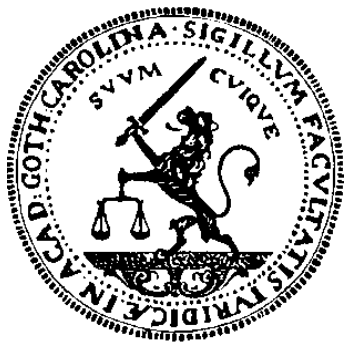


FACULTY OF LAW
Lund University

Kristina Christensen

Exhibiting transparency without opening the 'Black Box'

Balancing act between Data Protection and Trade Secrets Rights in Solely Automated Decision-Making AI system in Healthcare

JAEM03 Master Thesis

European Business Law
30 higher education credits

Supervisor: Ana Nordberg
Term: Spring 2020

Table of content

Summary

What was once called science fiction has developed over the years to be one of the most strategic technologies of the 21st century – artificial intelligence (AI) is real. The rapid digitalization has opened new pathways in Swedish healthcare, by increasing productivity and the effectiveness of care delivery as well as helping more patients in receiving better care. Yet, when fully automated decision-making AI system is at stake, where medical decisions are delegated to an AI algorithm, a conflict between two rights arise – the right of the patient to a transparent processing of its data concerning health and the right of the healthcare provider to keep its AI algorithms used in automated processing as a trade secret. Since no medical decisions have been fully delegated to an AI algorithm within the Swedish healthcare, this thesis aims at examining the risks and opportunities of such situation.

Patient's data protection rights to a transparent processing of its data concerning heath in automated decision making are found in the General Data Protection Regulation (GDPR) and complementary Swedish legislation. These rights are mainly the notification obligations, the right to access and additional safeguards, according to which the patient has the right to receive and access the 'meaningful information about the logic involved' of such automated processing. On contrary, the trade secret protection of automated decision-making AI algorithms, makes it difficult for the healthcare provider to comply with their transparency obligations under the GDPR, due to the opaqueness of such algorithms, e.g. 'black box' issue. The analysis shows that although the formulation of the 'meaningful information' can be relied upon by the healthcare provider, because notion of 'meaningful' shall be determined from the perspective of the patient where they do not need to receive the mathematical explanation of the processing method, the GDPR still makes clear that trade secrets cannot be relied upon to refuse to provide all of the information to the patient.

Consequently, when all of the 'meaningful information' cannot be provided to the patient without healthcare provider reveals some of its precious AI algorithms protected by trade secrets, the question thus arises – which of the conflicting rights prevails? By taking a closer look at the legislation protecting the rights in conflict, a preference for patient's data protection rights is confirmed. Yet, the GDPR allows Member States to introduce national restrictions, where trade secret protection have a restricting factor on transparency rights of the patient. Additionally, due to the pressure from the regulators and the society, new approaches are being introduced by researchers and practitioners, which are further presented in the thesis. The thesis concludes that the future of AI requires a dialogue between developers and the society about not only what is *possible*, but also what is *reasonable*. But for now, transparency in automated AI systems continue to be in need for careful examination, both by Data Protection Authorities and the national courts, together with the European Court of Justice, to find a solution where transparency can be exhibited without opening up the 'black box'.

Keywords: Artificial Intelligence, Healthcare, Automated Decision-Making, Transparency, Data Protection, GDPR, Trade Secrets, TSA, Balancing Act

Preface

My Master's program in European Business Law at Lund University has come to an end. I can confidently say that this has been an amazing journey, which I, as promised, faced with passion, dedication and discipline. It has been an honor to study at the Faculty of Law together with with fellows from different backgrounds and cultures, which has enabled me to develop academically and as a person. Honestly, at times, it has been very difficult, where I had to push my limits in order to make it. But as can be said, sometimes the greatest storms bring out the greatest beauty.

In this regard, I would like to emphasize a special Thank You to my supervisor Ana Nordberg, who has been a true inspiration during my master thesis as well as Patent Law course, where all my interest in Artificial Intelligence begun. I would like to Thank You for the time and effort in supervising me as well as the encouragement to take on challenges, in order to face my weaknesses and strengthen my self-confidence. I am incredibly grateful for all the knowledge and skills that you have shared with me and I look forward to discussing this topic with you in the near future.

Nevertheless, I would like to thank my family and friends for supporting me, for understanding me and always being there for me no matter what. In particular, I would like to thank my fiancé who has been a true mainstay during all the hard times and my mum who has given me so much love and support, especially during the struggle of getting this thesis completed. They have been enormously patient and stood out with me during my most stressful days. Nevertheless, I have always been able to talk to them and express my thoughts and feelings and always received back useful advice. Thank you!

Additionally, I would like to express a big thanks to my dear fellows for taking the time to discuss questions raised during the program and for being a great support.

This has been the best two years of my life. I thank you God for leading me the right way.

Kristina Christensen

Lund, Sweden

28 May 2020

List of Abbreviations

AI	Artificial Intelligence
ADM	Automated Decision-Making
DPA	The Act with supplementary provisions to the EU Data Protection Regulation (2018:218) (Data Protection Act)
EU	European Union
EUCJ	Court of Justice of the European Union
GDPR	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
SALAR	Swedish Association of Local Authorities and Regions
TEU	Treaty on the European Union
TFEU	The Treaty on the Functioning of the European Union
TSA	The Swedish Act on Trade Secrets (2018:558)
TSD	Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure
TRIPS	The Agreement on Trade-Related Aspects of Intellectual Property Rights
WP29	Article 29 Data Protection Working Party

List of Glossaries

Due to the fact that this thesis examines artificial intelligence (AI) in automated decision-making (ADM) within the healthcare domain, definitions that are used in current legislations are changed in order to enable the reader to follow the thesis in a better way. The following glossaries are used throughout this thesis;

Automated Decision-Making Artificial Intelligence (ADM AI) – meaning the process, used interchangeable with the notion of 'ADM AI system', of making a medical decision solely by automated means, including profiling, without any human intervention with the help of AI or machine learning (ML) algorithm.

Black-box – used interchangeable with 'opaque' in the thesis, meaning a complex AI or ML algorithm that can be observed in terms of its inputs and outputs, whose inner working system is hidden or not readily understood.

Data concerning health –meaning special categories of personal data under article 9 (1) GDPR, that is especially being processed within the healthcare. The notion of data concerning health is further described in the recital 35 GDPR and article 4 (15) GDPR.

Healthcare provider – meaning a data controller under article 4 (7) GDPR who processes data concerning health under article 9 (1) General Data Protection Regulation (GDPR); and a trade secret holder keeping processing AI algorithms used in ADM as trade secret within the meaning of Trade Secrets Directive (TSD) and Swedish Act on Trade Secrets (2018:558) (TSA) when processing data concerning health.

Patient – meaning a data subject whose special categories of personal data is being processed by a healthcare provider in the context of healthcare domain, within the meaning of GDPR.

"In 2025, Sweden will be the best in the world at using the opportunities offered by digitization and eHealth to make it easier for people to achieve good and equal health and welfare, and to develop and strengthen their own resources for increased independence and participation in the life of society".

- *Vision for eHealth 2025*[1]

[1] Government Offices of Sweden and Swedish Association of Local Authorities and Regions (SALAR), *Vision for eHealth 2025 – common starting points for digitization of social services and health care*, (2016), S2016.012, page 3 <https://www.government.se/4a3e02/contentassets/b0fd09051c6c4af59c8e33a3e71fff24/vision-for-ehealth-2025.pdf> accessed 1 February 2020

1. Introduction

1.1 Background

Today, healthcare is one of the biggest items in the Swedish public budget, making Sweden one of the countries of the Organization for Economic Co-operation and Development that invest most in healthcare.[2] The rapid development in software, artificial intelligence (AI) programs and automation has opened new pathways in the Swedish healthcare, by increasing productivity and the effectiveness of care delivery and help more patients in receiving better care.[3] Thus, the digitalization of healthcare is part of a transformational shift affecting Swedish economy and society and taking advantage of these possibilities will be crucial in addressing citizen's high expectations of healthcare and the growing needs of an aging population.[4]

Today, AI and machine learning (ML) are mainly used as a decision support – and not a substitute for the healthcare provider – in the Swedish healthcare, meaning that there are, insofar, no decisions that have been fully delegated to an AI algorithm. However, due to the rapid development of AI technology and an increasing attention given to the AI in healthcare, the Swedish National Board of Health and Welfare (hereinafter 'Welfare Board') has pointed out that the core concerns linked to AI are connected to solely automated decision-making (ADM) process, where decisions are made by automated means without any human intervention. Thus, with the rise of solely ADM the notion of transparency is becoming a key topic.[5]

It is well acknowledged that access to right data is the lifeblood of AI and a crucial part of its infrastructure.[6] In terms of right data when it comes to healthcare means special categories of personal data or data related to health (hereinafter 'data concerning health'), *inter alia*

---

[2] OECD, *Health at a Glance 2017: OECD Indicators,* (2017), OECD Publishing, page 133 <https://dx.doi.org/10.1787/health_glance-2017-en> accessed 3 February 2020; See Annex 1 for further ranking of OECD countries that invest most in healthcare, where Sweden is among top 10.

[3] Mårten Blix and Charlotta Levay, *Digitalization and Health Care – a report to the Swedish Government's expert group on public economics*, (2018), 2018:8 English version, page 3 <https://eso.expertgrupp.se/wp-content/uploads/2019/08/Digitalization-and-health-care-2018_6-English-version.pdf> accessed 3 February 2020

[4] Swedish eHealth Agency, *Annual Report 2019 – trends on e-health*, S2018/06066/RS, (2019), 2091/04068, page 13 <https://www.ehalsomyndigheten.se/globalassets/dokument/rapporter/arsrapport-2019_e-halsomyndigheten.pdf?fbclid=IwAR3qvGZhnjZTcwn_1E_sFekCQTvc36eZ2OScPYVQDzMqO33H-J4cX0KSOgM#page13> accessed 3 February 2020; See also Blix and Levay (n 3), page 3

[5] Swedish National Board of Health and Welfare, *Digital care services and artificial intelligence in healthcare*, (2019), 2019-10-6431, page 67 <https://www.socialstyrelsen.se/globalassets/sharepoint-dokument/artikelkatalog/ovrigt/2019-10-6431.pdf> accessed 3 February 2020

[6] Government Offices of Sweden, *National approach to artificial intelligence*, (2018), N2018.36, page 10 <https://www.regeringen.se/4aa638/contentassets/a6488ccebc6f418e9ada18bae40bb71f/national-approach-to-artificial-intelligence.pdf> accessed 3 February 2020

anamnesis[7], electronical health records, diagnosis and clinical treatment, data from electrocardiograph and X-rays.[8] The value of such data is of big importance for private healthcare providers for the development of AI, as it drives efficiency in terms of costs and innovation. Thus, healthcare increasingly turns to AI algorithms to solve complex health issues.[9] However, the automated ways of algorithms to analyze data concerning health and make medical decisions, can makes it difficult to access the rationale behind decision-making process, often called the 'black box' issue, whereas such methods for processing, including AI algorithms, are often protected by healthcare provider's trade secrets.[10]

Consequently, a potential conflict arises between, on the one hand, patient's data protection rights to a transparent processing of its data concerning health and, on the other hand, healthcare provider's trade secrets rights in keeping its AI algorithms as trade secret, because both concern the same content, namely data concerning health. Hence, how willing will the patients be to accept AMD AI algorithms for processing of their data concerning health, where the working of the algorithm as well as the data underlying its development is a mystery? On contrary, can the need for transparency in solely ADM justify the force of healthcare providers to reveal trade secrets and thus leaving them vulnerable to having their software stolen and reproduced?[11]

Recently enacted European legislation on General Data Protection Regulation (GDPR)[12], which is supplemented by the Swedish Data Protection Act (2018:218) (DPA), is set to decrease the opacity of ADM process. The GDPR enables the patient to control its data in a clear way, by receiving information about the logic involved in solely ADM process, as well as receive an explanation for an algorithmic output.[13] This underlines the urgent significance of human interpretability in algorithmic design.[14] In this regard, the GDPR does not denote a ban on

[7] Anamnesis means a medical or psychiatric patient case history, particularly using the patient's recollections.
[8] Recital 35 GDPR different examples of what can constitute personal data concerning health; See further Intersoft Consulting, *GDPR – Personal Data*, <https://gdpr-info.eu/issues/personal-data/> accessed 16 February 2020
[9] W. Nicholson Price II, *Regulating Black-Box Medicine*, (2017) Volume 116, Issue 3, Michigan Law Review, page 432
[10] Kari Gimmingsrud, *Artificial Intelligence and data privacy*, (2019), Expert Guides, <https://www.expertguides.com/articles/artificial-intelligence-and-data-privacy/aruywukr?fbclid=IwAR2giJSJDn7AeAThkZcs7JN1786Uf4Yr7-ebFuBmNPu7D8bu38gn-2xBnHE> accessed 16 February 2020
[11] Heike Felzmann et al., *Transparency you can trust: Transparency requirements for artificial intelligence between legal norms and contextual concerns*, (2019), Big Data & Society, page 1
[12] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (GDPR) [2016] OJ L119/1
[13] Norwegian Data Protection Authority, *Artificial intelligence and privacy*, (2018), page 5 <https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf?fbclid=IwAR0-yZ4HlAAVj5TEfJB_09dngs08MTzEtXwEW9SP5cY3DV6QMlVLZbqiuBY> accessed 16 February 2020
[14] Bryce Goodman and Seth Flaxman, *European Union regulations on algorithmic decision-making and a 'right to explanation'*, (2017), Volume 38, Issue 3, AI Magazine, page 1

automatic learning approaches or an obligation to explain everything all the time, however, there must be a possibility to make the medical decision taken by automated means re-traceable on the demand of the patient.[15]

At the same time, the already existing Trade Secrets Directive (TSD)[16], harmonizes the national laws on trade secret protection within EU. The TSD aims to foster innovation and competition as well as increase trust in trade secrets as a form of protection.[17] Furthermore, the TSD has been transposed into Swedish Act on Trade Secrets (2018:558) (TSA), which fulfills the aim of the TSD as well as it introduces stricter national measures. Although, the existence of TSA, it is clear that private healthcare provider's trade secrets rights usually end up in the center of attention. Consequently, the conflict between GDPR and TSA, applied in conjunction with the TSD, is clear – the former aims to protect patient's rights and open up the logic behind ADM AI system, while the latter aims at keeping the logic of such system as a trade secret.

In this regard, it appears all more pressing to consider balancing measures to consolidate trade secret rights and patient's rights to a transparent processing of the data concerning health in the solely AMD AI system. Hence, due to the fact that there are no decisions that have been fully delegated to AI algorithm in Swedish healthcare, it is of outermost importance to examine and clarify the rights and obligations akin to automated processing, in order to fulfill the aims of the *vision for eHealth 2025* presented by the Swedish Government and the Swedish Association of Local Authorities and Regions (SALAR).[18]

1.2 Purpose and research questions

The main purpose of this thesis is to analyze two central interests in the algorithmic transparency in healthcare, namely the patient's protection rights in transparent processing of the data concerning health and healthcare provider's trade secret rights in solely ADM process. The focus is particular on the AI technology used in ADM within the Swedish healthcare domain. The main research question of the thesis is as follows:

[15] Andreas Holzinger et al., *What do we need to build explainable AI systems for the medical domain?,* (2017), Volume 1, page 1 <https://arxiv.org/pdf/1712.09923.pdf> accessed 17 February 2020
[16] Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (Trade Secrets Directive) (TSD) OJ L 157/1
[17] Recital 16 TSD
[18] Government Offices of Sweden and SALAR (n 1)

- In what way can the patient's rights to a transparent processing of its data concerning health be reconciled with the healthcare provider's rights in keeping its AI algorithms used in solely ADM as a trade secret within the healthcare?

The main research question is further supplemented by sub-questions, which can be divided as follows:

- What are the patient's rights to a transparent processing of its data concerning health as regards solely ADM process under the GDPR?
- What are the healthcare provider's trade secret rights behind the protection of its AI algorithms used in solely ADM process?
- How can the patient's rights to a transparent processing of its data concerning health and healthcare provider's trade secret rights in solely ADM process be balanced and resolved within the healthcare?

Due to the fact that there have not yet been any decisions that have been fully delegated to an AI algorithm within the Swedish healthcare, the above described questions are examined and answered with the probability of such situation in mind.

1.3 Demarcation

As mentioned above, the main research interest of the thesis is within the Swedish healthcare sector. However, solely AMD, including profiling, are fairly new phenomena and the topic is heavily affected by many of the upcoming legislative changes being made on both EU and national levels. Therefore, the thesis is intended to view the topic with a focus on Swedish national level, supplemented with the EU law and viewpoints, in order to make an overall understanding of the current state of the art. When references are made to national implementation of the EU legislation and recommendation, these are made form a Swedish point of view.

Furthermore, the scope of the thesis is limited to the processing of the data concerning health by a private healthcare provider with a commercial purpose, where the interest of protecting trade secrets is at stake. Disclosure of the data concerning health to public authorities, in terms of technical incident, is left outside the scope of this thesis. This is due to the fact that technical

incidents containing personal data are subject to usual confidentiality assessment, which falls under the Swedish freedom of information laws.[19]

Nevertheless, the thesis focuses on the right to a transparent processing of the data concerning health within the solely ADM AI system set out in article 22 GDPR, but the right not to be subject to decision based solely on automated processing under article 22 (1) GDPR falls outside scope of this thesis. This is due to the fact that, when analyzing automated process of the data concerning health, it is supposed that the data has been lawfully obtained from the patient and the processing is lawful *per se*. Furthermore, any assessment of the requirements for lawful processing, including the exceptions under article 22 (2) GDPR, are not discussed in detail but mentioned briefly. Additionally, because profiling can be a part of the solely ADM process under article 22 GDPR, it is thus supposed that profiling is included in the notion of 'solely ADM' used throughout this thesis and is not examined separately.[20]

Finally, since the aim of the thesis is limited to data protection and trade secrets, other areas such as patent, trademark and copyright law, are not examined. Hence, trade secrets are most likely to conflict with the right to transparent processing of the data concerning health. Even though computer programs are protected by copyright law, the underlying algorithms, principles and structure falls outside scope of such protection. Likewise, computer programs are excluded from patentability as such under article 52 (2) (c) European Patent Convention (EPC), however, it has been subject to interpretation by European Patent Office.[21]

1.4 Method and material

The main method that is being used throughout this thesis is the legal dogmatic method. Under the traditional view, the legal dogmatic research entails two main parts which are the core of the methodology, namely systematization and interpretation of legislation. Firstly, the systematization of legal rules is made through the construction of legal concepts. The hierarchy of the sources used in the legal dogmatic method are predominantly those that are used in the legal process; primary statues, which is further supplemented by the case law from the courts and where possible by the lawyer's literature expounding the rule and lastly a reflection on those rules.[22]

[19] Freedom of the Press Act (SFS 1949:105); Public Access to Information and Secrecy Act (SFS 2009:400)
[20] See section 3.2.2 for the description of different processing methods, including profiling.
[21] European Patent Office, *Guidelines for Examination in the European Patent Office* (2019), Part G – Chapter 2
[22] Christopher McCrudden, *Legal research and the social science*, (2006), The Law Quarterly Review, Oxford Legal Studies Research Paper No. 33/2006, page 633

Secondly, the interpretation of the legal rules is reached through examination of their content and their intentional application. Thus, the legal dogmatic method answers the questions by looking at the accepted legal sources, for instance European or national primary and secondary law, *inter alia* treaties and acts, regulations and directives, case law and doctrine.[23] The purpose of using the legal dogmatic method is to examine the three big components of the thesis, namely AI, data protection rights and trade secrets rights. Thus, the interpretation of the mentioned legislation will be reached by the use of teleological and linguistic grounds for interpretation.[24]

Traditionally, legal sources are divided into three categories, namely primary, secondary and supplementary sources of law. Primary law contains fundamental rights of the constitutions, national laws and international treaties that are incorporated into national legislation. Binding EU law, which is external to national law, is also considered to be strongly binding source that consists of the Treaty on European Union (TEU)[25] and the Treaty on the Functioning of the European Union (TFEU)[26]; Charter of Fundamental Rights of the European Union[27] (hereinafter EU Charter) and the European Convention on Human Rights[28] (hereinafter EU Convention). [29]

The body of law that comes from principles and objectives of the above described treaties is known as secondary legislation, also called delegated legislation or subordinate legislation, which consists of regulations, directives, decisions, recommendations and opinions listed in article 288 TFEU. These sources of law are binding, and they shall not be set aside.[30] Due to the fact that this thesis examines both a regulation and a directive, it is important to highlight their relation to national law. Regulations are binding in their entirety and are directly applicable as the national law according to article 288 TFEU, which is further supplemented by national legislation.[31] Directives are only binding as to the end to be achieved but leaves it up to each

[23] Jörgen Hettne and Ida Eriksson, *EU-rättlig metod, Teori och genomslag i svensk rättstillämpning*, (2011), 2nd edition, Nordstedts juridik, page 40
[24] Hettne and Eriksson (n 23), page 158-170; see also Jerzy Stelmach and Bartosz Brozek, *Methods of Legal reasoning*, (2006), Volume 78, Law and Philosophy library. Additionally, other traditional interpretation theories are taken into account: objective approach that describes the original intentions of the legislator; and teleological approach that focuses on the objective content of the law; and systematic approach focusing on the systematical and structural connection of the norms in relation to each other.
[25] Consolidated version of the Treaty on the European Union [2012] OJ C 326/01
[26] Consolidated version of the Treaty on the Functioning of the European Union [2012] OJ C 326/01
[27] Charter of Fundamental Rights of the European Union [2012] OJ C 326/391
[28] Protocol 1 to the European Convention for the Protection of Human Rights and Fundamental Freedoms
[29] Paul Craig and Grainne De Burca, *EU law – text, cases, and materials*, (2015), 6th edition, Oxford University Press, page 266; see also Aulis Aarnio, *Essay on the doctrinal study of law*, (2011), University of Tampere, page 152-153
[30] Craig and De Burca (n 29), page 105; see also European Commission, *Types of EU law*, <https://ec.europa.eu/info/law/law-making-process/types-eu-law> accessed 12 February 2020)
[31] Craig and De Burca (n 29), page 107

Member State (MS) to choose form and method for implementation into national law under article 288 TFEU. Directives are particularly useful when the aim is to harmonize the laws within a certain area, or to introduce complex legislative changes.[32]

Nevertheless, supplementary sources of law that are not specifically mentioned in the treaties, such as general legal principles and arguments presented in doctrine, are not binding but are often used as a support when presenting legal arguments.[33] Additionally, case law of the Court of Justice of the European Union (CJEU) and the European Court of Human Rights have certain precedents, but is, however, according to article 288 TFEU binding to whom it is addressed and only to them. Throughout this thesis, preference will be given to the all of the above-mentioned sources of law.

Since 25th of May 2018, the Swedish Personal Data Act from 1998 has been replaced by the GDPR, which is directly applicable as the Swedish law and is further supplemented by the new Swedish DPA.[34] The biggest difference between the GDPR and previous Swedish Personal Data Act, is that the former means that a company cannot own personal data, but only borrow it. Thus, GDPR strengthen individual's rights, by obliging companies and other organizations to provide information on how and why they process personal data.[35] However, MS retain the ability under article 23 GDPR to restrict by way of legislative measure, the scope of the obligations and right, when such restrictions respect the essence of the fundamental rights and freedoms and are necessary and proportionate.[36]

In the healthcare domain, the GDPR is supplemented by Patient Data Act (2008:355), which is a framework law that contains fundamental provisions for processing of personal data of the patients within the healthcare and is applied by all care providers, both public and private; Patient Act (2014:821), that aims to reinforce and clarify the position, integrity, self—determination and participation of the patients; and Patient Safety Act (2010:659), which aims

[32] Craig and De Burca (n 29), page 108
[33] Craig and De Burca (n 29), page 226; see also Sources of European Union law, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Al14534> accessed 12 February 2020
[34] Swedish Data Protection Authority, *The General Data Protection Regulation (GDPR),* <https://www.datainspektionen.se/other-lang/in-english/the-general-data-protection-regulation-gdpr/> accessed 10 February 2020
[35] Kristina Stensson Ljungdahl et al., *AI and automation for first-line care – a report from Inera AB and the feasibility study Digital healthcare advice (Swedish version,* (2017), page 39 <https://www.inera.se/globalassets/projekt/nya-1177-vardguiden/ineras-rapport-ai-och-automatisering-for-forsta-linjens-vard.pdf?fbclid=IwAR3BJ8TGFt5rIFExyp1v6TvJslebikDHfWigZzUjNp1jIBj7lb1RXnxZ5oQ#page26> accessed 17 February 2020
[36] See 5 c. of the Swedish Data Protection Act (2018:218)

to promote a high level of patient safety and to reduce the number of medical injuries.[37] Additionally, Patient Data Act (2008:355) is further supplemented by the Patient Data Regulation (2008:360) and the Swedish Welfare Board's regulation and general guidelines concerning patient records and processing of personal data within health and medical care (HLSLF-FS 2016:40).[38] The complementary Swedish legislation is only applicable in case where it is compatible with the GDPR.[39]

On the EU level, there have previously not been rules on the protection of trade secrets. Thus, on 8 of June 2016, the TSD was adopted in order to strengthen the competitiveness of companies and to improve the conditions for innovation and knowledge transmission within the internal market.[40] On the national level, Sweden has since 1990 been the only country within the EU having a national legislation specifically protecting trade secrets. In order to comply with the aims of the TSD, the Swedish parliament have enacted a new TSA, which came into force on 1 of July 2018. Nevertheless, the TSA, in accordance with article 6 TSD, introduces national measures, procedures and remedies necessary to ensure the availability of civil redress against the unlawful acquisition, use and disclosure of trade secrets.

Besides examining the primary and secondary sources of law described above, e.g. EU regulation and directive and Swedish national acts, this thesis also builds upon non-binding EU and national sources, *inter alia* the Government Bills on the DPA and TSA, to examine the objective and scope of respective legislations and interpretation of important definitions; guidelines and opinions from WP29 as well as Swedish Data Protection Authority on the transparency requirement in the ADM; reports from Swedish Welfare Board, the Swedish Government's Expert Group as well as Swedish Governmental Agency for Innovation Systems (hereinafter 'Vinnova'), in order to analyze the current state of the art of the AI within the Swedish healthcare domain; online journals and articles from legal scholars, for instance *Gianclaudio Malgieri* with *Giovanni Comande* and *Sandra Watcher et al.* actively debating on the conflict between data protection rights and trade secrets rights in ADM, as well as *Agata Ferretti et al.* assessing the conflict in question, with the particular focus on the healthcare sector; and the case law and doctrine in order to support author's claims.

