia

Aleksei Kelli, *Dr. iur., Professor*
Faculty of Social Sciences, University of Tartu, Estonia

THE INTERACTION BETWEEN ALGORITHMIC TRANSPARENCY AND LEGALITY: PERSONAL DATA PROTECTION AND PATENT LAW PERSPECTIVES

Keywords: artificial intelligence, transparency, data protection, patent

Summary

Artificial Intelligence and its sub-field Machine Learning in the European Union has been directed as one of the political priorities towards the augmentation of human prosperity. However, due to its characteristics, for instance, the "black-box" problem, AI may pose challenges within the existing legal framework.

The article focuses on analysing the legality of algorithmic transparency in two fields in the EU-data protection (obligation to provide information to the data subject) and under the criteria of "sufficient disclosure" of the patent legal framework – to improve legal clarity concerning the issue.

Introduction

Artificial Intelligence (hereinafter – AI) and its sub-field Machine Learning (hereinafter – ML)[1] are promising innovations having the potential to increase our life quality. They have many advantages and potential to augment human

[1] ML focuses on enabling computers to self-learn by identifying data patterns, building explaining models, and conducting predictions without programmed models and rules. Some algorithms follow a pre-defined function; others, more sophisticated algorithms consist of neural networks and are attributed to deep that mimics representation learning of biological processes.
Maini V., Sabri S. Machine Learning for Humans. Available: https://everythingcomputerscience.com/books/Machine%20Learning%20for%20Humans.pdf [viewed 09.10.2021.], pp. 9, 71–77.

prosperity[2]. However, one of the drawbacks that may be displayed by the ML in deep learning models is the lack of algorithmic transparency or the so-called "black box" paradigm[3]. Namely, it is unclear how AI makes the "decision". The lack of transparency could relate to 1) inability to explain the underlying logic of data correlation; 2) deficiencies (misrepresentation) in the input, training data. At the same time, transparency is required by data protection and patent law. Therefore, there is a tension between the transparency requirement originating from the General Data Protection Regulation[4] (hereinafter – GDPR) and the condition of sufficient disclosure of a patented invention provided by the European Patent Convention[5] (hereinafter – the EPC) and algorithmic transparency.

The authors outline challenges that algorithmic transparency may face regarding compliance with legality requirements in the EU, particularly those stemming from GDPR and "sufficient disclosure" criteria of the patent legal framework under the EPC. The authors of the article also aim to analyse potential solutions and their sufficiency preliminarily. The interaction between both regimes is considered to render "black box" algorithms to "white box" (understandable).

1. Personal data protection and algorithmic transparency

The GDPR contains several requirements that must also be fulfilled for AI applications. For instance, the data subject[6] must be informed on the existence of automated decision-making, including profiling and meaningful information about the logic involved[7]. The requirement is also enlightened in the SyRi case[8]. Additionally, automated decision-making and profiling are prohibited (Art. 22(1)) except in the specific cases ensuring adequate safeguards (Art. 22(2)(3)) including a human in the loop; privacy by design, default (Art. 25), and others.

In the "black box" algorithms, issues might appear to determine who should or can pursue an oversight and what other safeguards may prevent risk. For instance,

[2] The European Parliament. Report on a comprehensive European industrial policy on artificial intelligence and robotics. Available: https://www.europarl.europa.eu/doceo/document/A-8-2019-0019_EN.html [viewed 09.10.2021.].

[3] Ibid., p. 5.

[4] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. Luxembourg: Official Journal of the European Union, L 119, 2016.

[5] The Convention on the Grant of European Patents. Signed in Munich on 05.10.1973 [in the wording of 17.11.2020.].

[6] The data subject is an identified or identifiable natural person whose personal data is processed (GDPR Article 4 (1)).

[7] GDPR Article 13 (3) f).

[8] Rechtbank Den Haag judgment of 5 February 2020 in Case No. C-09-550982-HA ZA 18-388. Available: https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2020:1878 [viewed 09.10.2021.].

anonymization may not guarantee complete depersonalization if person-specific characteristics are processed[9]. Besides, there might be an overarching desire to cloak disclosure of information under trade secrets as was in the COMPAS[10] case.

