



# AI, Machine Learning & Big Data

# 2020

**Second Edition**

Contributing Editor:  
**Matt Berkowitz**

# CONTENTS

<b>Introduction</b>	<i>A Framework for Understanding Artificial Intelligence</i> Matt Berkowitz, <i>Shearman &amp; Sterling LLP</i>	1
<b>General chapters</b>	<i>Considerations in Venture Capital and M&amp;A Transactions in the AI Mobility Industry</i> Alan Bickerstaff, K. Mallory Brennan & Emma Maconick, <i>Shearman &amp; Sterling LLP</i>	11
	<i>AI Changes Society. Society Changes the Law. The Bright Future of the Smart Lawyer</i> Gabriele Capecchi & Giovanna Russo, <i>Legance – Avvocati Associati</i>	27
	<i>AI and the Evolution of Payment Services</i> Bas Jongmans & Xavier Rico, <i>Gaming Legal Group</i>	32
<b>Country chapters</b>		
<b>Australia</b>	Anthony Borgese, Jonathan Thompson & Alice Scamps-Goodman, <i>MinterEllison</i>	39
<b>Austria</b>	Günther Leissler & Thomas Kulnigg, <i>Schönherr Rechtsanwälte GmbH</i>	56
<b>Belgium</b>	Steven De Schrijver, <i>Astrea</i>	63
<b>Brazil</b>	Eduardo Ribeiro Augusto & Pedro Rangel Lourenço da Fonseca, <i>Siqueira Castro Advogados</i>	73
<b>Bulgaria</b>	Grozdan Dobrev & Lyuben Todev, <i>DOBREV &amp; LYUTSKANOV Law Firm</i>	80
<b>Canada</b>	Simon Hodgett, Ted Liu & André Perey, <i>Osler, Hoskin &amp; Harcourt, LLP</i>	89
<b>China</b>	Susan Ning & Han Wu, <i>King &amp; Wood Mallesons</i>	102
<b>Denmark</b>	Timo Minssen, Tue Goldschmieding & Søren Sandfeld Jakobsen, <i>Gorrissen Federspiel</i>	113
<b>France</b>	Claudia Weber, Jean-Christophe Ienné & Arthur Poirier, <i>ITLAW Avocats</i>	129
<b>Germany</b>	Christian Kuß, Dr. Michael Rath & Dr. Markus Sengpiel, <i>Luther Rechtsanwalts-gesellschaft mbH</i>	140
<b>Hong Kong</b>	Alan Chiu, Charles To & Salina Ip, <i>Ella Cheong &amp; Alan Chiu Solicitors &amp; Notaries</i>	150
<b>India</b>	Divjyot Singh, Kunal Lohani & Kumari Poorva, <i>Alaya Legal Advocates</i>	155
<b>Italy</b>	Massimo Donna & Lavinia Carmen Di Maria, <i>Paradigma – Law &amp; Strategy</i>	168
<b>Japan</b>	Akira Matsuda, Ryohei Kudo & Haruno Fukatsu, <i>Iwata Godo</i>	176
<b>Korea</b>	Won H. Cho & Hye In Lee, <i>D’LIGHT Law Group</i>	188
<b>Mexico</b>	Alfredo Lazcano & Andrea Avedillo, <i>Lazcano Sámano, S.C.</i>	197
<b>Netherlands</b>	Louis Jonker, Berber Bosch & Lodewijk Heinsman, <i>Van Doorne</i>	205
<b>Portugal</b>	Nuno da Silva Vieira & Daniela Guimarães, <i>Antas da Cunha Ecija &amp; Associados, Sociedade de Advogados, R.L.</i>	216