[37] SOU 2017:52, *This is how we strengthen personal integrity* (2017), Elanders Sverige AB, page 112; See also Swedish Data Protection Authority, *The Patient Data Act*, <https://www.datainspektionen.se/other-lang/in-english/the-patient-data-act/> accessed 10 February 2020
[38] SOU 2017:52 (n 37), page 119; See also Swedish Data Protection Authority (n 37)
[39] Swedish Data Protection Authority (n 37)
[40] Recital 16 TSD

1.5 State-of-the-art

So far, it has been hard to identify Sweden as a key player in the use of solely AMD AI system, especially within the healthcare domain. The Swedish Welfare Board have noted in its report on AI and digital services that a lot of research is going on within the AI area, but the actual use of it does not, however, occur to the same extent, especially when it comes to solely ADM where such methods have not yet been introduced into the Swedish healthcare.[41]

During fall of 2017, a couple of major events occurred in Sweden, *inter alia* Knut and Alice Wallenberg's foundation has announced a billion investment in the area of autonomous systems and vehicles; Kinnevik has since previously been one of the major investors in British Babylon Health; and several Swedish banks have started using AI.[42] Nevertheless, Vinnova has invested in a project with the goals of developing new solutions that have a great potential in improving public health and elderly care in Sweden with the help of AI.[43]

Today, the use or support of AI within the Swedish healthcare includes a total of 59 different areas.[44] AI support is mainly used in the field of anamnesis, diagnosis and decision support.[45] Even though, no solely ADM AI system exists within the Swedish healthcare, there are other areas where such system is used. In the Municipality Trelleborg in Sweden, the decision to grant economic aid through social services is now mainly done by an AI algorithm. This has resulted in more time for the secretaries to focus on the meetings where human intervention is required. Furthermore, the Swedish Social Insurance Agency has increased the satisfaction of its users with the help automated routines and by reducing the cost of managing the service almost by 36 percent.[46] Yet, even though there are many advantages with the use of solely ADM, there is still some uncertainty about the actual application of it, where the Swedish Government shall have the responsibility in providing support, guidelines and legislation.[47]

---

[41] Swedish National Board of Health and Welfare (n 5), page 8
[42] Kristina Stensson Ljungdahl et al. (n 35), page 24-25
[43] Vinnova report, *Artificial Intelligence in Swedish business and society – Analysis of development and potential* (summary), (2018), VR2018:09, page 9 <https://www.vinnova.se/contentassets/29cd313d690e4be3a8d861ad05a4ee48/vr_18_09.pdf> accessed 20 February 2020
[44] Swedish National Board of Health and Welfare (n 5), page 56
[45] Ibid, page 9; See further Section 2.3 in the thesis for more detailed description of the current implementation of AI within the Swedish healthcare.
[46] Blix and Levay (n 3), page 33-34
[47] Heike Erkers and Simon Vinge, *Obehörig algoritm tar beslut i socialtjänsten*, Svenska Dagbladet, 18 January 2020 <https://www.svd.se/obehorig-algoritm-tar-beslut-i-socialtjansten> accessed 6 May 2020

There is a number of ongoing works both in Sweden and internationally on ethical issues in relation to the development and use of AI.[48] For instance, the European Commission has in 2018 established two working groups, e.g. the European AI Alliance, to build around a diverse multistakeholder online platform and open up to all members of the society, and the High-Level Expert Group on AI, which is advising the Commission on difficulties and prospects arising from AI.[49] Thus, the Ethics Guidelines for Trustworthy AI prepared by the High Level Expert Group in 2019 is the base in addressing the specificities of the healthcare sector and will help to set world standards for AI and at the same time give the guarantees needed for the patients, and society as a whole, to trust AI technologies and for companies to further invest in them.[50]

Nevertheless, the Commission has set up a broader environment to enable digital and analytics led innovation, which is reflected in the Communication on Transformation of Health and Care in the Digital Single Market from April 2018.[51] In its Communication on eHealth, the Commission point out that digital technologies shall be seen as an integral part of healthcare and the swift deployment of innovative digital healthcare solutions will be best achieved by working together, sharing experiences in deploying and transferring innovation across MS and regions. Thus, the Commission holds that it will support cooperation on digital healthcare between MS by promoting common principles for validating and certifying health technology, as well as promote knowledge and skills of the patients and the health professionals in using digital solutions.[52]

On the Swedish national level, as a point of departure for continued development work in the area of eHealth, the Government Offices of Sweden and the SALAR have decided to endorse a common *vision for eHealth up to 2025*[53], which aims to support efforts to make use of the opportunities of AI in healthcare.[54] The vision builds upon the latest strategy from 2010, with

[48] Swedish National Board of Health and Welfare (n 5), page 10
[49] EIT Health and McKinsey & Company, *Transforming healthcare with AI – The impact on the workforce and organizations,* (2020), page 35 <https://www.mckinsey.com/~/media/McKinsey/Industries/Healthcare%20Systems%20and%20Services/Our%20Insights/Transforming%20healthcare%20with%20AI/Transforming-healthcare-with-AI.ashx> accessed 4 February 2020
[50] High Level Expert Group on AI set up by European Commission, *Ethics Guidelines for Trustworthy Artificial Intelligence* (2019); See further Denis Horgan et al., *Artificial Intelligence: Power for Civilization – and for better healthcare,* (2019), Public Health Genomics, page 146-147 <https://www.karger.com/Article/Pdf/504785> accessed 15 February 2020
[51] European Commission, *Communication on enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society*, Brussels, 25 April 2018 COM(2018) 233 final
[52] European Commission (n 51), page 13
[53] Government Offices of Sweden and SALAR (n 1)
[54] Ibid, page 9-10

the intention on providing sufficient support to various actors in the area of eHealth, both long and short terms. Nevertheless, the aim of the vision is to achieve efficiency and equality, as well as accessibility, usability and stronger privacy protection in the digital health.[55] Additionally, the Swedish Government in its national approach to AI, emphasize the need for Sweden to develop rules, standards, norms and ethical principles to guide ethical and sustainable AI and the use of AI.[56] As the Government holds;

> *'The goal is to make Sweden a leader in harnessing the opportunities that the use of AI can offer, with the aim of strengthening Sweden's welfare and competitiveness'.*[57]

1.6 Outline

This thesis is divided into six chapters. The first chapter provides information regarding the topic of this thesis, as well as the presentation of research questions, limitations, methods and sources that are being used in order to support author's claims. The second chapter provides a general introduction to AI and explains the current position of it within the Swedish healthcare, by introducing some examples where AI has already made a great progress.

Chapter three presents legal and ethical challenges between AI and the patient's rights under GDPR within the healthcare. This chapter describes the scope of application of the GDPR, the notion of solely ADM process, provides a description of the patient's transparency rights including the highly debated 'right to explanation' when the patient is subject to lawful ADM process, and provides a discussion on the consequences on patient's rights in healthcare due to the lack of transparency. Chapter four describes the notion of trade secret, the legislation that regulates the protection of such rights and how and when AI algorithms used in solely ADM can be protected by trade secrets without interfering with the fundamental rights of the patient.

Chapter five is the main chapter of the thesis, where an attempt in finding a balance between patient's rights to a transparent processing of its data concerning health and healthcare provider's rights to protection of AI algorithms as trade secrets in solely AMD is conducted.

Finally, chapter six summarize the discussion from previous chapters by answering all of the research questions and presents an overall conclusion.

---

[55] Government Offices of Sweden and SALAR (n 1), page 7-8
[56] Government Offices of Sweden (n 6), page 10
[57] Ibid, page 5

2. The potential of AI in healthcare

2.1 Designation of AI

What was once called science fiction has developed over the years to be one of the most strategic technologies of 21th century - AI is real. It might not always be obvious, but we are living in the age of intelligent machines, where it is changing the world before our eyes.[58] Even though AI can be seen as a modern innovation, it has existed for more than a half century. The term AI was coined in 1955 by a professor of computer science John McCarthy. This was the beginning of the research within the AI field.[59]

For a subject that is so widely researched, it is somehow surprising that no uniform definition currently exists to describe the term AI.[60] In this regard, Swedish Government in its national approach describes AI as:

> *'[…] a broad field that encompasses many technologies, not least machine learning and deep learning. What distinguishes AI from other automation methods is the ability of AI technology to learn and become smarter over time'.*[61]

The Government's national approach for AI also refers to the Vinnova report, where AI is defined as:

> *'[…] the ability of a machine to imitate intelligent human behavior. Artificial intelligence also denotes the area of science and technology that aims to study, understand and develop computers and software with intelligent behavior'.*[62]

Nevertheless, the European Commission has on the European level defined AI as 'a generic term that refers to any machine or algorithm that is capable of observing its environment, learning, and based on the knowledge and experience gained, taking intelligent action or

---

[58] Matthew U. Scherer, *Regulating artificial intelligence systems: risks, challenges, competencies, and strategies*, (2016), Volume 29, Issue 2, Harvard Journals of Law & Technology, page 354
[59] John McCarthy, *What is Artificial Intelligence?*, (2007), Stanford University, page 2 <http://jmc.stanford.edu/articles/whatisai/whatisai.pdf> accessed 18 February 2020; See also WIPO, *Technology Trends 2019: Artificial Intelligence,*(2019), Geneva: World Intellectual Property Organization, page 19 <https://www.wipo.int/edocs/pubdocs/en/wipo_pub_1055.pdf> accessed 19 February 2020
[60] Dr Noam Shemtov, *A study on inventorship in inventions involving AI activity*, (2019), Commissioned by the European Patent Office, page 9 <http://documents.epo.org/projects/babylon/eponet.nsf/0/3918F57B010A3540C125841900280653/$File/Concept_of_Inventorship_in_Inventions_involving_AI_Activity_en.pdf> accessed 19 February 2020
[61] Government Offices of Sweden (n 6), page 5
[62] Vinnova report (n 43), page 7

proposing decision'.[63] European Commission also acknowledged the importance of AI, by stating that it can significantly improve people's lives and bring major of benefits to the society and the economy.[64]

However, in order to fully understand the meaning of AI, one must comprehend the definition of algorithm and software. An algorithm is a set of decision-making rules, which runs on computers. They are thus programs that make and execute decisions in response to external circumstances.[65] Further, software is generally understood as the implementation of algorithms in source or object code, but without distinguishing between technical and non-technical processes. Thus, AI system is a combination of algorithms and software, or each of them separately.[66]

2.2 Emerging applications of AI in healthcare

In the beginning of the 21st century, a wave of AI emerged consisting of two big elements, namely ML and its sub-area of Deep Learning (DL).[67] ML is a set of techniques and tools, when provided with a large amount of data, is able to find novel patterns and knowledge and further generate models that can be used for effective predictions about such data.[68] With the ability to learn without being explicitly programmed, ML can automatically be improved with the experience.[69] DL is a further developed form of ML based on building greater complexity in the neural network, where it is more knowledgeable about the details of the amount of data it is being trained on and can reach more advanced conclusions, *inter alia* detecting breast cancer tumors at an earlier stage by analyzing millions of mammography images.[70]

Within the healthcare domain, complex algorithms that rely on ML, is described by *Price* as 'computer-based algorithms that help make medical decisions or analyze medical

[63] Massiomo Craglia et al., *Artificial Intelligence – A European Perspective*, (2018), EUR 29425 EN, Publications Office Luxemburg, JRC113826, page 18; See also EPO, *Guidelines for examination in the European Patent Office* (2019), Part G, section 3.3.1 for the patentability of AI

[64] European Commission, *Factsheet: Artificial Intelligence for Europe*, (2019) <https://ec.europa.eu/digital-single-market/en/news/factsheet-artificial-intelligence-europe> accessed 12 February 2020

[65] Lynn M. LoPucki, *Algorithm Entities*, (2018), Volume 95, Issue 4, Washington Law Review, page 897

[66] European Patent Office, *Patents for software? European law and practice* (2009), page 2-3 <https://ciencias.ulisboa.pt/sites/default/files/fcul/inovacao/PI-Pack-INPI-E-Patents-for-Software-EPO.pdf> accessed 13 February 2020

[67] Ibid, page 3; See Annex 2 that clarified timeline of AI development and its sub-areas mostly used in healthcare

[68] Norwegian Data Protection Authority (n 13), page 6

[69] Henrik Ahlén, *Artificiell Intelligence and machine learning for healthcare and life science*, (2017), page 6 <https://ssci.se/sites/default/files/Artificiell%20Intelligens%20och%20machine%20learning%20f%C3%B6r%20sjukv%C3%A5rd%20och%20life%20science.pdf> accessed 14 February 2020

[70] Marcus Österberg and Lars Lindsköld, *AI and machine learning for decision support in healthcare – a preliminary study investigating services and the art of developers working on machine learning,* (2018), 1st edition, Swelife, page 36; see further Vinnova report (n 43), page 25; See further section 2.3 of the thesis.

information'.[71] The primary aim of such algorithms is to examine relationships between prevention or treatment techniques and patient outcomes and thus help healthcare providers to make better decisions in several areas.[72] These include *inter alia* the ability to determine appropriate treatments that would be of most benefit to an individual patient; application that provide customized health advice based on a patient's specific genetic make-up; diagnostic tests aimed at personalized medicine that evaluate a drug dosage based on a patient's weight, sex and genetic sequences; and a program that evaluates a magnetic resonance image for the presence of a tumor.[73]

Nevertheless, ML can also use Bayesian probability models to see the relationship between symptoms and illnesses, where all of the relevant data is not available, which is very common within the healthcare.[74] Thus, the ability of ML algorithms to analyze these multiple and rich data types at a scale not previously been possible brings a step change in health and epidemiology.[75] The examples are numerous and as *Harrer* states:

> *'AI is not a magic bullet and is very much a work in progress, yet it holds much promise for the future of healthcare and drug development'*.[76]

2.3 Current implementations in Sweden

As mentioned in the introduction, Sweden is one of the countries that invest most in healthcare.[77] According to Vinnova and EU Commission, the digital development and access to digital tool communication channels in Sweden is considered to be high, compared to most other countries.[78] According to Swedish Government's Expert Group, the accessibility of Swedish healthcare started to improve in 2016, when private telemedicine firms, such as *Kry*, *MinDoktor* and *Doktor24*, began offering video-calls via smartphone apps.[79] AI-nurse, or an AI system that *Doktor24* has developed (under Aleris X), has had an extremely high number of

[71] W. Nicholson Price II (n 9), page 425
[72] Nicole Lewis, *Artificial Intelligence to play key role in population health*, (2017) <https://www.medicaleconomics.com/medical-economics-blog/artificial-intelligence-play-key-role-population-health> accessed 15 February 2020
[73] Denis Horgan et al. (n 50), page 146-147
[74] Henrik Ahlén (n 69), page 6
[75] Denis Horgan et al. (n 50), page 150
[76] Stefan Harrer et al., *Artificial Intelligence for Clinical Trial Design*, (2019), Volume 40, Issue 8, Trends in Pharmacological Science, page 589
[77] Blix and Levay (n 3), page 13; See further Annex 1.
[78] Vinnova report (n 43), page 13; European Commission (2018), *Benchmark Deployment of eHealth among General Practitioners – Final report*, (2013), Publications Office of the European Union, page 10
[79] Blix and Levay (n 3), page 3

visitors since its startup.[80] Thus, in June 2018, the Swedish Welfare Board presented a survey on the progress and use of telemedicine and AI in healthcare, where it showed that the digital healthcare visits were almost doubled between April 2017 and April 2018.[81]

Doktor24 works with so called triaging, which means that an assessment is made by an AI algorithm of the patient's symptoms in order to allocate the patient to the correct level of care. The same is physically made by a human nurse at health centers across the country. In this regard, *Jacob Stedman*, Chief Product Officer at *Doktor24*, states that an advantage with an AI-nurse is availability, since the system based on ML, can handle an unlimited number of patients at the same time and that the care itself becomes equal as it always happens in the same way. Furthermore, *Stedman* highlights the importance of the 'follow-up' system, where the AI returns after few days to feedback to the patient.[82]

In 2015 a Swedish startup named Optolexia began offering a new method for early and reliable detection of dyslexia, by using eye-tracking software and ML to identify patterns that are unique in children with characteristics of dyslexia. Today, Optolexia is sold directly to schools and municipalities to predict dyslexia at an early stage and thus prevent it from being developed.[83] Furthermore, in 2016 the Swedish Welfare Board and the Swedish Cancer Society has confirmed that more than 60 000 people were diagnosed with cancer.[84] Today, by training DL algorithms with over million mammography images combined with clinical data from the Breast Cancer Registry, AI helps in reducing the number of deaths by detecting tumors earlier.[85] Nevertheless, according to a study made by Acta Orthopaedica from 2017, a number of researchers had existing AI image-recognition algorithms to analyze thousands of X-rays of hands, wrists and ankles from the Danderyd Hospital archive, which was trained to identify

[80] Swedish National Council on Medical Ethics, *Artificial intelligence – promising technology with ethical challenges*, (2019), Smer conference report 2019:2, page 25 <http://www.smer.se/wp-content/uploads/2019/06/Smer-konferensrapport_2_webb.NY-REV.pdf> accessed 17 February 2020
[81] Swedish National Board of Health and Welfare (n 5), page 17
[82] Ibid, page 26-27
[83] Paulina Modlitba*, Four changes driving forces for AI in healthcare*, (2018), SSF-report number 29, page 18 <https://strategiska.se/app/uploads/livet-med-ai.pdf?fbclid=IwAR0fR2OqVQh3DYvT2Y6ktWIWMcxp5yXO_2si5eYso7k3Hw_NwOJQXHniwII> accessed 17 February 2020
[84] Swedish National Board of Health and Welfare and Swedish Cancer Society, *Cancer in numbers 2018 – popular scientific facts about cancer,* (2018), page 18 <https://www.socialstyrelsen.se/globalassets/sharepoint-dokument/artikelkatalog/statistik/2018-6-10.pdf> accessed 18 February 2020
[85] Vinnova report (n 43), page 25

fractures independently.[86] As a result, on 11th October 2019, AI has been used for the first time in real clinical cases, where it together with doctors assessed patient's ankle fracture.[87]

Thus, technological advancements occurring over the past years have enabled the growth of health-related applications of AI and according to Swedish Welfare Board a lot is yet to come.[88] In the area of anamnesis, diagnosis and decision support, ML is used *inter alia* as a tool for image analysis and diagnosis in digital pathology[89], ultrasound[90] and mammography[91]. Furthermore, it is used for automatic classification of dental X-rays to improve quality of the assessments and save time; decision support on the basis of health data for the treatment of mainly chronic diseases; and decision support to detect the risk of stroke.[92] These are just few of the areas where AI is making substantial progress.

The Swedish Welfare Board states that AI generally performs tasks more reliably than humans. Medical performances offered by human healthcare providers are more variable depending on different circumstances, which can result in both advantages and disadvantages. According to the Swedish Welfare Board, the quality of healthcare would benefit from utilizing a machine-to-human collaboration to exploit the strength of it, where people would give an overall interpretation while the machines would perform a more defined task. Nevertheless, public and private healthcare providers believe that the quality of the healthcare is improved when medical assessments are based on a large amount of data. Therefore, this leaves less room for subjectivity in the assessments, but it does not, however, exclude the risk algorithmic bias completely.[93]

It can be concluded that AI brings many benefits for today's healthcare system in Sweden, *inter alia* by saving time, reduce costs and discover and prevent diseases, sometimes even better than

[86] Acta Orthopaedica, *AI analyses X-rays as well as doctors*, Karolinska Institutet, (2017), <https://news.ki.se/ai-analyses-x-rays-as-well-as-doctors> accessed 5 February 2020
[87] Jesper Cederberg, *First patients at Danderyd's hospital assessed with AI*, (2019), Medical journal, <https://lakartidningen.se/Aktuellt/Nyheter/2019/10/Forsta-patienterna-pa-Danderyds-sjukhus-bedomda-med-AI/> accessed 17 February
[88] Swedish National Board of Health and Welfare (n 5), page 60; See Annex 3 how the use of AI is allocated within the different areas in Swedish healthcare
[89] Pathology is the study of the causes and effects of a disease or an injury.
[90] Diagnostic ultrasound, also called sonography or diagnostic medical sonography, is an imaging method that uses high-frequency sound waves to produce images of structures within the body.
[91] Mammography is a breast screening tool that is able to show whether an individual have breast cancer or are at a risk of getting it.
[92] Swedish National Board of Health and Welfare (n 5), page 59
[93] Ibid, page 9; See chapter 3 for the discussion on algorithmic bias in healthcare and non-medical areas.

human beings. This has enabled AI to become a part of the Swedish healthcare eco-system.[94] In this regard, the Swedish Welfare Board predicts that AI will in the near future lead to significant progress, where decisions will be fully delegated to AI algorithms.[95] However, when AI system is at stake the questions of personal integrity arise, where personal data concerning health shall be processed in accordance with the GDPR, read in conjunction with the supplementary Swedish national legislation, especially when it comes to solely ADM process. This is subject to examination in the next chapter.

[94] PWC, *No longer science fiction, AI and robotics are transforming healthcare*, (2017-2020), <https://www.pwc.com/gx/en/industries/healthcare/publications/ai-robotics-new-health/transforming-healthcare.html> accessed 15 February 2020

[95] Swedish National Board of Health and Welfare (n 5), page 8

3. AI and the GDPR: Legal and ethical challenges in healthcare

3.1 Introduction

As can be seen in the previous chapter, AI is developing at a furious pace by acting as a decision support in the Swedish healthcare. In this regard, the core concerns linked to AI are connected to solely ADM process, namely decisions that are entirely delegated to an AI algorithm.[96] While most healthcare providers recognize the promise of using AI, many patients are worried about the use of their personal data concerning health by autonomous computer programs for medical purposes.[97] This is due to the opaqueness of AI systems, e.g. 'black box' issue, where it is hard or even impossible to determine the underlying logic of the automated medical decision produced by an AI algorithm.[98]

According to *Pasquale*, AI systems deserves the 'black-box' mark because of the ability to collect a large amount of data concerning health using sophisticated ML techniques and process it by automated means, without patients being aware about such process.[99] Furthermore, *Burell* holds that the relationships used in a black-box AI algorithm are incomprehensible, because even though acting in accordance with explicit rules, those rules are too complex for healthcare provider to understand or to know exactly what factors go into the final decisions and further explain the results to the patient.[100]

In this regard, the Swedish Welfare Board emphasized the importance of transparency in the use and the development of AI in Swedish healthcare, where there is a need to understand the connection between input and output of data.[101] Unless the logic behind such system is understood, there is a risk that the healthcare provider will blindly trust the systems, which can impair the autonomy of the patient and lead to discriminatory or biased outcomes. Thus, it is important to analyze of what opacity of AI systems amounts to and how healthcare providers can fulfill demands of better transparency for processing of the data concerning health.[102]

---

[96] Swedish National Board of Health and Welfare (n 5), page 67
[97] Agata Ferretti et al., *Machine Learning in medicine: Opening the New Data Protection black box*, (2018), Volume 4, Issue 3, European Data Protection Law Review, page 321
[98] W. Nicholson Price II (n 9), page 429-430
[99] Frank Pasquale, *The Black Box Society*, Harvard University Press, Cambridge, MA, 2015 James Woodward, *Making things happen – a theory of casual explanation*, Oxford University Press, 2003; See also Agata Ferretti et al. (n 97), page 325
[100] Jenna Burrell, *How the machine 'thinks': Understanding opacity in machine learning algorithms*, (2016), Big Data & Society, page 4-5 <https://journals.sagepub.com/doi/pdf/10.1177/2053951715622512> accessed 18 February 2020
[101] Swedish National Board of Health and Welfare (n 5), page 67
[102] Agata Ferretti et al. (n 97), page 323

3.2 Privacy and Data protection rights

3.2.1 Fundamental rights and the GDPR

The protection of privacy, integrity and personal data are not new and has for a long time been a fundamental right protected by legal orders.[103] Yet, due to the rapid digitalization and technology development in the society, it is only during recent years that the notion of privacy has been subject to different views and increasingly detailed regulation. Privacy can be understood as individual's right to control access to and the way of processing its personal information.[104] On the EU level, protection of personal data is rooted in the main European systems, namely the EU Charter and the EU Convention.[105] On Swedish national level, there exists no central bill of rights.[106] Instead, a number of fundamental rights and freedoms of citizens are enshrined in the second chapter of the Instrument of Government (1974:152).[107]

Article 7 of the EU Charter states that every individual has the right to respect for his or her private and family life, home and communications. Furthermore, article 8 of the EU Charter forms the basis for the protection of personal data as a fundamental right, which states that such data must be processed fairly for specified purpose and must be based on the consent of the person concerned, or other legitimate grounds stated by law. This is also confirmed by article 16 TFEU. According to article 16 (2) TFEU, EU has the competence to legislate on data protection matters, which has resulted in the regulation on data protection, namely GDPR.

Since May 2018, the GDPR is the primary source that provides a strong privacy protection in processing of personal data, especially regarding automated processing of the data concerning health, and is an important part of the AI framework.[108] Most of the provisions contained in the GDPR concern the modernization of the rules on protection of personal data laid down in previous legislations, in order to bring them into line with the modern digital society, increase legal certainty and most importantly to recapture individual's trust in the digital processing.[109]

---

[103] See Article 12 Universal Declaration of Human Rights, proclaimed by the United Nations General Assembly in Paris on 10 December 1948 (General Assembly resolution 217 A)
[104] Melanie Biurassa Forcier et al., *Integrating artificial intelligence into healthcare through data access: can the GDPR act as a beacon for policymakers?,* (2019), Volume 6, Issue 1, Journal of Law and the Biosciences, page 322
[105] Justine Pila & Paul Torremans, *European Intellectual Property Law*, (2019), 2nd edition, Oxford University Press, page 497
[106] Committee Reviewing, *European Convention and protection for private life in Sweden*, (2003), Yttrandefrihetskommittén, Ju 2003:04, page 2
[107] See 2 c. 1-18 §§ of the Instrument of Government (SFS 1974:153)
[108] Government Offices of Sweden (n 6), page 10
[109] See Recital 7 and 9 of the GDPR.

Nevertheless, the protection of patient's privacy and integrity within the Swedish healthcare is also emphasized in the supplementary Swedish legislation, *inter alia* 10 c. 1 § Patient Act (2014:821) and 1 c. 2 § Patient Data Act (2008:355).

3.2.2 The purposes and scope of the GDPR

According to article 2 (1) GDPR, the regulation applies to *processing* of *personal data* wholly or partly by automated means. Furthermore, the GDPR applies to any kind of operations and activities, *inter alia* private companies, associations, authorities and private individuals.[110] There are, however, certain exceptions where GDPR does not apply, for instance where the data processing is performed by natural person in the course of a purely personal or household activities[111], or to issues of protection of fundamental rights and freedoms[112].