To tackle issues with AI, additionally to the relevant guidelines regulating the legality of AI applications, there has been a proposal to enact an AI Act[11] that prohibits specific AI applications, classifies high-risk applications, as well as sets respective safeguards. For instance, mandatory, confidential disclosure of underlying data, source code, a certification that would approve the safety and the legality of the AI system, and others.

In this regard, the authors take a stand that coverage under the trade secrecy would be hindered for high-risk systems that want to place AI system on the market or put it into service and use in the EU. It also appears that the AI Act tries to establish features of *sui generis* legal framework for AI that will also have an impact on indirectly linked fields.

Additionally, the authors deem that apart from pure disclosure of the input and training data, the description should outline in detail the source, the relevance of data (for instance, only historical data may not be appropriate to predict future behaviour), the impartiality of data (demographic, geographical coverage) and other aspects to facilitate validation of the AI system.

Besides, AI Act does not foresee that "black box" algorithms *per se* without a noted effect, application (Art. 5, 6) should be prohibited or identified as high-risk. Nevertheless, non-prohibited, non-high-risk algorithms due to the "black box" could still bring challenges of realization of respective rights. For instance, applications related to lifestyle, well-being (water consumption, step counter), the function, and posed risk of which are not as such to classify and certify them as medical devices. Thus, the authors of this article opine that equivalent certification could be offered at least as voluntary to tackle outlined challenges with non-prohibited, non-high-risk "black box" algorithms.

Alternatively, there is a suggestion of "experimental proportionality"[12], according to which unproven AI systems are placed in use upon informing the data subjects and prohibited if proven disproportionate or unsafe. Although, to some extent, this correlates with the existing approach; however, this suggestion could

[9] Council of Europe. The protection of individuals with regard to automatic processing of personal data in the context of profiling and explanatory memorandum. Available: https://rm.coe.int/16807096c3 [viewed 09.10.2021.], p. 36.

[10] Decision of the Supreme Court of Wisconsin of 13 July 2016 in Case No. 2015AP157-CR. Available: https://caselaw.findlaw.com/wi-supreme-court/1742124.html [viewed 09.10.2021.].

[11] Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts. Available: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52021PC0206 [viewed 09.10.2021.].

[12] Marion O., Grace J., Urwin S., Barnes G. C. Algorithmic risk assessment policing models: lessons from the Durham HART model and 'Experimental' proportionality, Information & Communications Technology Law, 2018, No. 27(2), p. 242.

have difficulties fulfilling other AI transparency requirements in the EU, especially if the AI Act is enacted.

Besides, in the view of the authors, in cases of non-high-risk "black box" algorithms, the revelation of underlying data and source code proposed in the AI Act could instead serve as the last option, if least revealing measures, namely, the written description, could not be sufficient to verify safety and legality of the algorithm.

2. The criteria of "sufficient disclosure" in the patent legal framework

Art. 83 of the EPC stipulates that "patent application shall disclose the invention in a manner sufficiently clear and complete for it to be carried out by a person skilled in the art". Rule 42 of the Implementing Regulations[13] states the criteria for the content of the description, generally requiring a written form. Besides, according to Art. 100(b) of the EPC, non-compliance with Art. 83 could serve as a ground for the opposition to revoke the patent.

Rule 42 does not require the expert to carry out the invention (for example, write a code or train a model). Realization *per se* is related to: a) usefulness – the feasibility to realize the technical problem (the desired outcome) from the provided description, examples; b) completeness (realization could be conducted by simple verification tests applying reasonable effort without additional experimentation); c) repeatability (the invention could be reproduced with a statistically acceptable frequency)[14].

Under "clearness" essential features, their interconnection, impact on the result cannot be omitted, ambiguous due to the mass of information[15]. For example, the patent application T 161/18[16] was rejected because the suitable input and training data were not expressly mentioned limiting the description to "such data should cover a wide range of patients". Additionally, it was stated that only an indication that "weight values are determined by learning" does not exceed the prior state of the art.

The *ratio* of training data disclosure is that the performance of an identical process does not guarantee the same output if the logic remains unknown. An algorithm could not be disclosed if the invention does lie in the data that is not

[13] Implementing Regulations to the Convention on the Grant of European Patents. Signed in Munich on 05.10.1973 [in the wording of 15.12.2020.].

[14] Haedicke M., Timmamm H. Patent Law: A Handbook on European and German Patent Law. München: Verlag C. H. Beck, 2014, pp. 207–208, 210–211.

