【Article】

Interface of Patent and Trade Secret Protection for Artificial Intelligence in Personalized Medicine

LEE Nari[*]

Contents

I. Introduction

Personalized medicine is a developing field that carries a great potential for future healthcare applications, for prediction, diagnostic and treatment. Personalized medicine allows targeted treatment of different subgroups of patients, making it possible to tailor the treatment to the best-responding patients, while avoiding non-responders who are likely to

[*] Professor of Intellectual Property Law, Hanken School of Economics, Helsinki, Finland. This paper is based on the chapter submitted for publication in, Jens Schovsbo, Timo Minssen and Thomas Riis (eds), 'The harmonization and protection of trade secrets in the EU – an appraisal of the EU Directive' (forthcoming, Edward Elgar).

suffer adverse effects. Data that allows identification of the applicable patient group and correlating them to underlying conditions is crucial in the research for personalised medicine. As commercial opportunities expand and develop without heed to legal categories, every new technological disruption such as personalized medicine and artificial intelligence (AI) may raise claims of inadequacy of intellectual property (IP). Over and under protection and fragmentation or overlaps in exclusivity may harm efficient use of resources. While the need to share personal and private genetic information to advance research and industrial development is acknowledged, there are fundamental moral and ethical discomfort against exclusive control of an individual right holder over genetic data.

Trade secret protection seems to provide a perfect solution to this problem.[1] Trade secret protection could include most subject matters of intellectual property as well as other ineligible subject matters, such as raw data, information and knowledge. In the new technologies, trade secrets protection may indeed become a substitute for other types of IP, especially when greater restrictions are imposed on traditional subject matters. Arguably, when the US Supreme Court imposed stricter subject matter requirements for patents in software and biogenetic technology,[2] businesses have migrated to protect data or algorithm directly using trade secret law.[3] Moreover, as expressive works or methods may also be protected by trade secrets, works such as computer program codes produced by Artificial Intelligence (AI), as well as algorithms for AIs may be protected as trade secrets even though their protectability under copyright may be more uncertain. As regulations on public disclosure for public access to information treat trade secrets differently from other types of information,[4] trade secret protection may be considered a versatile tool to avoid public

[1] Jerome H. Reichman, Legal Hybrids Between the Patent and Copyright Paradigms, *94 Columbia Law Review 2432-2558* (1994)

[2] *Alice Corp. v. CLS Bank International*, 134 S. Ct. 2347 (2014); *AMP v Myriad Genetics*, 133 S.Ct. 2107 (2013).

[3] See for example, Dan L. Burk, Patents as Data Aggregators in Personalized Medicine, *21 Boston University Journal of Science and Technology Law 233* (2015) at 242-245; Jacob S. Sherkow & Christopher Thomas Scott, The Pick-And-Shovel Play: Bioethics For Gene-Editing Vector Patents, 97 *North Carolina Law Review* (forthcoming 2019)

[4] For example, the US Freedom of Information Act exempts trade secrets categorically from its scope. 5 USC § 552(b)(4). See for a comparative study, Sharon K. Sandeen and Ulla-Maija Mylly, Trade Secrets and the Right to Information: A

scrutiny over sensitive information.

Restricting patenting of algorithms for fear of depriving the public of the basic research tools, simultaneously creates incentive to protect them with other means such as trade secret, which then would be used as a way to deprive the public of the access to the information. Indeed scholars have already started to notice the switch and warned of the impact on incentives and competition.[5] Burk, for example noted that while patents in personalized medicine may fail to provide necessary incentives for innovation and yet could be used as to aggregate and re-capture valuable sub-patentable data which the companies may protect with trade secret protection.[6] Likewise, Sherkow and Scott documented a problematic trend among the vector developers for gene editing technology - what they call a 'pick and shovel' play, using secrecy as a way to sell gene editing equipment.[7]

This paper explores the interface of patent and trade secret protection of AI algorithm and data in Europe.[8] The paper first examines current status of using AIs in personalised medicine and explores if patent or trade secret protection would be better suited to deal with the problems faced by use of AI on personalised medicine. From the policy perspective, patents that allow disclosure may be a better choice. Although concurrent use may be allowed, this chapter argues that trade secrets misappropriation may limit such uses, and concludes

Comparative Analysis of EU and US Approaches to Freedom of Expression and Whistleblowing (August 26, 2019). *North Carolina Journal of Law and Technology,* Forthcoming. Available at SSRN: https://ssrn.com/abstract=3442744

[5] William Nicholson II Price, Expired Patents, Trade Secrets, and Stymied Competition (December 22, 2016). 92 *Notre Dame L. Rev.* 1611 (2017)

[6] Dan L. Burk, Patents as Data Aggregators in Personalized Medicine (April 22, 2015). 21 *Boston University Journal of Science and Technology Law* 2:233-255 (2015) at 244-245.

