Legal AI from a Privacy Point of View: Data Protection and Transparency in Focus

Cecilia Magnusson Sjöberg

Topic Introduction and Outline

The title of this book chapter implies that the topic chosen is multifaceted. Here, this means that there is a diversity of components to be considered in order to investigate the problem area. Starting points for forthcoming studies are also consequently artificial intelligence (AI)[1] within the legal domain, from the perspective of

[1] A sample of explanatory references in the field comprises Max Tegmark, *Life 3.0: Being Human in the Age of Artificial Intelligence* (London: Penguin Books, 2017); Olle Häggström, *Here Be Dragons: Science, Technology and the Future of Humanity* (Oxford: Oxford University Press, 2016). See further the Swedish Foundation for Strategic Research, *Livet med AI*, SSF report no. 29 (Stockholm: Swedish Foundation for Strategic Research, 2018); the Swedish Ministry of Enterprise and Innovation, *Regeringens nationella inriktning för artificiell intelligens*, N2018.14 (Stockholm: Swedish Ministry of Enterprise and Innovation, 2018); Vinnova, *Artificiell intelligens i svenskt näringsliv och samhälle: Analys av utveckling och potential*, VR 2018:08 (Stockholm: Vinnova, 2018). A policy initiative worth mentioning in this context is addAI, whose mission can be summarized as follows: "What will it mean to be a human in the future? The Swedish-based initiative addAI is collaboration between experts in academia, government and companies to discuss and explore the impact of smart algorithms and AI on society. Sociology: What are the best ways to interact with AI and how may it change the relations between humans? Law: How much responsibility should AI have? AI and the rule of law? Business: What does a AI strategy mean for an organization or a country?" The author of this chapter is a cofounder of addAI.

How to cite this book chapter:
Magnusson Sjöberg, Cecilia. "Legal AI from a Privacy Point of View: Data Protection and Transparency in Focus." In *Digital Human Sciences: New Objects—New Approaches*, edited by Sonya Petersson, 181–202. Stockholm: Stockholm University Press, 2021. DOI: https://doi.org/10.16993/bbk.h.

privacy taking data protection and transparency into particular consideration when aiming also for openness.

In terms of an outline, the notion of legal AI[2] will be addressed first. Then attention will be paid to the surrounding privacy framework. Thereafter, challenges of transparency will be discussed. The quest for regulatory management is illustrated by the Swedish case of being a digitalized European Union (EU) Member State including automated procedures and decision-making. Finally, a selection of ways forward will serve as concluding remarks.

The general hypothesis is that legal AI presupposes privacy in the context of personal data processing. This comprises transparency, which is a kind of overall data protection principle associated with openness and access rights that, in turn, needs to be effectively implemented and managed in order to provide legal safety.[3]

The overall methodological approach in this study can roughly be described as both interdisciplinary and multidisciplinary. The interdisciplinary character is shown by the interplay of law (legal

[2] Wikipedia is a questionable fact-finding source. In a legally oriented text, a limited use can be justified when it comes to the technical domain. (Otherwise it can be questioned if a non-techie is competent to choose one particular definition within the field of computer science.) Here, this concerns a general description of what AI means: "In computer science, artificial intelligence (AI), sometimes called machine intelligence, is intelligence demonstrated by machines, in contrast to the natural intelligence displayed by humans and animals. Colloquially, the term 'artificial intelligence' is used to describe machines that mimic 'cognitive' functions that humans associate with other human minds, such as 'learning' and 'problem solving'." ("Artificial intelligence," *Wikipedia*, https://en.wikipedia.org/wiki/Artificial_intelligence). For a more official source, see Nationalencyklopedin ("Artificiell intelligens," *Nationalencyklopedin*, https://www.ne.se/uppslagsverk/encyklopedi/l%C3%A5ng/artificiell-intelligens), explaining AI as first intelligence ascribed to computer systems and second as a research field oriented toward computer systems exhibiting intelligent behavior.

[3] According to Article 5.1 a) Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 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): "Personal data shall be: (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')."

science) and informatics (computer and systems sciences) being integrated with each other.[4] More precisely, the core of this legal field concerns how law can be proactively embedded at early stages of system design, development, implementation, and management.[5] To exemplify, the quite common question concerning whether a formal legal requirement of a signature in a contract can be fulfilled electronically requires both an understanding of technical means and governing legislation. Adequate problem-solving in such a case would also require an understanding of civil law and/or public law in order to conclude whether an electronic signature at a certain security level would be sufficient to meet evidential requirements, *et cetera*.[6] This kind of legal system management must, in practice, be supplemented by substantive IT law regarding how to interpret and apply legal rules and regulations in digital environments such as the internet. It is here that the multidisciplinary character of this legal field becomes visible by way of requiring command of several legal subject areas, such as security legislation, data protection law, contract law and intellectual property rights.[7]