<b>Romania</b>	Cristiana Fernbach & Cătălina Finaru, <i>KPMG – Toncescu și Asociații S.P.A.R.L.</i>	220
<b>Russia</b>	Rustam Rafikov, <i>Rafikov &amp; Partners</i>	231
<b>Singapore</b>	Lim Chong Kin, <i>Drew &amp; Napier LLC</i>	237
<b>South Africa</b>	Fatima Ameer-Mia, Christoff Pienaar & Nikita Kekana, <i>Cliffe Dekker Hofmeyr Inc.</i>	248
<b>Spain</b>	Sönke Lund, <i>Grupo Gispert Abogados &amp; Ecomistas</i>	262
<b>Sweden</b>	Elisabeth Vestin, Caroline Sundberg & Jesper Nevalainen, <i>Hannes Snellman Attorneys Ltd</i>	270
<b>Switzerland</b>	Clara-Ann Gordon & Dr. András Gurovits, <i>Niederer Kraft Frey Ltd.</i>	281
<b>Taiwan</b>	Robin Chang & Eddie Hsiung, <i>Lee and Li, Attorneys-at-Law</i>	291
<b>United Arab Emirates</b>	Nadim Bardawil, <i>BSA Ahmad Bin Hezeem &amp; Associates LLP</i>	300
<b>United Kingdom</b>	Rachel Free, Hannah Curtis & Barbara Zapisetskaya, <i>CMS Cameron McKenna Nabarro Olswang LLP</i>	304
<b>USA</b>	Nathan Greene, David Higbee & Brett Schlossberg, <i>Shearman &amp; Sterling LLP</i>	316

# Sweden

Elisabeth Vestin, Caroline Sundberg & Jesper Nevalainen  
Hannes Snellman Attorneys Ltd

## Trends

In 2018, the Swedish Government set a goal for Sweden to become the global leader within innovation and the use of digital solutions. One of the technologies to achieve this goal is artificial intelligence (“AI”).

Compared to other countries, Swedish society is characterised by a high standard of digitalisation. This is partly due to a well-developed IT infrastructure, public data access, and a high technical literacy, all of which are fundamental elements for the advancement and development of AI competence and AI applications.<sup>1</sup> The Government has pinpointed four key focus areas to be considered in order for Swedish society to realise the full potential and benefits of AI: (i) framework and infrastructure; (ii) education and training; (iii) research; and (iv) innovation and use. The report *National Approach to Artificial Intelligence* addresses the question of how Sweden will strengthen each of these areas to enhance its position for businesses, researchers, and AI developments.<sup>2</sup>

AI is expected to impact many different industries that will have to evolve and adapt to new technologies. Successful AI initiatives in Sweden within certain industries include: cloud-based movement analysis monitoring of people in need of care; remotely controlled vehicles in mining preventing accidents; medical diagnosis and image analysis within healthcare; and optimisation of deep learning and improving the processes of industries.

Additionally, the Government has pinpointed some of the challenges for Sweden within the field of AI and digitalisation such as regulatory development, the threat to privacy and intellectual property rights, lack of higher education institutions providing AI education, lack of AI standards, and IT security. Consequently, despite the fact that Sweden has a relatively advanced IT infrastructure, there are still significant challenges which must be addressed in order for Sweden to be able to fully utilise the benefits of AI. If these challenges are left unaddressed, the Swedish Government fears that this will have a detrimental effect on consumer trust in data sharing, AI, and IT security, factors which, in the long run, may even have detrimental effects on democracy itself.

In light of how industries can expectedly be impacted as a result of AI development, it is important to note that innovation and growth require not only coherent and strategic policies but also regulations. However, any regulatory changes required must find a proper balance between the fundamental right of privacy, ethics, trust and social protection, and the level of data access necessary to create AI applications. Qualitative data is essential for developing AI. Within the EU/EEA, including Sweden, regulations such as the EU General Data Protection Regulation (the “GDPR”) will thus likely play a vital role in the management of risks and benefits of AI during the coming years. In addition, regulatory frameworks

and continuing cooperation between European countries across industries to create new standards at an early stage is essential for Sweden to meet the demands posed by the latest technological developments.

The Government's report states clearly that Sweden needs to create a strong collaboration between higher education institutions, research, and innovation. Financial investments for AI research have been an important element in the governmental approach to increase Sweden's position as a leading nation in the field of AI. Research on AI in Sweden is performed by several institutions, which successfully occupy niches and specialised fields – both in fundamental research and applied research and product development. For example: AI Innovation of Sweden, which consists of stakeholders from industry, the public sector, and academia, is a national centre for innovation and AI-related research; the AI Sustainability Centre focuses on the social and ethical aspects of scaling AI; and RISE Research Institutes of Sweden is Sweden's research institute and innovation partner, which gathers research institutes to increase the pace of innovation in Swedish society.

Recent notable developments in AI research and education include the Wallenberg AI, Autonomous Systems and Software Program – Humanities and Society, which focuses on challenges and impact of upcoming technology shifts and the practice of human and societal aspects of AI and autonomous systems. The research program has during the last year (2019) raised over EUR 66 million and continues to be a leading institute within its field.