[7] Jacob S. Sherkow and Christopher Thomas Scott, The Pick-and-Shovel Play: Bioethics for Gene-Editing Vector Patents (June 27, 2019). *North Carolina Law Review, 2019*, vol. 97, pp. 1497–1552.

[8] 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 (Text with EEA relevance) OJ L 157, 15.6.2016, p. 1–18 [hereinafter Trade Secrets Directive], 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, 4.5.2016, p. 1–88 [hereinafter GDPR] Directive 98/44/EC of the European Parliament and of the Council of 6 July 1998 on the legal protection of biotechnological inventions OJ L 213, 30.7.1998, p. 13–2; Agreement on a Unified Patent Court, Document no. 16351/12. (11 Jan. 2013) [hereinafter, 'UPCA']. Convention on the Grant of European Patents of 5 Oct. 1973, as revised [hereinafter 'EPC'].

that it may have become necessary to introduce additional regulatory measures to require disclosure of AIs algorithm for public interest. However, such measure needs to take both technical solutions to make AI more understandable if not transparent into consideration and regulatory solution to preserve the secrecy of AI information.

II. Regulatory Challenges in the Use of AI in Personalised Medicine

AI is a combination of theories, techniques and applications that make machines behaving 'in ways that would be called intelligent if a human were so behaving.'[9] AI thus may include various different technologies using different methods of making machines behave 'intelligently' - sense, read and understand things around them, collect text and image data that they so gathered and analyse, and make decisions. The essence of AI's 'intelligence' is when such decision-making seems autonomous of human agents' instructions or interferences, and machines may appear to be sentient and learning autonomously - so called 'Machine Learning' (ML). The idea of sentient machine has been around for some time. But, the investments and interests in AIs have increased dramatically with the reports of successful AI and ML, resulting from better and more computing power and digital computing tools (code libraries), developments in communication and network technology, emergence of new learning algorithms (deep neural networks) and availability of training data (big data).

Using AI in personalized medicine marries two uncertain and yet exciting disruptive technologies - digital computing and bio-genetic medicine. In both fields, technologies seem to promise much possibilities and opportunities to increase efficiency in health care and yet, at the same time, present complex uncertainties, which may invite regulators' scrutiny. Personalized medicine and smart digital technology have brought on both promises and concerns for society that to the degree that one author declared the end(s) of law.[10] Despite foreboding predictions and fanatic enthusiasms brought on by private and public sector

[9] J.McCarthy, M.L.Minsky, N. Rochester, & C.E. Shannon. A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence, August 31, 1955. *AI Magazine*, 27(4), 12. (2006) https://doi.org/10.1609/aimag.v27i4.1904

[10] Mireille Hildebrandt, *Smart Technologies and the End(s) of Law*, Cheltenham: Edward Elgar (2015)

financing, personalized medicine or precision medicine have yet to deliver a panacea in health care.[11] Benefits from personalized medicine, which promise to deliver targeted and tailored healthcare have yet to be fully materialized and at the same time, problems that an extreme personalised medicine have already been noted.[12] Gene editing using CRISPR-Cas system,[13] which promises ultimate personalization[14] has raised several difficult question of rights fragmentations[15] as well as question on genuine inventorship.[16] Experimentation on human genome using the technology,[17] resulted in scientists' call for moratorium on the use of the technologies on heritable genome editing.[18]

Similarly, use of AI in medicine created unique problems and challenges. For regulators, using AI in decision-making raises questions of transparency and accountability that are

[11] See for example, Liz Szabo Are We Being Misled About Precision Medicine? *New York Times*, 11 September 2018 https://www.nytimes.com/2018/09/11/opinion/cancer-genetic-testing-precision-medicine.html,

[12] See for example, Shubha Ghosh, Decentering the consuming self: personalized medicine, science, and the market for lemons, *Wake Forest JL & Pol'y* 5 (2015): 299.

[13] Martin Jinek et al. A- programmable dual-RNA–guided DNA endonuclease in adaptive bacterial immunity, *Science* Vol 337 Issue 6096 (2012): 816-821.

[14] Anjana Ahuja, Beyond 'superbabies': how CRISPR is revolutionising medicine, *Financial Times* Jan 14. 2019, https://on.ft.com/2Rpf1iu

[15] Jorge L Contreras and Jacob S. Sherkow, CRISPR, Surrogate Licensing, and Scientific Discovery. *Science,* Vol. 355, Issue 6326 (2017) 698-7000

[16] See EPO CRISPR opposition decision of 17.1.2018 revoking EP 2771468 (2018) https://register.epo.org/application?documentId=E1N2PXYP4751DSU&number=EP13818570&lng=en&npl=false US PTAB Decision (2017)- CAFC appeal actually is pending (30.4.2018 oral hearing) 13818570. See for a good review of the conflicts among the patenting priorities, Timo Minssen, and Esther van Zimmeren, and Jakob Wested, Clearing a Way Through the CRISPR Patent Jungle (May 8, 2018). *Life Sciences Intellectual Property Review (LSIPR),* No. 8/5 2018, (2018). Available at SSRN: https://ssrn.com/abstract=3359717

[17] See David Cyranosk, CRISPR baby scandal. The CRISPR-baby scandal: what's next for human gene-editing, *Nature* 566, 440-442 (2019) doi: 10.1038/d41586-019-00673-1. Technology was not mature enough and as a result, it is expected that babies' mortality is high. See Xinzhu Wei & Rasmus Nielsen, CCR5-Δ32 is deleterious in the homozygous state in humans, *Nature Medicine,* volume 25: 909–910 (2019).