[4] This paradigm becomes quite clear in Peter Seipel, *Computing Law: Perspectives on a New Legal Discipline* (Stockholm: Liber Förlag, 1977); Cecilia Magnusson Sjöberg, ed., *Rättsinformatik: Juridiken i det digitala informationssamhället* (Lund: Studentlitteratur, 2021); Peter Wahlgren, ed., *50 Years of Law and IT – The Swedish Law and Informatics Research Institute 1968–2018* (Stockholm: Stockholm Institute for Scandinavian Law, 2018). The interdisciplinary approach has also characterized the Swedish Ministry of Finance inquiry, chaired by the author of this book chapter, about how law can support the digitalization of the public sector of society. Swedish Ministry of Finance Public Inquiry, *Juridik som stöd för förvaltningens digitalisering*, SOU 2018:25 (Stockholm: Swedish Ministry of Finance, 2018). On this theme see also Cecilia Magnusson Sjöberg, "Förvaltningslagen och digitaliseringen," *Förvaltningsrättslig tidskrift*, no. 3 (2018): 519–530; Markku Suksi, "Automatiserat beslutsfattande enligt den svenska förvaltningslagen," *JFT* 154, no. 6 (2018): 463–472.

[5] See attempts and achievements in this direction in Christopher Millard, ed., *Cloud Computing Law* (Oxford: Oxford University Press, 2013).

[6] Yet another perspective that has emerged relatively recently is referred to as legal tech, which can be described as modern business models offering legal services through digital means and methods.

[7] See for instance Daniel Westman, "AI, big data och upphovsrätten," in *Rättsinformatik: Juridiken i det digitala informationssamhället*, ed.

A study of this kind requires certain delimitations. The jurisdictional scope is primarily the EU and its Member State Sweden. However, this does not exclude reflections about the state of affairs in other jurisdictions as well as references to literature published internationally. Technologically speaking, the text has been authored by a "non-techie," which means that the author's expertise does not lie in, for instance, analyses of specific code (computer programs) but rather in the ability to reveal how the development and use of AI has legal consequences. Neither will there be specific attempts to clarify how to logically represent open textures and ambiguities in law. What will be addressed though, is a set of focal points regarding the kind of dynamic algorithms, emanating from machine learning taking advantage of huge datasets commonly referred to as big data. As already stated, the perspective of this development will be privacy and more specifically legal means for accomplishing transparency.

Legal AI

Applying compliant legal AI

With reference to the above-presented scientific approach within the research field of law and informatics, we can distinguish two major aspects of legal AI. First, there is the methodological theme about integrating law into different kinds of AI-based applications. Second, there is IT law oriented toward substantive issues of how to interpret and apply legislation (broadly speaking) as well as case law in digital environments.

Consequently, AI applied in the legal domain has potential to enhance e-government in the context of decision-making. Public information supply is another application area comprising, in particular, conventional legal sources such as legislation, decided court cases, documents reflecting the history of lawmaking, and doctrine authored by legal scholars. In this context, hopes are to improve recall and precision within information retrieval and to make relevance ranking mechanisms more intelligent, not least using probabilistic (statistical) and linguistic methods and

Cecilia Magnusson Sjöberg, 4th ed. (Lund: Studentlitteratur, 2021), 639–668.

advanced mathematics. In order to reuse public sector information (PSI) and generate open data, AI attracts increasing attention.

Of course, legal AI has much to contribute also applied in the private sector of society. With regard to the legal profession, conventional and often quite burdensome due diligence processes associated with mergers and acquisitions, which are nowadays commonly carried out by younger lawyers at business law firms, are in the long run expected to be replaced by AI solutions.[8] Similarly, so-called smart contracts based on blockchain technologies have become topical. Mention should also be made of customer profiling, which is a business activity that is already using AI-based methods for assessments of creditworthiness, *et cetera*.

So, while we have AI applied in the legal domain supporting major aspects of legal system management, there must in parallel be supplementary assessments of whether current AI applications are legally compliant. What about self-driving cars and liabilities?[9] Are pricing algorithms on the competitive market at all permissible?[10] To what extent, if at all, are automated assessments of creditworthiness adherent to data protection regulation? There are many questions open for discussion and a selection must be made that follows from the below.

Problem area

Legal AI is a problem area of great interest to both legal scholars and practitioners. Over the years different questions have attracted attention. This is true also when it comes to descriptions of what more specifically is meant by the notion of “legal AI.” Though there are many more or less successful attempts to capture what AI stands for, today there is a variety of concepts that

[8] See further Richard Susskind, *Tomorrow’s Lawyers: An Introduction to Your Future* (Oxford: Oxford University Press, 2017).

[9] Read more in the report of the Swedish Ministry of Enterprise and Innovation Public Inquiry, *Vägen till självkörande fordon – Introduktion*, SOU 2018:16 (Stockholm: Swedish Ministry of Enterprise and Innovation, 2018).

[10] See further Stanley Greenstein, *Our Humanity Exposed: Predictive Modeling in a Legal Context*. Dissertation (Stockholm: Stockholm University, 2017).

appears to be adequate if not comprehensive. This means that the analysis needs to navigate in a landscape characterized by, in particular, digitalization, automation, robots, and what may be referred to as core AI. For instance, many people refer to AI without being precise about whether the term "automation" in a given context refers to conventional use of static algorithms or dynamic ones based on machine learning and trained data.