The notion of 'processing' is described in article 4 (2) GDPR, as any operation performed on personal data or sets of personal data, whether or not by automated means. Other ways of processing that are highly pertinent in the context of AI, and accordingly in this thesis, are ADM and profiling. According to article 4 (4) GDPR, profiling means *any form of automated processing* that is carried out on *personal data* and is intended to *evaluate personal aspects* about natural person.[113] Furthermore, ADM process is the ability of making decisions by automated means without human involvement.[114] However, profiling and ADM are not necessarily separate activities, because it is difficult to imagine situations where processing of personal data not leading to profiling would lead to a decision as a result of ADM.[115]

In order to process personal data in accordance with the GDPR, Article 5 (1) GDPR establishes data processing principles that must be observed. Among other processing principles, article 5 (1) (a) GDPR recognizes transparency as a basic principle of data processing, in conjunction with lawfulness and fairness, especially in the case of solely ADM process.[116] In this regard, according to principle of accountability under article 5 (2) GDPR, healthcare provider is bound

[110] Article 4 (7) GDPR, 'controller' can be any natural or legal person, public authority, agency or other body.
[111] Recital 18 GDPR
[112] Recital 16 GDPR
[113] Article 29 Data Protection Working Part (WP29), *Guidelines on Automated individual decision-making and profiling for the purposes of Regulation 2016/679*, (2017), (wp251rev.01), page 6-7
[114] Ibid, page 8
[115] Maja Brkan, *Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond*, (2017), Volume 27, Issue 2, International Journal of Law and Information Technology, page 97; As mentioned in section 1.3 it is assumed that profiling is included in the notion of 'solely AMD' used throughout this thesis.
[116] Agata Ferretti et al. (n 97), page 324; Other general principles applying to the processing of personal data include purpose limitation under article 5 (1) (b); data minimization under article 5 (1) (c); data accuracy under article 5 (1) (d); storage limitation under article 5 (1) (e); integrity and confidentiality under article 5 (1) (f).

to be responsible for and demonstrate compliance with all of the processing principles. Additionally, as a key accountability tool, article 35 GDPR requires that a data protection impact assessment (DPIA) is made by a healthcare provider, when automated processing that uses new technologies is likely to result in a high risk to the rights and freedoms of the patient.[117] According to article 35 (3) (b) GDPR, the DPIA is particularly required when healthcare provider process on a large scale of data concerning health, e.g. by using AI or ML algorithms.

Moreover, the GDPR distinguish between personal data under article 4 (1) GDPR, which is *any* information that refers to an identified or identifiable natural person[118], and special categories of personal data under article 9 (1) GDPR, *inter alia* data concerning health. Recital 35 GDPR further describes what is to be seen as data concerning health, which includes *inter alia* information on disease, anamnesis or clinical treatment.[119] The special categories of data are subject to a higher level of protection and the processing of such data is prohibited under article 9 (1) GDPR, because it can create significant risks to the fundamental rights and freedoms of the patient.[120]

However, article 9 (2) GDPR provides a substantial list of exceptions to the general prohibition principle, *inter alia* explicit consent from the patient, which is also emphasized in 2 c. 3 § Patient Data Act (2008:355).[121] In this regard, due to the opaqueness of AI algorithms used solely ADM, obtaining explicit consent from the patient in order to process its data concerning health can be very difficult for the healthcare provider.[122] It is thus of outermost importance to clarify the aim behind, the risks and opportunities relating to solely AMD process, in order to gain trust from the patients and for the Swedish healthcare sector to be prepared to meet the upcoming digital changes.

---

[117] DPIA means that the healthcare provider must prior to processing carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. Requirements for the assessment is described in article 35 (7) (a)-(d) GDPR. See further recital 91 GDPR that describes situations where DPIA is nor required.

[118] The non-exhaustive list of examples is wide and covers 'any information' that can be connected to the individual; See further Information Commissioner's Office (ICO), *What is personal data?,* <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/> accessed 22 February 2020

[119] According to Article 9 (1) GDPR, special categories of personal data include genetic, biometric and health data, for instance historical patient data, electronical health records, diagnosis and treatment. See further recital 35 GDPR for further description of the notion of data concerning health.

[120] See Recital 51 GDPR; On contrary, according to 2 c. 3 § Patient Data Act (2008:355) the processing of personal data which is permitted under this Act may still be carried out even if the patient objects to it.

[121] For the purpose of the thesis, exceptions will not be further discussed; See also Judgement of the Supreme Administrative Court of Sweden on December 4th 2017 in case 3716-16, where the Administrative Court emphasized that the explicit consent from the patient cannot outweight privacy protection regulated in Patient Data Act (2008:355), *inter alia* the patient's explicit consent cannot be used as legal ground for providing 'direct access' to patients medical records to others, e.g. a proxy, under the same conditions as for the patient himself.

[122] Margot E. Kaminski, *The right to explanation, Explained*, (2019), Volume 34, Issue 1, Berkley Technology Law Journal, page 196

3.3 Automated decisions subject to the GDPR

3.3.1 Designation of solely automated decision-making

Solely ADM process using AI technology is a part of the everyday life. Being assessed by an AI system may seem strange in general, and especially in healthcare, but automated assessments are already a reality.[123] Specific provisions on solely ADM process are contained in article 22 (1) GDPR, which states that;

> '[…] the data subject shall have the right not to be subject to a decision based *solely* on automated processing, including profiling, which produces *legal effects* concerning him or her or *similarly significantly affects* him or her'.[124]

Article 22 (1) GDPR establishes a general prohibition on decision-making that is based solely on automated processing. This applies irrespective of whether or not the patient takes an action regarding processing of data concerning health.[125] Furthermore, article 22 (2)-(4) GDPR set forth exceptions to the general prohibition.[126] According to article 22 (4) GDPR, decisions based on automated processing shall not be based on *inter alia* the data concerning health referred to in article 9 (1) GDPR, unless the patient have explicitly consented to that and when suitable measures in protecting patient's rights and freedoms as well as legitimate interests are in place.[127]

Due to advances in technology and the capabilities of AI, algorithmic intervention has become almost crucial.[128] However, according to WP29, automated ways of processing the data concerning health have a potential to significantly impact patient's rights and freedoms, because these processes are opaque.[129] Thus, in order for the patient to be subject to specific rights and safeguards under the GDPR, the decision taken lawfully by automated means must meet the cumulative conditions set out in article 22 (1) GDPR.[130] These are described below.

---

[123] Blix and Levay (n 3), page 33
[124] Article 22 (1) GDPR
[125] Recital 71 GDPR; See further WP29 (n 113), page 19–20; See also Watcher Wachter et al., *Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation*, (2017), Volume 7, Issue 2, International Data Privacy Law, page 94, where the authors interpret article 22 (1) GDPR in two different ways, as a *prohibition* and as a *right to object* which offer different protection to the interest of both the patient and the healthcare provider. Under the formed interpretation the healthcare provider would be prohibited to engage in ADM before showing that the condition for lawful processing are fulfilled, while the latter interpretation mean that the patient can object to the ADM only in case one of the conditions are fulfilled.
[126] As mentioned in section 1.3 of the thesis, all of the exceptions are not discussed in detail.
[127] Article 22 (4) GDPR; See section 3.4 in the thesis for the required safeguarding measures.
[128] Maja Brkan (n 115), page 95
[129] WP29 (n 113), page 5
[130] Agata Ferretti et al. (n 97), page 323

3.3.2 Clarifying definition of key terms

3.3.2.1 'Decision based solely on automated processing'

Firstly, article 22 (1) GDPR refers to a decision 'based solely' on automated processing, which according to WP29 means that there is no human intervention in the decision making process.[131] The definition of the word 'solely' is unclear from the GDPR's text alone and has not been further described, which allows for an interpretation that excludes any human involvement whatsoever. This offers a threatening gap that would render article 22 (1) GDPR inapplicable to numerous of the existing practices of ADM processes.[132]

According to *Kaminski*, the notion 'based solely' can be interpreted narrowly, meaning that any human involvement, even rubber-stamping, takes an automated decision made by an AI algorithm out of scope of article 22 (1) GDPR. While the required level of human involvement is not clear in practice, the narrow interpretation suggests that even some nominal human involvement is sufficient. Another way to interpret the notion of 'based solely', according to *Kamiski*, is the broader reading to cover all automated decisions made by AI algorithms that occur without *meaningful* human involvement.[133] Thus, additional meaningful intervention by a human is required before any decisions is applied to an individual, where the person should actively exercise a real influence on the medical decision made solely by automated means.[134]

In this regard, *Bygrave* and *Watcher et al.* argue that a relative broad interpretation of the notion 'based solely' is required for the phrase to be meaningful.[135] *Bygrave* further states that decisions formally attributed to humans, but which originate from an ADM process, where the result is not actively assessed by either the human or the AI algorithm before being formalized as a decision, would thus fall within the scope of article 22 (1) GDPR. This is confirmed by the wording 'decision *based* solely on'.[136] Likewise, WP29 seem to stand by the broader interpretation, because, firstly, this is most likely to be suitable and compatible with the intention of the provision not to render the whole provision irrelevant and, secondly, the

[131] WP29 (n 113), page 20
[132] Privacy International, *Data is power: Profiling and automated decision-making in GDPR,*(2017), page 13 <https://privacyinternational.org/sites/default/files/2018-04/Data%20Is%20Power-Profiling%20and%20Automated%20Decision-Making%20in%20GDPR.pdf> accessed 3 march 2020
[133] Margot E. Kaminski (n 122), page 197
[134] WP29 (n 113), page 21
[135] Lee Andrew Bygrave, *Article 22: Automated individual decision-making, including profiling*, n Lee Andrew Bygrave; Christopher Kuner & Christopher Docksey (ed.), *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford University. Commentary on Article 22, pp522 – 542; See further Sandra Wachter et al. (n 126), page 92, where the authors state that if the notion 'solely' is interpreted narrowly, the safeguards contained in article 22 (3) GDPR will have limited applicability.
[136] Lee Andrew Bygrave (n 135)

healthcare provider would thus not be able to escape liability when using solely ADM AI algorithms, by 'fabricating human involvement'.[137]

Nevertheless, according to WP29, the human involvement needs to be meaningful and carried out by someone who has both the authority and the competence to change the outcome of the final result. WP29 further holds as part of the analysis, that the human involvement shall consider all the relevant data, namely the input and the output data, meaning that the human must have access to additional information beyond the algorithmic output. Hence, by routinely apply automatically generated profiles to individuals without any actual influence would not be sufficient to fall outside scope of article 22 (1) GDPR. In such case, the human involvement has to be active, real and meaningful.[138]

3.3.2.2 'Legal' or 'similarly significant' effect

Subsequently, a decision based solely on automated processing must produce legal effect or similarly significantly affect the patient. The GDPR does not define the notion of 'legal' nor 'similarly significant', the wording, however, makes it clear that only serious impact on the patient will be covered by article 22 (1) GDPR. WP29 states that a legal effect requires that the solely automated decision adversely affect the patient's legal rights or legal status, either partly or fully, for instance the rights provided by Patient Data Act (2008:355) or Patient Safety Act (2010:659).[139] In addition, processing that similarly significant affect the patient if it influences their personal circumstances, their behavior or choices, e.g. patient's access to healthcare.[140]

According to WP29, the reference to the notion of 'similarly significant' provides that even though a decision-making process does not have an effect on patient's legal rights it could still fall within the scope of article 22 (1) GDPR, if it produces an effect that is equivalent or similarly significant in its impact. Thus, the threshold for 'significance' is equal for legal and other significant effects.[141] WP29 further hold that for solely ADM to significantly affect the patient, the effect must be 'sufficiently great or important' in order to be observed.[142] Hence, according to *Ferretti et al.*, in the context of healthcare, automated processing of the data concerning health arguably produces an effect of this sort, since, even at minimum, it affects

[137] WP29 (n 113), page 21
[138] Ibid, page 21-22
[139] Ibid, page 21; See also Patient Data Act (2008:355) and Patient Safety Act (2010:659)
[140] Margot E. Kaminski (n 122), page 202
[141] WP29 (n 113), page 10
[142] Ibid, page 22; See Recital 71 GDPR which provides some guidance on certain situations of 'significances', *inter alia* automatic refusal of an online credit application or e-recruit practices without any human intervention.

patient's circumstances and most likely patient's choices in a significant or otherwise important way.[143]

According to *Bygrave*, the notion of 'similarly significant' presents more problems, because the term itself is vague and requires interpretation. *Bygrave* state that 'significance' varies on the perception of the patient, for instance where the effect of receiving a rejection letter will depend on the economic situation of an individual, while impact on legal status can be decided according to the law. In this regard, *Bygrave* points out that it can put a heavy burden on the patient to prove that the medical decision taken solely by automated means significantly affect the patient.[144] However, even if some conditions contained in article 22 (1) GDPR can be widely interpreted, the patient has certain rights that it can refer to when it is subject to solely ADM process, which are described in the next section.

3.4 Transparency requirements in automated decision-making

3.4.1 Introduction

Given the potential risks and interference that article 22 (1) GDPR possess to the rights of the patient in case of solely ADM process using AI algorithms, the healthcare provider should be particularly mindful of their processing obligations.[145] According to the GDPR, where conditions under article 22 (1) GDPR are fulfilled, *inter alia* where a decisions is based *solely* on automated processing that produces *legal or similarly significant effects* on the patient, certain rights and safeguards become applicable that the patient can rely on. The below described provisions create a basis on deciding what level of transparency is required for AI technology in healthcare and how to implement it.[146]

3.4.2 Transparent processing

Transparency is a long-established feature of the law[147] and has often been suggested as a remedy to accountability issues for solely ADM process.[148] It is about creating trust in the processes which has a potential of affecting the patient by enabling them to understand, and if

[143] Agata Ferretti et al. (n 97), page 324
[144] Lee A Bygrave (n 135), page 522 – 542; See also Sandra Wachter et al. (n 125), page 93
[145] See also WP29 (n 113), page 24
[146] Luciano Floridi et al., *Healthcare, Artificial Intelligence, Data and Ethics – A 2030 Vision: How responsible innovation can lead to a healthier society*, (2018), page 22 <https://www.digitaleurope.org/wp/wp-content/uploads/2019/02/Healthcare-AI-Data-Ethics-2030-vision.pdf> accessed 5 March 2020
[147] See *inter alia* Article 1 TEU, Article 11(2) TEU and Article 15 TFEU on transparency between EU institutions and society, and Chapter 2 § 1 point 2 The Instrument of Government (1974:152) 'freedom of information'
[148] Frank Pasquale (n 99)

necessary, challenge the final decisions. Furthermore, it expresses the principle of fairness in relation to the processing of personal data under article 8 CFR. Additionally, transparency is linked to the new principle of accountability under article 5 (2) GDPR, where the healthcare provider must demonstrate compliance with transparent processing of personal data.[149]

While transparency is not clearly defined in the GDPR, the WP29 has issued guidelines on the interpretation of it in practice.[150] Additionally, the EU Commission conducted a study in 2018/2019 and analyzed the so-called algorithmic transparency to raise awareness and build a solid knowledge foundation for the challenges and opportunities for algorithmic decisions, by stating following;

> '*Algorithmic transparency* has emerged as an important safeguard for *accountability and fairness in decision-making* and for opening to scrutiny the way access to information is mediated online, especially on online platforms. This has large implication for *consumers and business* […] and is key to informed policy-making.'[151]

The principle of transparency is a core principle enshrined in article 5 (1) (a) GDPR which provides that personal data must be processed in a lawful, fair and transparent manner in relation to the patient. Nevertheless, recital 39 is informative as to the meaning and effect of the principle in the context of data processing, which states that '*transparency requires that any information and communication relating to the processing of […] personal data be easily accessible and easy to understand, and that clear and plain language be used*'.[152] In particular, transparency is achieved by providing the patient with processing details and applies to all kinds of data processing activities in healthcare.[153]

In this regard, WP29 describe transparency as being a *user-centric* rather than *legalistic*.[154] The meaning of the notion *user-centric* has been described by *Mazue et al.*, according to which the patient has the freedom of choice and ability to exercise control upon its data concerning health.[155] Nevertheless, as explained by the WP29 and the Swedish Welfare Board, this

[149] WP29, *Guidelines on transparency under Regulation 2016/679*, (2017), (wp260rev.01), page 5
[150] Article 29 Data Protection Working Party, *Guidelines on transparency under Regulation 2016/679*, 17/EN, WP260rev.01
[151] European Commission, *Algorithmic Awareness-Building*, (2019), <https://ec.europa.eu/digital-single-market/en/algorithmic-awareness-building> accessed 4 March 2020
[152] Recital 39 GDPR
[153] Agata Ferretti et al. (n 97), page 323
[154] WP29 (n 149), page 6
[155] Joanna Mazue et al., *GDPR: A step towards a user-centric internet?*, (2017), Volume 54, Issue 4, Intereconomics, page 207

principle is especially relevant to solely ADM AI system, because these processing activities are often invisible to the patient.[156]

The principle of transparency is placed in a number of articles in the GPDR, underlying the increased responsibility of the healthcare provider and highlight patient's rights under solely AMD process.[157] In particular, article 12 (1) GDPR sets out the general rules that apply to the provision of information (articles 13-14) and communication with patients concerning their rights (articles 15-22). Article 12 GDPR especially requires that the information or communication in question is 'concise, transparent, intelligible and easily accessible', where 'clear and plain language' must be used.[158] The notion of 'concise and transparent' means that the healthcare provider should present the information efficiently and succinctly in order to avoid information fatigue.[159]

3.4.3 The right to be informed

The right to be informed in the context of solely ADM is contained in article 13 GDPR (data obtained from the patient directly) and article 14 GDPR (data obtained from third party), which enables the patient to receive necessary information, *inter alia* information on who, for which purpose and under which circumstances such data will be processed, before they consent to the processing of the data concerning health.[160] According to articles 13 (2) (f) and 14 (2) (g), the information to be received includes;

> '[…] the existence of automated decision-making, including profiling, referred to in article 22 (1) and (4) and, at least in those cases, *meaningful information about the logic involved*, as well as the *significance and the envisaged consequences* of such processing for the data subject […]'.[161]

Even though, the wording of both articles is exactly the same, the difference is, however, the timing of the exercise of the right. The information under article 13 (2) (f) GDPR must be given at the time when the processing of personal data begins, for instance when the data concerning health is collected. On contrary, article 14 (2) (g) GDPR provides that where the data concerning health was stipulated to the healthcare provider by a third party, for instance through

[156] WP29 (113), page 7; see also Agata Ferretti et al. (n 97), page 324
[157] WP29 (149), page 7
[158] See recital 39 GDPR, which states that the information and communication relating to processing of personal data must be easily accessible and easy to understand.
[159] WP29 (149), page 6
[160] Ibid, page 14; See further Recital 39 GDPR
[161] Articles 13 (2) (f) and 14 (2) (g) GDPR

the external cooperation between private healthcare providers[162], incidentally based on a profile, or through other means, such information must be provided in accordance with a time frame contained in article 14 (3) GDPR.[163]

According to WP29, the notion of 'meaningful information about the logic involved', means that the healthcare provider must find a simple way to tell the patient about the rationale behind or the criteria applied when reaching the medical decision. Thus, the GDPR does not require to provide a complex explanation of the processing algorithms used or disclose the full algorithm. Instead, the WP29 state that the information shall be clear enough for the patient to understand the reasons for the decision.[164] Presumably, meaningfulness must be evaluated from the perspective of the patient, where the information about the logic involved must be meaningful *to the patient*, notably, a human and apparently without special technical experience.[165]

Malgieri and *Comandé* argue that information on ADM process conducted by an AI algorithm shall be 'relevant, significant, important' and must be 'intended to show the meaning' with the final decision. In other words, they hold that the in order for the information to be meaningful, the explanation about the automated processing shall be both 'complete and comprehensible' for the patient in question.[166] In this regard, both WP29 and *Kamarinou et al*. hold that revealing the underlying algorithms of the AI system might not be considered as meaningful, because the patient in most cases lacks technical skills to understand how an AI algorithm works.[167] However, the WP29 point out, with the reference to recital 58 GDPR, that complexity must not be an excuse for failing to provide the all the necessary information to the patient.[168]

Yet, the healthcare provider is not obliged to provide 'meaningful information about the logic involved' where there is non-solely automated profiling as stated in article 4 GDPR, e.g. the existence of a minimal degree of human intervention. In this regard, *Ferretti et al.* argue that, in the medical context, restricting providence of information other than being legally binding,

---

[162] See KRY information security, which states that parent company is to be regarded as the 'data controller', while subsidiary is only responsible for the technical platform and application 'KRY'. KRY, *Integritetspolicy*, <https://www.kry.se/legal/integritetspolicy/> accessed 15 May 2020
[163] Privacy International (n 132), page 15
[164] WP29 (n 113), page 25
[165] Christohper Kuner et al., *Machine learning with personal data: is data protection law smart enough to meet the challenges*, (2017), Volume 7, Issue 1, International Data Privacy Law, page 20; See further Andrew D. Selbst and Julia Powels, *Meaningful information and the right to explanation*, (2017), Volume 7, Issue 4, International Data Privacy Law, page 236
[166] Gianclaudio Malgieri and Giovanni Comandé, *Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation*, (2017), Volume 7, Issue 3, International Data Privacy Law, page 264
[167] Dimitra Kamarinou et al., *Machine learning with personal data*, (2016), Queen Mary School of Law Legal Studies Research Paper number 247/2016, page 20
[168] WP29 (n 113), page 25; Recital 63 GDPR

may have tangible consequences, *inter alia* hinder patient's trust in the use of AI systems in healthcare, as well as undermine the trustworthiness between the patient and the doctor. Nevertheless, this may give the patient an impression that they are being marginalized in decisional processes concerning their health, which can affect their decisional autonomy and their sense of self-determination.[169]

3.4.4 The right of access

Besides having the right to obtain meaningful information, the patients has, nevertheless, the 'right to access' meaningful information about the processing of its data concerning health.[170] Article 15 (1) (h) GDPR follows the same pattern of articles 13 (2) (f) and 14 (2) (g), by enabling the patient to have:

> '[…] *access* to the personal data and the following information: […] (h) the existence of automated decision-making, including profiling, referred to in Article 22 (1) and (4) and, at least in those cases, *meaningful information about the logic involved*, as well as the *significance and the envisaged consequences* of such processing […]'.[171]

Although, the language of article 15 GDPR is the same as of articles 13-14 GDPR, the role of these provisions is very different.[172] Articles 13-14 GDPR require healthcare provider to provide meaningful information to the patient when the data concerning health is obtained, while article 15 GDPR creates an individual right of access to the information which can be invoked by the patient at any time and has no deadline, including after an automated process has been made. The timeline of article 15 GDPR stems from recital 63 GDPR, which states that the patient shall exercise that right of access 'easily and at reasonable intervals'.[173]

Yet, the language and the timing of these articles has provoked debate. In its guidelines, the WP29 states that the healthcare provider shall provide the patient with information about the envisaged consequences of the processing and not an explanation of a *particular* decision.[174] Thus, according to both WP29 and *Wachter et al.*, the healthcare provider shall provide the

[169] Agata Ferretti et al. (n 97), page 327
[170] WP29 (n 113), page 26
[171] Article 15 (1) (h) GDPR
[172] Margot Kaminski (n 122), page 199; See also Sandra Wachter et al. (n 125), page 90
[173] Recital 63 GDPR
[174] WP29 (n 113), page 27. This is also confirmed by recital 63 GDPR, where the patient shall obtain 'communication' about automatic processing and the logic involved, and *at least* when based on profiling, the consequences of such processing.

'general information', e.g. factors that are taken into account when processing data by automated means and factors on their separate 'weight' on a combined level, where the patient shall be able to examine the lawfulness of the automated processing and invoke legal remedies.[175] On contrary, *Malgieri* and *Comandé* as well as *Selbst* and *Powels* have argued that the notion of 'meaningful information' indicates that article 15 GDPR can provide a deeper disclosure after the automated processing have taken place, including insight into a *particular* decision affecting.[176] However, the text of the GDPR itself does not clarify this conflict.[177]

In the context of healthcare, where patient protection is particularly strong, meaningful information must be conveyed in a way than can answer the questions that the patient might have *before* they give consent to the processing of their data concerning health (notification obligations) and *after* a decision has been made (right of access). This enables the patient to determine whether the processing is safe before consenting to the solely ADM process as well as to establish whether processing has been conducted unlawful or unfair.[178] For example, under article 22 (3) GDPR, which will be described below, the patient may request that any declined medical decision made by solely automated means is reassessed. However, when the patient is unable to receive information *after* the decision has been made, the patient must rely on the fact that the decision is being reassessed fairly, which creates a degree of uncertainty.[179]

In this regard, considering that article 22 GDPR only applies to decisions that have legal or significant effect, the above-described imbalance of power is very troubling, particularly when solely ADM using AI or ML, because such systems only makes hypothetical results. Thus, in cases that are essentially subjective, especially when it comes to patient health, this can make it very difficult for the patient to challenge decisions that affect its rights and freedoms and/or legitimate interests based only on the knowledge about the general functionality of the system.[180]

[175] WP29 (n 113), page 27; Sandra Wachter et al. (125), page 83. Following the recital 63 GDPR, the patient should have the right of access to personal data and to exercise the right 'in order to be aware of, and verify, the lawfulness of processing'; see also Judgment of the German Federal Court Bundesgerichtshof 28 January 2014 – VI ZR 156/13 (SCHUFA), where the German Federal Court emphasized the limitation of the right of access to the general information of the ADM by stating that an individual does not have a right to investigate fully the accuracy of ADM and the underlying formula which is protected by trade secrets.
[176] Malgieri and Comandé (n 166), page 244; Selbst and Powels (n 165), page 236
[177] Margot Kaminski (n 122), page 200
[178] Privacy International (n 132), page 15-16
[179] Ibid, page 15
[180] Ibid.

3.4.5 Additional safeguards in case of solely automated decision-making

In cases where solely ADM process lawfully takes place, e.g. under the exceptions stated in article 22 (2) (a) or (c), the patient is subject to additional safeguards under article 22 (3) GDPR, which includes 'at least the right to obtain human intervention […], to express his or her point of view and to contest the decision'.[181] According to WP29, the human intervention is the main element under article 22 (3) GDPR, meaning that any review must be carried out by somebody who has the proper ability and capability to change the decision, by undertaking an assessment of all the relevant data, including additional data provided by the patient.[182]

Furthermore, article 22 (3) GDPR is not aimed at informing or disclosing the information, rather rendering of the decision justiciable. Thus, this provision does not ask for a review, rectification or examination of the decision, it rather refers to the notions of fair treatment and accountability as values stemming from the transparency requirement under the GDPR. It is therefore possible to interpret right under article 22 (3) GDPR as complementary and further reinforcement of the obligation of conduct laid down in the right to access under article 15 GDPR with an obligation of result, namely making medical decision based solely on ADM process contestable.[183]

Additionally, recital 71 GDPR further clarifies the scope of the safeguards described above, which states that a patient that has been subject to solely ADM *in any case*;

> '[…] should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, *to obtain an explanation of the decision reached after such assessment* and *to challenge the decision*.'[184]

According to *Ferretti et al.*, the idea of the right of explanation stems from the significance of transparency in data processing, especially when it comes to solely ADM, and is intended to counterbalance the opacity of automated systems in healthcare.[185] However, the question of whether the patient can demand an explanation of the automated decision taken is unclear. This has led to lively discussions, especially among legal scholars, about its actual scope and definition, because such right is specifically challenging when exploiting the full power of AI

[181] Article 22 (3) GDPR
[182] WP29 (n 113), page 27
[183] Emre Bayamlioglu, *Transparency of automated decisions in the GDPR: An attempt for systematization*, (2018), Working paper, Tilburg University, page 39
[184] Recital 71 GDPR
[185] Agata Ferretti et al. (n 97), page 321

algorithms as the same time as managing with the logic that is understandable by humans.[186] Some scholars have taken an optimistic view on the right to explanation, while others are unsure that the right is contributing to anything at all.[187]

Initially, *Klimas* and *Vaiciukaite* argue that recital 71 GDPR is not legally binding and have no positive operation of its own, which means that it cannot cause legitimate expectations to arise. In this regard, they state that recitals are supposed to be general expressions of the purpose of the regulation, which in turn cannot properly justify reliance.[188] This line of reasoning has also been confirmed by the EUCJ, where it stated that 'whilst a recital in the preamble to a regulation may cast light on the interpretation to be given to a legal rule, it cannot in itself constitute such a rule'.[189] Therefore, healthcare provider does not have a real duty to provide explanation of the medical decisions made solely by automated means.