[18] See Adopt a moratorium on heritable genome editing Eric S. Lander, Françoise Baylis, Feng Zhang, Emmanuelle Charpentier, Paul Berg, Catherine Bourgain, Bärbel Friedrich, J. Keith Joung, Jinsong Li, David Liu, Luigi Naldini, Jing-Bao Nie, Renzong Qiu, Bettina Schoene-Seifert, Feng Shao,Sharon Terry, Wensheng Wei & Ernst-Ludwig Winnacke, *Nature* 567, 165-168 (2019) doi: 10.1038/d41586-019-00726-5, See arguments that these are not novel problems: John J. Mulvihill, Benjamin Capps, Yann Joly, Tamra Lysaght, Hub A. E. Zwart, Ruth Chadwick, The International Human Genome Organisation (HUGO) Committee of Ethics, Law, and Society (CELS), Ethical issues of CRISPR technology and gene editing through the lens of solidarity, *British Medical Bulletin*, Volume 122, Issue 1, (June 2017), Pages 17–29, https://doi.org/10.1093/bmb/ldx002. W. Nicholson Price II Black-box medicine. 28 *Harv. JL & Tech* 419 (2014).

embedded in the practice of medicine and pharmacology.[19] In medical practice, there are established process of peer review on the safety and efficacy of the process as well as verification of the validity of data that the medical professionals rely on to come to various health care related decisions. AIs, notability uses black box like decision-making process, and may not be able to provide explanation for its decision.

III. Trade-offs in the Use of AI in Personalized Medicine – Patents or Trade Secrets

Trade-off between patents and trade secrets in personalized medicine illustrates the interconnectedness of the policy agendas – the incentives through exclusive rights need to be coordinated to the transparent and accountable use and developments of the technology. For the regulatory goals of accountability, and transparency, disclosure and communication and explanation would play a big part. Other exclusive rights such as copyright over the codes for AIs, over training data are also important incentives for creation and investments and yet, publication and disclosure of codes or data will not affect their copyrights. In contrast, patent and trade secrets occupy opposite ends on the impact of disclosure as patent requires disclosure for protection and disclosure destroys trade secret protection. Moreover, there is underlying question concerning the status of personal data – health (including genetic) data that AI uses, if they may be made subject matters of exclusive rights at all.

1. AI as a Subject Matter of Patent or Trade Secret

AI includes various elements – algorithm and training process, training data, parameters including parameter weights, application, computer or other hardware devices. Application and implementation themselves could be computer programs and codes. As AIs are based on various techniques,[20] to state that all AIs can be categorised as (1) *algorithms and models* at

[19] Frank Pasquale, *The Black Box Society*. Harvard University Press (2015). See also Hildebrandt, supra n 10.

[20] For example, EPO Examination guidelines states that AI includes, computational models and algorithms for classification, clustering, regression and dimensionality reduction, such as neural networks, genetic algorithms, support

varying degree of abstraction (abstract algorithms, software, inference models, training process), (2) *data* (training data as well as intermediate data and data sets such as weights), and (3) *hardware* (computer, robots, cars, sensors, storage medium, other devices) would be a gross simplification. However, these three forms are useful in conceptualizing protection of AI through intellectual property because they are the basis of existing categories of patentable subject matters. Patent laws protect inventions of technology and yet excludes certain subject matters and distinguishes tangible hardware from software, and abstract algorithms from concrete computer implemented software, and abstract data from concrete data.[21] As copyright attaches to original works of expression and although flexible threshold, it does not protect underlying idea or functionality, facts nor raw data without originality. To conceive a copyright protection, whether these categorical elements of AIs (algorithm, data and hardware) can be expressed as original work (coded expression, original data or shapes) or not (algorithms, raw data, functionality) is an important exercise.