From a technical perspective, it is understandably important to be specific about what kind of technology is being referred to, but this does not necessarily apply to discussions and analyses in the legal domain. The point is that in this study it is mostly not necessary to uphold a strict distinction between, for instance, soft and hard AI. (The so-called singularity is an extreme situation when AI is tentatively in control of everything.) Currently, it can be argued that there is a scale of AI that gradually challenges legal infrastructures of different kinds. To summarize, the scope here is broad, allowing an open-minded approach to the topic.

The standpoint above means that certain relevance should be attributed to what may be referred to as the "old school" of AI, thriving some 30 years ago.[11] At that time AI developers were struggling with fundamental tasks of rule-based versus case-based reasoning, discussing forward chaining and/or backward chaining, when using so-called inference engines that could only be applied on relatively modest datasets. At that time, major questions concerned the distinction—if there were one—between a decision support system and a decision-making system, how to understand the expert system label,[12] and what the role of a so-called

[11] See, e.g., Anne von der Lieth Gardner, *An Artificial Intelligence Approach to Legal Reasoning* (Cambridge, MA: MIT Press, 1987); Patrick Henry Winston, *Artificial Intelligence* (Reading, MA: Addison-Wesley Publishing Company, 1984). More modern references can be found in Marcelo Corrales, Mark Fenwick, and Helena Haapio, eds., *Perspectives in Law, Business and Innovation: Legal Tech, Smart Contracts and Blockchain* (Singapore: Springer & Kyushu University, 2019); Marcelo Corrales, Mark Fenwick, and Nikolaus Forgó, eds., *New Technology, Big Data and the Law* (Singapore: Springer & Kyushu University, 2017); Marcelo Corrales, Mark Fenwick, and Nikolaus Forgó, eds., *Robotics, AI and the Future of Law* (Singapore: Springer & Kyushu University, 2018).

[12] See, e.g., Richard Susskind, *Expert Systems in Law: A Jurisprudential Inquiry* (Oxford: Oxford University Press, 1988). See also Cecilia

knowledge engineer would be in practice. Critical factors were no doubt the transformation of law into algorithms that would be coded so that computers could execute the programs on certain data input.

Once again it should be remembered that the overall position in this study is that transparency of transformation procedures of this kind is a condition for rightful privacy in the context of personal data processing taking place in an AI setting. However, as will be further deliberated, transparency conceived as a kind of openness is dependent on the existence of access rights and their implementation in various contexts.

Privacy Framework

Governing normative structure

Without here going into an in-depth analysis, there is no doubt that the current privacy framework[13] is important in a discussion about legal AI. Today's governing normative structure can be summarized as follows. Of major relevance is of course conventional law in terms of primarily legislation, case law, government bills, and other documents reflecting the history of lawmaking, doctrine authored by legal scholars, and contract law. One example is the General Data Protection Regulation (GDPR).

Adding to the picture is nowadays also what commonly is referred to as "soft law." Generally speaking, this expression refers

Magnusson Sjöberg, *Rättsautomation: Särskilt om statsförvaltningens datorisering*. Dissertation (Stockholm: Norstedts Juridik, 1992); Peter Wahlgren, *Automation of Legal Reasoning: A Study on Artificial Intelligence and Law*. Dissertation (Deventer-Boston, MA: Kluwer Law and Taxation Publisher, 1992).

[13] Here is not the place to seek understanding and definitions of the notion of privacy beyond a right to be let alone and to have a private sphere. However, a few topical references will be made. One is the Swedish Ministry of Justice public inquiry report about the state of art concerning personal integrity: Swedish Ministry of Justice Public Inquiry, *Hur står det till med den personliga integriteten? – En kartläggning av Integritetskommittén*, SOU 2016:41 (Stockholm: Swedish Ministry of Justice, 2016). Another is an anthology mirroring the modern digital information society: Russel Weaver, Jane Reichel, and Steven Friedland, eds., *Comparative Perspectives on Privacy in an Internet Era* (Durham, NC: Carolina Academic Press, 2019).

to legal steering documents that mostly are not formally binding. In this context, mention could also be made of the independent European Data Protection Board with the overall task of contributing to the consistent application of data protection rules throughout the EU. In addition to some formal decision-making, this is to be accomplished through general guidance and advice and also promoting cooperation between national supervisory authorities, *et cetera*.[14] It is somewhat challenging to add a third perspective of the privacy framework that could be referred to as AI law or digital law. Nevertheless, the major point is to acknowledge the normative steering mechanisms associated with, in particular, dynamic algorithms applied in the legal domain. Furthermore, AI indicates emerging new legal infrastructures past imagination merely a few years ago. Personal data processing comprising very large datasets, which was previously impossible to carry out, is now on the "to-do list" of both private enterprises and public authorities.