On contrary, according to *Malgeri* and *Comandé*, even though the right to explanation is excluded from the actual binding text of the regulation, recital 71 GDPR can still be used as a means to interpret what the legislator had in mind when requiring suitable measures and safeguards.[190] In their reasoning, they refer the negative explanation of the EUCJ, according to which the preamble of the regulation 'has no binding legal force and cannot be relied on as a ground for derogation from the actual provisions of the [regulation] in question'[191] and further clarifies that a 'recital cannot be relied upon to interpret [a regulation] in a manner clearly contrary to its wording'[192]. In this regard, *Malgeri* and *Comandé* make an *argumentum a contrario* by stating that recital 71 GDPR does not derogate from the binding article 22 GDPR, neither does it amend it contrary to its wording. Instead the recital itself helps to clarify what safeguards the healthcare provider should use in case of ADM process. Thus, the conclusion according to *Malgeri* and *Comandé* is that recital 71 GDPR is properly considered as a supplementary normative tool and whenever an ADM process is lawful the patient in question shall always be able to obtain an explanation of the medical decision.[193]

[186] Selbst and Powels (n 165), page 233
[187] Heike Felzmann et al. (n 11), page 3
[188] Tadas Klimas and Jurate Vaiciukaite, *The law of recitals in European Community legislation*, (2008), Volume 15, ILSA Journal of International & Comparative Law, page 66
[189] C-215/88, *Casa Fleischhandel v BALM* [1989], ECR 2789, para 31
[190] Malgieri and Comandé (n 166), page 261
[191] C-162/97 Gunnar Nilsson, Per Olov Hagelgren, Solweig Arrborn, [1998] ECR, I-7477, para 54
[192] C-308/97, Manfredi v Regione Puglia, [1998] ECR, I-7685, para 30
[193] Malgieri and Comandé (n 166), page 261; This line of reasoning is also confirmed by the European Commission, Commission's Communication on guidance for better transposition and application of Directive 2004/38/EC (COM/2009/0313)

Moving away from the legality of the recitals, *Wachter et al.* instead put an emphasis on the distinction between explanations in terms of their type and timing. According to *Watcher et al.*, an *ex ante* explanation, that occurs before the processing by automated means takes place, addresses the systems general functionality, while an *ex post* explanation that arises after an automated decision has been reached, includes explanation of the rationale, reasons and individual circumstances of a specific automated decision.[194] *Wachter et al.* state that article 22 (3) GDPR lists the minimum requirements that must be fulfilled in order for automated processing to be lawful. Thus, as long as these are met, a right to explanation in recital 71 in such case is not legitimately stipulated by the requirements contained in article 22 (3) GDPR.[195]

Nevertheless, *Watcher et al.* discuss on the alternative of including the right of explanation under article 15 GDPR, because this article enables the patient to request the information at any time.[196] In this regard, they state that because of the language used in the articles 13-15 GDPR, e.g. 'envisaged consequences' that must be presented before the actual consequence occur, this does not include any *ex ante* explanation on how the specific decision was made or reached, but rather addressed to the *ex ante* explanation of the systems functionality.[197] Consequently, according to *Watcher et al.*, the GDPR does not provide a right to explanation, but rather a limited 'right to be informed' about the existence of solely ADM and its general functionality.[198]

An opposite reasoning has been held by *Selbst* and *Powles*, where they hold that article 22 and recital 71 GDPR support the reading of articles 13-15 GDPR as an autonomous source of right. They explain that whenever an ADM process is conducted lawfully, such process must include suitable measures to safeguards the patient's rights and freedoms and legitimate interests contained in article 22 (3) GDPR. In this regard, recital 71 GDPR supplements article 22 GDPR taken as a whole, by proposing additional safeguards, *inter alia* the 'right to obtain an explanation of the decision reached'. Thus, *Selbst* and *Powles* argue that the right to explanation is neither recognized nor restricted by the safeguards contained in article 22 GDPR, because the main purpose of such safeguards is to 'safeguard rights, freedoms, and legitimate interests' of the patient at stake, which coincide with the purpose of information and access rights. Thus, they conclude that even though the right to explanation cannot be derived from article 22 GDPR

[194] Sandra Wachter et al. (n 125), page 78
[195] Ibid, page 80
[196] Recital 63 GDPR, containing the wording of 'at reasonable intervals'; See section 3.4.4 for the explanation of the time frame.
[197] Sandra Wachter et al. (n 125), page 83
[198] Ibid, page 90

itself, this article still supports the existence of such rights through the purpose of articles 13-15 GDPR.[199] In this regard, *Selbst* and *Powles* end their argumentation by stating that the right to explanation shall be understood 'functionally, flexibly, and should at a minimum, enable the [patient] to exercise his or her rights under the GDPR'.[200]

On contrary to legal scholars, the WP29 have not commented on the legal effect of the recital nor the time-framing when an explanation shall be provided. Instead, the WP29 suggest that *in any case* suitable safeguard shall also include 'specific information to the data subject […] and the right to obtain an explanation of the decision reached after such assessment and to challenge the decision'.[201] In this regard, the WP29 emphasize the need for transparency due to the fact that the patient will be able to challenge the decision or express its view *only* in case where the patient fully understands how the medical decision has been made and on what basis. The WP29 do not further describe what an explanation shall entail, instead it refers to the transparency requirements set out in article 13-15 GDPR.[202]

In this regard, *Woodward* holds that an explanation 'out to be such that it enables us to see what sort of difference it would have made for the [result] if the factors cited in the [explanation] had been different in various possible ways'.[203] The ability of the patient to intervene on the factor in question is also emphasized by the wording of the recital 71 GDPR itself, because the patient must be able to obtain information in a transparent manner, in first place, in order to take actions against it.[204] In this regard, it can be assumed that an explanation should outline the main reasons with the decision, which will enable the patient make use of the safeguards contained in article 22 (3) GDPR.[205]

Apart from all the above-presented arguments, *Malgieri* and *Comandé* make an overall conclusion by holding that the vagueness and broadness in the wording of the rights set out in articles 13-15 and 22 GDPR can be read in favor of the patient, because it can be extensively interpreted by the Data Protection Authorities and the national courts. Data Protection Authorities in turn can reject the restrictive interpretation, wholly or partly, with foreseeable

[199] Selbst and Powels (n 165), page 237
[200] Ibid, page 242 (emphasis added)
[201] WP29 (n 113), page 27
[202] Ibid; However, it seems to be the case that WP29 understand that articles 13-15 GDPR do not provide a right to an ex post explanation,
[203] James Woodward, *Making things happen: A theory of casual explanation*, (2003), Oxford University Press, page 11
[204] WP29 (n 113), page 27
[205] Stefnie Hänold, *Profiling an automated decision-making: legal implications and shortcomings* in Marcelo Corrales, Mark Fenwick and Nikolaus Forgó (ed), *Robotics, AI and the Future of Law*, (2018) Springer Nature Singapore, page 139

and serious consequences for the healthcare provider. *Malgieri* and *Comandé* state that the only certainty about the right to explanation and the wording of articles mentioned above is the uncertainness and openness to legal discretion.[206] Consequently, due to the fact that the right to explanation is a two-sided coin and the practical implementation of it is still unclear, this thesis leaves the right to explanation open to further interpretation.

3.5 The need for transparency in healthcare

The incorporation of AI and ML into clinical medicine holds promise for substantially improving healthcare delivery. However, most of the ML techniques obtain diagnostics or predictive accuracy at the expense of the ability of the humans to access to knowledge within the system.[207] As *Swartout* notes;

> '[…] when a physician consults an expert, the physician may question whether some factor was considered or what effect a particular finding had on the final outcome and the expert is expected to be able to justify his answer and show that sound medical principles and knowledge were used to obtain it […] In addition to providing diagnoses or prescription, a consultant must be able to explain what it is doing and justify why it is doing so'.[208]

Since decades ago, trust has been connected to the ability of explaining expert recommendations. Thus, the key element within the healthcare is 'proven experience', as it is necessary for the healthcare provider to be able to understand and explain the result for it to be regarded as viable and to be trusted by the patient.[209] But when a healthcare provider must deal with an automated decision made by an AI system that they do not have knowledge of or experience in, how is such system affecting patient's rights and autonomy? Why is transparency so important, especially when dealing with data concerning health? This raises ethical questions and challenges in the society, and especially within the healthcare domain.[210]

Firstly, when data concerning health is used in solely ADM process that predicts certain medical outcome, it might be impossible to track the casual explanation of the occasions between the

[206] Malgieri and Comandé (n 166), page 260
[207] Alex John London, *Artificial Intelligence and Black-Box medical Decisions: Accuracy versus Explainability*, (2019), Volume 49, Issue 1, Hastings Center Report, page 15
[208] William R. Swartout, *Explaining and Justifying Expert Consulting Programs*, (1981), From the Proceeding of the Seventh International Join Conference on Artificial Intelligence, Volume 2, pp 815-823; see also Alex John London (n 207), page 15
[209] Swedish National Board of Health and Welfare (n 5), page 71
[210] Alex John London (n 207), page 15

input and the output data. The explainability of such result and the obligation to communicate information about it is likely to affect the patient-doctor relationship, which is required from a legal basis, *inter alia* by Patient Act (2014:821) and Patient Safety Act (2010:659).[211] Thus, solely ADM AI system can depersonalize such relationship, by decreasing possibilities for direct personal interaction. Thus, patients may feel that their decisional autonomy and the capacity to influence their healthcare situation is undermined.[212]

As a consequence, patients will not disclose personal data due to the lack of information security and the fear of risking their personal integrity. A report made by the Swedish Data Protection Authority in 2019 have shown that patient's willingness to participate in research involving their generic data is affected by the concerns about their ability to protect their privacy. Although the statistics show that patients have a relatively high confidence in healthcare providers who process their data concerning health, however, only half of the them consider that they are being provided with enough information about the way and purpose of such processing.[213] As a result, the issue of trust can undermine the development of AI technology and forego the expected benefits such systems promise to deliver.[214]

Secondly, the Swedish Welfare Board notes the risk of inaccurate, unfair, biased or discriminatory outcomes of solely automated AI system, that can have negative impact on patient's care and safety.[215] Biases can accidentally be built into an AI or ML systems in healthcare by the information used to train the system. Such information can be misleading because it does not *inter alia* represent gender in a fair way, which in turn will not give reliable results. Furthermore, data may be biased in several other ways besides gender differences, *inter alia* deficiencies related to ethnicity, geography, age and disabilities.[216] In this regard, *Ho et al.* state that ML systems are not strictly mathematical or worthy neutral, instead they are created by imperfect people with bias, prejudice and potentially incorrect intensions.[217]

An example within the healthcare can be that if a healthcare provider always withdraw care in patients with a brain injury, a ML fed with such information may determine that this shall

[211] European Parliament, *Robots in healthcare: a solution or a problem?*, (2019), PE 638.391, Policy Department for Economic, Scientific and Quality of Life Policies, page 19
[212] Agata Ferretti et al. (n 97), page 331
[213] Swedish Data Protection Authority, *National Integrity Report 2019*, (2019), Report 2019:2, page 29-30 <https://www.datainspektionen.se/globalassets/dokument/rapporter/nationell-integritetsrapport-2019.pdf> accessed 7 March 2020; See Annex 4 for the statistic on the willingness of citizens to share their personal data.
[214] Agata Ferretti et al. (n 97), page 331
[215] Swedish National Board of Health and Welfare (n 5), page 80
[216] Ibid, page 81
[217] Calvin W.L. Ho et al., *Governance of automated image analysis and artificial intelligence analytics in healthcare*, (2019), Volume 74, Clinical Radiology, page 333-334

always be the case.[218] This has been confirmed in a non-medical field, where ADM AI system have already been shown to mirror human biases in the decision-making process. An AI system called Correctional Offender Management Profiling for Alternative Sanctions (COMPAS) used in U.S. courts to assess the risk of recidivism for defendants in pretrial hearings, have shown a troubling tendency for racial discrimination, where the system has imposed stricter jail sentences on a certain group of individuals.[219]

Nevertheless, in a report made by a group of researchers, *Caruana et al.* found that even though ML was more accurate at predicting the probability of death from pneumonia[220], it still ranked patients with asthma issues as having a lower probability *per se*. This is contrary to common-sense expectation, because patients with a history of asthma are typically admitted directly into the intensive care unit of the hospital for acuter care that gives such patients a lower likelihood of death. The result is seen as misleading because it does not reflect patient's underlying medical need. In this regard, *Cruana et al.* emphasize the importance of transparency, where healthcare provider can adjust the system in order for it to reflect current medical knowledge to avoid biased and unreliable outcomes that can be sufficiently harmful to counterbalance marginal gains in the predictive power.[221]

3.6 Conclusion

To conclude, the GDPR offers many rights to the patient relating to the principle of transparency under the processing of the data concerning health. The main rights in a transparent processing in solely ADM process lies in the information obligations under articles 13-14 GDPR and the right to access under article 15 GDPR, which are further safeguarded by the rights under article 22 (3) and the right to explanation in the (non-binding) recital 71 GDPR. However, the right to explanation, which aims to counterbalance the opacity of automated systems, is still unclear and will be subject to future discussion and clarification both from the

[218] Swedish National Board of Health and Welfare (n 5), page 81
[219] Robyn Calpan et al., *Algorithmic accountability: A primer*, (2018), Data & Society, page 4 <https://datasociety.net/wp-content/uploads/2018/04/Data_Society_Algorithmic_Accountability_Primer_FINAL-4.pdf> accessed 10 March 2020; See also Julia Angwin et al., *Machine Bias*, (2016) ProPublica, <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing> accessed 28 March 2020
[220] Inflammatory condition of the lung. See further Jonas Hedlund, *Lunginflammation*, (2020) 1177 Vårdguiden, <https://www.1177.se/sjukdomar--besvar/lungor-och-luftvagar/inflammation-och-infektion-ilungor-och-luftror/lunginflammation/> accessed 17 April 2020
[221] Rich Caruana et al., *Intelligible models for healthcare: Predicting pneumonia risk and hospital 30-day readmission*, (2015), International Conference on Knowledge Discovery and Data Mining, page 1721 <http://people.dbmi.columbia.edu/noemie/papers/15kdd.pdf> accessed 17 March 2020

Swedish Data Protection Authority and, keenly awaited, case law from the EUCJ and the national court.

Besides being troubling from the perspective of the patient about the processing of its data concerning health, where an emerging need for transparency within the healthcare is confirmed, AI algorithms used in solely ADM process somehow create issues on the part of the private healthcare provider, wanting to keep them as a trade secret. Thus, a conflict arises between, on the one hand, company's fundamental rights of freedom to conduct business and trade secret protection and, on the other hand, the fundamental rights of the patient to be provided with enough information to ensure that their rights are properly safeguarded within the healthcare. Thus, the next chapter examines trade secrets rights, when these are faced with the important principle of transparency.

4. Trade secrets as a market exclusivity mechanism for 'Black Box' algorithms

4.1 Introduction

Protection of trade secrets, which is a form of intangible monopoly on information, is an important tool and interest of the society. A cornerstone of healthcare provider's competitiveness, or every other company's *per se*, as well as preconditions for innovations is a strong trade secret protection. Not only do companies need to protect their final products and the production methods by intellectual property law, they also need to protect the accumulated knowledge from being exploited by others in an unduly manner. Thus, the protection of trade secrets is as valuable as the protection of tangible assets and intellectual property rights.[222]

Nowadays, the AI algorithms used in ADM process in healthcare are fundamental for every private healthcare provider, *inter alia* for the digital healthcare platforms *Kry*, *MinDoktor* and *Doktor24*.[223] These algorithms are protected as trade secrets, which gives a competitive advantage on the market.[224] In this regard, the healthcare provider has the ability to lawfully exclude others from getting access to their valuable knowledge, because it would result into significant losses, had the algorithms been revealed.[225]

However, when the notion of transparency is put in the same sentence as the notion of trade secrets a conflict arise, where the healthcare providers interest in keeping its AI algorithms used in solely ADM process collide with the patient's rights to a transparent processing of its data concerning health. In this regard, it is of special importance to examine when and how AI algorithms used in ADM process in healthcare can be entitled to trade secret protection, while avoiding depriving patients of their fundamental rights under the GDPR.

---

[222] Prop. 2017/18:200, *A new legislation on Trade Secrets*, (2018), page 19 <https://www.regeringen.se/495f60/contentassets/561250903e2a49f286ddf63b2c3515f1/prop-201718-200.pdf> accessed 18 March 2020

[223] National Board of Health and Welfare, *Digital healthcare services addressed to patients – survey and follow-up*, (2018), No 2018-6-15, page 21; See also section 2.3 in this thesis for the description of Aleris X algorithms used by *Doktor24*.

[224] Gianclaudio Malgieri, *Trade Secrets v Personal Data: A possible solution for balancing rights,* (2016), Volume 6, Issue 2, International Data Privacy Law, page 102; See also European Commission, *Trade secrets*, <https://ec.europa.eu/growth/industry/policy/intellectual-property/trade-secrets_en> accessed 20 March 2020

[225] Mariateresa Maggiolino, *EU trade secrets law and algorithmic transparency*, (2019), Bocconi Legal Studies Research Paper No. 3363178, page 1-2

4.2 Trade secrets and fundamental rights

4.2.1 Legal protection of trade secrets

For a long time, the protection of trade secrets has been regulated by the national laws of each MS, where they have been sufficiently protected by *inter alia* unfair competition law.[226] There are, however, some international foundations on which the area of trade secrets and various national approaches are built upon. Article 10*bis* in the Paris Convention on Industrial Property, adopted in 1883, was the first international treaty protecting industrial property in the widest sense and obliged MS to provide effective protection from unfair competition.[227] Furthermore, almost a century later in 1995, the first international treaty that addresses the protection of trade secrets, the Agreement on Trade-Related Intellectual Property Rights (TRIPS), came into force, which established common general standards on trade secret law for all countries. Article 39 TRIPS specifically deals with the protection of undisclosed information and sets forth a definition for trade secret, which has never existed earlier.[228]

When it comes to private companies, *inter alia* healthcare providers, the rights under the EU Charter are of the main interest. Article 16 of the EU Charter establishes that the freedom to conduct business in accordance with EU law and national law and practices is recognized. This article guarantees an economic freedom for companies to pursue economic activities.[229] Article 17 of the EU Charter establishes a right to property, meaning that everyone has the right to its lawfully acquire possessions, with certain exceptions. This article is based on Article 1 of the Protocol to the EU Convention and can thus be seen as protecting companies against misuse of trade secrets, by offering protection through intellectual property.[230]

However, even though intellectual property and trade secrets rights seem similar, trade secrets somehow differ from the former because they result from both technical and commercial types

[226] Pila & Torremans (n 105), page 513
[227] Marco Bronckers & Natalie Marie McNelis, *Is the EU obliged to improve the protection of trade secrets? An inquiry into TRIPS, the European Convention on Human Rights and the EU Charter of Fundamental Rights*, (2012), Volume 34, Issue 10, European Intellectual Property Review, page 674. Additionally, the Berne Convention for the Protection of Literary and Artistic Works, adopted few years later in 1886, aimed at protecting specifically copyrights
[228] Bronckers & McNelis (n 227), page 674
[229] C-4/73 *Nold KG v Commission*, para 14; C-230/78 *SpA Eridiana-Zuccherifici and others*, para 20 and 31, where the EUCJ recognized freedom of companies to exercise an economic and commercial activity; See also European Union Agency for Fundamental Rights, *EU Charter of Fundamental Rights, Article 16 – Freedom to conduct business* <https://fra.europa.eu/en/eu-charter/article/16-freedom-conduct-business> accessed 14 April 2020)
[230] Article 1 in Protocol No. 1 of the European Convention on Human Rights; See also European Union Agency for Fundamental Rights, *EU Charter of Fundamental Rights, Article 17 – Right to property*, <https://fra.europa.eu/en/eu-charter/article/17-right-property> accessed 14 April 2020

of information.[231] This has been highly debated by the legal scholars. *Bronckers* and *McNelis* argue that trade secrets shall be interpreted in accordance with article 17 EU Charter, because the notion of 'possession' shall equal to trade secrets that represent a substantial financial value and shall obtain the same protection as under the EU Charter and EU Convention.[232] On contrary, *Alpin* state that because trade secrets do not fall under the protection of intellectual property in most of the MS, they are therefore unlikely to be classified as such in EU primary and secondary legislation. Therefore, the classification of trade secrets as intellectual property under the TRIPS Agreement is done in a broad sense by not requiring it to be given intellectual property protection *per se*.[233]

Until 2016 there was no harmonized legislation relating to the protection of trade secrets at the EU level. As a solution the TSD was adopted, which impose on the MS a minimal form of harmonization and uniformity on the notion of trade secret in accordance with existing internationally binding standards. TSD does not, however, provide an EU right in relation to trade secrets, because the directive needs to be transposed into the national law of each MS.[234] Furthermore, the TSD clearly confirms that trade secret is not a form of exclusive intellectual property right but is rather seen as complementary.[235] Thus, once the secret information is revealed, the holder of a trade secret cannot prevent competitors form copying or using the same solution, unless where the confidential information was obtained by illegitimate means.[236]

On the national level, the specific provisions on protection of trade secrets under Swedish law has since 1990 been primarily stated in the TSA. Thus, Sweden is the only country in the EU with *ad hoc* Act that specifically protects trade secrets.[237] In order to comply with the aim of the TSD, the Swedish Parliament has enacted a new TSA, which entered into force 1 of July 2018. The new TSA is a partial transposition of the TSD, however, with additional national measures, procedures and remedies due to article 6 (1) TSD. Furthermore, trade secrets are not

---

[231] European Commission, *Study on Trade Secrets and Confidential Business Information* (2013), MARKT/2011/128/D, April 2013, page 1

[232] Bronckers & McNelis (n 227), page 684-685

[233] Tanya F. Alpin, *Right to Property and Trade Secrets* (2014). C Geiger (ed) Research Handbook on Human Rights and Intellectual Property (Edward Elgar, 2015), chapter 22, page 428

[234] European IPR Helpdesk, *Trade secrets: An efficient tool for competitiveness* (2017), page 3 <https://www.iprhelpdesk.eu/sites/default/files/newsdocuments/Fact-Sheet-Trade-Secrets.pdf> accessed 19 April 2020; See further section 1.4 for the explanation of transposition of the directives into national law.

[235] European Commission, *Trade secrets*, Internal Market, Industry, Entrepreneurship and SMEs, <https://ec.europa.eu/growth/industry/policy/intellectual-property/trade-secrets_en> accessed 17 April 2020

[236] European Commission, *FAQ: Protection against the unlawful acquisition of undisclosed know-how and business information (trade secrets),* Internal Market, Industry, Entrepreneurship and SMEs, <https://ec.europa.eu/growth/industry/policy/intellectual-property/trade-secrets/faq_en> accessed 17 April 2020

[237] Pila & Torremans (n 105), page 514; See further Annex 5 for the collocation showing that Sweden is the only country in the EU with specific legislation covering trade secrets.

considered to be an intellectual property right under the TSA, making Sweden one amongst others that do recognize trade secrets as a 'possession' in accordance with article 17 EU Charter or by relying on the definition in article 39 TRIPS Agreement.[238]

4.2.2 Trade Secret Act: The scope of application

The new TSA aims at strengthening company's competitiveness and improving the conditions for innovation and knowledge-based entrepreneurship. Furthermore, the TSA introduces new requirements for trade secret protection so it more closely follow the definition set out in the TSD and further extends the scope of prohibited acts and strengthens the protection of confidentiality of trade secrets in trial.[239] Nevertheless, according to 4 § TSA, in compliance with article 1 (1) and 4 TSD, the legislation only applies to unlawful acquisition, use and disclosure of trade secrets.

In general terms, a trade secret is confidential information in the context of business, commerce or trade, but there exists, however, no precise definition on *what kind* of information may constitute a trade secret. This means that in practice, different kinds of information can be covered. According to the Government Bill (Prop. 2017/18:200) on TSA, the notion of information that can constitute a trade secret shall be interpreted widely and most closely coincide with terms in daily use.[240] Nevertheless, information can be of a technical nature, *inter alia* a manufacturing process, data processing methods, software and algorithms, and of an economical nature, *inter alia* patient lists and all data related to patients.[241]

Some guidelines to determine the notion of 'trade secret' has been incorporated into the 2 § TSA, which states that there has to be a *secret* that has a *commercial value* and the healthcare provider must have taken *active measures* to keep such information as a secret. However, 2 § and 4 § TSA, read in conjunction with recital 14 TSD, the definition of trade secrets excludes the experience and skills gained by the employees as well as information that can constitute a crime or a serious misconduct. Hence, in order to obtain protection, requirements set out in 2 § of the TSA must be fulfilled.[242]

---

[238] Magnus Toness, *The protection of trade secrets and know-how in Sweden – Swedish report*, (2012), AND Law Advokatfirma KB, page 2 <http://www.ligue.org/uploads/documents/cycle%202015/Cycle%202015/Rapports%20B/2015rapportsuedoisBnovembre2015.pdf> accessed 18 April 2020

[239] See 2 § TSA and article 2 (1) TSD, of what the notion 'trade secret' shall entail, where Swedish TSA fulfills the requirements of the TSD. See also 8 § TSA for the protection in trial.