Such exercise would be unnecessary for trade secret protection. As the definition of trade secrets in the TRIPs Agreement and the article 2(1) of the Trade Secrets Directive provide,[22] a trade secret is information that is *secret, has commercial value due to secrecy* and has been subject to *reasonable steps* of keeping it secret. These elements of *secrecy, value and reasonable steps* – are commonly found in national laws.[23] Arguably, the reasonable steps of keeping the information secret and value are two strong requirements for the protection and factually difficult to prove.[24] However, as the definition of trade secret is information, all

vector machines, k-means, kernel regression and discriminant analysis. (EPO Guideline G-II.6 at 3.3.1) <http://documents.epo.org/projects/babylon/eponet.nsf/0/2A358516CE34385CC125833700498332/$File/guidelines_for_examination_2018_hyperlinked_showing_modifications_en.pdf>

[21] EPC Art 52. Alice Corp. v. CLS Bank International, 573 U.S. 208 (2014)

[22] TRIPS Agreement Article 39.2. Also Art 2(1) of Trade Secrets Directive.

[23] EU member state practice survey before the adoption of the EU Directive. Study on Trade Secrets and Confidential Business Information in the Internal Market, (2013). European Commission. Last visited 5 March 2018, http://ec.europa.eu/growth/content/study-trade-secrets-and-confidential-business-information-internal-market-0_en See also for example, US's DTSA in 18 USC§ 1839 (3). Japanese Unfair Competition Prevention Act (UCPA) Art 2(6) requires secrecy (not known), kept secret and commercial utility.

[24] For example, M. Risch, Why Do We Have Trade Secrets, 11 *Marq. Intell. Prop. L. Rev.*1 (2007). See also Bone Robert G, Trade secrecy, innovation and the requirement of reasonable secrecy precautions, IN Rochelle C. Dreyfuss and

aspects of AI – inference models, algorithms, all types of data (training data, intermediately produced data, nods, weights, finally produced data and the like), computer program codes as well as specific hardware for particular aspects of AI are inherently eligible for protection, if they are not known (secret), valuable and can subject to secrecy measures.

The qualitative difference for eligibility makes a strong case for why trade secret could be a flexible choice when formal IP right based protection is uncertain. As personalized medicine using AI marries two such contested subject matters, they may seem to be a perfect candidate for trade secret protection. Not only trade secret would allow protection of contested subject matters or sub-patentable elements, it may be useful in dynamically protecting the inputs as well as the intermediate or final outcomes of AIs. AIs classifies, infer and make decisions, which means generation of more algorithms, codes, weights and data sets and information while using them. These elements may not be fixed or stable enough to generate claims to a registrable right such as patents, but may be protected as trade secrets under secrecy measures against misappropriation, as long as their value lasts, without extra formalities of application and registration.

2. Patent Infringement vs Trade Secret Misappropriation

Patents has *erga omnes* effect and it is a right that may be enforced against anyone who are making, using or selling patented invention. Patents have obvious strengths in the enforcement over trade secrets. The objective construction of direct patent infringement liability makes patent based protection more attractive. In addition, there are particular aspects of patent protection that are often highlighted - potential protection against reverse engineering and product by process claim afforded to process invention to protect direct results of using a process. These are examined vis-à-vis protection afforded for trade secrets in the Trade Secret Directive.

Katherine J. Strandburg (eds) *The Law and Theory Of Trade Secrecy: A Handbook Of Contemporary Research*, Edward Elgar Publishing (2011): 46-76.

(1) Objective Patent Infringement and Subjective Trade Secret Misappropriation

Primary liability in patent is often explained as strict liability, which 'requires no knowledge or intention on the part of the alleged infringer, whose state of mind is wholly irrelevant' to infringement.[25] Knowledge and intent are often considered subjective requirements often associated with secondary or third party liability. As patents are published and disclosed, ignorance of patent - good faith infringement- may not be a defense. Secondary liability for indirect patent infringement extends it to a broader range of subject matters (parts) by a broader class of actors, who have active with knowledge or intent of their wrongdoing.

In contrast, trade secret protection seems to be a form of compensation for broken promises. Often trade secret protection is provided in unfair competition law, which targets commercially dishonest conduct of unfair competition. Before harmonization, some EU jurisdictions provided civil law remedies whereas others protected trade secrets by criminal law.[26] Trade Secret Directive extends primary liability to unlawful acquisition i.e. '*unauthorised* access to, appropriation of, or copying of any documents, objects, materials, substances or electronic files, lawfully under the control of the trade secret holder, containing the trade secret or from which the trade secret can be deduced' or other forms of commercially dishonest acquisition[27] and use and disclosure of trade secrets, without the consent of the trade secrets holder by a person who either unlawfully acquired or against a duty of confidence or other duties limiting its use.[28] As such, trade secrets seem to be a defensive right against specific wrongdoers, who are given explicit or implicit notice of a duty of confidence or non-disclosure.

[25] Citation is to UK's Supreme Court, Lord Neuberger, *Vestergaard Frandsen A/S and others v Bestnet Europe Limited and others* [2013] UKSC 31 at para 37. This type of statement is found in majority of patent textbook.