Organizational framework

A study of legal AI should not disregard the surrounding kind of organization as a subset of the privacy framework. This relates to the fact that the legal conditions for applying AI vary considerably between the public and the private sectors of society. To briefly illustrate, a public agency must adhere to all public law governing its activities. In addition to constitutional law, this comprises general as well as special administrative procedures legislation, principles of openness and secrecy, and of course data protection rules directed toward authorities specifically. A private party, on the other hand, is not burdened by the same rules and regulations. However, the market needs to be aware of, for instance, consumers' rights, potential liability, competition law, and also data protection regulation applicable to commercially active data controllers and processors.[15] Getting back to the public

[14] See further "About EDPB," European Data Protection Board, https://edpb.europa.eu/about-edpb/about-edpb_en.

[15] See Article 6 of GDPR, establishing legal grounds making processing lawful to certain extent depending on whether the controller is a public agency or not.

sector, it is worthwhile to note legal conditions and constraints also with regard to, for instance, litigation support in courts in comparison to public administration. The latter may in its turn often need to be divided into state applications on the one hand, and municipal ones on the other. This is all due to the fact that the governing legal framework for introducing AI varies considerably between organizations.

Information security

Every comprehensive digitalization effort nowadays gives rise to debates among specialists as well as the general public about how the latest kind of information and communication technology (ICT) will have an impact on society as a whole. Commonly, reflections concern both pitfalls and potentials with regard to anything from freedom of information and expression to job opportunities on the labor market. In this context AI may be referred to as a milestone rarely seen before. To some extent this reflects the overall privacy framework and its aforementioned normative structures. What appears missing, though, or at least too little discussed, concerns the impact of AI on information security and vice versa.[16] Consequently there is a demand for more studies of this perspective. Risk analyses of personal data processing that are directly oriented toward AI applications and managed accordingly therefore appear to be crucial for safe use of this kind of technology.

At a general level, the interplay between information security and data protection applied—also when using AI—could be read as follows: Personal data protection is one way of accomplishing information security. Information security is multifaceted. It covers at least requirements of confidentiality (contractual and/or legislative), integrity (correct/fair), and availability (agreed upon or laid down in law). At the same time, information security is a way of achieving privacy protection. Privacy protection comprises, in its turn, personal data processing (informative privacy) and/

[16] See for example Cyril Holm, ed., *Secure Digitalisation: Nordic Yearbook of Law and Informatics 2016–2018. The Swedish Law and Informatics Research Institute*. Skrifter utgivna av Juridiska fakulteten vid Stockholms universitet nr 86 (Stockholm: Poseidon Förlag, 2019).

or bodily protection. From the above follows that this study concerns privacy in the context of personal data processing.

Transparency Management

Critical factors

The heading of this section indicates that AI proves to be a challenge to transparency.

The underlying argument and associated circumstances can be summarized in the following points:

(a) AI applied in the legal domain requires transformation of law (broadly understood) into algorithms that can be coded and executed by computers.[17]
(b) AI does not merely take advantage of traditional static algorithms but also dynamic self-learning and possibly self-improving ones.
(c) AI is not only about algorithms but also has to do with, for instance, big data management.

Of major concern is how the abovementioned core features challenge transparency, which is a fundamental building block with regard not only to data protection but also to the rule of law as a whole.

Artificial intelligence—at least when it concerns more advanced applications—inherently includes a "black box" of complicated procedures of a kind that not even (the original) programmer is

[17] See, e.g., Magnusson Sjöberg, *Rättsautomation*. The legal implications of code as a kind of law are also discussed by Marek Sergot et al., "The British Nationality Act as a Logic Program," *Communications of the ACM* 29, no. 5 (May 1986): 370–386; See further Joe Collenette, Katie Atkinson, and Trevor Bench-Capon, *An Explainable Approach to Deducing Outcomes in European Court of Human Rights Cases using ADFs*, Department of Computer Science, University of Liverpool, April 2020. Read more about ADF (Abstract Dialectical Frameworks): https://cgi.csc.liv.ac.uk/~katie/comma20.pdf. Lawrence Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books, 1999) and more recently Boris Melvås, "En formaliserad rättsgrammatik," *Förvaltningsrättslig tidskrift*, no. 5 (2018): 937–972.

able to fully grasp. This implies that principles of transparency, legality, and equality are all at danger if clarity about what goes on internally in an AI application is not achieved. Considering the rapid technological development, it does not seem to be any ready-made solution to the problem of hidden data processing. Right now, the least we can do to master this kind of machine learning, based on trained data and encapsulated in a diversity of other data processing functions, is to aim for legally valid transparency management. Put simply: why not let a legal shield enclose the "black box," ensuring at least awareness of legal rules and principles and thus enhancing trustworthy AI?[18] Below follow a few reflections in this direction heading toward transparency management.

Access rights

Given the above starting point that transparency is a condition for privacy in the context of personal data processing based on AI methods, it is relevant to further examine the legal implications. A major keyword in this context is, as already pointed out, openness, which, however, is not equivalent to transparency. This is explained by the fact that an organization may very well be governed by principles of openness but still not provide transparency due to insufficient access rights taking into consideration also their implementation.