[15] Ibid., p. 211.

[16] Decision of the European Patent Office Board of Appeal dated 12 May 2020 No T 161/18. Available: https://www.epo.org/law-practice/case-law-appeals/recent/t180161du1.html [viewed 09.10.2021.].

a part of the algorithm[17]. Thus, both input and output should be considered[18]. It should be noted that disclosure only of the algorithm, training data without explaining the origin of data and other related aspects as previously outlined could still not be sufficient to carry out the invention.

In this regard, instead of disclosure of the actual library of data as such or the source code of the algorithm in all cases, the description of steps taken to create training data[19], features and parameters, amount of these data, training approach, functions, the model architecture and impact of each of the essential elements could be explained, if feasible. For instance, "images of human faces", considering that the invention could, in general, be reproduced by the algorithm, involved training steps (in cases of classification algorithms)[20].

Under the criteria of "completeness" (level of detail of the description), for instance, general data processing technology terms (kernel, and others) may pertain to specific technical aspects solely if explained in a level of detail that provides a sufficient picture of the architecture of the system and interaction between the constituting components[21]. For example, and for comparison, the patent application by Microsoft was initially rejected by the United States Patent and Trademark Office due to the lack of disclosure of the specific ML model[22]. Also, EPO deems that AI-related inventions may require disclosure of training steps and underlying algorithms; pure reference to the abstract models as "neural network", "support vector machine", and others lack technical character if claimed *per se*[23].

There is no requirement for the invention to be ready for commercialization; also, such aspects as the risk of injury, danger, and others do not prevent completeness and patentability[24]. In this regard, the authors deem that requirements of the AI Act for high-risk AI systems as well as AI applications

[17] European Patent Office. Report from the IP5 expert roundtable on artificial intelligence. Available: https://www.fiveipoffices.org/material/AI_roundtable_2018_report [viewed 09.10.2021.], p. 3.

[18] European Patent Office. Patenting Artificial Intelligence. Conference Summary, 30 May 2018, Munich. Available: https://e-courses.epo.org/pluginfile.php/23523/mod_resource/content/2/Summary%20Artificial%20Intelligence%20Conference.pdf [viewed 09.10.2021.], p. 8.

[19] European Patent Office. Guidelines for Examination: G II 3.3.1 Artificial intelligence and machine learning. Available: https://www.epo.org/law-practice/legal-texts/html/guidelines/e/g_ii_3_3_1.htm [viewed 09.10.2021.].

[20] European Patent Office. WIPO Conversation on Intellectual Property (IP) Artificial Intelligence. Revised Issues Paper on Intellectual Property Policy and Artificial Intelligence: Comments by the European Patent Office (EPO). Available: https://www.wipo.int/meetings/en/doc_details.jsp?doc_id=499504 [viewed 09.10.2021.], pp. 9–10.

[21] Haedicke M., Timmamm H. Patent Law: A Handbook on European and German Patent Law, pp. 220, 222–223.

[22] Lee J. A., Hilty R., Liu K. C. Artificial Intelligence & Intellectual Property. Oxford: Oxford University Press, 2021, p. 118.

[23] European Patent Office. Patenting artificial intelligence at the EPO. Available: https://www.wipo.int/edocs/mdocs/scp/en/scp_32/scp_32_c_quality.pdf [viewed 09.10.2021.].

[24] Decision of the European Patent Office Board of Appeal dated 25 June 1997 No. T 881/95. Available: https://www.epo.org/law-practice/case-law-appeals/recent/t950881du1.html [viewed 09.10.2021.].

that are intended to be prohibited in the scope of jurisdiction of the AI Act will not affect the patentability of such systems only in exceptional cases. Namely, if the patent is claimed in the country that is a member of EPC but will not be the subject of the AI Act. Delineating, if AI Act is enacted, it will become a part of *ordre public* of the respective states. Thus, non-compliance with the AI Act may serve as grounds to refuse patentability, especially because the AI Act (Recital 11) is intended to apply also to AI systems that are not yet placed in the market or used or put into service in the EU.