[240] Prop. 2017/18:200 (n 222), page 26

[241] European Commission (n 237)

[242] Pila & Torremans (n 105), page 516

Firstly, as a general rule, the concept of the healthcare provider that wishes to protect the information as a trade secret, must consist of any natural or legal person who professionally conducts business of an economic nature. Even though not expressively defined in 2 § TSA, read in conjunction with the recital 1 TSD, it is assumed that the information has an actual or potential commercial value, which provide competitive advantages and contributes to the development of the company.[243] Secondly, the information must be a secret, i.e. not be generally known among, or is readily accessible to, persons within the circles that normally deal with this kind of information. However, absolute secrecy is not required, meaning that information can be kept as a trade secret by several parties, as long as it is not known to others working in the same field or generally known as it is being kept as a secret, *inter alia* patient list.[244]

This leads to a third requirement, where the healthcare provider must take reasonable steps to keep the information as a secret. This indicates the obligation to *actively* protect the information and it shall not suffice that other persons, e.g. business partners, understands or assumes that the information is intended to be kept as a secret. According to the Government Bill (Prop. 2017/18:200) on TSA, the degree of activity shall be assessed on a case-by-case basis.[245] Fourthly, where the attack, which consists of unlawful acquisition, use or disclosure, described in 3 § TSA, read in conjunction with recital 14 TSD, is likely to undermine the healthcare provider's ability to compete, such information is to be considered as having commercial value and thus is seen as a trade secret. According to Government Bill (Prop. 2017/18:200) on TSA, it is not required that the damage actually occurs when the information is disclosed, but it is sufficient that such disclosure potentially leads to certain damage.[246]

4.2.3 Artificial Intelligence algorithms protected as trade secrets in healthcare

As can be seen above, the scope of trade secret protection is broad and can in theory protect various types of software, data processing algorithms, additional technical information and knowledge thereto and potentially allows for the protection of data sets contained in AI.[247] *Hamilton* states that in medicine the publication of data concerning health is essential for clinical adoption of the final outcome. However, *Hamilton* points out that the publication

[243] Prop. 2017/18:200 (n 222), page 27–28; See further Recital 1 TSD
[244] Prop. 2017/18:200 (n 222), page 30-31
[245] Ibid, page 31
[246] Ibid, page 30
[247] European IPR Helpdesk (n 234), page 2; See also David A Prange and Alyssa N Lawson, *Re-evaluating companies' AI protection strategies*, (2018), Patents and Trade Secrets AI, page 37-38 <https://www.robinskaplan.com/-/media/pdfs/reevaluating-companies-ai-protection-strategies.pdf?fbclid=IwAR2WJvL2RQVbTn6asNGNIhOFG8anqI0DnDrLUD4pdKzl9l8Djd-bAPirIWY> accessed 21 April 2020

presents challenges for healthcare provider developing and using AI algorithms in solely ADM process, as they must decide of submitting a patent application or keep AI algorithms as a trade secret.[248] Hence, the question that arise is what pros and cons do trade secret protection entail in healthcare and why does healthcare provider choose to keep its AI algorithms used in solely ADM process as a trade secret?

To start with, as mention above, the software and its algorithms are valuable 'recipes' for healthcare provider.[249] In this regard, a trade secret protection is well-suited for the rapidly developing and changing marketplace of AI innovations, because healthcare provider often innovate too fast for patents to be meaningful.[250] Furthermore, trade secret protection is cost and time effective, because there are no official fees to pay, which in turn enables healthcare provider to gain immediate protection and reduce the investment loss that is otherwise incur form the application process, because it is normally protracted.[251] Consequently, trade secrets can be protected for an unlimited period of time, which makes the protection particularly attractive for small and medium-sized healthcare providers.[252]

Moreover, if trade secrets are used to protect AI algorithms in solely ADM, then new processing methods or other medical devices that are found using the same AI algorithm, are likely to be inventive to obtain patent protection. This in turn enables healthcare provider to evolve and compete on the market with the help of already existing AI algorithms.[253] Additionally, when information meets the requirements set out in 2 § TSA, especially when sufficient steps have

[248] Foley & Larnner LLP, *AI is here to stay: Are you prepared?,* (2019), page 6 <https://www.knowbe4.com/hubfs/AI%20is%20Here%20to%20Stay%20-%20Are%20You%20Prepared%20-%20April%202019%20Report%20by%20Foley%20&%20Lardner.pdf?fbclid=IwAR00tvUxAO_UEauoUCgBLVVOkwDU1Md-J1Tz6TMGhFuk0p3vTrpAUmRiQSQ> accessed 22 April 2020

[249] Stefan Larsson et al., *Sustainable AI – Inventory of the state of knowledge for ethical, social and legal challenges with artificial intelligence*, (2019), AI Sustainability Center, page 21 <http://www.aisustainability.org/wp-content/uploads/2019/03/Hallbar_AI.pdf?fbclid=IwAR3Bch2Fk7QVyfNYCyv1-M_FegCu0nDdWfhc-j7TV8pv1f9VCcz4dEZ2LlM> accessed 22 April 2020

[250] Erik Birkeneder, *Protecting Explainable AI Innovations in Health Care*, Forbes, (2019) <https://www.forbes.com/sites/erikbirkender/2019/11/19/protecting-explainable-ai-innovations-in-health-care/?fbclid=IwAR0aJX7ZuDzqf5wO1kjFmU1M-iljc2jXwwP3umeqZJlXj5-gp8Ygp9Sp6bo#20f616df5126> accessed 20 April 2020

[251] Prange and Lawson (n 247), page 38

[252] Recital 2 TSD; See also European IPR Helpdesk (n 234), page 4

[253] Niall McAlister and Roland Wiring, *AI in Life Sciences – Legal perspective on the opportunities and challenges of AI for life sciences companies*, (2019), page 13 <https://www.abhi.org.uk/media/2249/ai-in-life-sciences-and-healthcare-cms.pdf?fbclid=IwAR0C6mny9Y4sqeblOUiM8A0edjewM-gSS9afrOs5o71nKh82-fmMnFWHboo> accessed 23 April 2020

been taken to protect the information, the healthcare provider is entitled to apply for remedies and measures under TSA, in case where the information has been unlawfully disclosed.[254]

This leads to examination of the negative, however mostly important, aspect of trade secret protection within the healthcare. Firstly, since algorithms and data are non-rival goods, once they are revealed their value can be considerably reduced and no longer be protected, unless, as mentioned above, protected by patent law.[255] In this regard, *Birkeneder* states that patenting digital diagnostics can often feel like 'trying to stand on two ships passing in the sea'.[256] Secondly, the issue of transparency is at stake, because given the fact that AI innovations happen within the proverbial 'black box', it is often hard to determine when a competing healthcare provider is infringing claims that are directed towards features of the AI algorithms in question.[257]

Nevertheless, it can be difficult to keep the AI algorithms in solely ADM process as a trade secret, when 'meaningful information about the logic involved' in automated process and an explanation about the medical decision has to be given to the patient. This may lead to a situation where the protected information, when shared with the patient, can be seen as not having been subject to reasonable steps of secrecy and would render information as generally known or at least 'readily available' to others. In this regard, unless the patient is subject to a non-disclosure agreement[258] when the information is disclosed, the trade secret protection is lost and cannot be resumed, which render trade secret protection meaningless.[259]

4.3 A looming AI war: Secrecy versus transparency in healthcare

The questions of trust, safety and transparency are already on top of the list of issues that healthcare provider know that they have to deal with. Yet, by keeping proprietary information hidden is the only way for healthcare provider to be able to prevent unlawful use, disclosure or acquisition of the information in the rapidly developing and changing marketplace of AI innovations. But where legal or social standards require full transparency, how does a

[254] Prop. 2017/18:200 (n 222), page 21; In case of unlawful disclosure or use of trade secrets the new TSA, accordance with article 6 TSD, contains measures, procedures and remedies, *inter alia* damage liability under 5-10 §§ TSA; injunction and interim injunction under 12-16 §§ TSA; and fines and sentence under 26-28 §§ TSA.
[255] Agata Ferretti et al. (n 97), page 326
[256] Erik Birkeneder (n 250)
[257] Foley & Larnner LLP (n 248), page 6
[258] Non-disclosure agreement (NDA) is a legal contract that prohibit someone from sharing information deemed confidential.
[259] McAlister and Wiring (n 253), page 13

healthcare provider comply with the lawful processing while protecting it proprietary information? This has been put into spotlight for active discussions, not least by the WP29.

Fischer-Hüber et al. emphasize the need for transparency within the healthcare, when the patient is subject to solely ADM process. They state that in order to give meaningful result to the right to information self-determination, it is essential for the patient to have the possibility of 'information self-awareness'. This stresses out the importance of strengthening patient's rights by disclosing AI algorithms in automated processing, in order to be able to provide information for the patient in 'intelligible form'.[260] Furthermore, *Watcher et al.* fear that in practice, healthcare provider can avoid the transparency principle under the GDPR, by citing a need for trade secret protection. Thus, they emphasize the need for explaining the logic involved in solely ADM process and they also clarify the scope of an explanation of the systems functionality under the GDPR, which entails system's requirement specifications, decision trees, pre-defined models, criteria and classification structures.[261]

On contrary, *Kroll et al.* hold that by requiring transparency of the AI algorithms as well as inputs and outputs for the relevant decision taken, it is to be seen as a naive solution to the problem of confirming procedural regularity. They state that even if transparency is a helpful tool for many cases, it does not, however, provide accountability in all situations. Firstly, *Kroll et al.* hold that solely ADM process can use as inputs, or by creating an output, data concerning health that shall not be broadly shared with others in order to protect *inter alia* privacy of other patients. In this regard, *Kroll et al.* argue that this can lead to a disclosure that undermines fairness and efficiency.[262] Within the Swedish healthcare, specifically, disclosure of such data is barred or limited by Patient Safety Act (2010:659), where *inter alia* patient's medical records are only allowed to be read by the ones who are currently treating the patient and the patient himself.[263] Furthermore, *Kroll et al.* put an emphasis on the fact that because AI systems change over time, there is the added risk that the information disclosed is outdated by the time it is analyzed, e.g. information becomes inaccurate.[264]

---

[260] Simone Fischer-Hüber et al., *Online Privacy – Towards Informational Self-Determination on the Internet,* (2013), IOS Press, page 133 <http://ioanniskrontiris.de/publications/Krontiris2013c.pdf> accessed 23 April 2020
[261] Sandra Wachter et al. (n 125), page 85
[262] Joshua A. Kroll et al., *Accountable Algorithms*, (2017), Volume 165, University of Pennsylvania Law Review, page 657 - 658
[263] Ingemar Karlsson Gadea, *Professional Secrecy and Confidentiality*, 1177 Vårdguiden, <https://www.1177.se/en/other-languages/other-languages/regler-och-rattigheter---andra-sprak/tystnadsplikt-och-sekretess---andra-sprak/> accessed 21 April 2020; See Chapter 6, §§ 12-16 Swedish Patient Safety Act (2010:659)
[264] Joshua A. Kroll et al. (n 262), page 660

Furthermore, according to *Kroll et al.* and *Calpan et al.*, while transparency may be desirable in certain cases, widespread transparency comes with additional concerns. For instance, it can lead to a situation where the patient is 'gaming the system', or manipulating it, by using the meaningful information about the logic involved, received from a healthcare provider, to obtain own benefits.[265] This can be done *inter alia* by reporting particular symptoms that are more serious than they really are, because this will result in a particular (false) diagnose that will benefit the patient, whenever such information is processed by automated means, for instance to obtain coverage for healthcare service that would otherwise not be possible.[266] In this regard, *Morreim* states that gaming is morally and medically hazardous, because it can harm the society, offend honesty and violate fundamental principles in the healthcare.[267]

In this regard, *Eslami et al.* state that transparency needs to have the right level of specificity to enhance trust and satisfaction from the side of the patient. Explanations of final decision that are too vague or too specific can create feelings of unease and distrust. Therefore, *Eslami et al.* argue that more algorithmic transparency can result in algorithmic disillusionment, where algorithms appear more fallible and inaccurate, rather than powerful and useful. Thus, they hold that increased transparency in AI processing algorithms might not always result in an expected outcome, but rather in a negative consequence.[268] In a similar vein, *Ananny* and *Crawford* state that investments in transparency by AI developers in the domain of healthcare can be costly, while the effects and benefits remain unclear. Additionally, they state that transparency can have an opposite effect, because it may thwart the notion of 'understanding' or create false dichotomies.[269]

Another issue is to interpret the notion of 'meaningful information about the logic involved' in solely ADM. According to *Malgieri* and *Comandé*, the 'logic involved' can be considered as a mathematical concept that can only be explained in technical terms. But in order for healthcare provider to give 'meaningful' information, it would require more than just the functionality of the algorithms, but also information about its contextual use, expected and actual impact,

---

[265] Joshua A. Kroll et al. (n 262), page 658; Robyn Calpan et al. (n 219), page 7; See also Nicholas Diakopoulos, *Accountability in Algorithmic Decision Making,* (2016), Volume 59, Issue 2, Communications of the ACM, page 58

[266] David A. Shore, *The trust prescription for healthcare: Building your reputation with consumer*, Health Administration Press, Chicago, IL, 2005, page 43

[267] E. Haavi Morreim, *Gaming the system - Dodging the rules, Ruling the dodgers*, Arch Intern Med. 1991, page 443-447

[268] Motahhare Eslami et al., *Communicating Algorithmic Process in Online Behavioral Advertising*, (2018), Paper Number 432, page 9 <https://dl.acm.org/doi/pdf/10.1145/3173574.3174006> accessed 23 April 2020

[269] Mike Ananny and Kate Crawford, *Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability*, (2016), New Media & Society, page 8-9; See also Heike Felzmann et al. (n 11), page 8

rationales and purposes.[270] As has already been held by several legal scholars and WP29, the notion of 'meaningful information about the logic involved' must be evaluated form the perspective of the patient, which according to recitals 39 and 58 GDPR must be 'easy to understand'.[271] Thus, because the patient in most cases lacks interest or technical skills in understanding these mathematical concepts, mathematical concepts of AI algorithm is not to be considered as 'meaningful'.[272] In this regard, even though the rationale and criteria behind the automated decision shall be provided to the patient, there is, however, no necessity for the healthcare provider to reveal its AI algorithms used in ADM process.[273]

Following the arguments presented above, *Diakopolous* have found a number of elements of the algorithmic process that can be disclosed without touching upon the trade secret protection. Firstly, *Diakopolous* states that the information on human involvement is highly important, which might include *inter alia* explaining the goal, purpose and intent of the algorithm, including editorial goals and the human editorial process. Secondly, *Diakopolous* holds that one avenue for transparency is to communicate the quality of the data concerning health, for instance information on its accuracy, completeness and uncertainty. Thirdly, the model and variables of the algorithm is an important aspect, which shows the data used by an AI algorithm in solely ADM process in order to produce an output. And lastly, the inferencing, including the margin of error predicted, as well as the information on whether an algorithm was actually used can be disclosed in order to provide transparency for the patient.[274]

As can be seen above, it can be confirmed that obliging a healthcare provider to disclose its algorithms that are protected by trade secrets is not required to prove transparency. However, not all of the information can be refused to the patient because of the trade secret protection. According to recital 63 GDPR, the patient has the right to have access to the information about the logic involved as well as the consequence of such processing, that shall be disclosed to the patient pursuant to articles 13-15 GDPR.[275] Yet, recital 63 GDPR also recognizes that such disclosure 'shall not affect the rights or freedoms of others, including *trade secrets* […]', but the right to trade secret protection shall 'not be a *refusal* to provide *all* information' to the

[270] Malgieri and Comandé, (n 166), page 265
[271] WP29 (n 113), page 25; Kuner et al. (n 165), page 20; Selbst and Powels (n 165), page 236; See further Recitals 39 and 58 GDPR
[272] Dimitra Kamarinou et al. (n 167), page 20; See also WP29 (n 113), page 25
[273] See section 3.4.3 for the discussion on this topic. See also WP29 (n 113), page 14, where the WP29 underlines that the patient is entitled to, in such situation, recognition of a legitimate interest in asking an expert to analyze the algorithms in order to better challenge the decision. This would otherwise be contrary to EU Charter and EU Convention.
[274] Nicholas Diakopoulos (n 265), page 60-61
[275] Recital 63 GDPR; See also Agata Ferretti et al. (n 97), page 327

patient.[276] In this regard, the WP29 in its guidelines on ADM and profiling somewhat end the trade secret loophole to algorithmic transparency. The guidelines explain, by reference to recital 63 GDPR, that while there is some protection against having to reveal trade secrets, healthcare provider cannot rely on the trade secret rights as an excuse to deny access or refuse to provide *all* the information to the patient.[277] While this does not eliminate the trade secret exception in recital 63 GDPR, it does, however, aim at prohibiting the use of overly broad trade secret claims.[278]

As a guideline, the WP29 set forth in its 'good practice recommendations' what information is to be provided, while keeping AI algorithms as trade secret. The WP29 hold that instead of providing a complex mathematical explanation of the processing method, the healthcare provider shall instead consider delivering the information mainly relating to the *categories of data used*, the *source of the data* and *why* this data is considered relevant.[279] Thus, according to WP29, the relevance of the information of the data processed is more important for complying with the transparency requirement and is generally more relevant and meaningful for the patient.[280] Yet, the WP29 does not exclude the disclosure of detailed technical description about how an AI or ML algorithm works when needed.[281]

4.4 Conclusion

After the examination above, based on the commentaries from legal scholars and WP29, the most reasonable solution for the healthcare provider is to rely on the wording of 'meaningful information', in the sense of it being 'understandable' for the patient. Thus, while technical details or mathematical concepts of how an automated AI algorithm comes to a medical decision when processing data concerning health can constitute '*information* about the *logic involved*' described in articles 13-15 GDPR, the same information is not seen as 'meaningful' from the perspective of the patient.

In this regard, the demarcation between 'information' and '*meaningful* information' is crucial, which enables healthcare provider to keep its ADM AI algorithms as trade secrets, while complying with the transparency requirements under articles 13-15 as well as article 22 GDPR.

[276] Recital 63 GDPR
[277] WP29 (n 113), page 17
[278] Margot E. Kaminski (n 122), page 203; This is also emphasized in recitals 34 and 35 TDS, which state that trade secrets shall respect the right to protection of personal data. This is discussed in the next chapter.
[279] However, by reference to recital 58 GDPR, the WP29 hold that complexity is no excuse for disclosing of detailed technical description about how an AI or ML algorithm works.
[280] WP29 (n 113), page 31
[281] Ibid, page 28

However, while WP29 confirms the above described line of reasoning, it also makes it clear, however, by referring to recital 63 GDPR, that trade secret protection cannot form the base for refusing to provide all of the necessary information to the patient, which enable the patient to understand the reasoning of the medical decision taken against him.

Yet, so far, the conflict between the right to a transparent processing of data concerning health and trade secret protection remains, somewhat, unclear. In this regard, by taking a closer look at the legislative framework as well as examining practical solutions proposed by legal scholars, the thesis attempts to find a possibility for reconciling the rights in conflict. Thus, the next chapter examines the balance between GDPR and TSD, read in conjunction with the Swedish legislation, together with the opinions of legal scholars as well as theories and techniques in the application of AI technology in practice.

5. Striking a balance: Towards an AI-supported healthcare

5.1 Introduction

To this point, the following can be confirmed: even though the GDPR does not denote a ban on solely ADM AI algorithms when processing patient's data concerning health, whereas both the patient and healthcare provider can rely on the wording of '*meaningful* information' of the logic involved in ADM process in the sense of it being 'understandable' from the point of view of the patient, the GDPR does, however, confirm that trade secret rights cannot be relied upon by the healthcare provider to refuse to provide *all* of the information.

Consequently, when *all* of the 'meaningful information' cannot be given without healthcare provider risking revealing some of the precious AI algorithms protected by trade secrets, the question thus arises – which of the conflicting right prevails? Even though there exist balancing recitals that regulate the conflict in both GDPR and TSD, they do not, however, form a clear hierarchy. So far, the thesis has provided a wide theoretical discussion on the balancing of rights in conflict within healthcare, it is thus highly relevant to in depth examine the legislative framework at hand and consider practical attempts in reconciling these rights.

5.2 Balancing act between trade secrets and data protection

5.2.1 The imbalance of the balancing recitals

In order to find the balance, the balancing recitals contained in both GDPR and TSD must be examined. In particular, recital 34 TSD states that the directive respects fundamental rights and observes the principles set out in the EU Charter, notably 'the right to respect for private and family life, the right to *protection of personal*, […] freedom to *conduct business*, the right to property, […] while respecting *business secrecy* […]'.[282] Furthermore, recital 35 TSD states that it is important that especially the right for private and family life as well as the right to protection of personal data of any person, whose personal data may be processed, must be respected when healthcare provider takes steps to protect the information as a trade secret.[283]

From the above-quoted recitals, it seems that in case of a conflict between patient's data protection rights and healthcare provider's right to trade secrets, the patient's privacy rights shall prevail. However, this conclusion is not so clear. A corresponding meaning is given in the

[282] Recital 34 TSD
[283] Recital 35 TSD

already mentioned recital 63 GDPR, as regards the right to access the information, which states the patient;

> '[…] should have the right of access to personal data which have been collected concerning him or her, […] including the right to have access to data concerning their health[284], […] and to have the right to know and obtain *communication* […] about the *logic involved* in any automatic personal data processing and, […] the *consequences* of such processing. That right should *not adversely affect* the rights or freedoms of others, including *trade secrets* […]. However, the result of such considerations should not be a refusal to provide *all* information to the patient'.[285]

As already mentioned, the WP29 and *Wachter et al.* have explained that the right to access, stemming from article 15 GDPR, requires limited disclosure of the 'logic involved' in ADM process, primarily concerning its functionality rather than an explanation of *specific* decisions, because it would otherwise adversely affect trade secrets.[286] This line of reasoning is also confirmed by *Ferretti et al.*, that holds that even if the healthcare provider may be required to provide information regarding the general characteristics of its systems, it may not, however, be obliged to explain what rules the AI system follows, how it came to a conclusion, or how it has taken an exact decision about a specific patient.[287] Yet, as mentioned in previous chapter, the WP29 has also concluded that healthcare provider cannot maintain complete silence by relying on the trade secret rights as an excuse to deny access or refuse to provide *all* the information to the patient.[288]

However, another interesting balancing recital that indirectly touches upon the balance between the rights in conflict is recital 73 GDPR, which is also entailed in the regulation itself, namely in article 23 (1) GDPR. As already mentioned, the GDPR is directly applicable as the Swedish law, meaning that healthcare provider must comply with the provisions contained in the GDPR and the complementary Swedish legislation, in case they are compatible with the regulation.[289] In this regard, article 23 (1) GDPR, read in conjunction with the recital 73 GDPR, provides a possibility for MS to impose restrictions concerning specific principles and rights, for instance

[284] For example, the data in their medical records containing information such as diagnoses, examination results, assessments by treating physicians and any treatment or interventions provided, see Recital 63 GDPR
[285] Recital 63 GDPR (emphasis added)
[286] WP29 (n 113), page 27; Sandra Wachter et al. (n 125), page 83; See further Judgment of the German Federal Court in case *SCHUFA* (n 175)
[287] Agata Ferretti et al. (n 97), page 327
[288] See section 4.3 in the thesis; See also WP29 (n 113), page 17
[289] See section 1.4 in the thesis for the description of the relationship between EU law and Swedish national law.

'restrictions concerning the *rights of information*, *access to* […] as far as necessary and proportionate in a democratic society to safeguard […] the protection of *the rights and freedoms of others'*.[290] Due to the fact that neither article 23 (1) GDPR nor recital 73 GDPR describes the meaning of 'rights and freedoms of *others'*, it can be assumed that the healthcare providers rights, in keeping its AI algorithms used in ADM process as a secrets, are covered.

These restrictions, which are now contained in 5 c. 1 § DPA[291], provide that the rights to information and the right of access under articles 13-15 GDPR, do not apply to the information that may not be provided pursuant to law or other statues, or by a decision that has been issued under the same statute.[292] The Government Bill (Prop. 2017/18:105) on DPA states that it is permissible to provide for exceptions on the data protection rights to ensure the enforcement of civil law requirements and with regard to the legitimate need of private companies to keep information confidential to protect its own interests.[293] Nevertheless, it concludes that such restrictions respect fundamental rights and freedoms and are necessary and proportionate in a democratic society, which is required by article 23 (1) GDPR.[294]

In this regard, it is probable that the healthcare provider can avoid conveying information on and providing access to the logic involved in the automated processing, e.g. functionality or a full description of the AI algorithm, when processing data concerning health, because such information must be subject to reasonable steps taken to keep it confidential in order for it to be lawfully protected under 2 § TSA.[295] Otherwise, as mentioned in previous chapter, since algorithms and data are non-rival goods, once they are revealed their value can be considerably reduced and no longer be protected, which render trade secret protection meaningless. Yet, as mentioned previously, according to the Government Bill (Prop. 2017/18:200) on TSA, the degree of activity shall be assessed on a case-by-case basis.[296]

---

[290] See Recital 73 GDPR and Article 23 (1) (i) GDPR
[291] Restrictions in the new DPA (2018:218) stem from 27 § of the old Data Protection Act (1998:204)
[292] Prop. 2017/18:105, *New Data Protection Act*, (2018), page 106 <https://www.regeringen.se/492373/contentassets/561c615d11104ad38c42b59cda9c33bc/ny-dataskyddslag-prop.-201718105> accessed 27 April 2020
[293] Ibid, page 107
[294] Prop. 2017/18:105 (n 292), page 107
[295] In the Government's Bill (Prop. 2017/18:105) the restrictions apply to information which would otherwise be protected by secrecy and confidentiality under the Public Access to Information and Secrecy Act (2009:400), which also cover private healthcare entities. These restrictions cover situation *inter alia* where information collected before a judicial process, if it can be assumed that disclosure of the information in question would impair the position of the data controller as a party in the trial. However, the author of this thesis took a different view, by focusing on the information about the *systems functionality*, e.g. meaningful information about the logic involved of automated processing, and not the personal information that may be protected by professional secrecy where a disclosure of such would lead to sufficient harm for the patient in question.
[296] See section 4.2.2 for the description of protection of trade secrets under the TSA

Consequently, while the patient has the right to receive the information containing its own personal data according to 5 c. 4 and 5 §§ Patient Data Act (2008:355) and article 20 GDPR[297], which the patient voluntarily supplied to the healthcare provider, the additional information, *inter alia* the logic involved in the automated processing, can be kept as a secret without healthcare provider risking of violating the transparency requirements under the GDPR. This is because such additional information needs to be protected pursuant to law, e.g. TSA, referred to in 5 c. 1 § DPA. Similar interpretation has been conducted by the Confederation of Swedish Enterprise, which states that the national restrictions mean that the notion of '*all* information', contained in recital 63 GDPR, can be escaped by the healthcare provider under situations supported by law, e.g. TSA, in order to protect its own rights and freedoms.[298]

Nevertheless, taking a closer look at the supplementary Swedish healthcare legislation, the following can be identified; while 8 c. 6 § Patient Data Act (2008:455) refers to additional requirements on what the healthcare provider shall present to the patient in addition to articles 13-14 GDPR, the Act does not, however, introduce any of the national restrictions on the patient's information and access rights.[299] Neither does the Act refer to the patient's right of access under article 15 GDPR, meaning that the patient can access the meaningful information about the logic involved in ADM upon the request. This indicates some possibility on the side of the legislator of accepting prevalence of healthcare provider's economic interest when patient's data protection rights are at stake.