The Government further emphasises the importance of a strong IT framework and infrastructure to enable the development and use of the emerging technology. The Government's broadband strategy from 2016, to provide high-speed internet to 95 per cent of the households with at least 100 Mbit/s broadband in 2020, was met already by the end of 2019. By 2025 the goal is to increase the percentage to 100 per cent, including rural areas.<sup>3</sup> Another important aspect for a strong IT infrastructure is cybersecurity and protection of data. In this regard, the focus for 2020 is to strengthen the ability to communicate confidential information across Government entities and build robust systems for discovering and countering cyber-attacks.<sup>4</sup>

With respect to open access to data, Sweden has a longstanding tradition of granting public access to data generated by authorities and other bodies in the public sector. According to Sweden's Innovation Agency, data availability is a prerequisite for building AI systems and gathering the volumes of data necessary for the advancement of AI. Data needs to be collected and processed in a way that allows innovation while still preserving the trust of users and avoiding unwanted effects caused by, for example, biases and ethical considerations. Thus, legislative measures regarding the access and use of data need to be developed to enable the desired result. Addressing data bias is already an established focus area within AI initiatives and research. Tackling such issues at an early stage has the potential to be one of the strongest advantages for Sweden. However, having appropriate safeguards in place to prevent wrongful access is vital and addressing legal uncertainties associated with the processing and sharing of extensive sets of data is considered one of the main challenges that Swedish AI development faces from a legal perspective.

The number of registered data-related patent applications is generally considered an indicator of a country's development capacity within AI. Pursuant to the Patent Index 2019, Sweden's development capability in AI was at a high and above-average level. In accordance with the latest report from the European Patent Office, Sweden is ranked 11<sup>th</sup> internationally in terms of the number of patent applications, and it has the most patent applications within the field of digital communication in the EU. In the last couple of years, the number of patent

applications has increased from Swedish leading companies, such as Ericsson, which has further strengthened its position especially within the field of digital communication with an increase in 2019 of eight per cent compared to the previous year.<sup>5</sup>

AI innovation is present in various industries in the Swedish business landscape. Sweden's Innovation Agency provides an overview of the most relevant industries in Sweden driving the development of AI innovation in Sweden in its report. Ericsson, with the largest R&D activity in Sweden, is an important stakeholder in the ecosystem of businesses innovation with the support of AI. AI is also being developed in the transport industry where a few Swedish founded companies that are global leaders in their industries, such as SAAB defence group (development and manufacture of both combat aircraft and submarines), Autoliv (vehicle safety), and automobile companies such as Volvo Cars, AB Volvo, and Scania, have extensive and multifaceted R&D projects relating to AI-based solutions. Development of AI-based solutions is also highly relevant in the life sciences industry. However, the lack of qualitative data and protective data privacy legislation constitutes an obstacle for the efficient development of AI in this industry. Finally, some Swedish internet-based companies are relying heavily on AI. Examples of such companies include Spotify (music streaming), Klarna and iZettle (payment services providers), as well as King and DICE (gaming companies).

### **Ownership/protection**

AI is based on computational models and algorithms, which are, *per se*, of an abstract mathematical nature. The purpose of this section is to introduce how an AI algorithm and data can be protected and owned under Swedish law.

#### The protection of an AI algorithm

There are currently three options available to legally protect ownership rights related to an AI algorithm: copyright; patents; and trade secrets.

AI can receive copyright protection if it is considered a computer program. Computer programs are literary works under the Computer Programs Directive 2009/24/EC which has been incorporated in the Swedish Copyright Act (1960:729). However, in recital 11 of the Computer Programs Directive, it is stated that only the expression of a computer program is protected, and that ideas and principles are not protected by copyright. Similarly, to the extent that logic, algorithms, and programming languages comprise ideas and principles, they are not protected under the Directive. Only the expression of those ideas and principles can be protected by copyright. Thus, the expression of an algorithm could be protected by copyright, but that would not prevent others from creating algorithms based on the same ideas and principles. In conclusion, relying on copyright is likely not the best option to protect an AI algorithm.