In the case of the "black box", difficulties might appear mainly in the process patents to describe the technical structure and steps, for instance, in diagnostics cases[25]. In this regard, the authors of this article opine that if the inventive step lies in the algorithm, then apart from the mentioned general features, appropriate datasets should be disclosed or the description on the data correlation. For instance, the application should reveal experimentation results following the proposed AI Act approach and the sample verification cases. Alternatively, the general description indicating the appropriate datasets could be supported by clinical, scientific evidence, decomposition, or building model-agnostic explainers as suggested to certify AI-related medical devices in "black box" cases[26].

It has been suggested that in the case of the application of deep neural networks, the requirement of sufficient disclosure could be supplemented with a model deposit requirement similarly as-is for biological materials[27] or training data deposit to foster understanding of output generation[28]. This approach might not be supported since the existing EPO system does not foresee substituting written description by a deposit. Besides, deposition of the whole algorithm could contradict trade secrets since "sufficient disclosure" does not require disclosing everything related to the invention to the public.

Nevertheless, the authors opine that in the case where the patent is claimed in the EU and for the inventions where disclosure of the input, training data is the only option to suffice the disclosure requirement under the patent legal framework of the EPC. The revelation of underlying data, source code that could be a part of the certification proposed in the AI Act could be used as a pre-step to evaluate the fulfillment of the criteria of "sufficient disclosure". In this regard, certification could serve as an addition to the written description, not a substitution for it. Besides, this would facilitate that data is disclosed only once, not imposing

[25] The Joint Institute for Innovation Policy, IViR. Trends and Developments in Artificial Intelligence: Challenges to the Intellectual Property Rights Framework. Available: https://digital-strategy.ec.europa.euen/library/trends-and-developments-artificial-intelligence-challenges-intellectual-property-rights-framework [viewed 09.10.2021.], pp. 11–114.

[26] Ordish J., Murfet H., Hall A. Algorithms as medical devices, Report. Available: https://www.phgfoundation.org/media/74/download/algorithms-as-medical-devices.pdf?v=1&inline=1 [viewed 09.10.2021.], pp. 26, 38.

[27] The Joint Institute for Innovation Policy, IViR. Trends and Developments in Artificial Intelligence: Challenges to the Intellectual Property Rights Framework, European Commission Report, p. 113.

[28] Ebrahim T. Y. Artificial Intelligence Inventions & Patent Disclosure. Penn State Law Review, 2020, Vol. 125, No. 1, pp. 215–217.

the additional burden for the inventors. Furthermore, those inventors who, upon enactment of the AI Act, will want to obtain the patent under the EPC regime and will want to place the AI system on the market or put it into service and use in the EU will, in any case, have to comply with both regimes. In this case, a revelation of the underlying data to the extent to suffice disclosure condition may not necessarily be required to be rendered public since the certification under AI Act could affirm the feasibility of realization. This proposal of cooperation between both systems would facilitate incentive to innovate in the EU, place the AI system on the market or put it into service and use in the EU. Besides, it would not require legal amendments but rather acceptance from the EPO.

Conclusion

Data protection and the existing AI-related soft law addresses various aspects of tackling the "black box" paradigm. However, the proposed AI Act will bring a significant addition to overcoming these challenges. Thus, this approach could be followed with non-high-risk "black box" algorithms.

Although EPO practice provides respective guidance about the criteria of "sufficient disclosure", more explanatory guidelines of how to manoeuvre it in AI-related patent applications, especially those that deploy deep neural networks, would be welcomed. By then, the approach proposed in the AI Act or that to certify "black box" medical devices could be applied.

AI Act proposes to establish features of *sui generis* legal framework for AI. It will also impact indirectly linked fields, for instance, patentability under the EPC, especially if the patent is claimed in the country that is a member of EPC and will be the subject of the AI Act.

One possibility to render "black box" systems as "white box" would be to establish cooperation between the proposed input, training data revelation under the AI Act and the EPC. Thus, it would suffice the invention disclosure criteria in cases where the revelation of the underlying data would be the only option.

BIBLIOGRAPHY

Literature

1. Ebrahim T. Y. Artificial Intelligence Inventions & Patent Disclosure. Penn State Law Review, 2020, Vol. 125, No. 1.
2. Haedicke M., Timmamm H. Patent Law: A Handbook on European and German Patent Law. München: Verlag C. H. Beck, 2014.
3. Lee J. A., Hilty R., Liu K. C. Artificial Intelligence & Intellectual Property. Oxford: Oxford University Press, 2021.
4. Maini V., Sabri S. Machine Learning for Humans. Available: https://everythingcomputerscience.com/books/Machine%20Learning%20for%20Humans.pdf [viewed 09.10.2021.].