In this regard, according to *Bergkamp*, even though national restrictions are necessary, these are at least not proportionate. *Bergkamp* holds that because privacy is so fundamental, *inter alia* inalienable and priceless, especially when processing data concerning health by automated means in healthcare, privacy protection should be absolute and non-waivable. Thus, *Bergkamp* argue that even if there is a need to protect economic interests of the healthcare provider, the protection of privacy cannot be waived in any manner.[300] Nevertheless, *Ferretti et al.* argue that, in the medical context, restricting providence of information other than being legally binding, may affect the fundamental rights of the patient and principle of transparency linked

[297] See 5 c. 5 § Patient Data Act (2008:355) and Article 20 GDPR 'right to data portability'.
[298] Confederation of Swedish Enterprise, *Questions and answers regarding General Data Protection Regulation and labour law*, (2018), page 42 <https://www.grona.org/siteassets/medlemskap/gdpr/qa-dataskydd_webb.pdf> accessed 16 May 2020
[299] According to article 23 (1) GDPR, MS may restrict by way of legislative measures the scope of right and obligations. Thus, the national legislation is not obliged to introduce such restrictions.
[300] Lucas Bergkamp, *EU Data Protection Policy: The privacy fallacy: Adverse effects of Europe's data protection policy in an information-driven economy*, (2002) Volume 18, Issue 1, Computer Law & Security Review, page 33-34. In his article *Bergkamp* focuses on the perspective of strong consumer protection when these rights conflict with the economic interest of both public and private entities.

thereto in an unduly manner. As a consequence, this will hinder patient's trust in the healthcare provider treating the patient as well as in the use of AI systems for the medical purposes.[301]

Considering the above, *Malgieri* proposes a solution of 'de-contextualization' to all of the above described issues, e.g. total refusal of providing all of the information to the patient; the need for necessity and proportionality to restrict patient's rights by national legislation; and the 'adverse effect' requirement contained in the recital 63 GDPR. This solution means that if the healthcare provider discloses a part of the information protected by trade secrets, such disclosure will not adversely affect trade secret *per se* and allow healthcare provider to comply with the transparency requirements under the GDPR. This conclusion is based on the fact that trade secrets are generally information taken as a whole and not just partly, *inter alia* information that can easily be attributed to another patient's personal data or identity or the full description of the AI algorithm used in solely ADM process.[302] Yet, *Malgieri* states that in case where de-contextualization is impossible, such situation shall be resolved on a case-by-case basis.[303]

The proposed solution of 'de-contextualization' stems from the proportionality requirements contained in both recital 4 GDPR and recital 21 TSD. Nevertheless, this solution is compliable with the notion of 'meaningful information about the logic involved' that must be provided to the patient, because the healthcare provider is able to select information depending on what it considers to be a meaningful one from the perspective of the patient. However, due to the lack of guidance from the national perspective, the question of application of national restrictions, when it comes to the rights in conflict, remains open for interpretation.

5.2.2 The legislative 'favor' for the data protection rights

After the overview of the balancing recitals contained in GDPR and TSD as well as restricting national measures, it is still quite confusing to find a balance between the rights in conflict. As *Malgieri* puts it 'European law proves to be schizophrenic'.[304] On the one hand, it can be confirmed that the protection of trade secrets prevails over the patient's rights under the GDPR, which appears to be presented by the the national restrictions enshrined in the supplementary Swedish DPA. On contrary, the prevalence of data protection rights on trade secrets is also confirmed, where the rights of the patient can never be overruled by an economic interest of

[301] Agata Ferretti et al. (n 97), page 327
[302] Gianclaudio Malgieri (n 224), page 107
[303] Gianclaudio Malgieri, *Decontextualization data sharing at the borderlines between Trade Secrets and Data Protection Rules*, (2015), SSRN Electronical Journal, 10.2139, page 52-53
[304] Gianclaudio Malgieri (n 224), page 104

the healthcare provider. Yet, a particular hierarchy can be extracted when linguistic and teleological interpretation of the legislation is being conducted.

When paying closer attention to the above-quoted balancing recitals of GDPR and TSD, a significant difference can be confirmed. Recital 63 GDPR state that the data protection rights 'must not *adversely* affect' trade secrets, whereas recital 35 TSD states that trade secret protection 'should not affect' data protection rights. Thus, the adverb 'adversely' indicates that whereas the application of data protection law can permit a disapplication of trade secret law as such, the latter can never require the disapplication of privacy rules.[305] This conclusion is also confirmed by the additional specification set out in recital 63 GDPR, which states that 'the result of these considerations should not be a refusal to provide *all* information' to the patient.[306]

In this regard, *Malgieri* holds that interpretation of the national restrictions, e.g. set out in 5 c. 1 § DPA (2018:218), which are allowed according to article 23 (1) GDPR, shall follow the path of reasoning described above.[307] Such interpretation is most likely to coincide with the aim of the supplementary Swedish healthcare legislation, which has since decades ago strong rules on protection of patient's personal integrity.[308] To be able to exercise self-determination and be able to choose and act independently, the patient must be well informed and be able to understand the information and reasons behind a medical decision or a way of treatment. Consequently, by limiting patient's rights in order to protect trade secrets, the patient's autonomy and the free will of choice can quickly become an illusion, because the patient is in a state of dependence where the healthcare provider has a margin of discretion to choose what shall be disclosed to the patient in order to protect its own interests.[309]

Additionally, recital 63 GDPR addresses the protection of the healthcare provider *only* in relation to the right of access.[310] According to *Malgieri* and *Comandé*, such reference leaves a loophole for the benefit of the patient to argue that even if trade secret rights can limit the access right under article 15 GDPR, the same recital cannot, however, in any case limit or restrict the notification obligations set out in articles 13-14 and additional safeguards under article 22 (3) and recital 71 GDPR.[311] Nevertheless, following the linguistic interpretation conducted above, *Malgieri* and *Comandé* state that in case where the right of access adversely affect the protection

[305] Gianclaudio Malgieri (n 224), page 104
[306] Recital 63 GDPR
[307] Gianclaudio Malgieri (n 224), page 106
[308] See 2 a § point 3 Health and Medical Services Act (SFS 1982:763)
[309] Simone Fischer-Hüber et al. (n 260) also emphasize the importance of self-determination.
[310] WP29 (n 113), page 17
[311] Malgieri and Comandé (n 166), page 263

of trade secrets, the right of access can be limited, but 'never totally denied'.[312] Thus, considering the preference for the data protection rights, *Malgieri* and *Comandé* conclude that the right of access to meaningful information about the logic involved in ADM process must be guaranteed as much as possible. [313]

In this regard, *Selbst* and *Powels* state that there is no justification for treating trade secret restrictions as 'axiomatic'[314], where the patient's rights in obtaining the logic involved in ADM process or obtaining an explanation of the decision taken against him/her must not be heavily curtailed to protect the interest of healthcare provider in in keeping its AI algorithms as a secret.[315] This is also confirmed by the opinion of the European Data Protection Supervisor *Peter Hustinx*, which states that the balancing recitals as well as articles on the balancing of rights contained in GDPR and TSA, delimit considerably the possibility to restrict patient's rights to data protection when its personal data is being processed by automated means.[316]

In conclusion, when comparing the balancing recitals of the GDPR with the TSD, as well as looking at the Swedish healthcare legislation, a preference for the data protection rights can be found. It might also seem obvious that in the healthcare domain, the right of the patient to receive meaningful information about the automated process and the reasoning behind the decision made by such processing based on the data concerning health must outweigh other protection rights, because after all the patient's health and wealthiness is at stake. However, it remains to be seen to what extent the healthcare provider will be able to rely on the trade secrets protection in order to limit their transparency obligations under the GDPR.

5.3 Other practical and theoretical solutions

5.3.1 Introduction

As has been presented throughout this thesis, solely ADM using AI algorithms can open new pathways to Swedish healthcare. Yet, if the doctors or patients lack understanding why or how such system has made a specific medical prediction, issues may arise on how much confidence to have in such systems, particularly in case where automated decisions can have a life-altering

[312] Malgieri and Comandé (n 166), page 263
[313] Ibid, page 264
[314] The notion of 'axiomatic' taken for granted or self-evident.
[315] Selbst and Powels (n 165), page 242
[316] Peter Hustinx, *Opinion of the European Data Protection Supervisor on the data protection reform package*, (2012), European Data Protection Supervisor, page 4 (21-22 §§) <https://edps.europa.eu/sites/edp/files/publication/12-03-07_edps_reform_package_en.pdf> accessed 5 May 2020

effects.[317] Even though healthcare provider can benefit from the opaqueness of AI algorithms, the 'black box' characteristic is one of the most worrying obstacles of complying with the transparency under the GDPR. As mentioned previously, the WP29 point out that the principle of transparency requires healthcare provider to explain the automated decision in an easily and understandable manner, but the complexity of AI algorithms cannot, however, be used as an excuse to avoid providing all the necessary information to the patient.[318] Yet, how can a balance be struck between these rights in conflict and is it somehow even possible to do so?

Edwards and *Veale* point out that GDPR have already introduced a number of new provisions, *inter alia* article 35 GDPR on DPIA, as an attempt to create an environment in which less 'toxic' solely ADM AI systems must be built.[319] This means that healthcare provider shall be able to assess the risks on patient's fundamental rights and freedoms prior to automated processing of data concerning health and understand and explain how such decisions are being reached. This stems from the long-existing evolution of 'privacy-by-design', e.g. a way of building 'privacy-aware' or 'privacy-friendly' systems.[320] However, as mentioned previously, explaining the logic about the system in ADM can substantially affects healthcare provider's trade secrets. Thus, in order to reconcile both interests, theoretical and practical solutions have been proposed, which are presented below.

5.3.2 Counterfactual explanations of individual automated decision

Achieving transparency and fairness of AI algorithms, their training data sets and clinical decisions that they produce, is an open issue. Due to the pressure from the regulators and the society, new approaches are being introduced by researchers and practitioners, either by theoretical considerations or new algorithms.[321] An interesting discussion on the balancing of rights has been conducted by *Watcher et al.*, where they present a method for 'counterfactual explanations' that may exhibit transparency in solely ADM process in accordance with the GDPR, without opening the 'black box' of the AI algorithms.[322] They state that, even though

[317] The Royal Society, *Explainable AI: the basics*, (2019), page 18 <https://royalsociety.org/-/media/policy/projects/explainable-ai/AI-and-interpretability-policy-briefing.pdf> accessed 8 May 2020; See further Davide Castelvecchi, *Can we open the black box of AI?*, (2016), Volume 538, Macmillan Publishers Limited, page 22-23; See also Agata Ferretti et al. (n 97), page 325

[318] See section 4.3 for the reasoning of the WP29.

[319] See also articles 25 on 'Data protection by design and by default' and 37 GDPR on 'Designation of the data protection officer'

[320] Lilian Edwards and Michael Veale, *Slave to the algorithm? Why a 'right to an explanation' is probably not the remedy you are looking for*, (2017), Volume 16, Issue 1, Duke Law & Technology Review, page 77

[321] Kacper Sokol and Peter Flach, *Counterfactual explanations of machine learning predictions: Opportunities and challenges for AI safety*, (2019), Volume 2301, CEUR Workshop Proceedings, page 1–2

[322] Sandra Watcher et al., *Counterfactual explanations without opening the black box: automated decisions and the GDPR*, (2018), Volume 31, Issue 2, Harvard Journal of Law & Technology, page 5

transparency is of a big importance and should be followed, it does not, however, mean that the patient concerned by the decision must understand how an AI algorithm operates. They state that by seeing explanations as a way of helping the patient to 'act', e.g. according to article 22 (3) GDPR, rather than only understanding the decision, the scope of explanation can be evaluated according to the specific goal or action that they are aimed to support.[323]

Accordingly, *Watcher et al.* propose three ways for achieving counterfactual explanations: firstly, informing and helping the patient to understand why a specific decision was achieved; secondly, providing grounds to contest dismissive decisions; and thirdly, helping the patient to understand what could be changed to obtain an anticipated result in the future, based on the current AI model.[324] Thus, 'counterfactual explanations' instead surfaces examples from the training set, learning on the patients interpretation of those examples, instead of explaining how an AI algorithm produces a particular output. Due to the fact that such examples are often used among humans, it can thus be more effective in explaining complex concepts.[325] In addition, *Watcher et al.* hold that even though the GDPR offers little support to accomplish any of these aims, it does not, however, hinge on explaining the internal logic of automated processing.[326]

In this regard, *Zafar et al.* state that counterfactual explanations are helpful in picking up unfair system behavior (disparate impact) and undue mistreatment of individuals (disparate treatment), which is of highly importance within the healthcare. Due to their short and easily understandable structure, such explanations are helpful tools in identifying errors in the underlying predative models.[327] Furthermore, *Sokol* and *Flach* confirm the already mentioned advantages and further add that counterfactual explanations can be actionable, interactive and carried out in a clear and plain language. Yet, there is a risk of having a detrimental effect on safety of an AI system by producing indirect harm to the patients in question, if wrong counterfactuals are picked. This risk depends on to the difficulty in determining the degree of importance in each of them.[328] However, it remains to be seen if 'counterfactual explanation' can be used within the healthcare domain.

---

[323] Sandra Watcher et al. (n 322), page 4
[324] Ibid, page 5
[325] Carrie J. Cai et al., *The Effects of Example-Based Explanations in a Machine Learning Interface*, (2019) page 258-259 <https://dl.acm.org/doi/pdf/10.1145/3301275.3302289> accessed 10 May 2020
[326] Sandra Watcher et al. (n 322), page 4
[327] Muhammad Bilal Zafar et al., *Fairness beyond disparate treatment & disparate impact: Learning classification without disparate mistreatment*, (2017), Proceedings of the 26th International Conference on World Wide Web, page 1171 <https://dl.acm.org/doi/pdf/10.1145/3038912.3052660> accessed 10 May 2020
[328] Sokol and Flach (n 321), page 2-3

5.3.3 Improving healthcare with visualization techniques

> *'Most people don't need to know every detail of how a study was conducted; they need quick, actionable takeaways. That's where data visualization can help. Data visualization brings the most important takeaways in the health industry into focus, helps identify patterns and correlations, and makes data analysis more efficient.*[329]

As already mentioned, the goal of transparency principle in ADM is to enable the patient to receive meaningful information about the logic involved in the decision making process, where such information shall be given in an easily accessible manner, easily understandable and in a clear and plain language, as required under article 12 (1) GDPR. Importantly, the principle of transparency is not limited to the oral or written communication of information. In this regard, WP29 holds that healthcare provider may use visualization techniques to aid algorithmic transparency, *inter alia* by creating images, diagrams or animations to communicate the logic about automated medical decision.[330]

By redesigning the means under which the information is given, allows the patient to better understand why certain recommendation or decision has been made and ultimately increase their informational self-determination.[331] In this regard, *Zhang et al.* hold that visualization techniques are of special importance within the healthcare, because they can *inter alia* help revealing data quality problems, e.g. diagnosing error, by removing human error in a highly risky environment and thus increasing patient safety; enable patient to better understand the reasoning behind certain medical decision or recommendation made by automated means; address the challenges of dealing with low-literacy populations and speakers of diverse languages; and improve satisfaction and health outcomes.[332]

---

[329] Erin McCoy, *How Data Visualization is transforming the health care industry*, (2019), Modus, <https://modus.medium.com/how-data-visualization-is-transforming-the-healthcare-industry-6761d7293dd2> accessed 13 May 2020

[330] WP29 (n 149), page 25; See further Killer Visual Strategies, *How a motion graphic on vaccines generated over 1 million views*, <https://killervisualstrategies.com/project/motion-graphic-the-history-of-vaccines> accessed 13 May 2020. This is an example on how visualization works, e.g. a motion graphic on history of vaccines. It shares some of the fundamental information about the work of vaccines in an understandable manner in order for the average persons to comprehend it, without revealing its inner 'informational secrecy'.

[331] Elizabeth Denham, *Big data, artificial intelligence, machine learning and data protection*, (2017), Version 2.2, Information Commissioner's Office, page 88 <https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf> accessed 15 May 2020

[332] Yiye Zhang et al., *Paving the COWpath: Learning and visualizing clinical pathways from electronic health record data*, (2015), Volume 58, Journal of Biomedical Informatics, page 192-195; See also Ben Shneiderman and Catherine Pkaisant, *Improving healthcare with interactive visualization*, (2013), Volume 46, Issue 5, IEEE, page 61-63

While visualization techniques allow healthcare provider to better fulfill its transparency obligations, it also allows them to protect its AI algorithms used in ADM as a trade secret by not disclosing the processing mechanism *per se*. For instance, the anamnesis of the patient includes *inter alia* current symptoms, history of illness, previous treatments and current medications, where the healthcare provider based on this information follow through a medical diagnostics chain that eventually includes a description of the treatment outcomes. Because patients often have a complex anamnesis, visualization can in such case present a picture that captures all health conditions of the past and present as a simple overview.[333] This enables the patient to see how a specific diagnosis was reached, as well as it enables healthcare physicians to learn from the outcomes.[334]

5.3.4 Explainable AI: Reaching consistency behind a diagnosis

As can be seen, in the medical domain there is a growing call in AI approaches, that are especially trustworthy, transparent, interpretable and explainable.[335] In this regard, explainable AI (XAI) is rapidly emerging by healthcare innovators that actually reveal the logic behind diagnoses. According to *Grégoire et al.*, in the context of XAI, the notion of 'understanding' usually means a 'functional understanding' of the system, in contrast to a low-level algorithmic understanding of it.[336] Thus, XAI aims at finding and characterize the performance of the 'black-box' system, without trying to reveal its inner working or its internal representations.[337] In this regard, whereas explainable algorithms provide some justification for their results, the training data and further technical details can generally be kept as a trade secret. This makes the investment in XAI diagnostics a very feasible opportunity.[338]

The first attempt in trying to create a more explainable AI is the U.S. Defense Advanced Research Projects Agency (DARPA).[339] According to DARPA, the XAI program aims to create

---

[333] Zhiyuan Zhang et al., *AnamneVis: A framwork for the visualization of patient history and medical diagnostics chain*, (2011), Proceedings of the IEEE VisWeek Workshop on Visual Analytics in Healthcare, page 1 <https://pdfs.semanticscholar.org/d9db/57f8bb04f723aa94d16a7ea7015529cb150d.pdf> accessed 16 May 2020

[334] Goutham Rao et al., *Identifying, Analyzing, and Visualizing diagnostic paths for patients with nonspecific abdominal pain*, (2018), Volume 94, Applied Clinical Informatics, page 909

[335] Carolina Wahlby, *Methods development for extracting relevant data for use in AI/ML*, (2019), Stockholm Life Science AI/ML Guide – Shaping the future of healthcare intelligently, page 9 <https://www.investstockholm.com/globalassets/invest/reports/stockholm-ai-report.pdf> accessed 16 May 2020

[336] Andreas Holzinger et al. (n 15), page 3

[337] Grégoire Montavon et al., *Methods for interpreting and understanding Deep Neural Networks*, (2018), Volume 73, Digital Signal Processing, page 2

[338] Erik Birkeneder (n 250)

[339] Broad Agency Announcement, *Explainable Artificial Intelligence (XAI),* (2016), Defense Advanced Research Projects Agency (DARPA), Information Innovation Office, page 5-6 <https://www.darpa.mil/attachments/DARPA-BAA-16-53.pdf> accessed 16 May 2020

a set of ML techniques that is, firstly, able to produce more explainable models, while keeping a high level of learning function (prediction accuracy), and, secondly, enabling both healthcare providers and patients to understand and appropriately trust the decisions made by solely ADM AI systems.[340] Thus, new AI systems will be able to explain the logic behind every decision, exemplify their strengths and weaknesses, and express an understanding of how they can/will behave in the future.[341] In this regard, *Holzinger et al.* emphasize the urgent need for XAI across the healthcare domain, in order to facilitate confidence, safety, security, privacy, ethics, fairness and trust.[342] All these aspects are important under the GDPR and XAI will be able to fulfill many of them.

5.4 Conclusion

In conclusion, when examining the balancing recitals within the GDPR and TSD, it can be seen that there is a preference for the data protection rights. At the same time, the Swedish DPA shows the opposite truth, according to which the trade secret protection has a strong restricting factor on the transparency rights contained in the GDPR. Nevertheless, no additional national restrictions have been introduced into supplementary Swedish healthcare legislation, *inter alia* Patient Data Act (2008:355), which further strengthen healthcare provider's trade secret rights. Yet, due to the lack of guidance in this area, it remains to be seen to what extent the healthcare provider will be able to rely on such restrictions to protect its trade secrets.

In the meantime, there have been several solutions proposed in order to resolve the conflict between both rights and exhibit transparency without opening the 'black box' of ADM AI systems, for instance counterfactual explanations, where the focus of a medical explanation is to help patient to act and achieve the preferred result, rather than just enable the patient to understand the systems functionality; visualization techniques by redesigning the means under which the information is given; and XAI where an explanation is given much alike the ones between two human beings, which enhance transparency and fairness within the healthcare domain.

---

[340] See Annex 6 for the concept of XAI presented by DARPA; See also Alejandro Barredo Arrieta et al., *Explainable Artificial Intelligence (XAI): Concepts, Taxanomies, Opportunities and Challenges towards Responsible AI*, (2020), Volume 58, Information Fusion, page 83

[341] Broad Agency Announcement (n 338), page 6; See also Dr. Matt Turek, *Explainable Artificial Intelligence (XAI),* Defense Advanced Research Projects Agency (DARPA), Program Information, <https://www.darpa.mil/program/explainable-artificial-intelligence> accessed 17 May 2020

[342] Andreas Holzinger et al. (n 15), page 3; See also Peter Kieseberg et al., *Trust for the 'Doctor in the Loop*, (2016), ERCIM News 104, page 32-33 <https://ercim-news.ercim.eu/images/stories/EN104/EN104-web.pdf> accessed 17 May 2020

6. Summary and concluding remarks

This thesis aimed at finding a balance between the patient's data protection rights to a transparent processing of its data concerning health in solely ADM and healthcare provider's rights in keeping its AI algorithms used in solely ADM as trade secrets within the healthcare. The research questions have been examined from a Swedish perspective, with the support of both Swedish and EU legislation. The legal dogmatic method was used as a base when analyzing the legal framework, in order to provide possible solutions on how the rights in conflict can achieve a balance. Due to the fact that there have not yet been any decisions that have been fully delegated to an AI algorithm within the Swedish healthcare, the thesis analyzed the research questions with the probability of such situation in mind.

In the beginning of the thesis, a *Vision eHealth 2025* was presented, which expresses Sweden's ambition in making Sweden the best in the world at using the opportunities offered by digitization and eHealth. However, the utterly rapid development of AI technology and the emerge of ADM AI algorithms, where medical decisions are delegated to autonomous AI systems, will make it difficult in achieving the vision that is based on a number of fundamental perspectives and principles, *inter alia* equality and efficiency, accessibility, usability, digital participation as well as protection of privacy and information security, due to the lack of transparency in AI systems, e.g. the 'black box' problem.

The GDPR establishes transparency principles which needs to be followed by the healthcare provider, in order to lawfully process patient's data concerning health by automated means. These rights are mainly notification obligations in articles 13-14 GDPR, access right in article 15 GDPR, as well as safeguard in article 22 (3) GDPR and the right to explanation in the (non-binding) recital 71 GDPR. The GDPR is further supplemented by the Swedish DPA as well as other national legislation within the healthcare domain, which puts stricter rules on the safety of the patient. The transparency rights described above are highly important within the healthcare, in order to avoid biased or unreliable outcomes and ensure that the patient's fundamental rights are observed. The right to receive an explanation of the decision, contained in the non-binding recital, is greatly debated and leaves the scope open for the interpretation.

Contrariwise, transparency does not only carry out benefits, but also disadvantages for those affected by the principle, in this case healthcare provider wanting to keep its AI algorithms used in solely ADM as trade secrets. Swedish TSA, which is the result of the transposition of TSD into Swedish law, protects any subject matter that fulfills the criteria set in 2 § STA, which is

highly relevant form of protection for healthcare companies developing and using rapidly evolving AI technology. Yet, whenever solely ADM AI system operating as a 'black box' is at stake, where the logic in the medical decision is impossible to understand and further convey to the patient, such system makes it difficult for the healthcare provider to comply with the GDPR requirement, without risking of revealing the processing mechanism of the AI system. This may result in the loss of the trade secret status, leaving healthcare companies vulnerable to having their software stolen and reproduced.

Thus, there is a clear clash between patient's rights to a transparent processing of data concerning health and healthcare provider's right to trade secret protection of AI algorithms used in solely ADM process. In this regard, based on commentaries from legal scholars and guidelines of the WP29, a balance between both rights can be found in the notion of a 'meaningful information' provided to the patient in case of solely ADM. What is to be considered as 'meaningful' shall be reviewed form the eyes of the patient. In this regard, while technical details of how an automated AI system comes to a medical decision when processing data concerning health can constitute '*information* about the *logic involved*', the same information is not seen as 'meaningful' from the perspective of the patient. Thus, the demarcation between 'information' and '*meaningful* information' is the crucial element, which enables healthcare provider to keep its processing algorithms as trade secrets, while complying with the transparency requirements under the GDPR. Yet, the GDPR also makes clear that trade secrets cannot be relied upon to refuse to provide *all* of the information to the patient.

So, when *all* of the 'meaningful information' cannot be given without healthcare provider reveals some of the precious algorithms protected by trade secrets, the balancing recitals contained in both GDPR and TSD, confirms a small preference for data protection rights. In this regard, by looking at the wording of these recitals, the adverb '*adversely'* contained in the recital 63 GDPR, indicates that whereas the application of data protection law can permit a disapplication of trade secret law as such, the latter can never require the disapplication of privacy rules. However, at the same time article 23 GDPR allows MS to introduce national restrictions on the right of information and the right to access, in order to protect rights and freedoms of others. In this regard, 5 c. 1 § DPA shows a reality where trade secret protection has a strong restricting effect on the mentioned transparency rights, where the information may not be provided pursuant to law or other statues, or by a decision that has been issued under the same statute. Thus, it is probable that the healthcare provider can deny conveying information and providing access to the logic involved in the ADM process in order to take active steps in

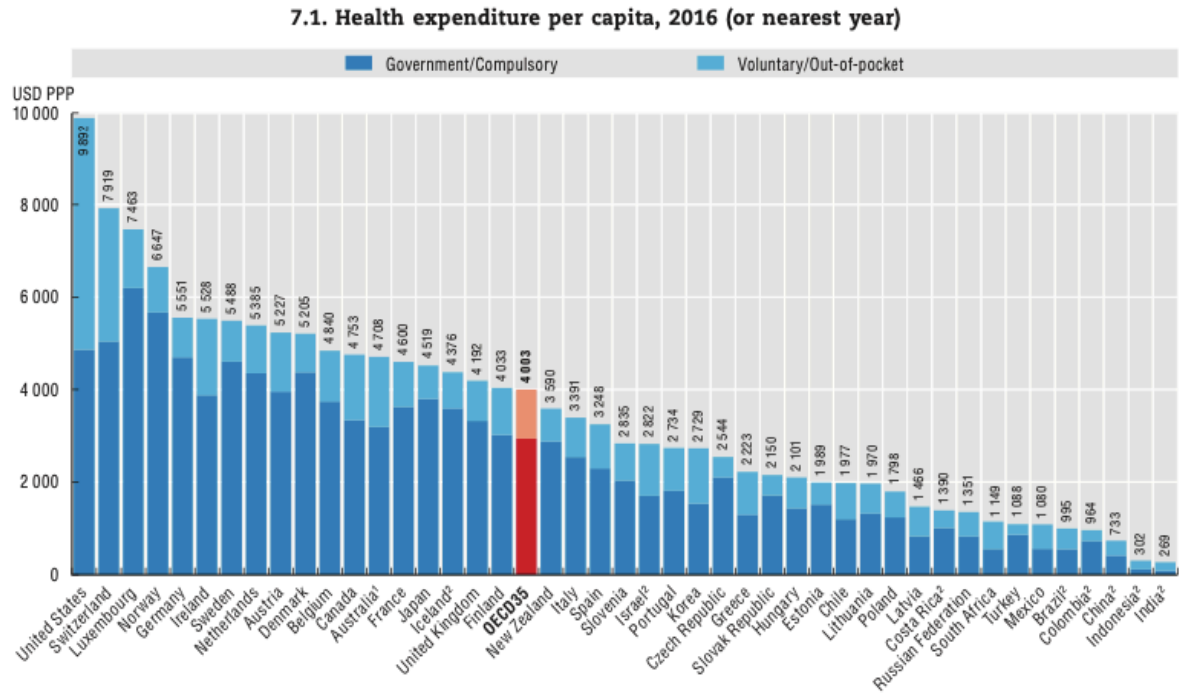
protecting its information as a secret to comply with 2 § TSA. Nevertheless, national restrictions on information and access right have not been introduced into the supplementary legislation Patient Data Act (2008:355), which shows some possibility on the side of the legislator of accepting prevalence of healthcare provider's economic interest when patient's data protection rights are at stake. Yet, due to the lack of guidance in this area, it remains to be seen how the national restrictions will be applied in practice.