Aiming for a holistic approach—here referred to as transparency management—a need for a legal shield emerges (as acknowledged above) in order to partially cope with the AI "black box" problem. Such a legal shield could very well address and hopefully proactively cover a whole set of legal issues depending on the kind of AI application that is at hand. Is it, for instance, dedicated to the

[18] The idea of a legal shield is not new as such but has been introduced within the framework of GDPR and the regulation of transborder flows of personal data (see Articles 44–49). An EU policy initiative worth mentioning in this context is the establishment of a High-Level Expert Group on Artificial Intelligence (AI HLEG): https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence. Among many different deliverables, it is here interesting to note ethical as well as legal guidelines aiming for trustworthy AI.

public and/or private sector of society, does it give rise to questions concerning intellectual property rights such as copyright, is the dimension of international private law central, *et cetera*?

Within the framework of the analysis carried out here, a major legal shield component concerns access rights. In the Swedish legal system, which will serve as an example for embedded law by way of a legal shield adhering to AI applications, there are three major categories of access rights and another one of a somewhat different kind.

Without any type of internal ranking, the first one concerns the Swedish principle of openness laid down in Chapter Two of the Freedom of the Press Act, dating back to 1766. In brief, this right gives anyone, whether a natural person or a legal person, a Swede or a foreigner, for any kind of purpose (nonprofit or commercial interest), a right of access to official documents that are deemed public. The second access right concerns case-based material. With reference to provision 10 of the Swedish Administrative Procedure Act (SFS 2017:900), any party has a right to be made aware of all material that has been added to the case from external sources. The third access right relates to data controllers' information duties and in particular data subjects' right of access according to Article 15 of the GDPR.

As indicated above, there is yet a legal framework that calls for attention in spite of not quite qualifying as an access right *per se*. It concerns the European Directive on the reuse of PSI.[19] This EU PSI regulation provides a legal platform enhancing open data, but also taking into consideration constraints associated with primarily third parties' rights. Important to note here is that the EU PSI legislation does not provide a strict right of access on behalf of the general public. It is rather a kind of law embracing public authorities to engage in open data solutions that will facilitate the digital society in general.

Implementation

The benefits of access rights are no more than what their implementation shows. To summarize, true openness presupposes

[19] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the reuse of public sector information.

transparency that, in its turn, depends on the presence of access rights that are rightfully implemented. Stakeholders are to be found both among the general public and in the private sphere. In practice, it necessitates both adequate rule interpretation and rule application of the legal framework of openness.

From the above follows that there is a whole chain of components that are crucial in order to accomplish openness based on transparency management. This reasoning gets even more complicated when AI is added to the picture. With this in mind, the three (almost four) aforementioned access rights will be commented upon in a more AI-oriented perspective. To begin with, the (Swedish) principle of openness with regard to the right of access to public official documents should be mentioned. Then there is the regulation authorizing parties in administrative procedures to receive all kinds of relevant case material. A fundamental aspect of privacy connected to personal data processing is transparency based on a right of access that once again calls for attention.

(a) One of the conditions in the Swedish Freedom of the Press Act for accessing what is referred to as compilations of data from already existing official documents requires that this be possible to achieve by so-called routine measures. The fundamental law itself does not explain what is to be understood by this concept, but some guidance can be found in the documents reflecting the history of lawmaking, in particular the underlying government bills, and also some case law. More precisely, it is made clear that so-called routine measures should be understood in terms of a simple effort, without any significant costs or other complications on behalf of the public authority keeping the digital compilation in question.

The key AI issue here is the dynamic character of the notion of routine measure. The major reason is that what qualifies as a simple effort in a more traditional digital environment will most probably not give the full picture in a future characterized by AI-based ICT. When (and if) AI is used, much more information will naturally fall within the scope of the principle of openness. Whether this is good or bad is a question with potential political consequences that needs a separate analysis regarding not only privacy but also freedom of expression and information. This also applies to options for a legal shield.

(b) In the Swedish Administrative Procedure Act, the major access right is to be found in 10 §. The context is that of case handling by public agencies and the right of external parties to take part of what has been added to their matter. The overall regulatory approach is characterized by technical neutrality, that is, without specifying any particular digital solution to (electronic) document management in the Act. There is, however, one exception to this and that is the fact that 28 § of the Act explicitly states that decisions can be made automatically. This leads us into yet another AI reflection.

The provision as such does not provide a right of access to a public agency's internal material such as coded algorithms and selected datasets used for machine learning. So what are the legal consequences of public agencies engaging in cross-organizational digital platforms using AI methods? Today there are already indications of governmental agencies being actively involved in sustainable and innovative AI solutions of this kind. This indicates that AI solutions will rapidly fall within the scope of 28 § of the Administrative Procedure Act, regulating automated decision-making. From the perspective of legal system management, this development is also relevant in a discussion about a legal shield embracing the "black box" commonly referred to in discussions about AI.

(c) Shifting the focus to rights of access by a data subject, current information duties on behalf of a controller are primarily to be found in Articles 13–15 and 22(1) of GDPR. Article 13 is applicable where personal data is collected from the data subject and Article 14 where personal data has not been obtained from the data subject but from another source. Article 15(1) h) is triggered as a right of access by a (potential) data subject, that is, a natural person as the GDPR is not applicable to legal persons (Article 1). Article 22(1) h) governs automated individual decision-making, including profiling. All these provisions except Article 15 are for the controller to be aware of and fulfilled on its own initiative. Article 15 is instead triggered upon a request by a data subject.