[26] See for EU member state practice survey before the adoption of the EU Directive. Study on Trade Secrets and Confidential Business Information in the Internal Market, (2013). European Commission. Last visited 5 March 2018, http://ec.europa.eu/growth/content/study-trade-secrets-and-confidential-business-information-internal-market-0_en

[27] Trade Secrets Directive, Art 4.(2)

[28] Trade Secrets Directive, Art. 4.3

(2) Reverse engineering of AI inference models in patent and trade secrets

As independent invention is not a defense to patent infringement, concurrent use of an invention by an independent inventor is still considered infringing working of the claimed invention[29]. Reverse engineering - a conduct of figuring out the underlying invention from openly available sources of information may well be covered by a patent protection, unless it could be excused from limitation and exceptions in patent law.

Although exceptions to patent right is not harmonized in Europe, UPCA provides a list of limitations and exceptions that are applicable to patents with unitary effect, if and when UPCA would go into effect.[30] While independent invention is still not a defense to patent infringement, Art 27 of the UPCA provides general exceptions for unitary and European patents to acts done privately and for non-commercial purposes; and acts done for experimental purposes relating to the subject matter of the patented invention.[31] Private use and experimental use exceptions are both widely present in national patent laws, although the scope on experimental use exception varies. By explicitly limiting the scope of experimental use exception to the 'purposes relating to the subject matter', the particular version of exception included in the UPCA makes its scope narrower than some of the national practices. Moreover, a new exception is inserted in consideration of right to reverse engineer[32] provided under Software Copyright Directive.[33] The text of the exception

[29] TRIPS Agreement Article 28

[30] UPCA is not yet in force and its taking effect in the near future is in serious doubt. Following Britain's withdrawal from the EU on 31 January 2020, UK has informed that despite their ratification in 2018, UK will not apply UPCA to Britain. Moreover Germany has still not ratified at the time of this writing, which is one of the required member states to ratify, as the seat of central division which include UK, Germany and France. On 13 February, 2020 German Federal Constitutional Court (Bundesverfassungsgericht) ruled that German Act on Unitary Patent was unconstitutionally legislated, based on procedural ground in the decision 2 BvR 739/17 (13.2.2020). Even if German parliament rectifies the situation by legislate the act and remedy the procedural errors, without UK, UPCA and the entire unitary patent package would require immediate revision.

[31] UPCA Art 27(a) and (b)

[32] UPCA Art 27(k) the acts and the use of the obtained information as allowed under Arts 5 and 6 of Directive 2009/24/EC, in particular, by its provisions on decompilation and interoperability.

[33] Directive 2009/24/EC of The European Parliament and of The Council of 23 Apr. 2009 on the legal protection of computer programs. OJ L 111, 5 May 2009 (hereinafter SW Directive).

however makes sure the right to reverse engineer is limited to particular types of reverse engineering (decompilation and interoperability). Thus it seems to be a narrower type of exception that could have been provided under the application of, for example, experimental use exception. In other words, reverse engineering to acquire the underlying knowledge of the claimed invention may be allowed under either the new exception or under the experimental use exception. However, application of the knowledge – for example, using it to create a competing product, that partially using the elements claimed in the patent invention would likely to fall outside the scope of the exception.

In contrast, as trade secret allows concurrent use of the same information, even in cases where the same information is used to create identical goods, if there is no unlawfulness in the acquiring, disclosing or using of the information. For example, in Art. 3(1)(a) and (b) of the Directive, it is provided that the independent discovery or creation and reverse engineering may be used lawfully to *acquire* trade secrets information.[34] Trade Secrets Directive provides in the article 3 as lawful the acquisition by 'independent discovery or creation and observation, study, disassembly or testing of a product or object that has been made available to the public or that is lawfully in the possession of the acquirer'.[35] As the use and disclosure of such lawfully acquired information is not explicitly provided as lawful, member states may seem to some latitude in legislation.[36]

However, a closer look reveals that such allowed reverse engineering seem to be limited, as they may still be considered misappropriation[37] if they meet the definition of unlawful use or disclosure provided under the article 4.3(b) or (c), which is a use or disclosure in breach of a confidentiality or non-disclosure, or contractual or *other duty to limit the use*.[38] Thus, if the trade secret holder restricts such use of lawfully acquired information,[39] use and

[34] Trade Secrets Directive, Art. 3

[35] Trade Secrets Directive Art 3.1 (a) and (b)

[36] Trade Secrets Directive Art 3.2

[37] Art 4 (2) provides two types of unlawful acquisition – acquisition without authorization or commercially dishonest acquisition.