An algorithm is a mathematical method and, as such, is excluded from the patentable area since it lacks technical character. According to the EPO Guidelines for Examination Part G-II-3.3.1, for an AI algorithm to be patentable, it must contribute to the technical field in a manner which exceeds a strictly non-technical contribution. Therefore, if an algorithm is used in a technical context, it is rather the technical solution that utilises the algorithm that may be patented.

It is also possible for companies to protect their AI algorithms by handling them as trade secrets. The Swedish Trade Secrets Act (2018:558) partially implements the Trade Secrets Directive (EU) 2016/943. Pursuant to the Swedish Trade Secrets Act, a trade secret means such information concerning the business or operational circumstances of a trader's business or a research institution's activities which: (i) is not generally known or readily accessible to

persons who normally have access to information of the type in question; (ii) the holder has taken reasonable measures to keep secret; and (iii) the disclosure of which is likely to lead to competitive injury to the holder. There are no requirements concerning the presentability of the algorithm. Thus, if the requirements laid out in the Swedish Trade Secrets Act are fulfilled, the AI algorithm can be protected as a trade secret.

When considering how to protect an AI algorithm it might be worth noting that in contrast to patents and copyright protection, trade secret protection has the advantage of being unlimited in time. On the other hand, keeping a trade secret confidential can, in reality, be quite difficult and the protection may be lost if the trade secret is disclosed, even by accident.

#### AI algorithms created by employees

The general rule under the Swedish Copyright Act stipulates that copyright shall automatically vest with the creator, with certain exceptions. Intellectual property rights do not necessarily constitute a right of ownership, but they provide exclusive right of use and reproduction to their holders. If the AI is considered as a computer program, then Section 40(a) of the Swedish Copyright Act would apply to works that are created by an employee. This section stipulates that the copyright automatically passes to the employer, provided it has been created in the scope of duties in an employment relation. Thus, the company that is an employer would in this situation have the copyright to such works.

Pursuant to the Swedish Right to the Inventions of Employees Act (1949:345), an employer can claim rights to an invention made by its employee. This will restrict the employee's right to apply for or obtain a patent, and the employer may acquire the right in the invention in whole or in part. Thus, if an employee creates an AI algorithm that could be patentable and the invention falls within the field of activity of the company or if the invention is the result of a task assigned to the employee more specifically, the employer can obtain the ownership to the invention.

In accordance with the Swedish Trade Secrets Act, during the term of employment, an employee may neither utilise unlawfully, nor disclose or appropriate the employer's trade secrets to a third party. After the employment expires, the employee would only in exceptional cases be held responsible for these acts and sufficient post-contractual confidentiality undertakings should, therefore, be entered into between the company and its employees. A confidentiality agreement can provide a wider protection against disclosures of AI algorithms than the protection that is provided under the trade secret legislation.

#### The protection and ownership of data

Data as such cannot be protected by copyright under Swedish law, but a compilation of data can be protected if the way in which data is compiled meets the requirement of originality. However, under the Swedish Copyright Act, in cases where the originality requirement is not fulfilled and a large amount of data is compiled, the person who has made such a catalogue, table or program shall have the exclusive right to control the whole or a substantial part thereof. This is a unique legal feature within the Nordic countries, which is unfamiliar in most other jurisdictions. The Swedish Copyright Act provides also a *sui generis* right for databases that applies to databases of which obtaining, verification, or presentation has required significant investments. On an EU level, the Database Directive 96/9/EC applies to databases that are a result of a significant investment. However, it should be noted that database protection protects the work behind the database – not the data as such. As mentioned above, similar to computer programs, the copyright to a database created by an employee will be transferred to the employer pursuant to the Swedish Copyright Act. In addition to copyright, data in the form of know-how and business information can be protected as trade secrets, as described above.

As a general rule, data and information cannot be owned under Swedish law. The definition of ownership applies poorly to data, since data is not an interchangeable object; transferring data or information from one party to another does not remove it completely from the party transferring it, and it does not prevent the other party from using it. Information and data can, however, belong to and be managed by various stakeholders, such as the one who owns the device or the service where the information and data are located. Thus, the ownership of the device or service is the default setting of data management when no agreements have been made. That being said, the importance of contracts is emphasised in case of ownership of data itself. Consequently, under Swedish law it is usually more beneficial to try to conclude whether there are any restrictions on the use of data as intended, rather than trying to determine who owns the data.