5. Marion O., Grace J., Urwin S., Barnes G. C. Algorithmic risk assessment policing models: lessons from the Durham HART model and 'Experimental' proportionality. Information & Communications Technology Law, 2018, No. 27(2).
6. Ordish J., Murfet H., Hall A. Algorithms as medical devices, Report. Available: https://www.phgfoundation.org/media/74/download/algorithms-as-medical-devices.pdf?v=1&inline=1 [viewed 09.10.2021.].

Court practice

7. Decision of the European Patent Office Board of Appeal dated 12 May 2020 No. T 161/18. Available: https://www.epo.org/law-practice/case-law-appeals/recent/t180161du1.html [viewed 09.10.2021.].
8. Decision of the European Patent Office Board of Appeal dated 25 June 1997 No. T 881/95. Available: https://www.epo.org/law-practice/case-law-appeals/recent/t950881du1.html [viewed 09.10.2021.].
9. Decision of the Supreme Court of Wisconsin of 13 July 2016 in Case No. 2015AP157-CR. Available: https://caselaw.findlaw.com/wi-supreme-court/1742124.html [viewed 09.10.2021.].
10. Rechtbank Den Haag judgment of 5 February 2020 in civil Case No. C-09-550982-HA ZA 18-388. Available: https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2020:1878 [viewed 09.10.2021.].

Other materials

11. Council of Europe. The protection of individuals with regard to automatic processing of personal data in the context of profiling and explanatory memorandum. Available: https://rm.coe.int/16807096c3 [viewed 09.10.2021.].
12. European Patent Office. Guidelines for Examination: G II 3.3.1 Artificial intelligence and machine learning. Available: https://www.epo.org/law-practice/legal-texts/html/guidelines/e/g_ii_3_3_1.htm [viewed 09.10.2021.].
13. European Patent Office. Patenting Artificial Intelligence. Conference Summary, 30 May 2018, Munich. Available: https://e-courses.epo.org/pluginfile.php/23523/mod_resource/content/2/Summary%20Artificial%20Intelligence%20Conference.pdf [viewed 09.10.2021.].
14. European Patent Office. Report from the IP5 expert round table on artificial intelligence. Available: https://www.fiveipoffices.org/material/AI_roundtable_2018_report [viewed 09.10.2021.].
15. European Patent Office. Patenting artificial intelligence at the EPO. Available: https://www.wipo.int/edocs/mdocs/scp/en/scp_32/scp_32_c_quality.pdf [viewed 09.10.2021.].
16. European Patent Office. WIPO Conversation on Intellectual Property (IP) Artificial Intelligence. Revised Issues Paper on Intellectual Property Policy and Artificial Intelligence: Comments by the European Patent Office (EPO). Available: https://www.wipo.int/meetings/en/doc_details.jsp?doc_id=499504 [viewed 09.10.2021.].
17. Implementing Regulations to the Convention on the Grant of European Patents. Signed in Munich on 05.10.1973. [in the wording of 15.12.2020.].
18. Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts. Available: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52021PC0206 [viewed 09.10.2021.].
19. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data

and on the free movement of such data, and repealing Directive 95/46/EC. Luxembourg: Official Journal of the European Union, L 119, 2016.

20. The Convention on the Grant of European Patents. Signed in Munich on 05.10.1973 [in the wording of 17.11.2020.].
21. The European Parliament. Report on a comprehensive European industrial policy on artificial intelligence and robotics. Available: https://www.europarl.europa.eu/doceo/document/A-8-2019-0019_EN.html [viewed 09.10.2021.].
22. The Independent High-Level Expert Group on Artificial Intelligence. A Definition of AI: Main Capabilities and Disciplines. Available: https://ec.europa.eu/digital-single-market/en/news/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines [viewed 09.10.2021.].
23. The Joint Institute for Innovation Policy, IViR. Trends and Developments in Artificial Intelligence: Challenges to the Intellectual Property Rights Framework. Available: https://digital-strategy.ec.europa.eu/en/library/trends-and-developments-artificial-intelligence-challenges-intellectual-property-rights-framework [viewed 09.10.2021.].