[38] Article 4 (3)

[39] Trade Secrets Directive, Art. 4.3(c).

disclosure of such information may also constitute basis for primary liability. While the duty of confidence/non-disclosure or contractual limit may be clearly understood, it is unclear when such 'other duty of limitation' may arise. Would it be sufficient when there is a unilateral notice of trade secret assertion sufficient to impose such duty? As there can be no ex ante notice of trade secret to the public, it would be crucial to narrowly interpret the cases where the duty of limitation arises, particularly in connection to the third party liability, in particular. As the Directive is a minimum directive,[40] member states at least provide these conducts as unlawful, and thus, in plain understanding of the text, if member states were to legislate use and disclosure of reverse engineering to be lawful, it would be allowed only in cases where there is no duty of confidence or limitation to the contrary.

Reverse engineering has been considered to be a weakness of trade secret protection for AI algorithms for example. For example, when an AI algorithm is used in a personalized medicine end user product - such as diagnostic kit, and patents cover only the product and algorithm is kept secret, reverse engineering may reveal the underlying AI algorithm. Arguably, if AI algorithms (such as inference models) are only protected with trade secrets and not patent, then reverse engineering could be used to identify the inference model. However, as we have seen in the above, it is entirely possible for a member state define a commercial use of reversely engineered trade secrets information unlawful.[41]

Moreover, the new liability that allows tracing of misappropriation via trading of infringing goods seem to shift trade secrets toward in rem like right. The EU Trade Secrets Directive provides secondary liability for third parties. In Article 4(4), the liability of third parties extends not only to the acquisition, but also to *use and disclosure* of the trade secrets, subject to actual or constructed knowledge requirement.[42] More importantly, a new type of liability is now imposed. Article 4(5) imposes liability on the knowing traders of 'infringing goods', defined as 'goods, the design, characteristics, functioning, production process *or*

[40] Article 1(1)

[41] See Art 6.2 SW Directive takes this position on the reversed engineered SW codes. The Directive however provides for a first sale exhaustion doctrine for distribution right, which may function as a general good faith purchaser's exception.

[42] Art 4(4) of Trade Secrets Directive.

marketing of which *significantly benefits* from trade secrets unlawfully acquired, used or disclosed.'[43] As the significant benefit is not tied to technical benefits, there is a theoretical possibility that the scope of protection could go beyond what is provided under the secondary liability for patent infringement (i.e. essential elements of the claimed invention).[44] While indirect patent infringement liability similarly extends liability to partial knowing users, it is limited to third parties who provides means relating to *essential* elements for putting the protected invention into effect.[45] The test for determining when a product is infringing for patents thus always require objective analysis, whilst the test for trade secret misappropriation is mostly subjective.

In sum, the scope of the lawful reverse engineering Trade Secret Directive seems to be aligned with patent exceptions envisioned under the UPCA Art 27(k). Moreover, with the new infringing goods liability imposed on the knowing trader, trade secret seems to be able to provide similar level of protection, as patents at least in cases where there are tangible goods used in personalized medicine. Such protection, as seen below, may be more efficient than relying on patent protection through product by process claim, directed to AI algorithms and processes.

(3) Product by Process in Patent and Trade Secrets

Theoretically, any automated data or information processing could result in a processed data sets or information that could be considered to be directly obtained by the process. If AI uses deep neural network (a form of machine learning algorithm), dynamic weights and nodes are formed where intermediary data are produced and processed. Whether patents

[43] Art 2(4) of Trade Secrets Directive, emphasis added. See for a discussion of various versions of the Directive, Tanya F. Aplin, A Critical Evaluation of the Proposed EU Trade Secrets Directive (July 18, 2014). King's College London Law School Research Paper No. 2014-25. Available SSRN: https://ssrn.com/abstract=2467946 or http://dx.doi.org/10.2139/ssrn.2467946

[44] UPCA Article 26(1).

[45] See UPCA, which provides in Art. 26: 'A patent shall confer on its proprietor the right to prevent any third party not having the proprietor's consent from supplying or offering to supply … with means, relating to an essential element of that invention, for putting it into effect therein, when the third party knows, or should have known, that those means are suitable and intended for putting that invention into effect.'

could extend to these intermediate data sets have been disputed and generally they would not have been considered a 'product obtained by the process.' As we have examined above, if interim data structures, data sets, or information that are produced by AIs would make patent protection of AI algorithm more efficient than trade secret. In EPC, the article 64.2 of EPC and at least a theoretical possibility to extend that to information an intermediate datasets or other types of 'products' exists. Indeed, if such interpretation is possible, patent claims to AIs would be able to be used to cover not only data and information produced by the AIs, but paintings, or patentable inventions that may be made by AIs.[46]

Ultimately, this is a question of scope of granted patents and without UPCA in effect, contracting states of EPC's national law would interpret this in light of their national equivalent clauses. Recent German interpretation is illustrative in this regard. In 2010, for example, the district court of Düsseldorf seemed to view that a process claim to perform a genetic rest for a dog does not cover the test result is viewed a pure information.[47] In contrast, in a case which involved question of method of encoding and decoding of video according to the MPEG-2 standard, where medium that contained the encoded data was shifted, while leaving the data intact and the German Federal Supreme Court ruled that the data may be the product directly produced by a process when 'it displays technical features and by its nature can be suitable subject matter of a patent.'[48] Applying these to medical diagnostic technology, the Court in 2016 ruled that the representation of a test result obtained by means of a patented

[46] In the example above, drug discovery done by EVE, on the new medical indication for tricslosan, may be covered by the claims to core of EVE algorithm.