### **Antitrust**

Competition law in Sweden is regulated by the Swedish Competition Act (2008:579), which, through Sweden's membership in the EU, is harmonised with EU competition law, specifically Articles 101 and 102 of the Treaty on the Functioning of the European Union. Consequently, Swedish competition law is also interpreted in accordance with the European Court of Justice's case law.

#### What happens when machines collude?

An antitrust concern which has arisen as a result of recent developments in data processing and AI is the idea of digital cartels, in other words, algorithmic collusion. The Swedish Competition Authority (the "SCA") has not released any official publication concerning AI as a method for collusion since the report of *Competition and Growth on Digital Markets*<sup>6</sup> in 2017, where the SCA discussed the ways in which the developments in the field of AI allow for automated price surveillance of competitors, which may facilitate the founding, stability, and continuance of cartels. However, the matter was recently discussed in an interview with the head of the unit for abuse of dominance and the head of the unit for cartels and concentrations.<sup>7</sup> In a broad sense, the discussion reiterated what the SCA has previously published on the topic. For instance, one of the main concerns with algorithmic collusion is that when a company raises its prices, an algorithm can alert competitors to raise their prices accordingly. Automated price adjustments based on competitors' prices could lower incentives for companies to compete with prices, as competitors' prices would be automatically and instantly harmonised, and as such one may discuss whether such algorithms could be likened to traditional price cartels. The SCA has concluded that further precedent is needed in order to provide guidance on how competition law should be applied in these types of situations, as there have not, to date, been any cases in Sweden that have explicitly dealt with such algorithms. However, the SCA has noted that the current enforcement policy is that there needs to be some form of conscious underlying consensus between the competitors on price tactics in order for the practice to be deemed unlawful.

In January 2020, the SCA published their new strategy for AI.<sup>8</sup> The strategy includes the aim to develop the ability to use AI and algorithms internally within the authority, which will make the SCA better equipped to understand and oversee markets that make use of those technologies. The aim of further integrating AI into the SCA's supervisory activities is also included in their operational plan for 2020–2022.<sup>9</sup>

#### Antitrust concerns related to big data

Towards the end of 2019 the SCA, the Swedish Consumer Agency and the Swedish Data Protection Authority produced a joint response with proposals and views on the Government's



research policy and the upcoming 2020 research policy bill.<sup>10</sup> In their response, the authorities highlighted the potential antitrust concerns of big data, specifically in relation to digital platforms and abuse of dominance.

Dominant platforms, through their access to large amounts of user data, give rise to so-called network effects, which in practice can generate monopolistic markets. For example, it may be difficult for a new streaming music service to challenge an established service, as existing players have been able to collect large amounts of user data which they can use to provide users with suggestions on music based on what users typically listen to. For the users, network effects can offer great added value and consequently lower incentives to choose other platforms that do not have access to the same amount of user data. The right to data portability, i.e. the right of the consumer to switch platforms and move “their” data, is regulated in data protection legislation (mainly in the GDPR), but few consumers are aware of this right, or how to make use of it. The importance of data in digital markets gives a great advantage to incumbents and can make it very difficult for potential competitors to enter the market.

### **Board of directors/governance**

In the area of Corporate Governance, AI, machine learning, big data, and similar technologies can contribute to improvements in both quality and efficiency. In Sweden, the central act regarding Corporate Governance is the Swedish Companies Act (2005:551). Furthermore, companies whose shares are listed on a regulated market in Sweden are obligated to apply the Swedish Corporate Governance Code. In addition to these, the Accounting Act (1999:1078), the Annual Accounts Act (1995:1554), the Securities Market Act (2007:528), and the Financial Instruments Trading Act (1991:980) are also important regulations in the field of Corporate Governance. As the legislation is technology-neutral, there are great opportunities for the use of specific technical solutions in this field. In fact, there are only a few constraints regarding digital solutions. For example, the annual financial statement and the shareholder’s register must be kept in digital format rather than in a physical format. The Swedish Companies Act sets forth that the board of directors is responsible for the organisation of the company and the management of the company’s affairs. Members of the board shall act in the best interest of the company and observe a duty of loyalty in the exercise of their responsibilities. In light of the members’ fiduciary duties, transferring such duties from natural persons to digital solutions would not be appropriate. However, it is possible that digital solutions may be appropriate in compliance with other stipulations in the Swedish Companies Act, such as the rule that all members of the board should be provided with sufficient supporting documentation before making a decision and the requirement of the board to regularly assess the company’s financial position and ensure that the company’s organisation is structured in such a way that the company’s finances are controlled satisfactorily. When it comes to the duties of the board of directors, technical solutions can be of support, mainly in situations where manual processing and review would not be possible, for example, when the data volumes are too large and complex for a natural person to manage. It is important that the effects and risks of using AI, machine learning, big data, and other similar solutions are evaluated before they are implemented.