What strikes as particularly noteworthy from an AI perspective is the requirement, under certain circumstances, to provide meaningful information about the logic involved in the context of automated decision-making in particular (Article 22(1) and (4), Recital 63). This kind of informed logic can be anticipated to cause problems considering that one central feature of AI is nonexplanatory machine learning capacities. The AI approach therefore becomes even more interesting as a tool for safeguarding privacy.

As a consequence, the following question arises: to what extent—if at all—is there reason do make a distinction between the logic behind a certain legal decision and the logic involved in the complete system?

(d) Mention should also be made of the legal framework for open data and reuse of PSI. As already pointed out, this is not an access right for individuals *per se*. Rather, it is a conditional right of access second hand, that is, in situations when public agencies have already assessed that certain information should be accessible for reuse outside the public sector.

One point of bringing AI into the discussion is to shed light on the fact that information resources management, including by way of dissemination of information, will probably be enhanced and more powerful in future digital environments.

Being a Digitalized EU Member State

This section provides a practical example of the challenges of being a digitalized EU Member State. For obvious reasons, the author being a Swede makes Sweden a good object for this minor excursion into the societal development of the digital information society in which AI already plays a central role. First, a few national characteristics will be noted. Throughout the text below AI will be referred to as both a facilitator and a risk.

Sweden has a long history of using personal identification numbers in digital environments. Generally speaking, this kind of data processing takes place without the general public being particularly upset, with some exceptions. One obvious explanation to this is historical reasons associated with the government and other public agencies being trusted. This has enabled early and smooth computerization of different kinds—including record linkages. This applies in particular to national transaction systems related to social insurance, social security,[20] taxation, study administration, *et cetera*. Furthermore, the moderate number of Swedish citizens[21] has favored complete and early use of information technologies. A disadvantage of this early adaptation to ICT is rather unexpectedly that Sweden has had to cope with a digital legacy[22] when entering the AI society.

From a legislative perspective, Sweden has been an early adopter of digitalization. A sign of this is the fact that Sweden was the first country to implement a national Data Protection Act (SFS 1973:289). Proactively, there have also been constitutional amendments in order to keep pace with digitalization. This is, however, not similar to saying that there is no need for a legal shield around Swedish AI applications. On the contrary, it all boils down to Sweden, in spite of being relatively well prepared for AI in society, having a large amount of work to carry out so as to avoid a surveillance society in contrast to a democracy. To a large extent, this is related to automatic decision-making based on personal data processing.

In spite of Sweden's long history of data protection legislation, being an EU Member State has involved quite a few difficult questions. A major concern has, as already pointed to, been and still is how to combine personal data processing with transparency. The scope of the long-established openness principle is quite far away from today's discussions about needs for data ownership and control. Therefore, it cannot be taken for granted that a Swedish legal approach to the mandatory GDPR will hold in front of the Court of Justice of the European Union.

Articles 85 (Processing and freedom of expression and information) and 86 (Processing and public access to official documents) of GDPR are of particular interest here. At first glance, the EU regulation seems to be compatible with Swedish law but a more detailed analysis reveals that it is not obvious how to combine the

[20] The so-called Robot Ernst is an early illustration of AI in a social security environment taking place in a municipal community. Fredrik Adolfsson, "Robot styr försörjningsstöd i Trelleborg," *Voister*, July 12, 2017, https://www.voister.se/artikel/2017/07/robot-styr-forsorjningsstod-i-trelleborg.

[21] Today's migration can no doubt be seen as a critical success factor when it comes to how AI might promote a multicultural digitalized Swedish.

[22] This could also be expressed in terms of a technological heritage (history).

right of access to compilations according to the Swedish Freedom of the Press Act with the scope of Article 86 of GDPR. Another example concerns the fact that it is unclear whether the regulation in 28 § of the Swedish Administrative Procedures Act permitting automatic decision-making meets the requirements of national legislation according to Article 22 of GDPR, regulating automated individual decision-making, including profiling. The doubts can partly be explained by the fact that the Swedish Administrative Procedure Act is subsidiary to other deviating national laws, rules, and regulations.

Ways Forward and Final Remarks

With reference to the above, the anticipation is that AI will have an immense impact on privacy-related personal data processing. This is, however, not similar to saying that development will be all good or bad. Instead, potentials and pitfalls depend highly upon how responsibly people and bodies will implement emerging AI. This may in turn be referred to as a kind of digital climate change risking privacy infringements—which is of course different from the current environmental crises affecting mother earth as a natural resource but still very severe. Legal AI calls not merely for sustainable and innovative technical infrastructures but also for legal infrastructures that are fit to master conditions for privacy in an open society not only today but also in the long run.

Through this lens, transparency is a condition for privacy in the context of personal data processing based on AI methods. In practice, this requires openness, which is not necessarily the same as transparency. This has to do with the fact that principles of openness and associated transparency might not reach out sufficiently due to lack of access rights and how those are implemented. Based on this reasoning, a few ways forward will be presented as concluding remarks in recognition of algorithms, machine learning, and big data.