[47] *Landgericht Düsseldorf* of 16 February 2010, Case 4b 0 247/09—Hunde-Gentest, available at: <https://www3.hhu.de/duesseldorfer-archiv/?p=813> (accessed 10 September 2016). Drexl argued that Court may be showing a policy consideration for free flow of data as the test was done in outside the country of patent grant, while only the result was communicated to the country of patent grant. See Josef Drexl, Designing Competitive Markets for Industrial Data – Between Propertisation and Access, (2017) 8 *JIPITEC* 257 at 270.

[48] MPEG-2-Videosignalcodierung" ("MPEG-2 video signal encoding"), Decision of the Federal Supreme Court (Bundesgerichtshof), Judgement of 21 August 2012, X ZR 33/10.

method is a presentation of information and thus is not covered by product by process protection in German law.[49]

The case concerned a method of diagnosing leukemia by detecting presence of mutation in FLT3 gene. The claimed process in the disputed was not explicitly directed to the AI method. However, there are already similar patents on genetic analysis using AI,[50] such as those offered by Sophia Genetics[51] as well as Watson for Oncology, which are in the market. The defendants practiced the each step of the invention dividedly- one processed the samples first and forwarded them to another defendant located in Czech Republic who then tested them and communicated the result of the analysis to the clients as well as other defendants. The court ruled that the product by process claim protection is afforded to 'a result is obtained that itself is in principle capable of being the subject matter of a patent…not falling within the scope.. are...results of pure work methods from which no new thing is created but a thing is merely affected by not change, for instance when the thing is tested, measured or transported.'[52] In distinguishing this from the case of MPEG-2 video data, the Court noted that…due to its *data structure and thus due to its technical characteristics*, the data were generally susceptible of patent protection…and not distinguished by a special technical type of representation nor does it display any other technical characteristics that have been given by the invention itself.'[53]

As seen in the above, the logic of the German court seem to be to denying the data or information that are the outcome of the process used if they do not show technical character or using the technical teaching of the invention. This may also mean that if the outcome uses the core of the technical teaching or the result has a technical means of presenting the information (i.e. information displayed on a device) there may be still a possibility to read the product by process claim differently.

[49] Receptor Tyrosine Kinase II (2016) Decision of the Federal Supreme Court (Bundesgerichtshof), 27 September 2016. Case No. X ZR 124/15 Reported in IIC (2018) 49:231-236.

[50] EP1222602 (9.12.2015)

[51] https://www.sophiagenetics.com/home.html, last visited on 30.8.2019.

[52] Receptor Tyrosine Kinase II (2016) Supra note 49, at para 17

[53] Receptor Tyrosine Kinase II (2016) Supra note 49 Para 21 and 24 (bb)

If the method of data analysis was trade secret, outcome of the analysis may be subject to a separate trade secret protection. However, as the outcome needs to be communicated to the client, it may not be subject to secrecy measures and thus may not receive protection of trade secret. However if the result is communicated using tangible goods, knowing trading of such goods would fall under the Art. 4(5) of the Trade Secret Directive. The 'infringing goods' is defined as 'goods, the design, characteristics, functioning, production process *or marketing* of which *significantly benefits* from trade secrets unlawfully acquired, used or disclosed.'[54] This definition of infringing goods makes it necessary to determine what such a 'significant benefit' would be in the case of directly or indirectly obtained trade secrets. Moreover, as 'marketing' is included in the definition of the benefit, the notion seems to go beyond technical features that are directly derived from the trade secret, and includes business secrets. For example, a diagnostic kit could very well be a mixed good embodying technical secrets only in some part. There may be cases where marketing efforts are made using business secrets only in part, or to market perfectly legal products. These cases of mixed goods require a kind of proportionality analysis for technical or business significance of trade secrets in comparison to other factors.[55]

Comparatively, in countries where similar wrongs exist, the wrongs are limited to strictly technical secrets, and there are strong good faith defenses. Indeed, exceptions or defenses for the good faith purchasers of tangible goods may in effect function as a trade secrets exhaustion doctrine for both technical and business secrets. For example in Japan, third party liability for the importers and exporters of products that result from trade secrets is limited to technical information, and the legislative history shows that the liability originally meant to cover object code of digital products produced by using secret source code.[56] The Japanese

[54] Art 2(4) of the EU Trade Secrets Directive, emphasis added. See for a discussion of various versions of the Directive, Tanya F. Aplin, A Critical Evaluation of the Proposed EU Trade Secrets Directive (July 18, 2014). King's College London Law School Research Paper No. 2014-25. Available SSRN: https://ssrn.com/abstract=2467946 or http://dx.doi.org/10.2139/ssrn.2467946

[55] For a concerned comment on the infringing goods misappropriation, see Richard Arnold, Lionel A. F. Bently, Estelle Derclaye, and Graeme B. Dinwoodie, The Legal Consequences of Brexit Through the Lens of IP Law, 101 *Judicature* 65 (2017).