### **Regulations/government intervention**

Specific laws relating to AI or machine learning that directly mention these terms do not yet exist in Swedish legislation. As Swedish legislation is generally technology-neutral, the

legislator has left it up to the courts to determine whether a particular technology, such as AI, machine learning, or big data, falls within the scope of the law. The preparatory works of the legislation, which in Sweden can be used when interpreting the intention of a law, may offer guidance for interpretation and do sometimes mention specific technologies.

Legislation regarding areas such as consumer protection, privacy, and product safety is applicable to AI systems even if they are not expressly mentioned in the legislation. This may, however, lead to inappropriate outcomes, as the legislation is not necessarily aimed to be applied to new technologies such as AI. For example, a consumer who cannot hold anyone but an AI system liable for damage may be deprived of their right to compensation.

The EU Commission has emphasised the need for harmonised AI legislation. Such legislation would have an impact on the Swedish legislation the same way as the harmonised legislation on consumer protection, privacy, and product safety. Sweden, in line with EU initiatives, concentrates on creating a legal framework enabling sustainable and ethical AI, which entails ethical, safe, secure, reliable, and transparent AI systems, products, and development. Secure AI by design is viewed as being able to prevent and minimise the risk of a system getting “hacked” and causing harm that way. Further updates in the Swedish policy on AI may be expected in light of the EU’s new plans for future actions relating to AI published in February 2020.<sup>11</sup> In order to ensure that AI development does not compromise individuals’ rights and health, while harnessing the potential of AI technologies, Sweden considers measures such as education, playgrounds for AI systems, constant testing and data collection from trials, and safeguards for individuals who are subject to unreasonable automated decisions important. Such balance also needs to be struck globally and at the EU level, and Sweden is active in developing such rules.

### **Civil liability**

According to the European Commission’s White Paper on AI published in February 2020, AI technologies present new safety risks when embedded in products and services. There is a lack of clear safety provisions regarding AI technologies, and the uncertainty increases the more autonomous the AI gets. In the EU, product safety regulations aim to minimise the risk of harm that new technologies, such as AI, may cause. A significant risk related to the use of AI technology concerns the application of rules designed to protect fundamental rights, safety, and liability-related issues. Under Swedish law, AI or autonomous systems do not have legal capacity and cannot be held liable for damages. Instead, harm caused by AI should be attributable to existing persons or bodies.<sup>12</sup> The purpose of this section is to highlight how the Swedish courts would likely interpret applicable laws in cases of damages caused by AI and automated systems.

#### Contract formation

Due to the lack of legal capacity, an AI system cannot be a party to a contract. However, the scope of the Swedish Contracts Act (1915:218) is not limited to the way parties enter into a contract, and it is therefore applicable in cases where AI is used as a tool to enter into a contract. Furthermore, AI systems can be subject to contracts, just like other products and services. The difference is that there may be challenges in allocating adequate responsibilities within the contract when the subject is an AI system.

#### Product liability

Under the Swedish Product Liability Act (1992:18) (the “PLA”), a manufacturer is liable for damage caused by a defective product. The issue with AI technology lies in the difficulty of proving that there is a defect in the product and that the damage that has occurred has a

causal link to the product. The PLA, which is an implementation of the EU Product Liability Directive (85/374/EEC),<sup>13</sup> is applicable to personal injuries and damage on consumer property caused by a product. The question is whether an AI system can be considered a “product” under the definition of the PLA. The matter has been discussed in the PLA’s preparatory works in relation to personal computers. Computer software can be considered part of the hardware, and hence a product, if it is highly integrated with the hardware and difficult for the user to access. Operating systems are examples of such integrated software. As such, in cases where the operating system causes damages, the producer of the computer may be held liable under the PLA regardless of whether the damage was caused by a logical software error or malfunctioning hardware. More standalone software is considered intellectual property, and logical errors in such software do not make, as a rule, programmers liable under the PLA. An additional difficulty with applying the PLA to AI systems is that the PLA applies to products once they have entered commercial circulation, meaning that the producers can be held liable for damages resulting from errors present at that time. In contrast, AI systems are constantly subject to updates after the product has been put in circulation and often include self-learning elements, meaning that they are constantly evolving. As a result, it is by no means certain that damages caused by an AI system can be found to have resulted from errors present at the time of production. Moreover, multiple actors can be responsible for making the updates in the AI system, which further dilutes the concept of producer liability under the PLA. Finally, legal uncertainty may arise in regard to what constitutes damage or a defect for the purposes of a liability claim, especially in cases of AI with machine learning elements.