Nevertheless, in the search of reconciling the rights in conflict, the visualization techniques and counterfactual explanations are able to help to provide meaningful information without opening up the 'black box'. In this regard, the healthcare provider can choose different ways of providing information about the decision taken, *inter alia* drawings, pictures or diagrams, or simply helping patient to 'act', e.g. according to article 22 (3) GDPR, rather than only understanding the algorithms behind the medical decision. Additionally, there is an ongoing project on XAI stemming from the 'privacy-by-design' approach, where algorithms are being constructed in a way that makes it easier both for the patient and the healthcare provider to understand the reasoning behind the automated decision taken. In this regard, due to the research funding provided by WASP, Sweden is on the way of achieving a good position on the market concerning AI, and the explainability thereto, within healthcare domain.

Overall, recent advances in AI within the healthcare have been remarkable and there is no suggestion that the rate of development is going to slow down, rather the opposite. Even though, Sweden is not recognized as a leading country when it comes to use of AI in different areas, including healthcare, with the big capacity of research and cooperation between both public and private sector, will enable Swedish health and welfare to achieve goals on digitalization set up by the *Vision eHealth 2025*. There is thus an emerging need for better legislation on the AI and data protection, especially when it comes to processing of data concerning health, either by introduction of new legislation or by enlargement of the current one. Sweden must ensure that AI is developed and applied in an appropriate framework, which promotes innovation and respects values and fundamental rights as well as ethical principles.

Concludingly, the practice of healthcare has strong ethical roots, which must not change with new technologies. Thus, the future of AI requires dialogue between developers and society about not only what is *possible*, but also what is *reasonable*. But for now, transparency in solely ADM AI systems continue to be in need for careful examination. It will thus be up to the Swedish Data Protection Authority and the national court, together with the EUCJ, to find a solution where transparency will be exhibited without opening the 'black box'.

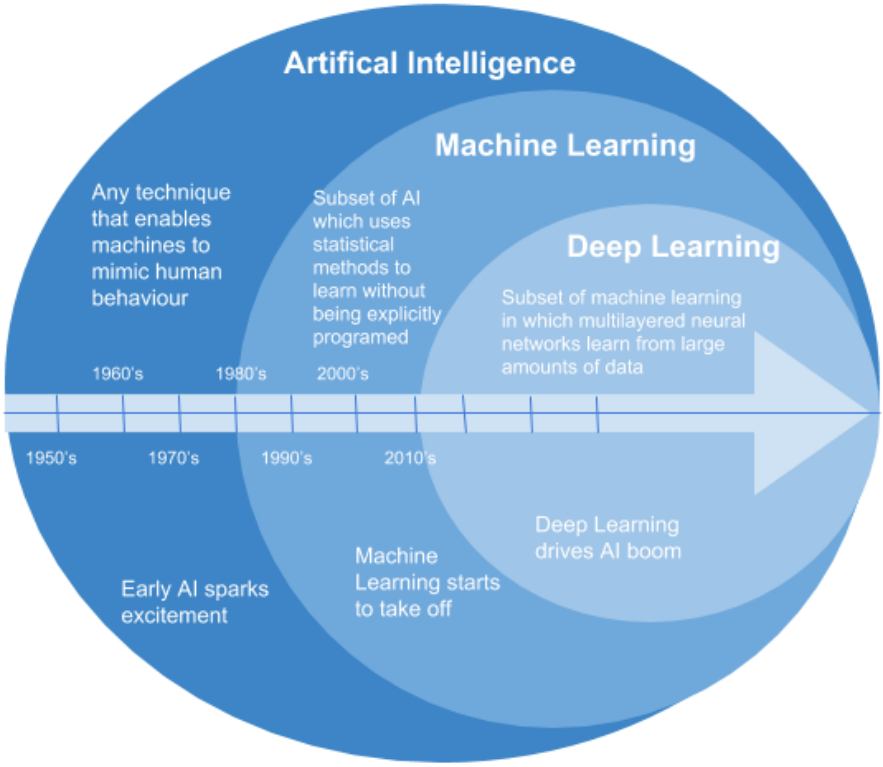
Annex 1[343]



Note: *Expenditure of health measures the final consumption of health services. This includes spending by both public and private sources on medical services, public health and prevention programs and administration. As can be concluded from the diagram, to compare spending levels between countries, Sweden is among the top 10 countries that invest most in healthcare sector, both by public and private actors.*

[343] OECD (n 2), page 133

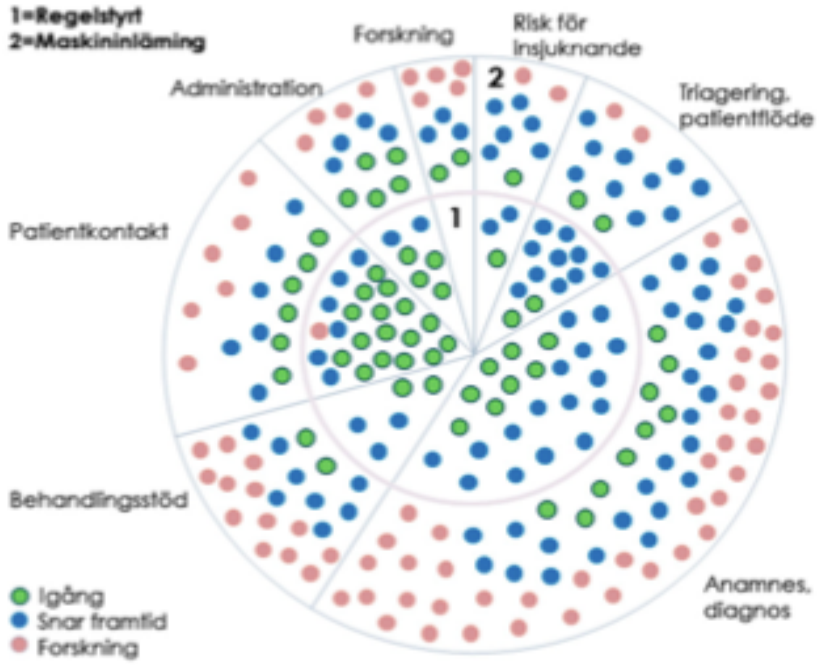
Annex 2[344]



Note: *The figure shows the timeline when sub-areas to AI begun to emerge. AI consist of more areas, inter alia logic programming, fuzzy logic, probabilistic reasoning, ontology engineering. However, only sub-areas shown above are of particular importance within the healthcare sector, due to their ability to analyze a large amount of medical data, predicting diagnosis and support healthcare providers in their decisions.*

[344] Helena Williams, *What is artificial intelligence all about anyway? – A brief summary of Artificial Intelligence,* (2019), Towards Data Science <https://towardsdatascience.com/what-is-artificial-intelligence-all-about-anyway-b57c7eb75f5f> accessed 24 April 2020

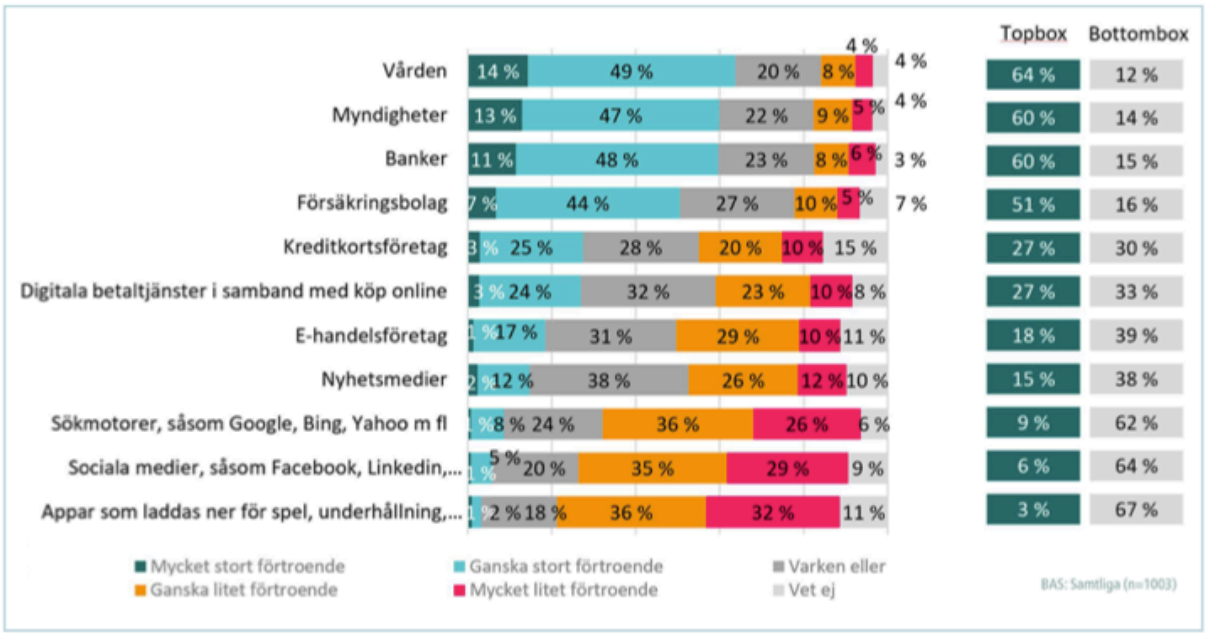
Annex 3[345]



Note: *This figure describes how AI applications are distributed in various areas in Swedish healthcare, and whether AI applications are already in use, are expected to be applied in the near future or such applications are research projects. The figure also shows the number of applications that are rule-based (the inner circle) and machine learning (the outer circle). According to Swedish Welfare Board, the size of different sector of the circle is proportional to the number of AI support in each area.*

[345] Swedish National Board of Health and Welfare (n 5), page 60

Annex 4[346]



Note: This diagram shows individual trust into different sectors. As can be seen, patients trust in healthcare providers is highest, however, patients are seldom aware that their personal data is being processed.

[346] Swedish Data Protection Authority (n 213), page 29

Annex 5[347]

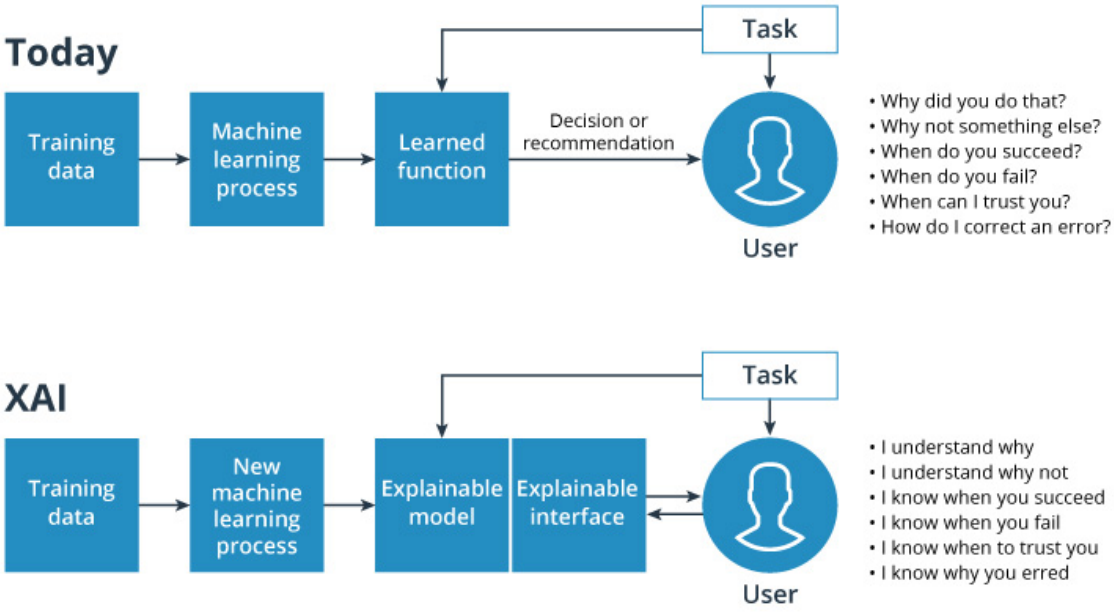
Countries	Are trade secrets (TS) viewed as intellectual property (IP)?	Is Directive 2004/48 on the Enforcement of IP Rights applicable to TS?	How are trade secrets protected?	Are there specific provisions on the protection of TS?
Austria	NO	NO	Federal Law on Unfair Competition Act Criminal Code Patent Act	NO
Belgium	NO	NO	General Tort Law Unfair Competition Law Labour Law	NO
Bulgaria	NO	NO	Law on Protection of Competition Law on Access to Public Information General Civil and Penal law	Unclear[131]
Cyprus	NO	NO	Commercial Description Law Competition Law Criminal liability only	NO
Czech Republic	NO	NO	Civil Law of Unfair Competition Criminal Law	YES TS as defined by art.39(2) TRIPS, which is directly applicable
Denmark	NO	NO	Unfair Competition Law Contract Law Employment Law Criminal Law	YES
Estonia	NO	NO	Competition Act Commercial Code Employment Contracts Act Penal Code	YES Case law: TS as defined by art.39(2) TRIPS
Finland	NO	Partial application of the Enforcement directive for procedural related issues pertaining to copyrights and industrial property rights claims	Unfair Business Practices Act Employment Contract Act Criminal Code	NO (but the Criminal Code defines "business secret")
France	YES: "manufacturing secrets" (secrets de fabrique) are viewed as IP rights	NO	Intellectual Code of Property Civil Code Labour Code Penal Code (cf. 23.01.2012 Proposition de loi[132])	YES
Germany	NO	NO	Act against Unfair Competition Criminal Law Civil law	YES
Greece	NO	NO	Unfair Competition Law Criminal Code Civil Code	NO
Hungary	NO	NO	Unfair Competition Act Civil Code Labour Code Criminal Code	YES (defined by the Civil Code)
Ireland	NO	NO	Common Law (breach of confidence, contract law, etc.) Criminal Law Equity Law	NO

[347] Bronckers & McNelis (n 227), 687-688, which summarizes the conclusions from the Study on Trade Secrets and Practices Copying (Look-alikes) MARKT/2010/20/D MARKT/2010/20/D (the *Hogan Lovells Report*), published by the European Commission on 13 January 2012

Countries	Are trade secrets (TS) viewed as intellectual property (IP)?	Is Directive 2004/48 on the Enforcement of IP Rights applicable to TS?	How are trade secrets protected?	Are there specific provisions on the protection of TS?
Italy	YES: TS meeting the requirements of the Code of Industrial Property are IP rights	YES	Code of Industrial Property Civil Code Criminal Code	YES
Latvia	YES	The Enforcement Directive applies (however, as the Civil Procedure Code does not mention TS, it is unclear whether the Civil Procedure remedies apply to TS)	Commercial Law Labour Law Unfair Competition Act Criminal Law Civil Code	YES
Lithuania	Unclear	NO	Law on Competition Civil Code Labour Law Criminal Code	YES
Luxembourg	NO	NO	Unfair Competition Law Criminal Law Tort Law Contractual Law	NO
Malta	NO	NO	Limited protection: contractual protection only	NO
The Netherlands	NO	NO	Civil Code Criminal Code Labour Code	NO
Poland	NO	NO	Unfair Competition Act Labour Code Act on Competition and Consumer Protection Code of Commercial Companies and Partnerships Civil and Criminal Code	YES
Portugal	NO	YES	Industrial Property Code Criminal Code Labour Code	YES
Romania	YES: Know-how (product or process information) is considered to be IP	NO	Unfair Competition Law Penal Code	YES
Slovak Republic	YES	YES	Commercial Code Penal Code	YES
Slovenia	Unclear	Enforcement Directive applies in particular circumstances	Company Act Employment Relationship Act Protection Competition Act Penal Code Code of Obligations	YES
Spain	NO[133]	NO	Unfair Competition Act Criminal and Civil Code	YES
Sweden	NO	NO	Trade Secret Act Penal Code	Only EU country to have an Act which specifically protects TS
United-Kingdom	Unclear[134]	Unclear	Common Law (breach of confidence, contract law, etc.) Criminal Law	NO (Equity Law Protection)

Note: State of play of the trade secret regimes across MS within the EU. This shows that Sweden is the only country within the EU that has a specific protection of trade secrets regulated in law since 1990.

Annex 6[348]



Note: This illustrates a XAI concept, which shows how an AI system process data and gives a result today and how the system will process data and give an understandable result in the future. This will also allow users of the system to understand how to correct system's mistakes.

[348] Broad Agency Announcement (n 338), page 6

Bibliography

Legal Sources

European Union

Treaties & Agreements

Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), Annex 1C to the Marrakesh Agreement (WTO 1994)

Berne Convention for the Protection of Literary and Artistic works (WIPO 1986)

Charter of Fundamental Rights of the European Union (2000/c 364/01) (CFR), OJ C 2012/C 326/02

Consolidated version of the Treaty on the European Union (TEU) , OJ C C115/13

Consolidated version of the Treaty on the Functioning of the European Union (TFEU), OJ C 326/01

Protocol No. 1 of the European Convention on Human Rights

WIPO Copyright Treaty (WIPO 1996)

WIPO Performance and Phonograms Treaty (WIPO 1996)

Directives

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

Regulation

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119/1

Sweden

SFS 1949:105. *Freedom of the Press Act*. Stockholm: Ministry of Justice

SFS 1974:152. *The Constitution of Sweden*. Stockholm: Ministry of Justice

SFS 2008:355. *Patient Data Act*. Stockholm: Ministry of Health and Social Affairs

SFS 2009:400. *Public Access to Information and Secrecy Act*. Stockholm: Ministry of Justice

SFS 2010:659. *Patient Safety Act*. Stockholm: Ministry of Health and Social Affairs

SFS 2014:821. *Patient Act*. Stockholm: Ministry of Health and Social Affairs

SFS 2018:218. *Data Protection Act*. Stockholm: Ministry of Justice

SFS 2018:558. *Act on Trade Secrets*. Stockholm: Ministry of Justice

Official Documents

European Union

Article 29 Data Protection Working Party (WP29), *Guidelines on Automated individual decision-making and profiling for the purposes of Regulation 2016/679*, 3 October 2017, WP251rev.01

Article 29 Data Protection Working Party (WP29), *Guidelines on transparency under Regulation 2016/679*, 17/EN, WP260rev.01

European Commission, Communication from the Commission *on enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society*, Brussels, 25 April 2018 COM(2018) 233 final

European Commission, Commission's Communication on guidance for better transposition and application for Directive 2004/38/EC (COM/2009/0313)

European Commission, *Study on Trade Secrets and Confidential Business Information in the Internal Market*, MARKT/2011/128/D, April 2013

European Patent Office, *Guidelines for Examination in the European Patent Office*, November 2019, OJ EPO 2019, A80

European Union Agency for Fundamental Rights, *The EU Charter of Fundamental Rights in Sweden*, 2019, Publications Office of the European Union

Independent High-Level Expert Group on Artificial Intelligence set up by European Commission, *Ethics Guidelines for Trustworthy AI*, 8 April 2019

Sweden

Ju 2003:04, *European Convention and protection for private life in Sweden*, Stockholm 2011

SOU 2017:52, *This is how we strengthen personal integrity*, Stockholm 2017

SOU 2017:45, New act on Trade Secrets, Stockholm 2017

Prop. 2017:18:105, *New Data Protection Act*, 2018, Stockholm 2018

Prop. 2017/18:200, *New legislation on trade secrets*, Stockholm 2018

Articles

Agata Ferretti, Manuel Schneider and Alessandro Blasimme, *Machine Learning in medicine: Opening the New Data Protection black box*, (2018), Volume 4, Issue 3, European Data Protection Law Review, pp 320-332

Alejandro Barredo Arrieta, Natalia Diaz-Rodriguez, Javier Del Ser, Adrien Bennetot, Siham Tabik, Alberto Barbado, Salvador Garcia, Sergio Gil-Lopez, Daniel Molina, Richard Benjamins, Raja Chatila and Francisco Herrera, *Explainable Artificial Intelligence (XAI): Concepts, Taxanomies, Opportunities and Challenges towards Responsible AI*, (2020), Volume 58, Information Fusion, pp 82-115

Alex John London, *Artificial Intelligence and Black-Box medical Decisions: Accuracy versus Explainability,* (2019) Volume 49, Issue 1, Hastings Center Report, pp 15-21

Andreas Holzinger, Chris Biemann, Constantinos S. Pattichis and Douglas B. Kell, *What do we need to build explainable AI systems for the medical domain?*, (2017), Volume 1, pp 1-28 <https://arxiv.org/pdf/1712.09923.pdf> accessed 17 February 2020

Andrew D. Selbst and Julia Powels, Meaningful information and the right to explanation, (2017), Volume 7, Issue 4, International Data Privacy Law, pp 233-242

Ben Shneiderman and Catherine Pkaisant, *Improving healthcare with interactive visualization*, (2013), Volume 46, Issue 5, IEEE Computer Society, pp 58-66

Bryce Goodman and Seth Flaxman, *European Union regulations on algorithmic decision-making and a 'right to explanation',* (2017), Volume 38, Issue 3, AI Magazine, pp 1-9 <https://arxiv.org/pdf/1606.08813.pdf> accessed 17 February 2020

Calvin W.L. Ho, Derek Soon, Karel Caals and Jeevesh Kapur, *Governance of automated image analysis and artificial intelligence analytics in healthcare*, (2019), Volume 74, Issue 5, Clinical Radiology, pp 329-337

Carrie J. Cai, Jonas Jongejan and Jess Holbrook, *The Effects of Example-Based Explanations in a Machine Learning Interface*, (2019), Proceedings of the 24th International Conference on Intelligent User Interfaces, pp 258-262 <https://dl.acm.org/doi/pdf/10.1145/3301275.3302289> accessed 10 May 2020

Christohper Kuner, Dan Jerker B. Svantesson, Fred H. Cate, Orla Lyskey and Christopher Millard, *Machine learning with personal data: is data protection law smart enough to meet the challenges,* (2017), Volume 7, Issue 1, International Data Privacy Law, pp 1-2

Christopher McCrudden, *Legal research and the social science*, (2006), Volume 122, The Law Quarterly Review; Oxford Legal Studies Research Paper No. 33/2006, pp 632-650

Danton S. Char, Nigam H. Shah, David Magnus, I*mplementing Machine Learning in Health Care – Addressing Ethical Challenges,* (2018), N Engl J Med., pp 981-983 <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5962261/pdf/nihms967800.pdf> accessed 17 April 2020

David A Prange and Alyssa N Lawson, *Re-evaluating companies' AI protection strategies*, (2018), Patents and Trade Secrets AI, Managing Intellectual Property, pp 35-38 <https://www.robinskaplan.com/-/media/pdfs/reevaluating-companies-ai-protection-

strategies.pdf?fbclid=IwAR2WJvL2RQVbTn6asNGNIhOFG8anqI0DnDrLUD4pdKzl9l8Djd-bAPirIWY> accessed 18 April 2020

Davide Castelvecchi, *Can we open the black box of AI?*, (2016), Volume 538, Macmillan Publishers Limited, part of Springer Nature, pp 21-23 <https://www.nature.com/news/polopoly_fs/1.20731!/menu/main/topColumns/topLeftColumn/pdf/538020a.pdf> accessed 19 April 2020

Denis Horgan, Mario Romao, Servaas A. Morré and Dipak Kalra, *Artificial Intelligence: Power for Civilization – and for better healthcare*, (2019), Public Health Genomics, pp 145-161 <https://www.karger.com/Article/Pdf/504785> accessed 19 April 2020

Dimitra Kamarinou, Christopher Millard and Jatinder Singh, *Machine Learning with personal data*, 8 November 2016, Queen Mary School of Law, Legal Studies Research Paper No. 247/2016

Emre Bayamlioglu (Researcher), *Transparency of Automated Decisions in the GDPR: An attempt for systematization*, (2018), Tilburg University, Working Paper

Gianclaudio Malgieri and Giovanni Comande, *Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation*, (2017), Volume 7, Issue 3, International Data Privacy Law, pp 243-265

Gianclaudio Malgieri, *Decontextualization data sharing at the borderlines between Trade Secrets and Data Protection Rules*, (2015), SSRN Electronical Journal, 10.2139, pp 1-71

Gianclaudio Malgieri, *Trade Secrets v Perosnal Data: A possible solution for balancing rights*, (2016), Volume 6, Issue 2, International Data Privacy Law, pp 102-116

Goutham Rao, Katherine Kirley, Paul Epner, Yiye Zhang, Victoria Bauer, Rema Padman, Ying Zhou and Anthony Solomonides, I*dentifying, Analyzing, and Visualizing diagnostic paths for patients with nonspecific abdominal pain*, (2018), Volume 94, Applied Clinical Informatics, pp 905-913 <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6301880/pdf/10-1055-s-0038-1676338.pdf> accessed 18 April 2020

Grégoire Montavon, Wojciech Samek and Klaus-Robert Müller, *Methods for interpreting and understanding Deep Neural Networks*, (2018), Volume 73, Digital Signal Processing, pp 1-15 <https://arxiv.org/pdf/1706.07979.pdf> accessed 1 May 2020

Heike Felzmann, Eduardo Fosch Villaronga, Christoph Lutz and Aurelia Tamo-Larrieux, *Transparency you can trust: Transparency requirements for artificial intelligence between legal norms and contextual concerns*, (2019), Big Data & Society, pp 1-14 <https://journals.sagepub.com/doi/pdf/10.1177/2053951719860542> accessed 16 February 2020