[56] Japanese Unfair Competition Prevention Act, Art.2(1)10

statute also limits its scope by the expression ‘produced by’ which implies that liability is limited to direct results of the use of the trade secret, and good faith purchasers of the goods are explicitly excused.

The combined reading of Art. 2(4) and Art. 4(5) suggests that the liability for the traders of infringing goods could be quite broad. With the liability under Art. 4(5), trading of any tangible good (genetic diagnostic kit connected to central AI databank, server with AI, for example) that utilizes trade secret AI algorithm or data sets, or data structure that significantly benefits the kit, would fall within the scope of misappropriation. Although the information that is produced by using the trade secret algorithm may not be protected as trade secret as it has to be disclosed to the clients, who requested the analysis, trading of the kit or device that may present such information would fall under this liability. In other words, trade secret protection would not only extend to the direct products produced by process i.e. tangible goods embodying the technical secrets, but also those that may significantly benefit from the use of the process i.e sale of kits, including tangible goods that may display the outcome of the trade secret process.

IV. Conclusion

The above discussions have shown that AI holds great promises for advancing personalized medicine. However, real world applications have not been always successful due to technological immaturity, poor data quality and opaque decision making process that hinders validation of technology against the risks. In addition to these challenges, comparison of protectable subject matter and doctrines for infringement and misappropriation in patent and trade secret law show that there could very well be cumulative protection.

The comparison reveals that patents and trade secrets may overlap over the same subject matters of AI algorithm and data. Under the EPC, a tendency to shift from patents to trade secrets may become real, in particular with regard to AI algorithms and data used in training an intermediate or final outcome of AI algorithms, due to their uncertain status as patentable invention. Moreover, their inclusion as elements of the claimed invention, as we have seen in the above may not receive the protection of product-by-process claims. In contrast, thanks to flexible definition of trade secrets, algorithms and data may very well be protected as trade secrets. While patents and trade secrets both may allow acquisition of algorithm using reverse engineering, patent protection would clearly protect against commercial use of acquired algorithms or inference models for AI. While the trade secret directive is silent on the use and disclosure, as seen in the above, unlawful use and disclosure against a duty of limitation would be considered to be a misappropriation of trade secrets. Thus there is a little latitude for member states to allow commercial use and disclosure of reversely engineered trade secrets against the expressed intent of the trade secret holder. Patent protection may not reach to the information or data that are produced by AI algorithm, if they are not patent eligible as such. Yet, with additional liability for those who are trading infringing goods under the Trade Secrets Directive, trade secrets over the AI algorithm may still be used effectively to prohibit the trading of products, such as sale of diagnostic kit, that may otherwise be outside the scope of patent protection.

The confluence of developments such as restrictive patent protection, strong personal data protection and expansive trade secret protection show that three main policy perspectives – (1) incentivising technological maturity and (2) quality in data and (3) the goal of making AI’s decision making process more transparent - may be thwarted. In particular, stronger trade secret protection which may be enforced against knowing traders of tangible goods without connection to the trade secrets holder, seems to elevate the status of trade secrets to near in rem rights. Patents not only incentivise investments in a particular technological prospects, but also stimulate follow on inventions based on disclosure.

Shifting protection to trade secrets may result in both under-use and over-protection of AI algorithms and data, as disclosure is necessary to ensure data validation i.e. safety, effect and efficacy of the AI used in the personalised medicine. To ensure such disclosure, goal-oriented and concentrated efforts, such as those seen in re-defining medical AI as medical device subject to medical device regulation, should ensure that such disclosure would not amount to the loss of secrecy status.

Disclosure may be necessary to guarantee that automated AI driven decision-making are in compliance with data protection regulations, such as GDPR. When AIs routinely processes private medical data, it is further imperative to make sure that such algorithm based decision-making is morally unbiased and ethically correct. Hence the disclosure of the algorithm may be necessary, or at least the possibility to be interpreted or explained, to make sure that it does not contain biases. In addition, technological solutions to make decision making less opaque should be considered. Despites the claims how AI cannot be explained and may obfuscate the biases hidden both in the data as well as in the machine learning algorithms used, there are claims that at least by design it is possible to build explainability or human interpretability. Such technical efforts may still be agnostic and the inference models and the models that it uses may still be irrelevant. However, it is important to continue with such efforts, since it would allow human agents to interpret the decision made by the AIs. This would increase the transparency of the algorithmic decision making without risking the disclosure of trade secrets.