#### Tort law

Tort liability outside the PLA or other speciality laws regarding liability must, as a rule, be based on negligence. Such liability can be based on the Swedish Tort Liability Act (1972:207) or, in some cases, on general principles of law. Liability for negligence in regard to an AI system requires negligence by the programmer or by the user. For a programmer, this entails, for example, an obligation to follow industry standards. For a user, negligence can mean disregarding instructions in the user manual. Alternative solutions to address liability issues for AI systems have been considered, such as vicarious liability rules or liability based on an obligation to supervise. Swedish courts have yet to rule on this matter.

The EU Commission has stated that legal uncertainty regarding AI and liability could impede innovation and investments in research and development. From a Swedish perspective, the risks are acknowledged and will be addressed as a gap in the current legal framework.<sup>14</sup>

### **Discrimination and bias**

A machine learning AI system will learn from the data input it gets. If the used data is biased or discriminatory in any way, then the AI system will be too. Due to the lack of transparency in many AI systems, the bias might be difficult to detect and address. The Swedish Discrimination Act (2008:567) prohibits direct and indirect discrimination based on sex, transgender identity or expression, ethnicity, religion or other belief, disability, sexual orientation, or age. The Equality Ombudsman, the government agency combatting discrimination, found that most of the focus areas in 2019 make use of some sort of AI or automated decision-making system. When AI is used, for example, for recruitment or granting of credit, the individual is protected by the Discrimination Act. The Ombudsman has stated that the lack of efficient sanctions for violations of the Discrimination Act makes today’s discrimination legislation inadequate for future, potentially large-scale, breaches of the same.<sup>15</sup>

## National security and military

AI is being used by the military. So far there are no specific laws relating to AI, machine learning, or big data in this context. Sweden is a part of the strategic framework for the development of AI technology within the EU, which includes a development plan for both civil and military use.

## Conclusions

Sweden has built a solid foundation for the continued advancement and integration of AI and digital solutions in the society. There is a high degree of investment and research in the field of AI taking place in Sweden. While the private sector has undoubtedly progressed further than the public, there are nonetheless notable developments taking place within the public sector as well, including both regulatory and supervisory developments. As noted herein, Sweden has an advanced IT infrastructure and a high degree of data access and technical literacy amongst its population. These factors all contribute to Sweden having a high standard of digitalisation and good prospects for the advancement and development of AI competence and AI applications. That being said, as discussed in this chapter, there are still many areas which require further development in order for Sweden to be able to reach its goal of being a global leader in the field of AI.

\* \* \*

## Endnotes

1. Sweden's Innovation Agency, *Artificial Intelligence in Swedish Business and Society*, May 2018.
2. Government Offices of Sweden, *National approach to artificial intelligence*, February 2019.
3. The Swedish Post and Telecom Authority's report, *Follow-up on the government's broadband strategy*, May 2019, and the Swedish Internet Foundation, *Meaningful Time online and the pros and cons of digital society*, Summary in English available here: <https://svenskarnaochinternet.se/rappporter/svenskarna-och-internet-2019/the-swedes-and-the-internet-2019-summary/>, October 2019.
4. The Swedish National Defence Radio Establishment, *Comprehensive cyber security action plan 2019–2022*, March 2020.
5. European Patent Office, *Patent Index 2019*, March 2020.
6. Swedish Competition Authority, *Competition and Growth on Digital Markets*, Report series 2017:2, March 2017.
7. Swedish Competition Authority's podcast, Episode 38, October 2019 (in Swedish), available at <http://www.konkurrensverket.se/globalassets/om-oss/podcast/avsnitt-38-podcast-konkurrenten-textversion.pdf>, April 2019.
8. Swedish Competition Authority, *Artificial intelligence (AI) Strategy or the Swedish Competition Authority*, Dnr. 82/2020, January 2020.
9. Swedish Competition Authority, *Business Plan 2020-2022*, Dnr. 110/2020, February 2020.
10. Swedish Competition Authority, *The Swedish Consumer Agency and Swedish Data Protection Authority, Regarding 2020 Research Policy Bill*, Dnr. 2019/915, October 2019.
11. European Commission, *White Paper: On Artificial Intelligence – A European approach to excellence and trust*, February 2020.