By way of letting law play a proactive role instead of merely a traditional reactive one when things have already gone wrong, transparency issues can be captured at early stages of system design, development, implementation, and further on to the management of applications.

In terms of innovative law, the notion of the "digital person" as a new legal entity could be discussed. The overall idea is that such an approach to AI would supplement long-established categories of "natural person" and "legal person," not least in the context of responsibilities and liabilities of, for example, robots in connection with AI. Being able to explain the logic involved is no doubt crucial for transparency.[23]

Remedies are also important. One approach could be a kind of algorithmic scrutiny oriented toward embedded (substantive) law concerning social insurance, social security, taxation, study administration, *et cetera*. Such an analysis would be based on a legal informatics approach bringing AI to the fore.[24]

What happens in the future is difficult—if not impossible—to foresee. However, one observation is that the impact of ethics seems to increase in the context of AI. This also has consequences for the legal domain. Expressed in another way, traditional law, be it civil or common, as well as the roles of legal professionals acting as judges, attorneys, *et cetera*, might have to step back in favor of ethical advice, vetting, and guidelines.

At the same time, it is of course important to protect and adjust legal safeguards toward what may be referred to as a rule of law 2.0, offering predefined datasets (reducing biased data), capacity restrictions scoring, and exploring different levels of automation, *et cetera*. In this context, the interplay of law and information security is a critical success factor. This all boils down to a quest for a transparent legal shield around the black boxes of AI algorithms.

In addition to the suggested ways forward above, the important understanding of the interplay between privacy, personal data processing, and modern technologies should finally be emphasized. Not least, means and methods for transparency management

[23] See further Cecilia Magnusson Sjöberg, "Digitala personer – en ny rättsfigur," in *Människor och AI: En bok om artificiell intelligens och oss själva*, eds. Daniel Akenine and Jonas Stier (Stockholm: Books on demand, 2019), 65–79; Morgan M. Broman and Pamela Finckenberg-Broman, "AI & Lagen – RAiLE© Projektet," *Arkiv Information Teknik*, no. 1 (2019): 18–20, including references representing a critical approach and for further reading in general. For an in-depth analysis see Visa A. J. Kurki, *A Theory of Legal Personhood* (Oxford: Oxford University Press, 2019).

[24] See further Stanley Greenstein in this volume.

appear to be an important task for further studies. In this context, autonomy of technology calls for particular attention and needs to be challenged from multiple perspectives. A legal approach to digital human sciences[25] appears to be a comprehensive resource for research when data subjects are exposed to AI for better or for worse.

References

"About EDPB." European Data Protection Board. https://edpb.europa.eu/about-edpb/about-edpb_en.

Adolfsson, Fredrik. "Robot styr försörjningsstöd i Trelleborg." *Voister*. July 12, 2017. https://www.voister.se/artikel/2017/07/robot-styr-forsorjningsstod-i-trelleborg.

"Artificial intelligence." Wikipedia. https://en.wikipedia.org/wiki/Artificial_intelligence.

"Artificiell intelligens." *Nationalencyklopedin*. https://www.ne.se/uppslagsverk/encyklopedi/l%C3%A5ng/artificiell-intelligens.

Broman, Morgan M., and Pamela Finckenberg-Broman. "AI & Lagen – RAiLE© Projektet." *Arkiv Information Teknik* 2019, no. 1 (2019): 18–20.

Collenette, Joe, Katie Atkinson, and Trevor Bench-Capon. *An Explainable Approach to Deducing Outcomes in European Court of Human Rights Cases using ADFs*. Department of Computer Science, University of Liverpool, April 2020. https://cgi.csc.liv.ac.uk/~katie/comma20.pdf

[25] One approach to digital humanities is found in Per-Olof Erixon and Julia Pennlert, eds., *Digital humaniora – Humaniora i en digital tid* (Gothenburg: Daidalos, 2017). For a somewhat broader approach, see the digital human sciences committee at Stockholm University. The committee's definition, originally expressed in Swedish, may be translated into English the following way: Digital human sciences means interdisciplinary studies of digital artifacts and environments and their meaning for human beings and society. This includes (1) studies concerning actors and their role in the digital society; (2) social and legal aspects of responsibility and ethics; and (3) interaction between human beings in digital systems and between human beings and digital entities.

Corrales, Marcelo, Mark Fenwick, and Helena Haapio, eds. *Perspectives in Law, Business and Innovation: Legal Tech, Smart Contracts and Blockchain*. Singapore: Springer & Kyushu University, 2019.

Corrales, Marcelo, Mark Fenwick, and Nikolaus Forgó, eds. *New Technology, Big Data and the Law*. Singapore: Springer & Kyushu University, 2017.

Corrales, Marcelo, Mark Fenwick, and Nikolaus Forgó, eds. *Robotics, AI and the Future of Law*. Singapore: Springer & Kyushu University, 2018.

Erixon, Per-Olof, and Julia Pennlert, eds. *Digital humaniora – Humaniora i en digital tid*. Gothenburg: Daidalos, 2017.