Jenna Burrell, *How the machine 'thinks': Understanding opacity in machine learning algorithms*, (2016), Big Data and Society, pp 1-23 <https://journals.sagepub.com/doi/pdf/10.1177/2053951715622512> accessed 8 May 2020

Joanna Mazue, Michal Palinski, Dr. Maciej Sobolewski, *GDPR: A step towards a user-centric Internet?*, (2017), Volume 52, Issue 4, Intereconomics, Review of European Economic Policy, pp 207-213

John McCarthy, *What is Artificial Intelligence?*, Stanford University, (2007), pp 1-17 <http://jmc.stanford.edu/articles/whatisai/whatisai.pdf> accessed 18 February 2020

Joshua A. Kroll, Joanna Huey, Solon Barocas, Edward W. Felten, Joel R. Reidenberg, David G. Robinson and Harlan Yu, *Accountable Algorithms*, (2017), Volume 165, University of Pennsylvania Law Review, pp 633-705

Julian Reiss and Rachel A. Ankeny, *Philosophy of Medicine, Stanford Encyclopedia of Philosophy*, (2016) <https://plato.stanford.edu/entries/medicine/> accessed 19 April 2020

Kacper Sokol and Peter Flach, *Counterfactual explanations of machine learning predictions: Opportunities and challenges for AI safety,* (2017), Volume 2301, CEUR Workshop Proceedings, pp 1-4 <http://ceur-ws.org/Vol-2301/paper_20.pdf> accessed 7 May 2020

Lilian Edwards and Michael Veale, *Slave to the algorithm? Why a 'right to an explanation' is probably not the remedy you are looking for*, (2017), Volume 16, Issue 1, Duke Law & Technology Review, pp 18-84

Lucas Bergkamp, *EU Data Protection Policy: The privacy fallacy: Adverse effects of Europe's data protection policy in an information-driven economy*, (2002) Volume 18, Issue 1, Computer Law & Security Review, pp 31-47

Lynn M. LoPucki, *Algorithm Entities*, (2018), Volume 95, Issue 4, Washington Law Review, pp 887-953

Maja Brkan, *Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond*, (2017), Volume 27, Issue 2, International Journal of Law and Information Technology, pp 91-121

Margot E. Kaminski, *The Right to explanation, Explained*, (2019), Volume 34, Issue 1, Berkeley Technology Law Journal, pp 189-218

Mariateresa Maggiolino, *EU trade secrets law and algorithmic transparency*, (2019) Bocconi Legal Studies Research Paper No. 3363178, pp 1-16

Matthew U. Scherer, *Regulating artificial intelligence systems: risks, challenges, competencies, and strategies,* (2016), Volume 29, Issue 2, Harvard Journals of Law & Technology, pp 353-400

Melanie Biurassa Forcier, Hortense Gallois, Siobhan Mullan and Yann Joly, *Integrating artificial intelligence into health care through data access: can the GDPR act as a beacon for policymakers?*, (2019), Volume 6, Issue 1, Journal of Law and the Biosciences, pp 317-335

Mike Ananny and Kate Crawford, *Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability*, (2016), New Media & Society <https://pdfs.semanticscholar.org/98ca/df9e8f69b44c5128d7915659086831a437e8.pdf?_ga=2.163379327.2118699855.1585645372-1703947962.1585552800> accessed 23 April 2020

Motahhare Eslami, Sneha R. Krishna Kumaran, Christian Sandvig and Karrie Karahalios, *Communicating Algorithmic Process in Online Behavioral Advertising*, (2018), Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, Paper No. 432, pp 1-13 <https://dl.acm.org/doi/pdf/10.1145/3173574.3174006> accessed 23 April 2020

Muhammad Bilal Zafar, Isabel Valera, Manuel Gomez Rodriguez and Krishna P. Gummadi, *Fairness beyond disparate treatment & disparate impact: Learning classification without disparate mistreatment*, (2017), Proceedings of the 26th International Conference on World Wide Web, page 1171 <https://dl.acm.org/doi/pdf/10.1145/3038912.3052660> accessed 10 May 2020

Niall McAlister and Roland Wiring, *AI in Life Sciences – Legal perspective on the opportunities and challenges of AI for life sciences companies*, (2019), CMS Cameron McKenna Nabarro Olswang LLP < https://www.abhi.org.uk/media/2249/ai-in-life-sciences-and-healthcare-cms.pdf?fbclid=IwAR0C6mny9Y4sqeblOUiM8A0edjewM-gSS9afrOs5o71nKh82-fmMnFWHboo> accessed 23 April 2020

Nicholas Diakopoulos, *Accountability in Algorithmic Decision Making,* (2016), Volume 59, Issue 2, Communications of the ACM, pp 56-62

Nicole Lewis, *Artificial Intelligence to play key role in population health*, (2017), Medical Economics < https://www.medicaleconomics.com/medical-economics-blog/artificial-intelligence-play-key-role-population-health> accessed 15 February 2020

Peter Kieseberg, Edgar Weippi and Andreas Holzinger, *Trust for the 'Doctor in the Loop*, (2016), Issue 104, ERCIM News <https://ercim-news.ercim.eu/images/stories/EN104/EN104-web.pdf> accessed 17 May 2020

Privacy International, *Data is power: Profiling and Automated Decision-Making in GDPR*, (2017), pp 1-17 < https://privacyinternational.org/sites/default/files/2018-04/Data%20Is%20Power-Profiling%20and%20Automated%20Decision-Making%20in%20GDPR.pdf> accessed 3 March 2020

Rich Caruana, Paul Koch, Yin Lou, Marc Sturm, Johannes Gehrke and Noémie Elhadad, *Intelligible models for healthcare: Predicting pneumonia risk and hospital 30-day readmission*, (2015), International Conference on Knowledge Discovery and Data Mining, pp 1721-1230 <http://people.dbmi.columbia.edu/noemie/papers/15kdd.pdf> accessed 17 March 2020

Robyn Calpan, Lauren Hanson, Joan Donovan and Jeanna Matthews, *Algorithmic accountability: A primer*, (2018), Data & Society, pp 1-12 <https://datasociety.net/wp-content/uploads/2018/04/Data_Society_Algorithmic_Accountability_Primer_FINAL-4.pdf> accessed 10 March 2020

Sandra Wachter, Luciano Floridi, Brent Mittelstadt, *Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation*, (2016), Volume 7, Issue 2, International Data Privacy Law, pp 76-99

Sandra Watcher, Brent Mittelstadt and Chris Russell, *Counterfactual explanations without opening the black box: automated decisions and the GDPR*, (2018), Volume 31, Issue 2, Harvard Journal of Law and Technology, pp 841-887

Simone Fischer-Hüber, Chris Hoofhagle, Ioannis Krontris, Kai Rannenberg, Michael Waidner and Caspar Bowden, *Online Privacy – Towards Informational Self-Determination on the Internet*, (2013), IOS Press, pp 123-138 <http://ioanniskrontiris.de/publications/Krontiris2013c.pdf> accessed 23 April 2020

Stefan Harrer, Pratik Shah, Bhavna Antony and Jianying Hu, *Artificial Intelligence for Clinical Trial Design*, (2019), Volume 40, Issue 8, Trends in Pharmacological Sciences, pp 577-591

Tadas Klimas and Jurate Vaiciukaite, *The law of Recitals in European Community Legislation,* (2008), Volume 15, Issue 1, ILSA Journal of International & Comparative Law, pp 61-93

Tanya Alpin, *Right to property and Trade Secret*, January 2014. C Geiger (ed) Research Handbook on Human Rights and Intellectual Property (Edward Elgar, 2015), ch 22, pp 421-437

The Royal Society, *Explainable AI: the basics*, (2019) <https://royalsociety.org/-/media/policy/projects/explainable-ai/AI-and-interpretability-policy-briefing.pdf> accessed 8 May 2020

W. Nicholson Price II, *Regulating Black-Box Medicine*, (2017), Volume 116, Issue 3, Michigan Law Review, PP 421-474

William R. Swartout, *Explaining and Justifying Expert Consulting Programs*, (1981), Volume 2, From the Proceeding of the Seventh International Join Conference on Artificial Intelligence, pp 815-823 <http://people.dbmi.columbia.edu/~ehs7001/Clancey-Shortliffe-1984/Ch16.pdf> accessed 7 March 2020

Yiye Zhang, Rema Padman and Nirav Patel, *Paving the COWpath: Learning and visualizing clinical pathways from electronic health record data*, (2015), Volume 58, Journal of Biomedical Informatics, pp 186-197

Zhiyuan Zhang, Faisal Ahmed, Arunesh Mittal, IV Ramakrishnan, Rong Zhao, Asa Viccellio and Klaus Mueller, *AnamneVis: A framwork for the visualization of patient history and medical diagnostics chain*, (2011), Proceedings of the IEEE VisWeek Workshop on Visual Analytics in Healthcare, page 1 <https://pdfs.semanticscholar.org/d9db/57f8bb04f723aa94d16a7ea7015529cb150d.pdf> accessed 16 May 2020

Books

Aulis Aarnio, *Essay on the doctrinal study of law*, University of Tampere, Springer 2011

Frank Pasquale, *The Black Box Society*, Harvard University Press, Cambridge, MA, 2015

James Woodward, *Making things happen – a theory of casual explanation*, Oxford University Press, 2003

Jerzy Stelmach and Bartosz Brozek, *Methods of Legal reasoning*, Law and Philosophy library, Volume 78, 2006 Springer

Justine Pila & Paul Torremans, *European Intellectual Property Law*, 2nd edition, Oxford University Press 2019

Jörgen Hettne and Ida Eriksson, *EU-rättlig metod, Teori och genomslag i svensk rättstillämpning*, Nordstedts juridik 2011

Lee A Bygrave, *Automated Profiling: Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling,* 2001, Computer Law & Security Review 17

Lee Andrew Bygrave, *Article 22: Automated individual decision-making, including profiling*, n Lee Andrew Bygrave; Christopher Kuner & Christopher Docksey (ed.), *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford University. Commentary on Article 22. s 522 – 542

Paul Craig and Grainne De Burca, *EU law – text, cases, and materials*, 6th edition, Oxford University Press, 2015

Marcus Österberg and Lard Lindsköld, *AI and machine learning for decision support in healthcare – A preliminary study investigating existing services and the art of developers working on machine intelligence*, SWElife, December 2018

Internet sources

Acta Orthopaedica, *AI analyses X-rays as well as doctors*, (2017), Karolinska Institutet <https://news.ki.se/ai-analyses-x-rays-as-well-as-doctors> accessed 5 February 2020

Dr. Matt Turek, *Explainable Artificial Intelligence (XAI),* DARPA, Program Information <https://www.darpa.mil/program/explainable-artificial-intelligence> accessed 17 May 2020

Erik Birkeneder, *Protecting Explainable AI Innovations in Health Care*, (2019), Forbes <https://www.forbes.com/sites/erikbirkender/2019/11/19/protecting-explainable-ai-innovations-in-health-care/?fbclid=IwAR0aJX7ZuDzqf5wO1kjFmU1M-iljc2jXwwP3umeqZJlXj5-gp8Ygp9Sp6bo#4446b7c51260> accessed 20 April 2020

Erin McCoy, *How Data Visualization is transforming the health care industry*, (2019), Modus <https://modus.medium.com/how-data-visualization-is-transforming-the-healthcare-industry-6761d7293dd2> accessed 27 April 2020

European Commission, *Factsheet: Artificial Intelligence for Europe*, (2019) <https://ec.europa.eu/digital-single-market/en/news/factsheet-artificial-intelligence-europe> accessed 12 February 2020

European Commission, *FAQ: Protection against the unlawful acquisition of undisclosed know-how and business information (trade secrets),* Internal Market, Industry, Entrepreneurship and SMEs <https://ec.europa.eu/growth/industry/policy/intellectual-property/trade-secrets/faq_en> accessed 17 April 2020

European Commission, *Trade secrets*, Internal Market, Industry, Entrepreneurship and SMEs <https://ec.europa.eu/growth/industry/policy/intellectual-property/trade-secrets_en> accessed 17 April 2020

European Commission, *Types of EU law*, <https://ec.europa.eu/info/law/law-making-process/types-eu-law> accessed 12 February 2020

European IPR Helpdesk, *Trade secrets: An efficient tool for competitiveness*, (2017), Fact Sheet <https://www.iprhelpdesk.eu/sites/default/files/newsdocuments/Fact-Sheet-Trade-Secrets.pdf> accessed 19 April 2020

European Union Agency for Fundamental Rights, *EU Charter of Fundamental Rights, Article 17 – Right to property*, (2007-2020) <https://fra.europa.eu/en/eu-charter/article/17-right-property> accessed 14 April 2020

Helena Williams*, What is artificial intelligence all about anyway? – A brief summary of Artificial Intelligence,* (2019), Towards Data Science <https://towardsdatascience.com/what-is-artificial-intelligence-all-about-anyway-b57c7eb75f5f> accessed 24 April 2020

Information Commissioner's Office (ICO), *What is personal data?*, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/> accessed 22 February 2020

Ingemar Karlsson Gadea, *Professional Secrecy and Confidentiality*, 1177 Vårdguiden, < <https://www.1177.se/en/other-languages/other-languages/regler-och-rattigheter---andra-sprak/tystnadsplikt-och-sekretess---andra-sprak/> accessed 21 April 2020

Intersoft Consulting, *GDPR – Personal Data*, <https://gdpr-info.eu/issues/personal-data/> accessed 16 February 2020

Jesper Cederberg, *First patients at Danderyd's hospital assessed with AI*, (2019), Medical Journal <https://lakartidningen.se/Aktuellt/Nyheter/2019/10/Forsta-patienterna-pa-Danderyds-sjukhus-bedomda-med-AI/> accessed 17 February 2020

Jonas Hedlund, *Lunginflammation*, (2020), 1177 Vårdguiden <https://www.1177.se/sjukdomar--besvar/lungor-och-luftvagar/inflammation-och-infektion-ilungor-och-luftror/lunginflammation/> accessed 17 April 2020

Julia Angwin, Jeff Larson, Surya Mattu and Lauren Kirchner, *Machine Bias*, (2016), ProPublica <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing> accessed 28 March 2020

Kari Gimmingsrud, *Artificial Intelligence and Data Privacy*, (2019), Expert Guides <https://www.expertguides.com/articles/artificial-intelligence-and-data-privacy/aruywukr?fbclid=IwAR2giJSJDn7AeAThkZcs7JN1786Uf4Yr7-ebFuBmNPu7D8bu38gn-2xBnHE> accessed 6 May 2020

Killer Visual Strategies, *How a motion graphic on vaccines generated over 1 mullion* views, (2020), <https://killervisualstrategies.com/project/motion-graphic-the-history-of-vaccines> accessed 13 May 2020

Knut and Alice Wallenberg Foundation, *Major research initiative will put Sweden on the map in artificial intelligence and quantum technology fields*, (2017), <https://kaw.wallenberg.org/en/research/major-research-initiative-will-put-sweden-map-artificial-intelligence-and-quantum> accessed 18 May 2020

Magnus Johanssson, *New Act on the Protection of Trade Secrets*, Lexology, (2018), Lexology <https://www.lexology.com/library/detail.aspx?g=6d6a7ef5-a085-4fcc-b9f0-f3bd5edc1979> accessed 16 April 2020

PWC, *No longer science fiction, AI and robotics are transforming healthcare*, (2017-2020), <https://www.pwc.com/gx/en/industries/healthcare/publications/ai-robotics-new-health/transforming-healthcare.html> accessed 15 February 2020

Swedish Data Protection Authority, *The Patient Data Act*, <https://www.datainspektionen.se/other-lang/in-english/the-patient-data-act/> accessed 10 February 2020

Swedish Data Protection Authority, *The purposes and scope of the General Data Protection Regulation,* <https://www.datainspektionen.se/other-lang/in-english/the-general-data-protection-regulation-gdpr/the-purposes-and-scope-of-the-general-data-protection-regulation/> accessed 10 February 2020

Swedish National Data Protection Authority, *What is meant by sensitive personal data?*, <https://www.datainspektionen.se/other-lang/in-english/about-privacy/what-is-meant-by-sensitive-personal-data/> accessed 11 February 2020

WIPO, *Sweden: Act on Trade Secrets (2018:558),* (2018), <https://www.wipo.int/news/en/wipolex/2018/article_0013.html> accessed 16 April 2020

Reports

Broad Agency Announcement, *Explainable Artificial Intelligence (XAI),* (2016), Defense Advanced Research Projects Agency (DARPA), Information Innovation Office <https://www.darpa.mil/attachments/DARPA-BAA-16-53.pdf> accessed 16 May 2020

Carolina Wahlby, *Methods development for extracting relevant data for use in AI/ML*, Stockholm Life Science AI/ML Guide – Shaping the future of healthcare intelligently <https://www.investstockholm.com/globalassets/invest/reports/stockholm-ai-report.pdf> accessed 16 May 2020

Christoph Schmon, *Automated decision making and Artificial Intelligence – a consumer perspective*, (2018), BEUC Position Paper, European Consumer Organization <https://www.beuc.eu/publications/beuc-x-2018-058_automated_decision_making_and_artificial_intelligence.pdf?fbclid=IwAR1JEImm6dLDYxBvNyQRK9rcw7FFjvSC311ga4KmFdW_ohUWfUHwpVgHpe4> accessed 10 March 2020

Dr Noam Shemtov, *A study on inventorship in inventions involving AI activity*, (2019), Commissioned by the European Patent Office <http://documents.epo.org/projects/babylon/eponet.nsf/0/3918F57B010A3540C125841900280653/$File/Concept_of_Inventorship_in_Inventions_involving_AI_Activity_en.pdf> accessed 18 February 2020

Elizabeth Denham, *Big data, artificial intelligence, machine learning and data protection*, (2017), Information Commissioner's Office <https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf> accessed 15 May 2020

European Commission, *Benchmark Deployment of eHealth among General Practitioners* (2018), EU publications <https://op.europa.eu/en/publication-detail/-/publication/3ba2eb8b-5c07-11e9-9c52-01aa75ed71a1/language-en/format-PDF> accessed 15 February 2020

European Parliament, *Robots in healthcare: a solution or a problem?*, (2019), Policy Department for Economic, Scientific and Quality of Life Policies

<https://www.europarl.europa.eu/RegData/etudes/IDAN/2019/638391/IPOL_IDA(2019)638391_EN.pdf> accessed 6 March 2020

European Patent Office, *Patents for software? European law and practice*, (2009) <https://ciencias.ulisboa.pt/sites/default/files/fcul/inovacao/PI-Pack-INPI-E-Patents-for-Software-EPO.pdf> accessed 13 February 2020

Foley & Larnner LLP, *AI is here to stay: Are you prepared?*, (2019), A 2019 report prepared by Foley & Lardner LLP – Explosed Oppotrunities and Challenges <https://www.foley.com/en/insights/publications/2019/04/-/media/8d7c95a40e97461698c2ceb488542491.ashx> accessed 22 April 2020

Government Offices of Sweden and Swedish Association of Local Authorities and Regions (SALAR), *Vision for eHealth 2025 – common starting points for digitization of social services and health care*, (2016), Stockholm <https://www.government.se/4a3e02/contentassets/b0fd09051c6c4af59c8e33a3e71fff24/vision-for-ehealth-2025.pdf> accessed 1 February 2020

Government Offices of Sweden, *National approach to artificial intelligence*, (2018), Ministry of Enterprise and Innovation <https://www.regeringen.se/4aa638/contentassets/a6488ccebc6f418e9ada18bae40bb71f/national-approach-to-artificial-intelligence.pdf> accessed 3 February 2020

Henrik Ahlén, *Artificiell Intelligence and machine learning for healthcare and life science*, (2017), Stockholm Science City Foundation <https://ssci.se/sites/default/files/Artificiell%20Intelligens%20och%20machine%20learning%20f%C3%B6r%20sjukv%C3%A5rd%20och%20life%20science.pdf> accessed 11 February 2020

Kristina Stensson Ljungdahl, Maria Ekendahl, Stefan Gustavsson and Göran Lindsjö, *AI and automation for first-line care – a report from Inera AB and the feasibility study Digital healthcare advice (Swedish version)*, (2017), Inera <https://www.inera.se/globalassets/projekt/nya-1177-vardguiden/ineras-rapport-ai-och-automatisering-for-forsta-linjens-vard.pdf?fbclid=IwAR3BJ8TGFt5rIFExyp1v6TvJslebikDHfWigZzUjNp1jIBj7lb1RXnxZ5oQ#page26> accessed 17 February 2020

Luciano Floridi, John Frank and Neil Jordan, *Healthcare, artificial intelligence, data and ethics – a 2030 vision: How responsible innovation can lead to a healthier society*, (2018), Microsoft <https://www.digitaleurope.org/wp/wp-content/uploads/2019/02/Healthcare-AI-Data-Ethics-2030-vision.pdf > accessed 5 March 2020

Magnus Boman, *Collaborating on AI/ML in academia*, Stockholm Life Science AI/ML Guide – Shaping the future of healthcare intelligently <https://www.investstockholm.com/globalassets/invest/reports/stockholm-ai-report.pdf> accessed 18 May 2020

Magnus Toness, *The protection of trade secrets and know-how in Sweden – Swedish report*, (2012), AND Law Advokatfirma KB <http://www.ligue.org/uploads/documents/cycle%202015/Cycle%202015/Rapports%20B/2015rapportsuedoisBnovembre2015.pdf> accessed 18 April 2020

Mårten Blix and Charlotta Levay, *Digitalization and Health Care – a report to the Swedish Government's expert group on public economics*, (2018), The Expert Group on Public Economics, 2018:8 English version <https://eso.expertgrupp.se/wp-content/uploads/2019/08/Digitalization-and-health-care-2018_6-English-version.pdf> accessed 3 February 2020

McKinsey & Company, *Transforming healthcare with AI – The impact on the workforce and organizations*, (2020), EIT Health <https://eithealth.eu/wp-content/uploads/2020/03/EIT-Health-and-McKinsey_Transforming-Healthcare-with-AI.pdf> accessed 3 February 2020

Norwegian Data Protection Authority, *Artificial intelligence and privacy*, (2018), <https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf?fbclid=IwAR0-yZ4HlAAVj5TEfJB_09dngs08MTzEtXwEW9SP5cY3DV6QMlVLZbqiuBY> accessed 16 February 2020

OECD, *Health at a Glance 2017: OECD Indicators*, (2017), OECD Publishing <https://www.oecd-ilibrary.org/docserver/health_glance-2017-en.pdf?expires=1589453901&id=id&accname=guest&checksum=4C51C23427EC5E86A256AEE7A310811E> accessed 3 February 2020

Paulina Modlitba*, Four changed driving forces for AI in healthcare*, (2018), SSF-report nr 29 <https://strategiska.se/app/uploads/livet-med-ai.pdf?fbclid=IwAR0fR2OqVQh3DYvT2Y6ktWIWMcxp5yXO_2si5eYso7k3Hw_NwOJQXHniwII> accessed 17 February 2020

Stefan Larsson, Mikael Annerith, Anna Felländer, Li Felländer-Tsai, Fredrik Heintz and Rebecka Cedering Ångström, *Sustainable AI*, (2019), AI Sustainability Center <http://www.aisustainability.org/wp-content/uploads/2019/03/Hallbar_AI.pdf?fbclid=IwAR3Bch2Fk7QVyfNYCyv1-M_FegCu0nDdWfhc-j7TV8pv1f9VCcz4dEZ2LlM> accessed 22 April 2020

Swedish Data Protection Authority, *National Integrity Report 2019*, (2019), Data Protection Authority report 2019:2 <https://www.datainspektionen.se/globalassets/dokument/rapporter/nationell-integritetsrapport-2019.pdf> accessed 7 March 2020

Swedish eHealth Agency, *Annual Report 2019 – trends on e-health*, (2019), S2018/06066/RS <https://www.ehalsomyndigheten.se/globalassets/dokument/rapporter/arsrapport-2019_e-halsomyndigheten.pdf?fbclid=IwAR3qvGZhnjZTcwn_1E_sFekCQTvc36eZ2OScPYVQDzMqO33H-J4cX0KSOgM#page13> accessed 3 February 2020

Swedish National Board of Health and Welfare and Swedish Cancer Society, *Cancer in numbers 2018 – Popular scientific facts about cancer*, (2018) <https://www.socialstyrelsen.se/globalassets/sharepoint-dokument/artikelkatalog/statistik/2018-6-10.pdf> accessed 18 February 2020

Swedish National Board of Health and Welfare, *Digital care services and artificial intelligence in healthcare*, (2019), <https://www.socialstyrelsen.se/globalassets/sharepoint-dokument/artikelkatalog/ovrigt/2019-10-6431.pdf> accessed 3 February 2020

Swedish National Board of Health and Welfare, *Digital healthcare services addressed to patients – survey and follow-up*, (2018), <https://www.socialstyrelsen.se/globalassets/sharepoint-dokument/artikelkatalog/ovrigt/2018-6-15.pdf?fbclid=IwAR3TVW7mWFkpmU4dE4KlBjqwS520QrQqn6zQHGXU1-mMkS33d0rStdPe75Q#page17> accessed 19 March 2020

Swedish National Council on Medical Ethics, *Artificial intelligence – promising technology with ethical challenges*, (2019), Smer conference report 2019:2 <http://www.smer.se/wp-content/uploads/2019/06/Smer-konferensrapport_2_webb.NY-REV.pdf> accessed 17 February 2020

Vinnova report, *Artificial Intelligence in Swedish business and society – Analysis of development and potential* (summary), (2018), VR2018:09 <https://www.vinnova.se/contentassets/29cd313d690e4be3a8d861ad05a4ee48/vr_18_09.pdf> accessed 20 February 2020

Vinnova, *Artificial Intelligence for better health – An announcement within the program innovations for the future of health*, (2017), Swedish Governmental Agency for Innovation Systems < https://www.vinnova.se/globalassets/utlysningar/2016-01596/omgangar/utlysningstext_aihalsa-rev.pdf851375.pdf> accessed 209 March 2020

WIPO Technology Trends 2019, *Artificial Intelligence*, (0219), World Intellectual Property Organization <https://www.wipo.int/edocs/pubdocs/en/wipo_pub_1055.pdf> accessed 19 February 2020

Table of Cases

EU

C-4/73, *Nold KG v Commission* [1974] ECR 491, ECLI:EU:C:1974:51

C-230/78, *SpA Eridiana-Zuccherifici and others* [1979] ECR 2749, CLI:EU:C:1979:216

C-244/95, *Moskof*, [1997] ECR I-544

C-162/97, *Gunnar Nilsson, Per Olov Hagelgren, Solweig Arrborn* [1998] ECR I-7477

C-308/97, Manfredi v Regione Puglia, [1998] ECR, I-7685

C-173/99, *BECTU* [2001] ECR I-4881

C-110/05, *Commission v Italy* [2009] ECR I-519, Advocate General Léger Opinion

C-435/06, *C* [2007] ECR I-10141

Germany

Judgement of German Federal Court Bundesgerichtshof 28 January 2014 – VI ZR 156/13.

Sweden

Judgement of the Supreme Administrative Court of Sweden on December 4th 2017 in case number 3716-16 (HFD 2017:67)