12. European Union, Expert Group on Liability and New Technologies – *New Technologies Formation, Liability for Artificial Intelligence and other emerging technologies*, November 2019.
13. Council Directive *on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products (85/374/EEC)*, July 1985.
14. Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee, *Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics*, February 2020.
15. The Equality Ombudsman of Sweden (DO), *Annual Report*, February 2020.



### Elisabeth Vestin

**Tel: +46 760 000 009 / Email: [elisabeth.vestin@hannessnellman.com](mailto:elisabeth.vestin@hannessnellman.com)**

Elisabeth heads Hannes Snellman's Intellectual Property & Technology practice at the Stockholm office. Her fields of expertise include IT/technology, telecommunication, AI, data, IP, marketing, consumer, retail/e-commerce, and franchising/distribution, sports, media and entertainment law, as well as general commercial law. Innovation, technology, trade secrets, data, e-commerce, a strong brand and other intellectual property rights are often central to the businesses that Elisabeth advises.

Her practice includes drafting, interpreting, negotiating and disputing commercial agreements. She also advises on M&A in the IP & TMT field.

“Elisabeth Vestin combines IP knowledge with a wide range of IT experience.” *The Legal 500, 2019* (IT and telecoms).

Ranked as one of the world's leading franchise lawyers, *Who's Who Legal, 2016, 2017, 2018, 2019 and 2020*.



### Caroline Sundberg

**Tel: +46 760 000 004 / Email: [caroline.sundberg@hannessnellman.com](mailto:caroline.sundberg@hannessnellman.com)**

Caroline specialises in the law related to the IT and technology sector, with a particular focus on commercial agreements and data privacy (GDPR). She regularly advises her clients on a wide variety of arrangements, including IT sourcing, outsourcing, cloud services and cybersecurity law. Her practice includes drafting, interpreting, negotiating and disputing commercial agreements.

In her practice she has obtained considerable experience of matters related to new technologies such as fintech, health tech, open source, IoT and e-commerce.

Recommended in IT and telecoms, *The Legal 500, 2019*.



### Jesper Nevalainen

**Tel: +358 40 5827 826 / Email: [jesper.nevalainen@hannessnellman.com](mailto:jesper.nevalainen@hannessnellman.com)**

Jesper heads our Technology practice in the Helsinki office, and his practice focuses on commercial, technology, and data protection law, including outsourcing in the TMT sectors, and he has particular expertise in open source licensing issues. He advises both buyers and suppliers of information technology on a wide range of business-critical matters ranging from strategic advice contract drafting, negotiations, data and data protection and disputes to re-engineering of distressed projects.

“Jesper is a very practical lawyer who is always focused on providing his services in an easily to understand, fast and efficient manner.” *Client Choice, 2020*.

“Jesper Nevalainen provides expert advice on outsourcing, contractual and procurement matters, as well as related disputes. Clients praise his skills and outside-the-box thinking, with one particularly endorsing his great commercial awareness.” *Chambers Europe, 2020*.

## Hannes Snellman Attorneys Ltd

P.O. Box 7801, SE-103 96 Stockholm, Sweden  
Tel: +46 760 000 000 / URL: [www.hannessnellman.com](http://www.hannessnellman.com)

[www.globallegalinsights.com](http://www.globallegalinsights.com)

Other titles in the **Global Legal Insights** series include:

- **Banking Regulation**
- **Blockchain & Cryptocurrency Regulation**
- **Bribery & Corruption**
- **Cartels**
- **Corporate Tax**
- **Employment & Labour Law**
- **Energy**
- **Fintech**
- **Fund Finance**
- **Initial Public Offerings**
- **International Arbitration**
- **Litigation & Dispute Resolution**
- **Merger Control**
- **Mergers & Acquisitions**
- **Pricing & Reimbursement**



Strategic partner