Gardner, Anne von der Lieth. *An Artificial Intelligence Approach to Legal Reasoning*. Cambridge, MA: MIT Press, 1987.

Greenstein, Stanley. *Our Humanity Exposed: Predictive Modelling in a Legal Context*. Dissertation, Stockholm: Stockholm University, 2017.

Holm, Cyril, ed. *Secure Digitalisation: Nordic Yearbook of Law and Informatics 2016–2018*. The Swedish Law and Informatics Research Institute. Skrifter utgivna av Juridiska fakulteten vid Stockholms universitet nr 86. Stockholm: Poseidon Förlag, 2019.

Häggström, Olle. *Here Be Dragons: Science, Technology and the Future of Humanity*. Oxford: Oxford University Press, 2016.

Kurki, Visa A. J. *A Theory of Legal Personhood*. Oxford: Oxford University Press, 2019.

Lessig, Lawrence. *Code and Other Laws of Cyberspace*. New York: Basic Books, 1999.

Magnusson Sjöberg, Cecilia. *Rättsautomation: Särskilt om statsförvaltningens datorisering*. Dissertation, Stockholm: Norstedts Juridik, 1992.

Magnusson Sjöberg, Cecilia. "Förvaltningslagen och digitaliseringen." *Förvaltningsrättslig tidskrift*, no. 3 (2018): 519–530.

Magnusson Sjöberg, Cecilia, ed. *Rättsinformatik: Juridiken i det digitala informationssamhället*. 4th ed. Lund: Studentlitteratur, 2021.

Magnusson Sjöberg, Cecilia. "Digitala personer – En ny rättsfigur." In *Människor och AI: En bok om artificiell intelligens och oss själva*, edited by Daniel Akenine and Jonas Stier, 65–79. Stockholm: Books on demand, 2019.

Melvås, Boris. "En formaliserad rättsgrammatik." *Förvaltningsrättslig tidskrift*, no. 5 (2018): 937–972.

Millard, Christopher, ed. *Cloud Computing Law*. Oxford: Oxford University Press, 2013.

Seipel, Peter. *Computing Law: Perspectives on a New Legal Discipline*. Stockholm: Liber Förlag, 1977.

Sergot, Marek, Fariba Sadri, Robert Kowalski, Frank Kriwaczek, Peter Hammond, and Terese Cory. "The British Nationality Act as a Logic Program." *Communications of the ACM* 29, no. 5 (May 1986): 370–386.

Suksi, Markku. "Automatiserat beslutsfattande enligt den svenska förvaltningslagen." *JFT* 165, no. 6 (2018): 463–472.

Susskind, Richard. *Expert Systems in Law: A Jurisprudential Inquiry*. Oxford: Oxford University Press, 1988.

Susskind, Richard. *Tomorrow's Lawyers: An Introduction to Your Future*. Oxford: Oxford University Press, 2017.

Swedish Foundation for Strategic Research. *Livet med AI*. SSF report no. 29. Stockholm: Swedish Foundation for Strategic Research, 2018.

Swedish Ministry of Enterprise and Innovation. *Regeringens nationella inriktning för artificiell intelligens*. N2018.14. Stockholm: Swedish Ministry of Enterprise and Innovation, 2018.

Swedish Ministry of Enterprise and Innovation Public Inquiry. *Vägen till självkörande fordon – Introduktion*. SOU 2018:16. Stockholm: Swedish Ministry of Enterprise and Innovation, 2018.

Swedish Ministry of Finance Public Inquiry. *Juridik som stöd för förvaltningens digitalisering*. SOU 2018:25. Stockholm: Swedish Ministry of Finance, 2018.

Swedish Ministry of Justice Public Inquiry. *Hur står det till med den personliga integriteten? – En kartläggning av Integritetskommittén*. SOU 2016:41. Stockholm: Swedish Ministry of Justice, 2016.

Tegmark, Max. *Life 3.0: Being Human in the Age of Artificial Intelligence*. London: Penguin Books, 2017.

Vinnova. *Artificiell intelligens i svenskt näringsliv och samhälle: Analys av utveckling och potential*. VR 2018:08. Stockholm: Vinnova, 2018.

Wahlgren, Peter. *Automation of Legal Reasoning: A Study on Artificial Intelligence and Law*. Dissertation, Deventer-Boston, MA: Kluwer Law and Taxation Publisher, 1992.

Wahlgren, Peter, ed. *50 Years of Law and IT – The Swedish Law and Informatics Research Institute 1968–2018*. Stockholm: Stockholm Institute for Scandinavian Law, 2018.

Weaver, Russel, Jane Reichel, and Steven I. Friedland, eds. *Comparative Perspectives on Privacy in an Internet Era*. Durham, NC: Carolina Academic Press, 2019.

Westman, Daniel. "AI, big data och upphovsrätten." In *Rättsinformatik: Juridiken i det digitala informationssamhället*, edited by Cecilia Magnusson Sjöberg, 4th ed., 639–668. Lund: Studentlitteratur, 2021.

Winston, Patrick Henry. *Artificial Intelligence*. Reading, MA: Addison-Wesley Publishing Company, 1984.